

ENISA Threat Landscape Report 2018

15 Top Cyberthreats and Trends

FINAL VERSION
1.0
ETL 2018
JANUARY 2019

www.enisa.europa.eu European Union Agency For Network and Information Security

WIZ, Inc. EXHIBIT - 1026
WIZ, Inc. v. Orca Security LTD.

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors

Andreas Sfakianakis, Christos Douligeris, Louis Marinos (ENISA), Marco Lourenço (ENISA), and Omid Raghimi.

Editors

Louis Marinos (ENISA) and Marco Lourenço (ENISA).

Contact

For queries on this paper, please use enisa.threat.information@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the members of the ENISA ETL Stakeholder group: Pierluigi Paganini, Chief Security Information Officer, IT, Paul Samwel, Banking, NL, Jason Finlayson, Consulting, IR, Stavros Lingris, CERT-EU, Jart Armin, Worldwide coalitions/Initiatives, International, Thomas Häberlen, Member State, DE, Neil Thacker, Consulting, UK, Shin Adachi, Security Analyst, US, R. Jane Ginn, Consulting, US, Andreas Sfakianakis, Industry, NL, Thomas Hemker, Industry, DE. The group has provided valuable input, has supported the ENISA threat analysis and has reviewed ENISA material. Their support is highly appreciated and has definitely contributed to the quality of the material presented in this report. Moreover, we would like to thank CYjAX for granting access pro bono to its cyber risk intelligence portal providing information on cyberthreats and cyber-crime.

Legal notice
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice
© European Union Agency for Network and Information Security (ENISA), 2019
Reproduction is authorised provided the source is acknowledged.

ISBN 978-92-9204-286-8, ISSN 2363-3050, DOI 10.2824/622757

Table of Contents

1. Introduction 10

1.1 Policy context 11

1.2 Target audience 12

1.3 Structure of the document 13

2. Cyberthreat Intelligence and ETL 14

2.1 Cyberthreat Intelligence: State of Play 14

2.2 Cyberthreat Intelligence Maturity Model 18

3. Top Cyberthreats 24

3.1 Malware 26

3.1.1 Description of the cyberthreat 26
3.1.2 Interesting points 26
3.1.3 Trends and main statistics 29
3.1.4 Top malware families by type 30
3.1.5 Specific attack vectors 31
3.1.6 Specific mitigation actions 31
3.1.7 Kill Chain 32
3.1.8 Authoritative references 32

3.2 Web Based Attacks 33

3.2.1 Description of the cyberthreat 33
3.2.2 Interesting points 33
3.2.3 Trends and main statistics 34
3.2.4 Specific attack vectors 35
3.2.5 Specific mitigation actions 36
3.2.6 Kill Chain 36
3.2.7 Authoritative references 36

3.3 Web Application Attacks 37

3.3.1 Description of the cyberthreat 37
3.3.2 Interesting points 37
3.3.3 Trends and main statistics 38
3.3.4 Top Web Application Attacks 39
3.3.5 Specific mitigation actions 39
3.3.6 Kill Chain 40
3.3.7 Authoritative references 40

3.4 Phishing 40

3.4.1 Description of the cyberthreat 40
3.4.2 Interesting points 40
3.4.3 Trends and main statistics 43
3.4.4 Top Phishing Themes 44
3.4.5 Specific mitigation actions 45

3.4.6 Kill Chain 46
3.4.7 Authoritative references 46

3.5 Denial of Service 47
3.5.1 Description of the cyberthreat 47
3.5.2 Interesting points 47
3.5.3 Trends and main statistics 49
3.5.4 Top 5 DDoS attacks 51
3.5.5 Specific attack vectors 51
3.5.6 Specific mitigation actions 52
3.5.7 Kill Chain 53
3.5.8 Authoritative references 53

3.6 Spam 54
3.6.1 Description of the cyberthreat 54
3.6.2 Interesting points 54
3.6.3 Trends and main statistics 56
3.6.4 Top Spam sources 57
3.6.5 Specific mitigation actions 57
3.6.6 Kill Chain 58
3.6.7 Authoritative references 58

3.7 Botnets 59
3.7.1 Description of the cyberthreat 59
3.7.2 Interesting points 59
3.7.3 Trends and main statistics 61
3.7.4 Top Botnet Attacks 62
3.7.5 Specific attack vectors 62
3.7.6 Specific mitigation actions 62
3.7.7 Kill Chain 63
3.7.8 Authoritative references 63

3.8 Data Breaches 64
3.8.1 Description of the cyberthreat 64
3.8.2 Interesting points 64
3.8.3 Trends and main statistics 65
3.8.4 Top Data Breaches 66
3.8.5 Specific attack vectors 67
3.8.6 Specific mitigation actions 67
3.8.7 Kill Chain 68
3.8.8 Authoritative references 68

3.9 Insider threat 69
3.9.1 Description of the cyberthreat 69
3.9.2 Interesting points 69
3.9.3 Trends and main statistics 69
3.9.4 Top IT and other assets vulnerable to insider attacks 70
3.9.5 Specific attack vectors 71
3.9.6 Specific mitigation actions 72
3.9.7 Kill Chain 73
3.9.8 Authoritative references 73

3.10 Physical manipulation/damage/theft/loss **74**
3.10.1 Description of the cyberthreat 74
3.10.2 Interesting points 74
3.10.3 Trends and main statistics 76
3.10.4 Specific mitigation actions 77
3.10.5 Kill Chain 77
3.10.6 Authoritative references 78

3.11 Information Leakage **79**
3.11.1 Description of the cyberthreat 79
3.11.2 Interesting points 80
3.11.3 Trends and main statistics 81
3.11.4 Top data leaks incidents 82
3.11.5 Specific attack vectors 83
3.11.6 Specific mitigation actions 83
3.11.7 Kill Chain 84
3.11.8 Authoritative references 84

3.12 Identity Theft **85**
3.12.1 Description of the cyberthreat 85
3.12.2 Interesting points 86
3.12.3 Trends and main statistics 87
3.12.4 Top identity theft threats 88
3.12.5 Specific attack vectors 89
3.12.6 Specific mitigation actions 90
3.12.7 Kill Chain 91
3.12.8 Authoritative references 91

3.13 Cryptojacking **92**
3.13.1 Description of the cyberthreat 92
3.13.2 Interesting points 92
3.13.3 Trends and main statistics 96
3.13.4 Top 5 cryptojacking threats 97
3.13.5 Specific attack vectors 97
3.13.6 Specific mitigation actions 99
3.13.7 Kill Chain 99
3.13.8 Authoritative references 99

3.14 Ransomware **100**
3.14.1 Description of the cybe-threat 100
3.14.2 Interesting points 100
3.14.3 Trends and main statistics 101
3.14.4 Top ransomware threats 103
3.14.5 Specific attack vectors 105
3.14.6 Specific mitigation actions 105
3.14.7 Kill Chain 106
3.14.8 Authoritative references 106

3.15 Cyber Espionage **107**
3.15.1 Description of the cyberthreat 107
3.15.2 Interesting points 107

3.15.3 Trends and main statistics 109
3.15.4 Top cyberespionage attacks 110
3.15.5 Specific attack vectors 113
3.15.6 Specific mitigation actions 113
3.15.7 Kill Chain 113
3.15.8 Authoritative references 114

3.16 Visualising changes in the current threat landscape 115

4. Threat Agents 116

4.1 Threat agents and trends 116

4.2 Top threat agents and motives 118

4.3 Threat Agents and top threats 123

5. Attack Vectors 125

5.1 Attack vectors taxonomy for this year's threat landscape 125

5.2 Misinformation/Disinformation 126

5.3 Web and browser based attack vectors 128

5.4 Fileless or memory-based attacks 129

5.5 Multi-staged and modular threats 130

6. Conclusions 133

6.1 Main CTI-related cyber-issues ahead 133

6.2 Conclusions and recommendations for this year's ETL report. 136

Executive Summary

2018 was a year that has brought significant changes in the cyberthreat landscape. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors. Monetization motives have contributed to the appearance of crypto-miners in the top 15 threats. State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks. These developments are the subject of this threat landscape report.

Developments have been achieved from the side of defenders too. Through the emergence of active defence, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts, leading thus to more efficient defence techniques and attribution rates. Initial successes through the combination of cyberthreat intelligence (CTI) and traditional intelligence have been achieved. This is a clear indication about the need to open cyberthreat intelligence to other related disciplines with the aim to increase quality of assessments and attribution. Finally, defenders have increased the levels of training to compensate skill shortage in the area of cyberthreat intelligence. The vivid interest of stakeholders in such trainings is a clear indicator for their appetite in building capabilities and skills.

Recent political activities have underlined the emergence of various, quite novel developments in the perceived role of cyberspace for society and national security. Cyber-diplomacy, cyber-defence and cyber-war regulation have dominated the headlines. These developments, when transposed to actions, are expected to bring new requirements and new use cases for cyberthreat intelligence. Equally, through these developments, existing structures and processes in the area of cyberspace governance will undergo a considerable revision. These changes will affect international, European and Member States bodies. It is expected that threat actors are going to adapt their activities towards these changes, affecting thus the cyberthreat landscape in the years to come.

In summary, the main trends in the 2018's cyberthreat landscape are:

- Mail and phishing messages have become the primary malware infection vector.
- Exploit Kits have lost their importance in the cyberthreat landscape.
- Cryptominers have become an important monetization vector for cyber-criminals.
- State-sponsored agents increasingly target banks by using attack-vectors utilised in cyber-crime.
- Skill and capability building are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.
- The technical orientation of most cyberthreat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.
- Cyberthreat intelligence needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.
- The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.
- The absence of cyberthreat intelligence solutions for low-capability organisations/end-users needs to be addressed by vendors and governments.

All these trends are included in the content of the ENISA Threat Landscape 2018 (ETL 2018). Identified open issues leverage on these trends and propose actions to be taken in the areas of policy, business and

research/education. They serve as recommendations and will be taken into account in the future activities of ENISA and its stakeholders. An overview of identified points is as follows:

Policy Conclusions:

- The EU will need to develop capabilities (human and technical) to address the needs for CTI knowledge management. EU Member States are requested to introduce measures to increase its independence from currently available CTI sources (mostly from outside the EU) and enhance the quality of CTI by adding a European context.
- As CTI is perceived as a public good, capabilities will be required to offer "baseline CTI" to all interested organisations. EU governments and public administrations are requested to share "baseline CTI", covering sectorial and low-maturity needs of organizations.
- Regulatory barriers to collect CTI exists and should be removed. Coordinated efforts among EU Member States is required in the collection and analysis of CTI, as crucial activity in the implementation of proper defence strategies.

Business conclusions

- Businesses will need to work towards making CTI available to a large number of stakeholders, with focus on the ones that lack technical knowledge. The security software industry needs to research and develop solutions using automation and knowledge engineering, helping end-users and organizations mitigating most of the low-end automated cyberthreats, with minimum human intervention.
- Businesses will need to take into account emerging supply chain threats and risks. The technology industry needs to introduce qualitative measures into its production processes, perform end-to-end security assessments and adhere to certification schemes.
- Businesses will need to bridge the gap in security knowledge among the operated services and end-users of the service. The consumption of CTI knowledge is a major step to achieve this goal.

Technical/research/educational conclusions

- The ingestion of CTI knowledge needs to be enlarged to include accurate information on incidents and information from related disciplines. CTI vendors and researchers have to find ways to enlarge the scope of CTI, while reducing necessary manual activities.
- CTI knowledge management needs to be the subject of standardisation efforts. Of particular importance are the developments of standard vocabularies, standard attack repositories, automated information collection methods and knowledge management processes.
- Research needs to be conducted to better understand attack practices, malware evolution, malicious infrastructure evolution and threat agent profiling. Advances in those areas may significantly reduce exposure to cyberthreats and advance CTI practices.
- Much more training offerings need to be developed in order to satisfy the current market needs in CTI training.

In the last chapter of this document (see chapter 6), a number of important issues leading to the above conclusions are mentioned, providing more elaborated conclusions. It is proposed to consider these issues and identify their relevance by reflecting them to the own situation and elaborate on it accordingly.

The figure below summarizes the top 15 cyberthreats and trends in comparison to the landscape of 2017.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	⇑	2. Web Based Attacks	⇑	→
3. Web Application Attacks	⇑	3. Web Application Attacks	➲	→
4. Phishing	⇑	4. Phishing	⇑	→
5. Spam	⇑	5. Denial of Service	⇑	↑
6. Denial of Service	⇑	6. Spam	➲	↓
7. Ransomware	⇑	7. Botnets	⇑	↑
8. Botnets	⇑	8. Data Breaches	⇑	↑
9. Insider threat	➲	9. Insider Threat	⇓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	⇑	11. Information Leakage	⇑	↑
12. Identity Theft	⇑	12. Identity Theft	⇑	→
13. Information Leakage	⇑	13. Cryptojacking	⇑	NEW
14. Exploit Kits	⇓	14. Ransomware	⇓	↓
15. Cyber Espionage	⇑	15. Cyber Espionage	⇓	→

Legend: Trends: ⇓ Declining, ➲ Stable, ⇑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

1. Introduction

This is the 2018 version of the ENISA Threat Landscape (ETL 2018) yearly report. It is the seventh in a series of ENISA reports analysing the state-of-the-art in cyberthreats based on open source material[1]. This report is the result of a one-year long collection, analysis and assessment activity of cyberthreat related information found in the public domain. Moreover, it captures experience gained through interactions with experts during various ENISA events on the topic of Cyberthreat Intelligence (CTI)[16,19]. The time span of the ETL 2018 is ca. December 2017 to December 2018 and is referred to as the "reporting period" throughout the report.

In essence, ETL 2018 has maintained the structure of the previous ETL[2] by using the same template for the description of the assessed cyberthreats.

As part of the annual improvement process, some adaptations have been applied to the ETL 2018. These improvements, originated from discussions with internal/external experts, helped increasing the efficiency in generating the report, collecting and disseminating the information and establishing better coherence among a variety of ENISA materials on cyberthreats. As opposed to the ETL 2017, in 2018 these advancements are merely content-oriented. Firstly, we included some work performed by ENISA in the area of CTI Maturity Model. Secondly, the assessment of threats has been brought into a wider basis, leveraging upon contributions of additional experts who have supported the information collection and the assessment exercise.

An additional step in advancing ETL 2018 has been the inclusion of CTI knowledge obtained within related ENISA events. Both the ENISA - FORTH Summer School and the ENISA event of CTI (CTI EU)[3] have delivered valuable insights into the trends governing current CTI state-of-the-art. This knowledge has been integrated in this report by means of content related to CTI State-of-Play, the assessed cyberthreats and the conclusions drawn.

The channels used for information collection, ENISA has used information provided by the MISP platform[4], by CERT-EU[5] and by also using threat intelligence of the cyber-security portal CYjAX[6], granted as access pro bono to ENISA. Confidential information found in these platforms has been taken into account in our analysis without any disclosure or reference to this material.

Finally, it is worth mentioning that in 2018 ENISA has advanced with an established liaison with the EU agencies with cyber-security on the mandate. This involves the European Defence Agency (EDA), CERT-EU and EC3. This has been implemented by means of discussions for a more enhanced cooperation among all

[1] It is worth mentioning, that in this chapter some parts of the ETL 2017 text have been reused, in particular regarding the sections policy context and target group. These two topics are considered mostly identical to the previous landscapes. Some changes have been added to policy context to reflect recent developments in EU–regulations.
[2] https://www.enisa.europa.eu/news/enisa-news/enisa-report-the-2017-cyber-threat-landscape, accessed November 2018.
[3] https://www.enisa.europa.eu/events/2018-cti-eu-event, accessed November 2018.
[4] http://www.misp-project.org/, accessed November 2018.
[5] https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html, accessed November 2018.
[6] https://www.cyjax.com/, accessed November 2018.

four organisations, on the basis of a Memorandum of Understanding that has been signed in the reporting period[7].

The links to these institutions already existed at a working level. ENISA has a tight cooperation with CERT-EU in the area of threat information. This is implemented by means of mutual reviews of cyberthreat assessments, use of CERT-EU services and by intensive personal communication.

While with EC3 and EDA a working relationship already exists, this year cooperation in the area of CTI has advanced with the ENISA CTI EU event that was commonly supported by all four institutions. In addition, in 2018, ENISA has intensified its cooperation with the Commission services by engaging resources from DG Connect and European Security and Defence College within its CTI EU event[16].

1.1 Policy context

The Cyber Security Strategy of the EU[8] underscores the importance of threat analysis and emerging trends in cyber security. The ENISA Threat Landscape contributes towards the achievement of objectives formulated in this strategy, in particular by contributing to the identification of emerging trends in cyberthreats and understanding the evolution of cyber-crime (see 2.4 regarding proposed role of ENISA).

Moreover, the ENISA Regulation[9] mentions the need to analyse current and emerging risks (and their components), stating: "*the Agency, in cooperation with Member States and, as appropriate, with statistical bodies and others, collects relevant information*". In particular, under Art. 3, Tasks, d), iii), the new ENISA regulations states that ENISA should "*enable effective responses to current and emerging network and information security risks and threats*".

ETL 2018 also relates to the context of the NIS-Directive[10], as it contributes towards the provision of cyberthreat knowledge needed for various purposes defined in the NIS-Directive (e.g. article 69). Moreover, it comprises a comprehensive overview of cyberthreats and as such, it is a decision support tool for EU Member States used in various tasks in the process of building cybersecurity capabilities.

Of particular interest is, however, the important role of threat landscaping and threat intelligence within the proposed new ENISA regulation/ ENISA mandate[11]. Article 7.7 foresees that "*The Agency shall prepare a regular EU Cybersecurity Technical Situation Report on incidents and threats based on open source information, its own analysis, and reports shared by, among others: Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact (in accordance with NIS Directive Article 14 (5)); European Cybercrime Centre (EC3) at Europol, CERT EU.*". ENISA's work in the area of threat analysis (as exemplified by this report) largely satisfies this requirement, while articles 9 and 10 states the role of emerging cyberthreats, both to perform long-term analysis and feed research initiatives. Despite the fact that this proposal may be modified during the review process, the role of threat analysis assigned by this draft regulation is indicative for its future importance.

---

[7] https://www.eda.europa.eu/docs/default-source/documents/mou---eda-enisa-cert-eu-ec3---23-05-18.pdf, accessed November 2018.

[8] http://www.ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, accessed November 2018.

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF, accessed November 2018.

[10] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed November 2018.

[11] https://www.enisa.europa.eu/news/enisa-news/european-commission-proposal-on-a-regulation-on-the-future-of-enisa, accessed November 2018.

Concluding the entire policy context with regard to cybersecurity, one has to mention an announcement of the Commission services that puts all cybersecurity related initiatives in the context policy areas in the EU space[12]. Besides repeating some of the policy documents mentioned above, this source touches upon domains that are related to cybersecurity, thus underlying the importance of understanding the emerging threat landscape. Of particular interest are the developments in the area of cyber defence, being one of the most dynamic ones in the current and forthcoming Commission activities[13].

1.2 Target audience

The information in this report has mainly strategic and tactical relevance[14] of approximately one year. It is directed at executives, security architects and security managers. Nonetheless, the information provided is also of use by non-experts. For all these target groups, ENISA has developed a web application that will facilitate the use of the ETL information.

Looking at the details provided by this report and ETL in general, one can distinguish between the following information types and target groups:

- The first part of the document found in chapter 2 is a description of the current state-of-play in cyberthreat intelligence (CTI). It reflects discussions performed in 2018 with the ENISA Threat Landscape Stakeholder Group (ETL SG) and within the ENISA event on Cyberthreat Intelligence in the EU (CTI EU)[16]. This information targets **security professionals** or **scholars** interested in open/emerging issues of CTI.
- The top cyberthreats may find a wider group of potential stakeholders who are interested in understanding the threat landscape in general or deepen their understanding to cover particular threats and their aspects. Hence, **decision makers**, **security architects**, **risk managers**, **auditors** clearly belong to the target group. **Scholars** and **end-users** who wish to be informed about the where-about of various cyberthreats may find this material useful. Finally, ETL 2018 can be a useful tool for **professionals of any speciality** who are interested in understanding the state-of-play in the area of cyberthreats.

Besides the information on cyberthreats, ETL 2018 is offering an overview of the entire cybersecurity threat "ecosystem", by covering the relationships of various objects, such as threat agents, trends and mitigation controls. These interconnections make up the context of cyberthreats and can be used in various other activities, such as, any kind of security assessment, identification of protection needs or categorization of assets.

Together with ETL 2018, interested readers may find a series of publications analysing cyberthreats based on contemporary incidents. These reports are published as Cybersecurity Infonotes[15], issued in a regular basis.

---

[12] https://ec.europa.eu/digital-single-market/en/cyber-security, accessed November 2018.
[13] https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/cyber-defence-council-updates-policy-framework/, accessed November 2018.
[14] https://www.cpni.gov.uk/documents/publications/2015/23-march-2015-mwr_threat_intelligence_whitepaper-2015.pdf?epslanguage=en-gb, accessed December 2017.
[15] https://www.enisa.europa.eu/publications/info-notes#c5=2008&c5=2018&c5=false&c2=infonote_publication_date&reversed=on&b_start=0, accessed November 2018.

1.3 Structure of the document

The structure of ETL 2018 is as follows:

Chapter 2 "*Cyberthreat Intelligence and ETL*" provides an overview of recent developments in cyberthreat intelligence, positions the ETL and summarizes some cyberthreat intelligence issues that are seen as emerging.

Chapter 3 "*Top Cyberthreats*" is the heart of the ENISA Threat Landscape. It provides the results of the yearly threat assessment for the top 15 cyberthreats.

Chapter 4 "*Threat Agents*" is an overview of threat agents with short profiles and references to developments that have been observed for every threat agent group, in the reporting period.

Chapter 5 "*Attack Vectors*" provides an overview of important attack vectors that have led to the most important incidents in 2018.

Chapter 6 "*Conclusions*" concludes this year's ETL report. Synthesizes a generic view from the assessed cyberthreats, it provides some policy, business and research recommendations.

2. Cyberthreat Intelligence and ETL

2.1 Cyberthreat Intelligence: State of Play

In 2018, Cyberthreat Intelligence (CTI) has continued improving with regard to good practices, tools, training courses and standards. These developments are the response to an increasing demand for contextualized and actionable information about threats. Just as in 2017, large organisations continue to be the main customer base for CTI. It is worth mentioning, that CTI has matured in concert with other related cybersecurity disciplines, such as Security Operation Centres (SOC), threat hunting and Security Information and Event Management (SIEM). Nevertheless, CTI experts worry about the differences between cycles of cybersecurity related processes. In particular, syncing CTI with Incident Management, Vulnerability Management and Risk management seems to be a necessity in order to keep the focus on incidents that matter for the protection of respective "crown jewels"[19].

Though higher maturity levels are gradually implemented in large organisations, experts argue about the appropriateness of CTI in terms of a positive contribution to the enhancement of the level of defence[16,17]. The main concerns here are the increasing technical nature of CTI, the variability between CTI and other cybersecurity management disciplines in the organisation (e.g. Risk Management) and the potential diversification of objectives among them. Shortage of CTI skills aggravates these deficiencies[18]. The immense interest of experts in CTI trainings is a clear indicator of the market need for CTI trainings[19]. Moreover, the adequacy of CTI for small and medium organisations is a valid concern within CTI experts.

Through the analysis of CTI publications[20,21], but also through a series of consultations with experts, ENISA has identified the following topics as a summary of current CTI state of play.

Some positive CTI developments:

- Pretty good information collection of publicly available CTI: information collection engines and tools exist, comprising of comprehensive collections in some cases grouped according various threat/attack types[22,23,24].
- Good information sharing, especially for low confidentiality incidents/threats: there are already either ad-hoc or established CTI information sharing networks[25,26,27]. Loosely coupled individuals and user groups establish repositories with CTI information for the most common threats.

---

[16] https://www.enisa.europa.eu/events/2018-cti-eu-event, accessed November 2018.
[17] https://www.darkreading.com/vulnerabilities---threats/5-reasons-why-threat-intelligence-doesnt-work/a/d-id/1333188?print=yes, accessed November 2018.
[18] https://www.sans.org/reading-room/whitepapers/analyst/membership/38285, accessed November 2018.
[19] https://nis-summer-school.enisa.europa.eu/, accessed November 2018.
[20] https://www.researchgate.net/publication/323704364_ODNI_COMMON_CYBER_THREAT_FRAMEWORK_A_NEW_MODEL_IMPROVES_UNDERSTANDING_AND_COMMUNICATION, accessed November 2018.
[21] https://repository.stcloudstate.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1085&context=msia_etds, accessed November 2018.
[22] https://embed.kumu.io/0b023bf1a971ba32510e86e8f1a38c38#apt-index, accessed November 2018.
[23] https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections, accessed November 2018.
[24] https://github.com/topics/attack, accessed November 2018.
[25] https://www.cyberthreatalliance.org/, accessed November 2018.
[26] https://www.dhs.gov/ciscp, accessed November 2018.
[27] https://www.misp-project.org/, accessed November 2018.

- Sufficient training opportunities for most aspects of CTI: both professional and non-profit organisations offer comprehensive trainings on CTI[4,28,29]. Although available trainings cover most of the market needs, it seems that additional elements regarding the use of CTI towards non-technical stakeholders are still necessary.
- Good CTI practices with very comprehensive content: various state, academic and private organisations have issued CTI good practices (CTI-related frameworks, e.g. MITRE ATT&CK FRAMEWORK[30], CTI maturity models[31,32]). The high degree of uptake of these good practices manifested through references in publications and presentations.
- Good support of tools at the collection and correlation levels, especially for operational CTI: numerous tools (both commercial and open source) do exist that facilitate correlation of CTI feeds and the identification of corrective actions to mitigate threats[33].

Despite the positive developments in CTI, experts argue about several issues that are not optimally settled. Areas where CTI could do better are:

- Sharing of CTI information about higher confidentiality incidents: it has been argued, that CTI needs yet to penetrate important areas of cybersecurity. In particular, the use of CTI in emergency response has not been yet sufficiently addressed[34]. Examples on the use of CTI in the Commission blueprint on Coordinated Response to Large Scale Cybersecurity Incidents and Crises[35], or the use of CTI in the area of Industrial Control Systems[36].
- Legal requirements regarding actions during collection of CTI information (e.g. vulnerability assessment): the legal frameworks for the collection of CTI needs to be further analysed. While in some countries/sectors this matter is regulated[37], in many others, collecting intelligence is considered a crime, putting thus limitations to corresponding activities of white hat actors[38,39]. This issue is acute

[28] https://www.sans.org/course/cyber-threat-intelligence, accessed November 2018.
[29] https://www.giac.org/about/mission, accessed November 2018.
[30] https://attack.mitre.org/, accessed November 2018.
[31] https://www.tno.nl/en/about-tno/events/2017/using-cyber-threat-intelligence-to-defend-against-advanced-cyber-threats-the-theories-and-practice/, accessed November 2018.
[32] https://www.eclecticiq.com/resources/white-paper-threat-intelligence-maturity-model, accessed November 2018.
[33] https://github.com/hslatman/awesome-threat-intelligence, accessed November 2018.
[34] https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cti-eu-2018-dgcnt-panel.pdf, accessed November 2018.
[35] https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF, accessed November 2018.
[36] https://www.computerweekly.com/news/252436129/Cyber-threat-to-industrial-control-systems-highest-yet, accessed November 2018.
[37] https://www.recordedfuture.com/threat-intelligence-regulations/, accessed November 2018.
[38] https://www.csoonline.com/article/3268761/data-protection/insider-threat-legalese.html, accessed November 2018.
[39] https://www.dhs.gov/sites/default/files/publications/Securing%20High%20Value%20Assets_Version%201.1_July%202018_508c.pdf, accessed November 2018.

as regards to all activities related to vulnerability management[40] (e.g. penetration testing, brute force attacks to running systems).

- Better/accurate identification of operational environment (crown jewels): CTI should not only follow technological trends. It needs to connect to business as early as possible[41]. Of particular importance is the identification of "crown jewels" to be protected[42]. Albeit being a tedious task due to its dynamic nature, asset identification introduce risks when threat-hunting/incident management activities lead to the recognition of (mostly intangible) assets that for some reason (nefariously or unintentionally), have been omitted from asset identification efforts.
- Asynchronous cycles among cybersecurity disciplines: due to the inherent agility of CTI and related disciplines (incident management, incident response, threat hunting, and vulnerability management), it does not properly connect to enterprise risk management cycles[41]. It is necessary to interlink these cycles in order to avoid a mismatch between these disciplines, to avoid diversified, technology-centred viewpoints[2] and lose the benefit from its synergies.
- Relevant CTI stakeholders need to be identified and integrated into CTI cycle: as it has already been identified in previous points, this is one of the main concerns of CTI professionals for the time being[2,41]. The solution seems to rely on better interaction with stakeholders during the requirements analysis phase. Though this matter is not new in cybersecurity processes, it seems that it lags behind the desired maturity. This might be a result of technology bias from cybersecurity experts and the need for increased management attention.
- Strategic CTI needs to be better communicated to business at a strategic level: CTI needs to adapt to the vocabulary of business and strategy[1]. One step towards this goal is the use of standardised terminology[30] and its proper communication to the executive level.
- CTI needs to be better interfaced to thematic areas: there is no one-size-fits-all CTI. CTI makes better sense if targeted towards a particular thematic, business or IT components of an organisation. In accordance with the mentioned areas, it becomes evident that CTI needs to be tailored to the peculiarities of businesses and certainly to the dependencies of the "crown jewels" under protection.
- Presentation, use and analytics of CTI reports need to be enhanced: not much effort has been invested in making CTI available to a wider audience than the CTI team. This may require a style-guide for CTI information depending on the audience it is directed to[41]. Main elements of such a style-guide are visualisations, analytics and Bottom-Line Up First (BLUF)[41]. ENISA released this year a smart cybersecurity search engine named Open-CSAM[43]. A tool developed aiming the continuous monitor of sources, highlighting trending stories and news regarding cybersecurity threats, using artificial intelligence (AI).
- CTI Skill profiles and roles need to be developed and adapted to the CTI (maturity) model adopted: it is a matter of fact that there is a skill shortage in CTI[44]. During the reporting period, some proposals

[40] https://www.law.com/newyorklawjournal/2018/03/02/pen-testing-the-good-the-bad-and-the-agreement/?slreturn=20181012043755, accessed November 2018.
[41] https://threatintel.eu/2018/11/10/lets-make-cti-great-again/, accessed November 2018.
[42] https://www.moorestephens.co.uk/MediaLibsAndFiles/media/MooreStephensUK/Documents/Moore-Stephens-A-guide-to-Intellectual-property_1.pdf?ext=.pdf, accessed November 2018.
[43] https://webapp.opencsam.enisa.europa.eu/, accessed November 2018.
[44] https://www.information-age.com/cyber-threat-landscape-skills-crisis-123471070/, accessed November 2018.

have been made including a combination of automated tools[45],[46] and more precise CTI skill profiles for the various levels of CTI maturity levels. Although this proposal may lead to a better coverage of CTI skills, existing CTI skill profile descriptions[47] are not considering the requirements of various CTI maturity levels (see also corresponding conclusion point in this chapter).

- Interlink between intelligence and CTI: to date, most CTI good practices are based on technical issues of information collection and analysis. Yet, in 2018, the relevance of CTI and traditional intelligence has come to the forefront[48]. Experts argue that bridging these two disciplines will bring CTI closer to a number of non-technical stakeholders, while at the same time, enhance the quality of assessments.
- CTI to be understood as a function: CTI needs to depart from a purely technological discipline to be rooted in the economic, geographic, regulatory, economic and strategic areas as a discrete function. For this purpose, various roles of experts need to be defined aiming at the increase of visibility and usability of CTI.

Concluding the state-of-play of CTI, we would like to mention a few topics that have been identified and regard the necessity for a European engagement in this area. After a discussion with experts in the field, it is considered that European businesses, Member States and organisations would need to initiate activities for establishing the following CTI artefacts.

- European raw data repositories: CTI is based on large amounts of collected information from operational systems. An important tool already operating in this area is Shadowserver[49]. Despite the major sponsorship from US companies, Shadowserver also collects European data. It is imperative for Europe to develop similar information collection capacities in order to develop its autonomy in this critical sector. Such capability will help resolving overseas geopolitical dependencies and will allow an independent mobilization of this resource in cases of emergencies within the EU.
- Leveraging on EU CTI capabilities (planning, collection, collation, analysis, evaluation, dissemination): Europe needs to develop its' own CTI capabilities to achieve an independent CTI knowledge base. Once developed, these European CTI capabilities need to be included as a function in various European initiatives that requires CTI feeds for the resolution of emergencies. This will include Law Enforcement Agencies (LEAs), CSIRTs, Cyber Defence, European Research and crisis management capabilities, just to mention a few.
- CTI Maturity Model: together with national and international partners, a CTI maturity model needs to be developed. Given the novelty of such activity, involved actors may contribute with their requirements, views or experience, thus leading to a good practice guide that is actionable for a variety of CTI needs. In the reporting period, ENISA worked on the development of such model together with EU and US partners. The involvement of experts has been achieved through the mobilization of members of the ENISA Threat Landscape Stakeholder group. A first overview of the work conducted by ENISA is presented in the next chapter (see chapter 2.2).
- Development of CTI skill profiles/roles according to maturity levels: it is necessary to define various CTI roles and profiles[50] and adapt them to the maturity model. A European activity in this area would

[45] https://www.sciencedirect.com/science/article/pii/S1361372318300733, accessed November 2018.
[46] http://pageone.ph/best-practices-for-defeating-automated-attacks/, accessed November 2018.
[47] https://www.insaonline.org/wp-content/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf, accessed November 2018.
[48] https://www.sans.org/event/cyber-threat-intelligence-summit-2019/summit-agenda, accessed November 2018.
[49] https://www.shadowserver.org/wiki/, accessed November 2018.
[50] https://www.information-age.com/cyber-threat-landscape-skills-crisis-123471070/, accessed November 2018.

lead as a basis for relevant educational activities. This, in turn, would strengthen the European CTI job market and would increase Europe's independency on CTI resources.

- CTI capabilities, CTI-as-a-Service (CaaS) for small and medium enterprises: Small and Medium Enterprises (SMEs) are the majority engaged in implementing IT systems, either directly or via supply chains. Given their role in the digital economy, SMEs are an important recipient of CTI knowledge. Yet, due to the absence of skills, CTI is barely consumed by this type of organisations. Novel models of CTI using tools and automation need to be developed and implemented for this purpose. Potentially, the results of existing Horizon 2020 projects could build a good basis for this effort[51,52].
- Promoting a CTI culture: CTI practitioners need to organize themselves as a community to promote a "CTI culture" based on good practices, knowledge and experience sharing.

These and other topics have been debated in the ENISA CTI EU event, a CTI expert's forum. Interested individuals may find the event material in the corresponding web site[16] and/or attend the event.

2.2 Cyberthreat Intelligence Maturity Model

The interest in CTI increased during the last five years, largely due to the need to have a better understanding about threats, adversary's behaviour, tools and techniques in anticipation of cyberattacks.

With the adoption of automated monitoring and response solutions (based on AI and ML), cybersecurity professionals and decision makers are looking into new ways to prevent potential attacks. Part of the solution is to obtain data and information that allows them to analyse and investigate the intention, behaviour, tools, tactics and techniques of adversaries shifting from reactive to a proactive defence strategy. The answer is to implement a ***CTI Program*** within the organization. Figure 1 illustrates the core elements and its interdependencies in a CTI Program.

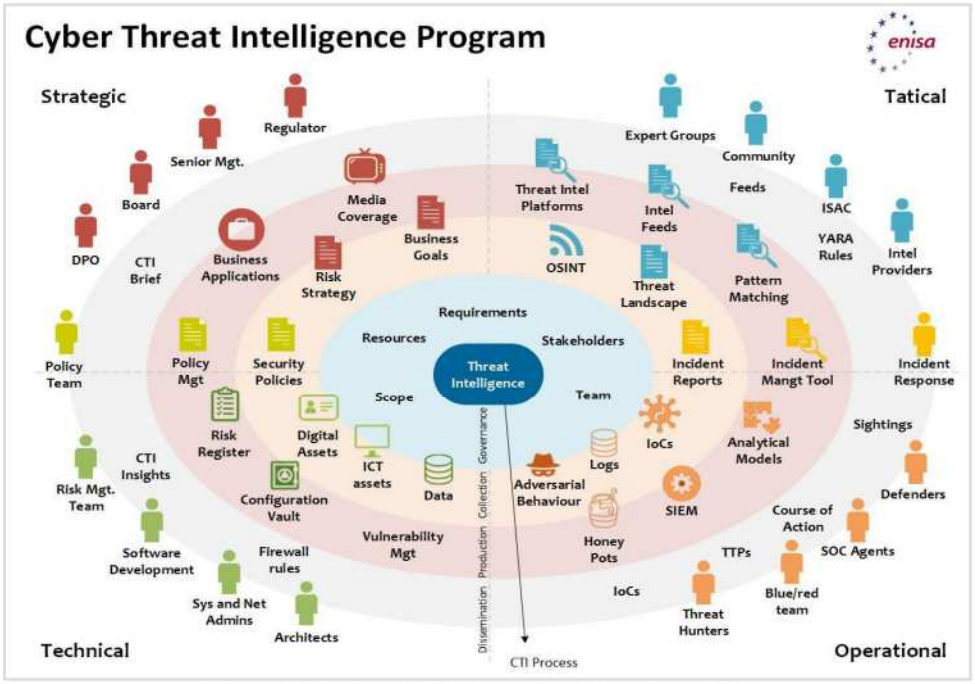


Figure 1: Cyberthreat Intelligence Program representation

[51] https://project-saint.eu/, accessed November 2018.
[52] https://sissden.eu/, accessed November 2018.

A ***Cyberthreat Intelligence Program*** covers the implementation of a ***Process*** and ***Capabilities*** aiming at the continuous production of relevant, contextualized and actionable information, in support of the organizations' ability to prevent cyberattacks.

The ***Objectives*** of a CTI Program are:

Promote resilience to cyber security threats.	*Mitigate the risks from cyber security threats.*	*Promote a culture of awareness over cyber security threats.*

By implementing such a program, the organization realizes a number of significant benefits, including:

- Proactive identification of threats in the environment;
- Increased efficiency of security and technical resources;
- Improved communication of threats with sectorial, business and geographical context;
- Increased capability for disseminating cyberthreat intelligence;
- Improve communications with business Executives;

The expectation around the results produced by the CTI Program will ultimately depend on the how the program is planned, managed and evaluated. Much of the success in reaching the objectives will rely on the governance model adopted during the first steps of the program. The following list captures some of the core elements required to implement a CTI Program.

- The ***Stakeholders*** ultimately define what is expected from a CTI Program. A CTI Program to be effective requires the alignment of information needs from stakeholders with the reality of the threat landscape and the business context. The critical success factors rely on the capture of internal needs, aligned with the ones from key stakeholders, to build people, process and technology that is fit for purpose.
- To implement a CTI program, the appointment of a ***Team*** is required***.*** The size of the team depends on the scope of the Program, requirements from stakeholders and resources available in the organization to produces CTI. In smaller organizations, security related activities are typically performed by someone from the ICT team, an outsourced company (e.g. cloud- based or service provider) or an information security officer. In this situation, a program manager should be appointed to interface with the various technical and non-technical stakeholders, identify the requirements and assess the resources required. In larger organizations, the CTI Program team typically remains within the Security Operation Center (SOC) under the Security Management Team. Considering the CTI Program as a function, separate from the purely technical disciplines, positions the CTI Program Team closer to business and the risk management as a discrete function.
- The ***Scope of the Program*** refers to the various elements that may affect the production of CTI. The definition of the scope helps the CTI Program Team to select the sources, collect the information and analyse it in context to the needs of the organization and its operating environment. Examples of technical infrastructure, future adoption of technology, policy, business strategy, among others are strong candidates to outline the scope of the program.
- The ***Outcomes*** of a CTI Program are dependent on the scope and stakeholders intelligence requirements, classified into four categories: strategic, operational, technical and tactical. ***Strategic***

CTI is considered high-level information, consumed by senior management of an organization. ***Operational CTI*** is relevant to the work of security staff such as defenders, penetration testers and incident responders. ***Technical CTI*** typically feeds the ICT staff to adjust the monitoring systems with security configuration requirements. ***Tactical CTI*** is often referred to as Tactics, Techniques and Procedures (TTPs) produced internally or obtained from external sources.

- The ***Process*** progresses through five clearly defined steps. The first step establishes the governance structure of the program. The following steps include the collection, processing and analysis of data and information from various sources. The last steps focus on the evaluation, sharing and distribution of the CTI produced.
- The ***Capabilities*** required for the implementation of the Program are multiple and include the management of stakeholders, scope, requirements, sources of information, ingestion of structured and unstructured data and information, production, evaluation and dissemination of CTI. Not all organizations possess the resources and organizational structure required to implement a complete CTI Program. In this case, the decision might be to narrow the scope and requirements or to outsource some of the capabilities. In any case, the aforementioned objectives are still valid.
- Each capability requires the execution of ***Activities*** with well-defined inputs, processing and outputs. Certain activities can be supported by systems - more automated solutions based in software - or manual procedure - less automated. The option to adopt a system or a manual procedure depends on the workload and resources available to the CTI program.

A CTI Maturity Model helps in evaluating the state of play of the Program within an organization. The model here proposed evaluates the process and each capability required to achieve the expected outcomes.

The following fourteen questions try to ascertain whether certain preconditions are met in the implementation of a CTI Program.

1. Is the CTI Program known internally to the organization?
2. Are the CTI Program objectives clearly defined and aligned with those of the organization?
3. Does a process exists to identify and maintain information from relevant stakeholders?
4. Does a process exists, to register and/or maintain stakeholders' priorities and intelligence requirements?
5. Does the information about systems, digital assets and critical information exists and is accessible to the CTI Program team?
6. Is there an assessment and planning of resources required for the implementation of the CTI Program?
7. Does the CTI Program team has access to the organization's security information and event management data?
8. Does a clearly defined process exists for collecting structured and unstructured threat data and information?
9. Does an internal repository for threat data and information collected exists?
10. Does the CTI Program team uses threat analysis and modelling techniques to produce CTI?
11. Does the organization has an internal/external CTI dissemination policy?
12. Does a process exists to support and manage the internal and external dissemination of CTI?

13. Does an independent process of qualitative and quantitative evaluation of CTI exists?
14. Is there a clearly defined process of continuous learning and improvement, leading to proactive response to threats?

From the answers obtained, it will be possible to identify the level of maturity of each capability and the general state of the CTI Program. The maturity model considers four levels of evaluation:

- ***Initial*** - An initial level, where the process is informal and information is generated in an unpredictable and reactive manner. There is no internal knowledge of the Program and no expectation or value drawn. CTI is generated based on external information provided by third parties, particularly through alerts from specialized press or security vendors alerts.
- ***Managed*** - A more advanced level, with greater control over the management of the program. A process involving stakeholders is established to discuss and agree on their expectations and intelligence requirements, although CTI is sporadically used. At this level, data (IoCs mainly) and information is collected from internal sources into a single repository, and later enriched with external information. An internal sharing process is established mainly based on distribution lists.
- ***Repeatable*** - With greater management control, the next level considers the qualitative and quantitative evaluation of the results obtained, ensuring that these are aligned with those of the organization and its stakeholders. Recommendations and course of actions (CoA) are produced based on analytical models through the association, correlation of data and information about motives, capabilities, targets and behaviour of adversaries. CTI is integrated automatically into stakeholders systems and processes.
- ***Optimized*** - The last level considers the constant improvement of the Program with the main focus on learning and optimization. The program success results from the collaboration and effort from all stakeholders and the CTI program team. CTI is recurrently used by all the stakeholders for decision-making and action.

The following table maps the evaluation criteria defined to the levels and capabilities of the maturity model.

Capability/level	INITIAL	MANAGED	REPEATABLE	OPTIMIZED
1 – PLANNING PHASE				
1.1 Stakeholders Management	No knowledge about who are the stakeholders.	Stakeholders identified and registered.	Management of all Stakeholders interaction throughout the program.	All information from stakeholders, requirements, scope and resources are integrated and later associated with the CTI produced.
1.2 Scope Management	No knowledge about digital assets, systems and processes in the organization.	Digital assets, "crown jewels", processes and systems identified.	Management of all interaction with information from digital assets, "crown Jewels", processes and systems.	All information from stakeholders, requirements, scope and resources are integrated and later associated with the CTI produced.
1.3 Requirement Management	No knowledge about the stakeholders' intelligence requirements.	Registration of stakeholder' priorities and intelligence requirements.	Manage all interaction with stakeholders' priorities and intelligence requirements.	All information from stakeholders, requirements, scope and resources are integrated and later associated with the CTI produced.

Capability/level	INITIAL	MANAGED	REPEATABLE	OPTIMIZED
1.4 Resource Management	No resource requirements defined for the program.	Resource requirements identified for each of the activities.	Manage the resource allocation to activities throughout the program.	All information from stakeholders, requirements, scope and resources are integrated and later associated with the CTI produced.
1.5 Program Management	The program is unknown to stakeholders.	The Program obtains organizational by-in but there is no general perception on how CTI may add value to stakeholder's work. CTI is sporadically used by stakeholders to take decisions and/or actions.	The Program objectives are aligned with the objectives and requirements of the organization and its stakeholders. CTI is often used by stakeholders to take decisions and/or actions.	CTI created collaboratively. Stakeholders have full control over the timing, delivery method, and production of CTI. CTI is recurrently used by stakeholders to take decisions and/or actions.
2 – COLLECTION PHASE				
2.1 Ingestion of unstructured information and data	Sporadic consumption of information from open sources and vendor recommendations/alerts.	Access to external platforms for consumption of unstructured information such as news feeds, vendor and expert reports.	Collection of internal and external reports, investigation from communities, sectorial and industry.	Use of sectorial threat landscape, expert and industry reports. Use of a centralized repository to store internal and external unstructured information.
2.2 Ingestion of structured information and data	Attempt to analyse data from internal firewalls, IDS and server logs.	Manual collection of internal IoCs from system such as SIEM. Access to external repositories of IoCs, signatures, IPs, hashes, etc.	Collection of internal and external IoCs in "machine-readable" format into a centralized repository. Use of deception mechanisms to collect TTPs data.	Automatic collection of internal and external structured and contextualized data integrated into security and workflow controls.
3 – ANALYSIS AND PRODUCTION PHASE				
3.1 Production management	Recommendations produced using non-contextualized information obtained from external sources. The CTI produced is often seen as an awareness tool about threats.	Production of recommendations based on internal IoCs enriched with external information. The CTI produced is contextualized and actionable mostly for operational and technical stakeholders.	Production of CoAs and recommendations based on the use of analytical models. Association and correlation of internal and external IoCs with information about motives, capabilities, targets and behaviours of adversaries.	Production of recommendations and CoAs from the analysis of trends, incidents, behaviours and evidences from threats, adversaries and MO in accordance with the Program objectives, scope and stakeholders requirements.
4 – DISSEMINATION PHASE				
4.1 Management of internal information dissemination	There is occasional share of CTI and upon request. Dissemination done directly from sources.	A process exists to distribute CTI across the organization but mostly on-demand.	A policy is defined to regulate the dissemination of CTI internally. Dissemination supported by a system that distributes CTI internally.	Automated integration of CoAs and recommendations into stakeholders systems (e.g. security controls, risk mgt, etc.). Adoption of a style guide depending on the audience.
4.2 Management of external information dissemination	The external share of CTI is almost inexistent.	There is an exchange process for non-confidential information between members of similar organizations.	A policy is defined for the external dissemination of CTI. The share is mainly informal and conducted through a distribution list or a CERT.	Trust relationships established with external entities for the exchange of CTI, supported by a sharing platform.
5 – EVALUATION PHASE				

Capability/level	INITIAL	MANAGED	REPEATABLE	OPTIMIZED
5.1 Evaluation management	No evaluation conducted to the process or the CTI produced.	Quantitative metrics are used to evaluate CTI, but only at end of the program.	Qualitative and quantitative metrics used throughout the program.	There is a process to evaluate the program promoting continuous learning.

Table 2 - CTI Maturity Model Evaluation Criteria

The use of metrics allows a qualitative and quantitative evaluation of the CTI produced. The following table presents the evaluation criteria using five qualitative metrics per type of CTI.

Metric/ Type of CTI	STRATEGIC	OPERATIONAL	TECHNICAL	TACTICAL
Contextualized	CTI takes into consideration the organization's business, geography and operating environment.	CTI takes into consideration the security design of the organizations' technical infrastructure.	CTI takes into consideration the organization' operating environment (systems, software, devices, machinery, etc.).	CTI takes into consideration the learnings from similar organizations and type of business.
Actionable	The CTI outcome presents specific action(s) that may lead to a senior management decision(s).	CTI includes CoA that can be followed and/or integrated by the security team (defenders, threat hunters, pen. testers and incident responders).	CTI includes policy, system configuration rules, strategies, recommendations, patches and vulnerability information.	CTI includes step-by-step mitigation from industry and communities.
Sharable	CTI includes style guides and narratives for executive communication.	CTI was formatted using industry standards for machine-readable security data such as STIX2, YARA, etc.	CTI was formatted using specific internal system formats such as JSON, XML, CSV, etc.	CTI was formatted using industry standards.
Trustable	CTI was confirmed by internal sources such as senior management, auditors, DPO, etc.	CTI was confirmed by trusted TIP providers.	CTI was confirmed by trusted ICT vendors (hardware, software, etc.).	CTI was confirmed by trusted experts and communities, regulator, ISACs, CERTs, authorities, etc.
Learnable	CTI includes recommendations to the organization's training and awareness program.	CTI was prepared for the use of pen. testers and in training program of security staff.	CTI was prepared for inclusion in the training program of technical staff.	CTI supports the learning and awareness of others outside the organization.

Table 3 - CTI Evaluation Metrics

The impact of a CTI Program can be assessed using the following quantitative metrics:

- ***Number of preventive actions*** - The number of preventive actions taken by operational and technical stakeholders using the CTI produced by the program. A threshold should be defined for an evaluation period based on the scope, resources and stakeholder's intelligence requirements.
- ***Number of decisions*** - The number of decisions taken by strategic stakeholders using the CTI produced by the program. A threshold should be defined for an evaluation period based on stakeholder's requirements.
- ***Number of training and awareness activities*** - The number of training, awareness sessions and penetration testing exercises using the CTI produced by the program.
- ***Response time*** – Time taken from identifying a cyberthreat until an action or decision is taken by a stakeholder based on the CTI produced by the Program. A baseline for the response time should be defined based on the scope, resources and stakeholder's intelligence requirements.

3. Top Cyberthreats

The fifteen Top Cyberthreats reviewed in this year's edition of the ETL results from the analysis of information collected throughout the reporting period. The information collected - mainly from publicly available sources (Open source intelligence - OSINT) and some other references from commercial providers - covers the majority of the most remarkable events and developments relevant to the study of the top cyberthreats. However, ENISA does not claim exhaustiveness of the topics from the information collected[53].

Continuing the trend from previous years, incidents and advancements in defence and attack tactics have increased in the reporting period. Among the many interesting developments in 2018, ransomware and cryptocurrency attacks have dominated the threat landscape. A further remarkable development is the massive increase in the number of phishing/spear phishing attacks: it has now covered the gaps created by lawful takedowns of malicious infrastructure components such as botnets and exploit kits, while the role of the latter has been significantly downgraded. The success of these methods is manifested by the new record in data breaches reported in 2018.

Reference to the tight cooperation with CERT-EU, ENISA permanent stakeholders group and CYjAX Intelligence Portal (access provide pro-bono) manifested in the support provided during the collection process for this research. Moreover, malware information has been taken into account through the malware information sharing platform MISP[54]. Though the information taken into account contained some classified information, this material has not been disclosed. It has just been taken into account during the analysis process, e.g. in the validation of performed assessments.

The presentation of the fifteen top cyberthreats follows the same structure defined for last year's ETL. The following list presents the structure of the ETL description template:

- a short description of the cyberthreat as it has manifested during the reporting period;
- a list of interesting points with remarkable observations for this cyberthreat;
- trends and main statistics including geographical information, when relevant;
- top incidents within this threat category;
- specific attack vectors used to launch this threat;
- specific mitigation actions;
- kill chain for this cyberthreat and
- authoritative references;

It is worth mentioning that the above elements might change depending on the findings and nature of each threat. Under certain conditions, kill-chains and mitigation actions (vectors) have been reused from previous ETL reports, adapted accordingly, with new evidence as deemed necessary.

[53] Due to the surging number of information on cyber-security incidents and threats and the limited available resources, it is likely that many articles, reports, white papers, etc. have escaped our attention. It may also be the case that missing reports have been intentionally left out from our references because they had significant overlaps with used references.

[54] https://www.misp-project.org/, accessed November 2018.

The fifteen top threats assessed reflect the dominance of the landscape during the reporting period. The list presents one new entry and relevant changes in the ranking. The changes reflect the incidence of threats throughout the reporting period. Some interesting observations regarding the researched cyberthreats and their ranking are as follows:

- It is considered that data breaches and identity theft are not typical cyberthreats. Rather, they are consequences of successful threats (i.e. actions on objectives, if formulated according to the kill-chain). In other words, in order to breach information, one has to successfully launch one or some of the other cyberthreats addressed in this chapter. As such, data breach and identity theft are maintained in our top list because they are found throughout the analysed material.
- Some of the 15 cyberthreats belong to same distinct threat category. Hence, they represent instances from 12 threat types, according to the threat taxonomy used[55]. Ransomware, for example, is a specialization of the threat type malware. Therefore, all malware protection measures must apply with additional measures that are specific for this threat, i.e. in this case ransomware. The same is true for Identity Theft that is a special category of Data Breach. Nonetheless, it is handled separately because this threat is launched by special malicious artefacts.
- Cyber espionage is more a motive than a cyberthreat. It has been maintained mainly because it unites almost all of the other cyberthreats in addition to some high-capability threats that are specially crafted by state-sponsored organisations, such as advanced hacking tools, vulnerability discovery and combination of military/law enforcement intelligence methods.
- The ranking in the list is indicative. The position is based on the number of incidents, impact and role played for other cyberthreats in the landscape. It was not considered the possibility of cyberthreats sharing the same position in the ranking. This leads to the interesting situation where - although a threat increases - it is being ranked lower just because another cyberthreat has been ranked higher, impacting thus the ranking of the ones below.

A web-based tool is available for consultation of the findings from each multiannual ETL report. The tool provides interactive and detailed cyberthreat information in a quicker and more efficient manner, allowing a better and more intuitive use of the ETL report.

[55] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy, accessed November 2018.

3.1 Malware

3.1.1 Description of the cyberthreat

Malware is the most frequently encountered cyberthreat and somehow involved in 30% of all data breach incidents reported334. During the reporting period, there are no evidences of a global malware outbreak similar to the ones that happened during 2017 (i.e. WannaCry and Petya). We have observed, though, the malware landscape evolved and malware authors are adjusting their TTPs in order to maximize their profits and effectiveness rates. Notable observations include the shift from ransomware to cryptojacking, the blurred lines between cyber criminals and cyber espionage actors, the high effectiveness of fileless attack techniques, the decline of exploit kits resulting in increased difficulty of delivering malware as well as the growing mobile threat landscape.

3.1.2 Interesting points

- **Advances in Command and Control (C2) communication.** The use of encrypted C2 communication has increased by 300% during the reporting period[193], a development that creates challenges for the blue teams (especially the ones that have not implemented TLS interception[56]). Moreover, the (ab)use of legitimate encrypted channels is also growing, making the threat detection even more difficult as domain and certificate intelligence are useless[193]. The percentage of malware samples that used legitimate C2 services increased from 4% in 2008 to 9% in 2016[59]. Finally, an emerging trend for C2 infrastructure is the use of blockchain technology that is decentralised and difficult to take down[57]. It is expected that threat actors will continue (ab)using encrypted legitimate channels for C2 communication, while the use of blockchain technology is expected to be leveraged (not widely though) by cyber criminals[58,59].
- **Malware authors increasingly targeting IoT devices.** One of the noteworthy events of 2018 was the VPNFilter malware[60,61,62] campaign. VPNFilter is a multi-stage malware that targeted home and small office routers and NAS devices. At the time of writing, it has compromised around 500.000 devices worldwide and thus created a huge anonymisation network for its creators[409]. Just like what

[56] https://www.enisa.europa.eu/news/member-states/ncsc-published-factsheet-on-tls-interception, accessed October 2018.
[57] https://www.fireeye.com/blog/threat-research/2018/04/cryptocurrencies-cyber-crime-blockchain-infrastructure-use.html, accessed October 2018.
[58] https://www.fortinet.com/blog/industry-trends/the-evolving-threat-landscape---looking-at-our-2018-predictions.html, accessed October 2018.
[59] https://content.fireeye.com/predictions/rpt-security-predictions-2019, accessed November 2018.
[60] https://blog.talosintelligence.com/2018/05/VPNFilter.html, accessed October 2018.
[61] https://blog.talosintelligence.com/2018/06/vpnfilter-update.html, accessed October 2018.
[62] https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html, accessed October 2018.

happened with Mirai[63], it is expected that VPNFilter malware will create copycats[427] , aligned with the volumes of attacks and vulnerabilities related to router and IoT devices during 2018[64,65,66,67].

- **The blurred lines between nation state actors and cyber criminals[68].** It has been always the case that cyber criminals follow and adopt TTPs used by nation state actors. During the reporting period, it has been observed that lines between actors are blurring and cyber criminals adopt advanced TTPs used by nation state actors[411,425]. Major TTPs that have been leveraged include fileless malware[69] and attacks against the RDP protocol[70]. Financial institutions and the retail sector are the most prominent targets[328] and it is highly likely that cyber criminals will continue to leverage advanced TTPs initially used by nation state actors.
- **The mobile malware landscape is steadily increasing.** Mobile malware threats increase year-over-year and the continued use of older operating systems amplifies the problem[248,418]. Major mobile threats include credential theft[71], mobile remote access trojans[421] and SIM card abuse/hijacking (followed by adware[72] and cryptomining[248], especially for Android devices[454]). Mobile threats are expected to increase due to the mobile market growth, users' shift to mobile banking and the upcoming rollout of the 5G mobile standard[241]. Moreover, it is expected that cyber criminals will put effort on increasing sophistication[421] of mobile malware as well as its' delivery vectors (e.g. Roaming Mantis spreading via DNS hijacking[73]). Finally, advanced cyber actors will further focus on high-end malware/spyware (e.g. Pegasus[74] and Dark Caracal[75,76]) and exploit mobile vulnerabilities.
- **Cyber criminals are moving from ransomware to cryptojacking**458. While the growth of ransomware has been slowed245, threat actors have moved to cryptojacking as it is simpler, more profitable and less risky for them244. It is expected that cyber criminals will be leveraging cryptojacking at scale, continue embedding cryptoming capabilities to malware families435 and mostly focus on targeted

---

[63] https://medium.com/threat-intel/router-attacks-iot-mirai-vpnfilter-hajime-4f2692d72563, accessed October 2018.
[64] https://www.us-cert.gov/ncas/alerts/TA18-106A, accessed October 2018.
[65] https://www.techrepublic.com/article/why-router-based-attacks-could-be-the-next-big-trend-in-cybersecurity/, accessed October 2018.
[66] https://www.darkreading.com/attacks-breaches/100000-plus-home-routers-hijacked-in-campaign-to-steal-banking-credentials/d/d-id/1332946, accessed October 2018.
[67] http://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf, accessed October 2018.
[68] https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018OverwatchReport.pdf, accessed October 2018.
[69] https://blog.minerva-labs.com/deconstructing-fileless-attacks-into-4-underlying-techniques, accessed October 2018.
[70] https://www.ic3.gov/media/2018/180927.aspx, accessed October 2018.
[71] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2017-mobile-threat-landscape, accessed October 2018.
[72] https://www.riskiq.com/blog/external-threat-management/q2-2018-mobile-threat-landscape-report/, accessed November 2018.
[73] https://www.kaspersky.com/blog/roaming-mantis-malware/22427/, accessed October 2018.
[74] https://www.zdnet.com/article/lawful-intercept-pegasus-spyware-found-deployed-in-45-countries/, accessed October 2018.
[75] https://cdn.riskiq.com/wp-content/uploads/2018/05/RiskIQ-The-Q1-2018-Mobile-Threat-Landscape-Report.pdf, accessed October 2018.
[76] https://www.csoonline.com/article/3250245/security/dark-caracal-hacking-group-targets-android-smartphones.html, accessed October 2018.

ransomware campaigns. More information on cryptojacking and ransomware threats can be found in the respective sections of this report (see Ransomware threat in chapter 3.14).

- **Fileless attack techniques are the new norm.** Fileless malware techniques operate without placing malicious executables on the file system[77]. Fileless attacks are divided into 4 major techniques[78]: 1) malicious documents (e.g. Microsoft Office with malicious macros, PDF files containing malicious JavaScript and abuse of DDE[79]), 2) malicious scripts (e.g. PowerShell, VBScript, batch files and JavaScript), 3) living-off-the-land techniques (e.g. WMI, LOLBins and LOLScripts[80]) and 4) malicious code in memory (e.g. PowerSploit[93], Doppelgänging[81]). During the reporting period, we have observed increasing fileless attack detections[82] the prevalence of which is so high that 77% of the attacks that successfully compromised organizations utilized fileless techniques[82]. We expect that fileless attack techniques will continue to be used by cyberthreat actors due to their effectiveness in evading detection by organisations' security controls. For more information about fileless attack-vector, please consult chapter 5.4.
- **A consistent year-over-year decline of financial trojans**[248]. While financial trojans are still one of the most prevalent consumer threats, the number of detections over the years is falling[248]. This can be attributed to improved security controls, law enforcement activities and the shift of cyber criminals towards other ways of making profit. It is interesting that some financial trojans do not only steal banking credentials but also cryptocurrency wallet logins[83], while some have also added cryptomining capabilities[172,436]. Most prevalent financial trojans during 2018 are Zeus, Emotet[84], URLzone, Ursnif and Trickbot[85]. It is expected that financial trojans will continue to be a key threat in the financial sector while cyber criminals are focusing on alternative ways to generate profits[241].
- **The first malware targeting safety systems of critical infrastructure.** During the reporting period, we have observed Triton which is the first malware that targets Safety Instrumented Systems (SIS)[86,87,88]. Safety instrumented systems are designed to shut down industrial processes when unsafe operating conditions are reached. Successful exploitation of such systems could lead to serious implications (see

[77] https://zeltser.com/fileless-malware-beyond-buzzword/, accessed October 2018.
[78] https://blog.minerva-labs.com/deconstructing-fileless-attacks-into-4-underlying-techniques, accessed October 2018.
[79] https://www.bleepingcomputer.com/news/security/microsoft-office-attack-runs-malware-without-needing-macros/, accessed October 2018.
[80] https://github.com/api0cradle/LOLBAS, accessed October 2018.
[81] https://thehackernews.com/2018/05/synack-process-doppelganging.html, accessed October 2018.
[82] https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends, accessed October 2018.
[83] https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/, accessed October 2018.
[84] https://www.us-cert.gov/ncas/alerts/TA18-201A, accessed October 2018.
[85] https://blog.barkly.com/top-10-banking-trojans-2018, accessed October 2018.
[86] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, accessed October 2018.
[87] https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html, accessed October 2018.
[88] https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html, accessed October 2018.

Stuxnet[89] and Industroyer[90]). It is expected that the ICS/SCADA domain will be increasingly targeted by advanced threat actors having the capability and intent to execute such operations.

- **Continued growth in the usage of open-source malware**[59]. The "*Githubification*"[91] of Infosec gave the opportunity for everyone to access hacking tools and frameworks like Mimikatz[92], Powersploit[93], Metasploit[94], Empire[95], PowerShell[96], PHP webshells[97], etc. Cyber-crime groups as well as cyber espionage groups have been extensively leveraging open source and publicly available tools for their campaigns. The goals of this approach are to make attribution efforts harder and to reduce their toolset development costs. We expect the continued usage and customization of such tools by both cyber espionage and cyber-crime actors.
- **Exploit kits in the back seat of preferred attack vectors.** While exploit kits are still a threat, cyber criminals prefer other attack vectors to deliver their malicious payloads[428]. This trend has been observed since 2016 when the disappearance of three prevalent exploit kits took place: Angler, Nuclear and Neutrino[242]. The decline of exploit kits poses additional challenges to cyber criminals in order to deliver their malware[454]. Major exploit kits now are RIG EK, GrandSoft EK, Magnitude EK, GreenFlash Sundown EK, KaiXin EK and Underminer EK[98]. The identified low threat posed by exploit kits has resulted in not including this threat in the Top 15 of this ENISA Threat Landscape 2018 report for the first time since 2013.

3.1.3 Trends and main statistics

- Although adware is one of the easiest ways to distribute malware and more often ignored by users, there has been few developments of this threat during the reporting period[428].
- According to Verizon DBIR[334], the frequency of detected malware types is: .js (37,2%), .vbs (20,8%), Windows executable (14,8%), MS Office (14,4%), .pdf (3,3%) other (7,0%).
- A prevalence of polymorphic malware has been observed in the last years as 94% of all malicious executables have been polymorphic[417].
- 79% of the detected malware in organisations were targeting Windows, 18% Linux and 3% Mac systems[436].
- The first Unified Extensible Firmware Interface (UEFI) malware has been discovered in the wild[99].
- Most of the mobile malware was hosted in 3rd part app stores and the app categories that most mobile malware was found were Lifestyle (27%) and Music & Audio (20%)[248].

---

[89] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, accessed October 2018.
[90] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/, accessed October 2018.
[91] https://www.slideshare.net/attackcon2018/mitre-infosec-john-lambert-microsoft, accessed November 2018.
[92] https://github.com/gentilkiwi/mimikatz, accessed November 2018.
[93] https://github.com/PowerShellMafia/PowerSploit, accessed November 2018.
[94] https://github.com/rapid7/metasploit-framework, accessed November 2018.
[95] https://github.com/EmpireProject/Empire, accessed November 2018.
[96] https://github.com/PowerShell/PowerShell, accessed November 2018.
[97] https://github.com/JohnTroony/php-webshells, accessed November 2018.
[98] https://blog.malwarebytes.com/threat-analysis/2018/08/exploit-kits-summer-2018-review/, accessed October 2018.
[99] https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf, accessed October 2018.

- On the positive side, a decline has been observed in the detections of PUA (Potential Unwanted Applications) tracking user behaviour[454].
- During 2018, there have been published a number of "*celebrity*" chipset vulnerabilities: Spectre and Meltdown[100,101], AMDFlaws[102] and Foreshadow[103].
- During the reporting period, the trend of pre-installed malware[455] has been observed in cases such as RottenSys[104] and Triada banking trojan[105].
- Remote Access Trojans are on the rise having FlawedAmmyy as the first ever RAT to appear in the top ten malware list[106].
- Endpoints are increasingly targeted and this is the result of the blurring organisation perimeter and mobility[334]. By targeting endpoints, attackers can conduct reconnaissance, move laterally and further execute their malicious actions. The figure below provides a historical perspective of cyber attack's targets over past years.

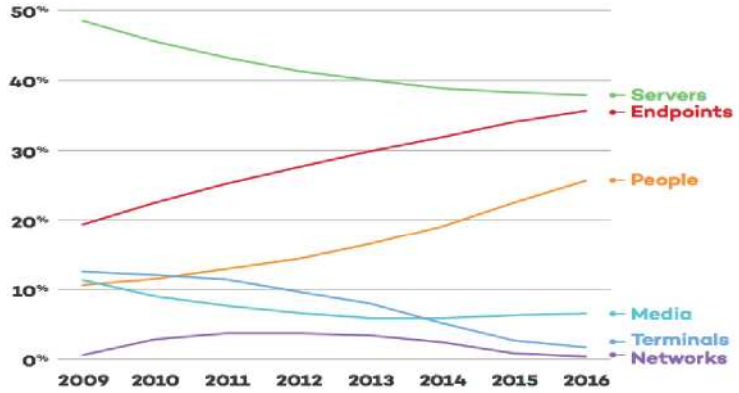


Figure 2: Percentage of threat detections per asset type[388]

3.1.4 Top malware families by type

Figure 3 presents a comparative analysis of malware families by type during the 2nd half of 2017 and 1st half of 2018.

[100] https://meltdownattack.com/, accessed October 2018.
[101] https://newsroom.intel.com/editorials/addressing-new-research-for-side-channel-analysis/, accessed October 2018.
[102] https://community.amd.com/community/amd-corporate/blog/2018/03/21/initial-amd-technical-assessment-of-cts-labs-research, accessed October 2018.
[103] https://foreshadowattack.eu/, accessed October 2018.
[104] https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/, accessed October 2018.
[105] https://news.drweb.com/show/?i=11749&lng=en&c=9, accessed October 2018.
[106] https://www.zdnet.com/article/this-remote-access-trojan-just-popped-up-on-malwares-most-wanted-list/, accessed November 2018.

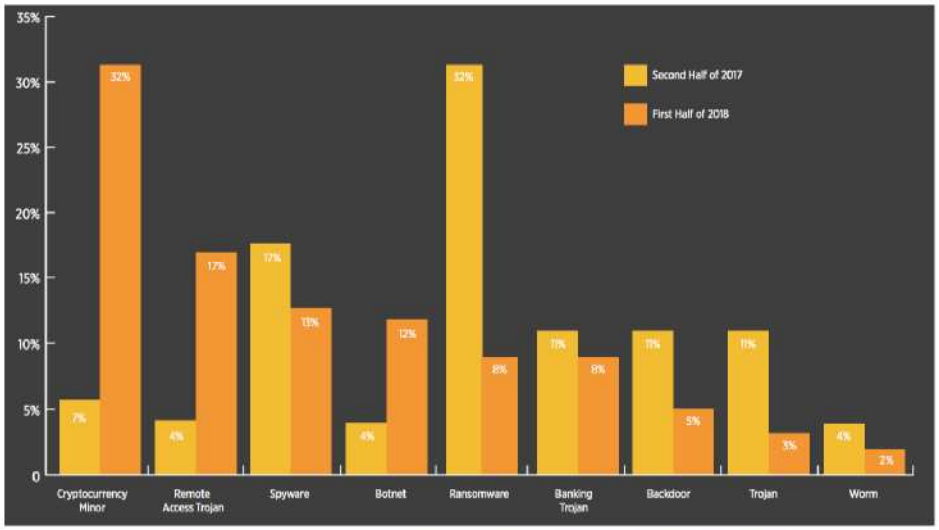


Figure 3: Malware families by type during 2H2017 and 1H2018[409]

3.1.5 Specific attack vectors

Again this year, it comes as no surprise that compromised email (phishing, spam and spear-phishing) is the dominating attack vector for malware infections. According to Verizon DBIR334, email compromise was the attack vector for 92,4% of detected malware, web and browser was the attack vector for 6,3% and 1,3% has been attributed to other attack vectors. Moreover, a non-negligible amount of malware still spreads via the web implying that web and browser based attack vectors such as exploit kits, malvertising, drive-by and strategic web compromise are not dead. Besides email and web, special attention should be given to the abuse of Remote Desktop Protocol (RDP) as an attack vector. The FBI has already published reports on the increasing usage of RDP to spread malware and more specifically ransomware70. Finally, supply chain attacks is another attack vector can be utilised for delivering the malicious payload to targeted organisations[107].

3.1.6 Specific mitigation actions

The mitigation vector for this threat contain the following elements:

- Relying exclusively on end-point or server malware detection and mitigation is not sufficient. Malware detection should be implemented for all inbound/outbound channels, including network, web and application systems in all used platforms (i.e. servers, network infrastructure, personal computers and mobile devices).
- Establish interfaces of malware detection functions (intelligence led threat hunting) with security incident management in order to establish efficient response capabilities.
- Use available tools on malware analysis as well as sharing of malware information and malware mitigation (i.e. MISP)[108].
- Develop a security policies that specify the processes followed in cases of infection. Involve all relevant roles, including executives, operations and end-users.

---

[107] https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/, accessed October 2018.
[108] http://www.misp-project.org/, accessed September 2018.

- Understand the capabilities of various security tools and develop security solutions. Identify gaps and apply defence-in-depth principle.
- Update the malware mitigation controls and adapt to new attack methods/vectors regularly (preferably using MITRE's ATT&CK framework[109]).
- Monitor the antivirus tests regularly[110,111].
- Monitor the log's via a SIEM solution. Indicative log sources should be Anti-Virus alerts[112], EDR[113] detections, proxy server logs[114], Windows Event[114] and Sysmon[115] logs, IDS logs[116], etc.

3.1.7 Kill Chain

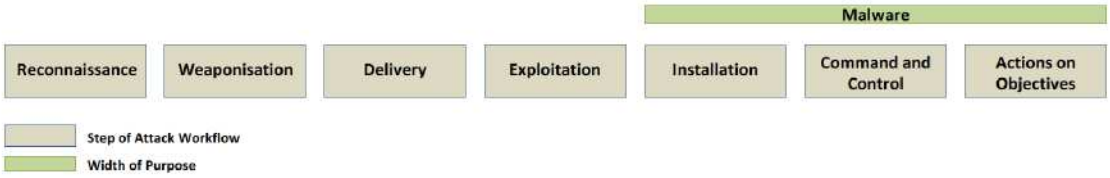


Figure 4: Position of malware in the kill chain

3.1.8 Authoritative references

"Internet Security Threat Report 23", Symantec; "Threats Report March 2018", McAfee; "Threats Report June 2018", "Cyber Attack Trends 2018 Mid-Year Report", Checkpoint; "IT Threat Evolution Q1 2018 ", Kaspersky; "IT Threat Evolution Q2 2018 ", Kaspersky; "Internet Organised Crime Threat Assessment (IOCTA) 2018", Europol; "2018 Mid-Year Security Roundup"; "2018 Global Security Report", Trustwave; "Cybercrime Tactics and Techniques Q1 2018" Malwarebytes; "Cybercrime Tactics and Techniques Q2 2018" Malwarebytes; "2018 Data Breach Investigations Report", Verizon.

[109] https://attack.mitre.org/, accessed October 2018.
[110] https://www.av-test.org/en/, accessed November 2018.
[111] https://www.av-comparatives.org/dynamic-tests/, accessed October 2018.
[112] https://threatintel.eu/2018/10/06/anti-virus-log-analysis-cheat-sheet-v1-5/, accessed October 2018.
[113] http://www.hexacorn.com/edr/IR_EndPointSolutions.xlsx, accessed October 2018.
[114] https://www.threathunting.net/data-index, accessed October 2018.
[115] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon, accessed October 2018.
[116] https://csrc.nist.gov/publications/detail/sp/800-94/final, accessed October 2018.

3.2 Web Based Attacks

3.2.1 Description of the cyberthreat

Web based attacks are those that use web systems and services as the main surface for compromising the victim/target. This includes browser exploitations and injections (including extensions), websites, Content Management System (CMS) exploitation, and web services. For instance, drive-by, watering-hole, redirection and man-in-the-browser attacks are a few known categories of such attacks. Web based attacks continued to be observed as one of the most important threats due to their wide spread surface across the threat landscape, from general ad related spamming campaigns to banking trojans[117] and multiple Advanced Persistent Threat (APT) groups[118] facilitating such attacks as their techniques to target victims. This threat is expected to increase as more malware and exploitation techniques rely more heavily on it, as a delivery mechanism, during the end-to-end attack path.

3.2.2 Interesting points

Below are some interesting points about web based attacks:

- **APTs, malware campaigns and potential usage of watering-hole attacks**. During March 2018 a security firm investigated a major telecommunication company in Hong Kong and identified a flash exploit (CVE-2018-4878) on their group's corporate website – a great example of watering-hole attacks[119]. In addition, roughly during the same time, another campaign was identified targeting national datacentres in central Asia potentially to conduct watering hole attacks, targeting employees and governments[120]. Since September, another aggressive attempt to get into Adobe ColdFusion vulnerable servers was observed which for now, are not yet used for any malicious purposes. Security researchers believe that these will be used for staging phase as watering-hole or delivering spear-phishing attacks[121]. On the other hand, in March 2018 the group behind Promethium (a.k.a StrongPity) had abused the deep packet inspection hardware, used by Turks telecom, redirecting customers in Turkey and Syria to download spyware[122].
- **New Financial malware with new web-based capability**. During Q1 2018, Dridex made a return and was found to be more active as a financial malware with its script injection/redirect capability to steal credentials. Emotet was observed delivering spam and financial malware payloads[123] while BackSwap appeared in Q2[124] with a more interesting technique - this banking trojan was observed using WinAPI to open the console of the developer mode and inject scripts in the page or browser by emulating keystrokes. Further updates to this trojan added the capability of using the same technique to inject the script to the address bar.
- **Browser Extensions and different Targets.** Around June 2018, the "*Desbloquear Conteúdo*" Chrome browser extension was identified targeting Brazilian's using online banking with the purpose of collecting banking credentials[125]. Moreover, fake extensions pretending to masquerade legitimate

[117] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, accessed November 2018.
[118] https://attack.mitre.org/techniques/T1189/, accessed November 2018.
[119] https://blog.morphisec.com/watering-hole-attack-hong-kong-telecom-site-flash-exploit-cve-2018-4878, accessed November 2018.
[120] https://securelist.com/luckymouse-hits-national-data-center/86083/, accessed November 2018.
[121] https://koddos.net/blog/atp-group-attacks-coldfusion-servers/, accessed November 2018.
[122] https://threatpost.com/strongpity-apt-changes-tactics-to-stay-stealthy/138503/, accessed November 2018.
[123] https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/, accessed November 2018
[124] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, accessed November 2018.
[125] https://securelist.com/a-mitm-extension-for-chrome/86057/, accessed November 2018.

extensions started compromising end-users by asking for elevated access levels during their installation[126]. Not surprisingly with the hype of cryptocurrencies, a Chrome Extension was identified by TrendMicro with multiple capabilities (FacexWorm - around April 2018) namely: injecting miners (.js), stealing credentials for crypto-trading platforms, hijacking transactions and hijacking traffic to attacker's referral links (for crypto related referral programs)[127].

- **Content Management Systems (CMS) compromises on the rise.** Early this year several attacks were observed against Drupal delivering browser-based cryptocurrency miners and social engineering toolkits[128]. Later on, in September 2018, a wave of attacks was seen targeting Wordpress vulnerable websites[129] and related plugins, delivering multiple threats to the client-side (i.e. malicious JavaScript, malicious code in the wp_posts table etc.).
- **The trend of web browser based (drive-by) exploit-kits is continuing**. According to Malwarebytes spring and summer report, the majority of exploit kits were observed in Asia. This might be related to the continued use of Internet Explorer (Japan, South Korea) in this part of the world. Apart from known browser type exploit-kits, researchers observed an increase in drive-by downloads labelled as "pseudo exploit-kits". These type of exploit-kits typically miss a solid infrastructure and often result from a single malicious software developer/actor copy and pasting from leaked or POC-type exploits[130].

3.2.3 Trends and main statistics

- In the topic of browser type exploits, Internet Explorer (CVE-2018-8174) and Flash (CVE-2018-4878) have been the most weaponised vulnerabilities for this type of web-based attacks[131].
- By Q2 2018:
  - A total of 351.913.075 unique malicious URLs were identified[132], representing an increase in the number of malicious URLs compared to Q1 totalling 282.807.433[133]. This is in contrast with the stats from 2017 Q1[134] and Q2[135] where the trend was showing a decrease over these quarters.
  - The US (45,87%), Netherlands (25,74%), Germany (5,33%) and France (4,92%) were the top four source countries for web-based attacks[136], representing an increase not only for each country compared to Q1 2018[137] but also to 2017[138] (figure 5).

[126] https://thenextweb.com/hardfork/2018/09/05/mega-browser-extension-hacked-google/, accessed November 2018.
[127] https://blog.trendmicro.com/trendlabs-security-intelligence/facexworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/, accessed November 2018.
[128] https://blog.malwarebytes.com/threat-analysis/2018/09/mass-wordpress-compromises-tech-support-scams/, accessed November 2018.
[129] https://labs.sucuri.net/?note=2018-09-18, accessed November 2018.
[130] https://blog.malwarebytes.com/threat-analysis/2018/08/exploit-kits-summer-2018-review/, accessed November 2018.
[131] https://blog.malwarebytes.com/threat-analysis/2018/10/exploit-kits-fall-2018-review/, accessed November 2018.
[132] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, accessed November 2018.
[133] https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/, accessed November 2018.
[134] https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/, accessed November 2018.
[135] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed November 2018.
[136] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, accessed November 2018.
[137] https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/, accessed November 2018.
[138] https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/, accessed November 2018.

- According to G-Data security research[139] more attacks are web based. Although the number of attacks is fluctuating, they are becoming more targeted[140].

*The overall trend of **web-based** attacks in 2018 is **INCREASING**.*

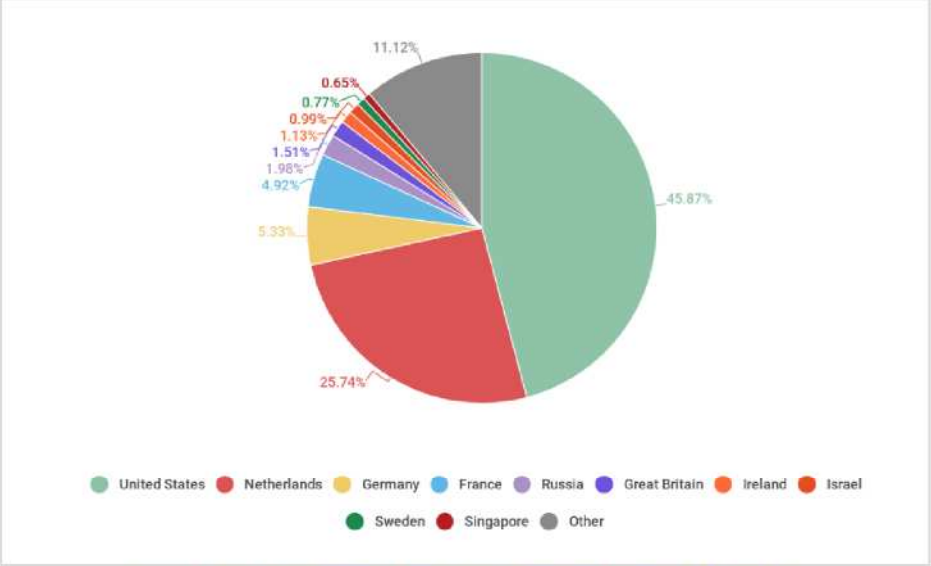


Figure 5: Web-Based Attack distribution by source Country (Q2, 2018)[141]

3.2.4 Specific attack vectors

- **Browser exploits:** are forms of malicious code that take advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach the browser security by altering the settings without the user's knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, Flash and other Web technologies and cause the browser to run arbitrary code.
- **Drive-by downloads:** is a common method of spreading malware as cybercriminals look for insecure web sites to plant a malicious script into HTTP or PHP code on one of the pages. This script may install malware directly onto the computer of someone who visits the site, or it may take the form of an IFRAME that re-directs the victim to a site controlled by the cybercriminals. In many cases, the script is obfuscated, to make it more difficult for security researchers to analyse the code. Such attacks are called 'drive-by downloads' because they require no action from the victim — beyond simply visiting the compromised web site: they are infected automatically (and silently) if their computer is vulnerable.
- **Malicious URL's:** are URL's created with malicious purposes, among them, to download any type of malware to the affected systems, which can be contained in spam or phishing messages, or even improve its position in search engines using Blackhat SEO techniques.

[139] https://www.gdatasoftware.com/blog/2018/09/31037-malware-figures-first-half-2018-danger-web, accessed November 2018.
[140] https://www.symantec.com/security-center/publications/monthlythreatreport, accessed November 2018.
[141] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, accessed November 2018.

- **Water-holing:** Is a malware attack in which the attacker observes the websites often visited by a victim or a particular group and infects those sites with malware. A watering hole attack has the potential to infect the members of the targeted victim group using specific configurations for the malware to be able to select the targets from the infected users (based on their IP for example).
- **Content Management System (CMS) Compromise**. Although this category might be briefly touched upon in other vectors, it is noteworthy that these types of compromise usually refers to plugins and functionalities on vulnerable system. Vulnerabilities that are subsequently exploited to deliver malicious content/malware to the victim directly or indirectly by redirecting the victim to malicious content.

3.2.5 Specific mitigation actions

The mitigation vector for this threat type includes:

- Use web-traffic filtering to detect and block malicious payloads and destinations (IP's, URL's).
- Use web-traffic encryption technologies such as SSL/TLS.
- Update/patch web-browsers and web-server technologies and products regularly.
- Update/patch CMS based websites regularly (i.e. WordPress, Joomla or Drupal) and avoid the utilisation of third-party plugins (usually responsible for most of the attacks against CMS's).
- Protect all endpoint systems from unpatched software containing known vulnerabilities.
- Avoid the installation of malicious programs through potentially unwanted programs (PUPs).
- Monitor the behaviour of software to detect malicious object, such as web browser plug-ins.
- Use web address, web content, files and applications reputation solutions, blacklisting and filtering to establish risk-oriented categorization of web resources.
- Check the application and web-browser settings to avoid unwanted behaviour based on default settings (esp. for mobile devices) to provide a more secure environment (i.e. disabling unused features, extensions and plugins – particularly from untrusted/unverified sources).

3.2.6 Kill Chain

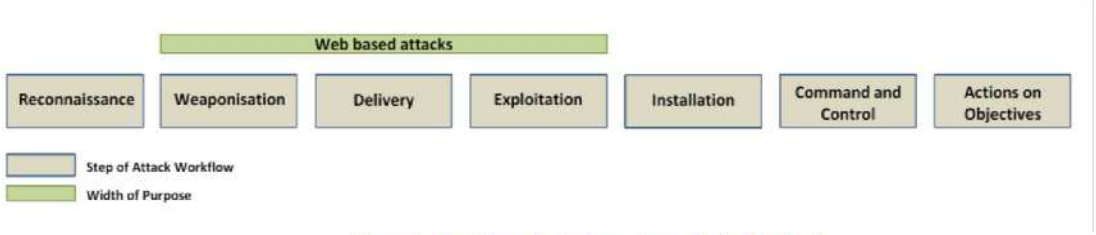


Figure 6: Position of web based attacks in kill-chain

3.2.7 Authoritative references

"IT Threat Evolution Q1 2018. Statistics", Kaspersky Labs, "IT Threat Evolution Q2 2018. Statistics", Kaspersky Labs, "Exploit kits: fall 2018 review", Malwarebytes Labs, "Exploit kits: summer 2018 review" Malwarebytes Labs, "Drive-by Compromise", MITRE ATT&CK.

3.3 Web Application Attacks

3.3.1 Description of the cyberthreat

Web Application Attacks are regarded as direct or indirect attempts to exploit a vulnerability or weakness in the services and applications on the web, abusing their APIs, runtime environments or services. In other words, the simple abuse of an active or passive component of a software available via web. Notably, these types of attacks overlap with web-based quite often due the shared services on the application side and attack surface on the threat side. Web applications are becoming more interesting targets for adversaries as more businesses and firms are becoming dependent on web services, both in revenue and reputation. However, the trend of attacks during the reporting period shows a slight decrease in these type of attacks[142]. Nevertheless, more firms are seeing what OWASP categorises as automated attacks[143] during their first sixty day of appearance[144], showing more efficient and automated exploiting capabilities on the adversary side. On the other side as web applications represent a large part of attacks on the internet[145], enterprises and organisations are investing more on web applications detection, protection and defense systems in 2018, which presents a positive move in the industry[146].

3.3.2 Interesting points

- **SQL injection continues to lead the attacks types**. SQLi attacks dominate the attack types in the web application category by 51% although they are one of the most understandable by both attackers and defenders. This include targeted (and non-targeted) scanning activity, which can easily be hidden from the sight of defenders due to amount of noise generally caused.
- **Local File Inclusion and Cross-Site-Scripting** count for the second and third most prominent attacks with 34% and 8% respectively of the attacks in the wild during summer 2018.
- **Orphan routes and APIs representing security blind spots.** "Dead code", also known as orphan routes/APIs are deprecated or abandoned parts of (web) applications with zero business purpose or value, in other words: "blind spots". Thus, the increase in usage of APIs and the business interconnectivity concepts affects the attack surface (cause by blind spots) to rise exponentially[147].
- **Fewer vulnerabilities observed for Finance, Retail and Healthcare**. Although the number of critical vulnerabilities in web apps grows year by year, White Hat security suggests that in 2018 less web applications were found with critical vulnerabilities comparing to 2017 which is potentially reflecting the investment of these industries in application security area[148].

---

[142] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf, accessed November 2018.
[143] https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications, accessed November 2018.
[144] https://info.tcell.io/hubfs/DemandGen_Content/Research%20Papers/tCell_wp-stateofsecurity-2018-web.pdf, accessed November 2018.
[145] https://blogs.akamai.com/2018/06/summer-soti---web-attacks.html, accessed November 2018.
[146] https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf, accessed November 2018.
[147] https://info.tcell.io/hubfs/DemandGen_Content/Research%20Papers/tCell_wp-stateofsecurity-2018-web.pdf, accessed November 2018.
[148] https://info.whitehatsec.com/rs/675-YBI-674/images/WhiteHatStatsReport2018.pd, accessed November 2018.

- **Legacy web application exploits are still among the top 20**. According to Fortinet Q3 2018 research, top 20 most prevalence web application exploits publish dates goes back to 2005. PHP injection as the second on the list with 33,6% dating back to 2012 (CVE-2012-2311, CVE-2012-1823)[149].

3.3.3 Trends and main statistics

- SQLi attacks still dominate the attack types this year by 51%[150], although this has almost stayed the same since Q2 2017[151].
- Similarly, LFI and XSS were the second and third most prominent attacks with 34% and 8% respectively of the attacks in the wild during summer 2018. The trend remained almost the same since Q2 2017 (33% and 9%) and somehow a slight decrease in SQLi attacks (with 36%) if we want to compare the trend to Q4 2017[152].
- According to a research by Edgescan team over vulnerability exposures and taxonomies: 29% of web application vulnerabilities were associated with insecure configuration/deployments, 24% were client-side related (i.e. XSS), 20% information leakage (i.e. default pages), 12% injections (i.e. SQLi), 6% authentication (i.e. CSRF), 5% authorisation weaknesses (i.e. file path traversals), 3% exposed interfaces (i.e. APIs) and 1% denial of services[153].
- Web Application attacks dominated the trend in EMEA regardless of source with 42% among the other attack types in 2018. Moreover, this type of attack is often linked to major data breaches worldwide[154].
- The United States continued to lead the chart based on the web application attack source by 30,1% (ca. 238 million attacks/alerts) and the Netherlands by 11,9% (ca. 94 million attacks/alerts). Subsequently China, Brazil and Russia each contributing with 7,1%, 6,2% and 4,4% were the major attack sources geographically speaking in the first half of 2018[155]. These are relatively close figures to web application attack during Q4 2017.
- During Q3 2018, 1.114 detections were reported per firm in the topic of web application attacks raising the overall index by 2%. However, 65,4% of the firms reported a severe malicious attempts (web) which is a 6,6% decrease comparing to same period in 2017 (79% Q3 2017[156] and 72% in Q4 2017[157])[158].

---

[149] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf, accessed November 2018.
[150] https://blogs.akamai.com/2018/06/summer-soti---web-attacks.html, accessed November 2018.
[151] https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf, accessed November 2018.
[152] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf, accessed November 2018.
[153] https://www.edgescan.com/wp-content/uploads/2018/05/edgescan-stats-report-2018.pdf, accessed November 2018.
[154] https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-global-threat-intelligence-report-v2-uea.pdf?sfvrsn=c761dd4d_10, accessed November 2018.
[155] https://blogs.akamai.com/2018/06/summer-soti---web-attacks.html, accessed November 2018.
[156] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Threat-Report-Q3-2017.pdf, accessed November 2018.
[157] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q4-2017.pdf, accessed November 2018.
[158] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf, accessed November 2018.

*The overall trend for **web application** attacks in 2018 is **STABLE**.*

3.3.4 Top Web Application Attacks

Similar to the trend in 2016 and 2017, this year the top 5 web app attacks are Injection (SQLi, PHPi), Local File Inclusion (LFI), cross-site scripting (XSS) and Remote File Inclusion with SQL injections on the top – figure 7.

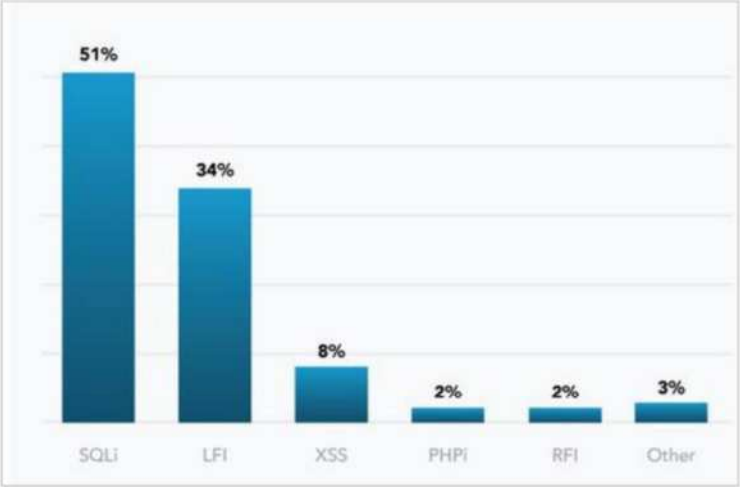


Figure 7: Web application attacks in 2018[159]

3.3.5 Specific mitigation actions

The mitigation vectors for this threat type are recommended as below:

- Formulate security policies for the development and operation of applications.
- Use authentication and authorization mechanisms with a strength corresponding to the state-of-the art.
- Install web application firewalling (WAF).
- Perform traffic filtering to all relevant channels.
- Perform input verification during development and code review phases up to production.
- Deploy bandwidth management capabilities.
- Deploy structured vulnerability assessment strategies to perform regular web application vulnerability scanning and intrusion detection.

[159] https://blogs.akamai.com/2018/06/summer-soti---web-attacks.html Accessed Nov. 2018

- Develop strategies for risk-based assessments, threat modelling and proactive measures[160] including the introduction of secure coding[161] best practices and code vulnerabilities checks during development.

3.3.6 Kill Chain

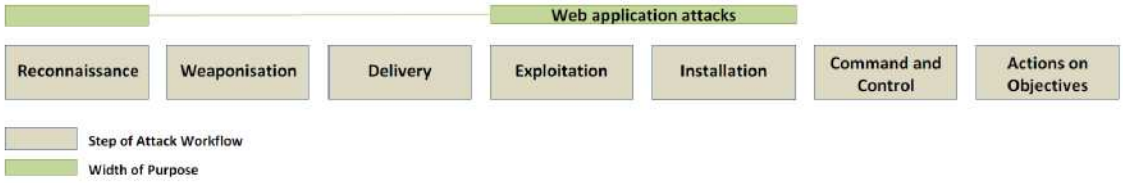


Figure 8: Position of web application attacks in kill-chain

3.3.7 Authoritative references

"Akamai State of the internet report – Summer 2018 ", Akamai 2018, "Akamai State of the internet report – Spring 2018 ", Akamai 2018, "Threat Report 2018", Fortinet, "Stats Report 2018", edgescan 2018, "The Evolution of the Secure Software Lifecycle" , Whitehat Security 2018, And OWASP Top 10 2017.

3.4 Phishing

3.4.1 Description of the cyberthreat

Phishing is the mechanism of crafting messages that use social engineering techniques so that the recipient will be lured and "take the bait". More specifically, phishers try to lure the recipients of phishing emails and messages to open a malicious attachment, click on an unsafe URL, hand over their credentials via legitimate looking phishing pages, wire money, etc. Phishing is the preferred way of compromising organisations[179] and it has been reported that 75% of EU's Member States disclosed cases of phishing[241]. Phishing is so heavily leveraged that over 90% of malware infections and 72% of data breaches in organisations originate from phishing attacks[334].

3.4.2 Interesting points

- **Phishing attacks became more targeted.** It is reported that while the traditional spam-related phishing still exists, the number of targeted phishing attacks continue to grow[411]. The volumes of hacked and leaked personal data give the opportunity for phishers to conduct convincing and targeted phishing campaigns[162] at scale (e.g. targeted sextortion scams[163]). Organised criminal groups also target rich individuals, people with access to financial accounts or sensitive business data or even public authorities that handle PII related data[428] (PII is becoming a juicy target in the age of GDPR). We assess that this trend will continue and phishing attacks will become increasingly targeted in the future.

[160] https://www.owasp.org/index.php/OWASP_Proactive_Controls, accessed Nov 2018.
[161] https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide, accessed Nov 2018.
[162] https://krebsonsecurity.com/2018/08/the-year-targeted-phishing-went-mainstream/, accessed October 2018.
[163] https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/, accessed October 2018.

- **Shift from consumer to enterprise targets.** While phishers mostly targeted consumers during the previous years, an evolution has been observed that malicious actors are focusing on enterprise targets[241]. This significant shift in threat actor motivations is profit-driven since enterprise data can be leveraged in multiple and more profitable ways compared to consumer data (e.g. extortion, selling data in underground marketplaces, etc.)[421]. This trend also aligned with the fact that, email services (e.g. Microsoft O365[164]) and online services (e.g. DocuSign[165] and Dropbox[166]) were the top phishing target (26%) for first time above financial institutions (21%)[421].
- **Steady growth in mobile phishing attacks.** Phishing attacks on mobile devices have grown by an average of 85% year-over-year since 2011[167]. Mobile devices give opportunities for cyber criminals to utilize more attack vectors instead of email phishing. It has been observed that phishing via SMS, mobile messaging (WhatsApp, Facebook Messenger, etc.) and social media apps (e.g. Instagram) has grown significantly[167]. More specifically, phishing of social media users has tripled during 2017 with phishers exploiting the inherent trust relationship between users and the social media platforms[421]. A new mobile attack method has been appeared (URL padding) that takes advantage of the small screen size of mobile phones[421]. Finally, during the reporting period, we observed advanced threat actors using mobile phishing techniques e.g. Dark Caracal[168] and Pegasus[169]. We assess that due to the attack surface that mobile devices provide as well as the increasing adoption of 2-factor authentication, phishing attacks against mobile devices will continue to evolve in sophistication and increase in occurrence.
- **Rapid increase in phishing sites using HTTPS.** It has been reported that one third of phishing web sites have been served via HTTPS during 2017 compared to 5% during 2016[421,454,170]. During the reporting period it was observed that, phishers are shifting techniques and used free certificate services (e.g. Let's Encrypt[171] or Comodo[172]) to challenge the misconception that, sites using HTTPS are secure, safe and trustworthy. This shift follows the trend with the Internet's wider adoption of HTTPS[173] and the fact that some browsers are starting to flag HTTP sites as "*Not Secure*"[174]. We expect that the usage of HTTPS for phishing sites will continue to grow.
- **The problem of Business Email Compromise (BEC)[241].** BEC is a type of phishing attack (also known as whaling) targeting C-level executives and employees in finance or human resources aiming to steal money from their organisations. From October 2013 to May 2018, ca. 78.000 BEC attacks have been reported worldwide responsible for US $12,5 billion of reported losses[175]. During the reporting period, the majority of BEC attacks have targeted the real estate sector[175] (fraud cases happening during the property transaction) as well as employees working in human resources[334]. Due to the fact that 65% of Member States have observed BEC phishing attacks[241], this type of crime has gain the attention of

[164] https://www.cbronline.com/news/microsoft-office-365-phishing, accessed October 2018.
[165] https://www.docusign.com/trust/alerts, accessed October 2018.
[166] https://www.psafe.com/en/blog/dropbox-phishing-attacks-are-on-the-rise/, accessed October 2018.
[167] https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-wp-us.pdf, accessed October 2018.
[168] https://www.lookout.com/info/ds-dark-caracal-ty, accessed October 2018.
[169] https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/, accessed October 2018.
[170] https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf, accessed October 2018.
[171] https://letsencrypt.org/, accessed October 2018.
[172] https://ssl.comodo.com/free-ssl-certificate.php, accessed October 2018.
[173] https://letsencrypt.org/stats/, accessed October 2018.
[174] https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html, accessed October 2018.
[175] https://www.ic3.gov/media/2018/180712.aspx, accessed October 2018.

law enforcement with successful arrests and takedown of fraud schemes[176,177,178]. We assess that the numbers of BEC attacks will remain stable[339] and proportional[179] to the total number of phishing attacks.

- **Spearphishing is the de facto delivery method for APT groups.** It is reported that 71% of APT groups have used spearphishing as infection vector[248]. During the reporting period, the most high profile organised crime groups were FIN7[180,181] and Cobalt Group[182]. Furthermore, nation state actors still use spearphishing as their primary infection vector for their espionage and disruption operations[183,184].
- **Trends in malicious attachments.** During 2017, phishers used 28% more malicious attachments compared to malicious URLs within phishing emails[183]. The most common malicious file types in phishing emails were Microsoft Office documents, archive files, JavaScript files, Visual Basic Scripts and PDFdocuments [248,193,334]. Phishers also used some new types of malicious attachments and some that were used in new ways[185]: .arj ("Archived by Robert Jung"[186]), .z (GNU Gzip[187]), .iqy (Internet Query Files[188,189]), and .pdf[190] files. Legitimate platform features have also been exploited with most notable the Microsoft Windows Dynamic Data Exchange (DDE)[191]. The most common vulnerability exploited in phishing campaigns was CVE-2017-0199[192] , targeting Microsoft Office OLE features.

[176] https://www.europol.europa.eu/newsroom/news/masterminds-behind-ceo-fraud-ring-arrested-after-causing-more-eur-18-million-of-damage, accessed October 2018.
[177] https://www.europol.europa.eu/newsroom/news/two-arrested-in-france-for-major-ceo-fraud, accessed October 2018.
[178] https://www.fbi.gov/news/stories/international-bec-takedown-061118, accessed October 2018.
[179] https://www.fireeye.com/company/press-releases/2018/new-fireeye-email-threat-report-underlines-the-rise-in-malware-l.html, accessed October 2018.
[180] https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html, accessed October 2018.
[181] https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100, accessed October 2018.
[182] https://www.theregister.co.uk/2018/08/31/cobalt_bank_hackers_phishing_campaign/, accessed October 2018.
[183] https://www.proofpoint.com/sites/default/files/pfpt-us-wp-human-factor-report-2018-180425.pdf, accessed October 2018.
[184] https://www.bankinfosecurity.com/blogs/nation-state-spear-phishing-attacks-remain-alive-well-p-2643, accessed October 2018.
[185] https://blog.trendmicro.com/trendlabs-security-intelligence/same-old-yet-brand-new-new-file-types-emerge-in-malware-spam-attachments/, accessed October 2018.
[186] https://www.onlinethreatalerts.com/article/2018/9/9/beware-of-arj-malicious-email-attachments/, accessed October 2018.
[187] https://www.bleepingcomputer.com/news/security/beware-of-fake-shipping-docs-malspam-pushing-the-darkcomet-rat/, accessed October 2018.
[188] https://blog.barkly.com/iqy-file-attack-malware-flawedammyy, accessed October 2018.
[189] https://www.virusbulletin.com/uploads/pdf/magazine/2018/201806-vbspam-comparative.pdf, accessed November 2018.
[190] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/spam-campaign-delivers-malware-via-wiz-targets-banks, accessed October 2018.
[191] https://sensepost.com/blog/2017/macro-less-code-exec-in-msword/, accessed October 2018.
[192] https://go.recordedfuture.com/hubfs/reports/cta-2018-0327.pdf, accessed October 2018.

3.4.3 Trends and main statistics

- The most common techniques[193] that phishers used were domain typosquatting[194], domain shadowing[195], maliciously registered domains, URL shorteners (mostly Bit.ly[196]) and subdomain services (e.g. 000WebHost[197]). Figure 9 depicts the current phishing attack landscape.

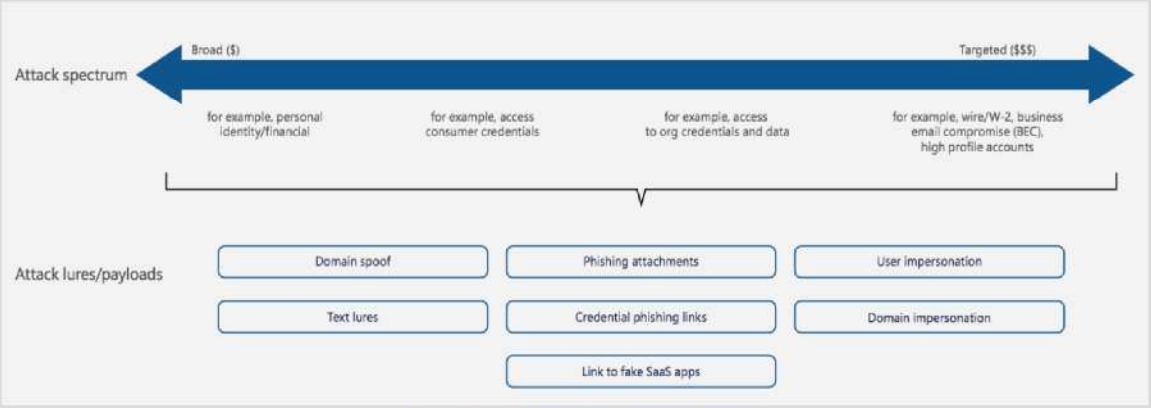


Figure 9: Phishing attack landscape[198]

- The 10 most frequent words in malicious emails during 2017 were: delivery (12,1%), mail (11,8%), message (11,3%), sender (11,2%), your (11,2%), returning (7,6%), failed (7,6%), invoice (6,9%), images (6,6%) and scanned (6,5%)[248].
- Tuesday has been observed as the most popular day for phishers to conduct their campaigns while the least popular day was Friday[199].
- Most frequent words used within BEC phishing emails are: payment (13,8%), urgent (9,1%), request (6,7%), attention (6,1%), important (4,8%), confidential (2,0%), immediate response (1,9%), transfer (1,8%), important update (1,7%) and attn (1,5%)[248].
- The most popular attachment name categories used in the attachments of BEC phishing attacks were: Purchase Order, Payment, Invoice, Receipt, Slip, Bill, Advice and Transfer.
- During 2018, a new trend has been observed towards phishing related to cryptocurrencies and new ICOs (Initial Coin Offerings)[250,247,455,183].
- During 2017, phishing campaigns have been reported to be short-lived since the phishing websites have been online for 4-8 hours[418].
- The number of phishing websites that used free hosting providers during 2017 has increased more than 100% compared to 2016[418]. The most popular free hosting provider was 000WebHost[200].

---

[193] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf, accessed October 2018.
[194] https://nakedsecurity.sophos.com/typosquatting/, accessed October 2018.
[195] https://www.sagedatasecurity.com/blog/threat-hunting-common-attack-vectors-and-delivery-channels, accessed October 2018.
[196] https://bitly.com/, accessed October 2018.
[197] https://www.000webhost.com, accessed October 2018.
[198] https://info.microsoft.com/rs/157-gqe-382/images/en-us_cntnt-ebook-sir-volume-23_march2018.pdf, accessed October 2018.
[199] https://www.menlosecurity.com/hubfs/pdfs/menlo-CredentialPhishing-wp_100118.pdf, accessed October 2018.
[200] https://www.000webhost.com, accessed October 2018.

- The most popular registrar of phishing domains during the first quarter of 2018 was GoDaddy[170].
- For large enterprises, it has been reported that for every legitimate brand registered domain, there are 20 suspiciously registered ones (typosquatted) that can be used to impersonate the brand[183].
- Phishing domains used for typosquatting include the following variations: 41% have an individual character swap, 32% have an additional character, 13% have added/removed leading or final domain's characters, 6% have removed a character and 5% are exact domain match but hyphenated[183].
- It has been reported that organisational susceptibility rates for phishing campaigns in 2017 (10,8%) have been reduced 2% compared to 2016 (12,%)[201]. This indicates the effectiveness of security awareness campaigns within organisations.
- Vishing was mostly reported within the financial sector while it was only one third of the EU Member States reporting this type of attack [241].
- Social media phishing has increased by 200% from 2016 to 2017. Social media accounts are useful for phishers as they can be leveraged to conduct further cybercrime activities[421].

*The overall trend of **phishing** attacks in 2018 is **INCREASING**.*

3.4.4 Top Phishing Themes

Given the nature of phishing, top phishing artefacts are characterised by topics addressed by phishing messages. Top 20 phishing themes[183] include:

1. Dropbox account phishing
2. Financial institution phishing
3. Generic email credential phishing
4. Microsoft OWA phishing
5. Office 365 account phishing
6. Adobe account phishing
7. Google Drive phishing
8. Docusign phishing
9. Netflix phishing
10. Paypal phishing
11. Amazon phishing
12. Apple account phishing
13. Microsoft Excel Online phishing
14. LinkedIn account phishing

[201] https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf, accessed October 2018.

15. Windows settings phishing
16. Postal/Shipping company phishing
17. MyEtherWallet phishing
18. Alibaba phishing
19. OneDrive phishing
20. Retail phishing

3.4.5 Specific mitigation actions

- Organisations should educate their staff to identify fake and malicious emails and stay vigilant. They should also internally launch simulated phishing campaigns to test both their infrastructure and the responsiveness of their staff.
- Use a security email gateway with regular (possibly automated) maintenance of filters (anti-spam, anti-malware, policy-based filtering).
- Consider applying security solutions that use machine learning techniques to identify phishing sites in real time.
- Disable automatic execution of code, macros, rendering of graphics and preloading mailed links at the email clients and update them frequently.
- SPF (Sender Policy Framework)[202], DMARC (Domain-based Message Authentication, Reporting & Conformance)[203] and DKIM (Domain Keys Identified Mail)[204] are the three email security standards for the reduction in spam. Relevant implementation of the aforementioned standards should be deployed in the organisations.
- Implement a fraud and anomaly detection system at network level for both inbound and outbound.
- Ensure that users do not click on links or download attachments if you are not absolutely confident about the source of an email.
- Ensure that users do not click on random links and especially short-links found in social media.
- Avoid the over-sharing of personal information in social media, e.g. time of absence from office or home, flight information etc. as it is actively used by threat actors to collect information about targets.
- Check the domain name of the websites you visit for typos, especially for sensitive websites, e.g. bank websites. Threat actors usually register fake domains that look similar to legitimate ones and use them to "phish" their targets. Looking only for an https connection is not enough.
- Enable two factor-authentication whenever applicable. Two factor-authentication can prevent account takeover.
- Use strong and unique password for every online service. Re-using the same password in various services is a serious security issue and should be avoided at all times. Using strong and unique credentials in every online service limits the risk of a potential account takeover to the affected

[202] http://www.openspf.org/, accessed October 2018.
[203] https://dmarc.org/, accessed October 2018.
[204] http://www.dkim.org/, accessed October 2018.

service only. The use of a password manager software would make the managing of the whole set of passwords easier.

- In case of wiring money to an account, double-check the bank information of the recipient through a different medium. Unencrypted and unsigned emails should not be trusted, especially for sensitive use-cases like these.
- Implement multiple controls (including two-factor authentication) for critical financial transactions.

3.4.6 Kill Chain

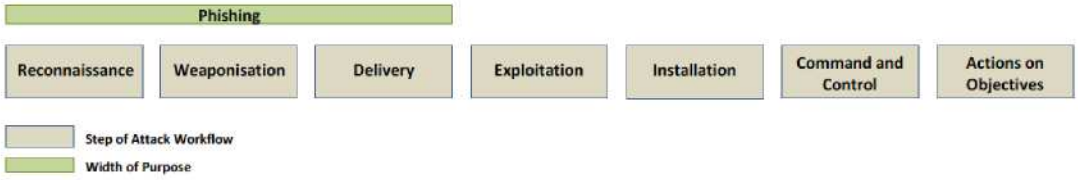


Figure 10: Position of phishing in the kill chain

3.4.7 Authoritative references

"Trend & Intelligence Report 2018", PhishLabs; "The Human Factor 2018", Proofpoint; "Internet Security Threat Report 23" Symantec; "Spam and phishing in Q1 2018", Kaspersky; "Spam and phishing in Q2 2018", Kaspersky; "Phishing Activity Trends Report 1Q 2018", APWG.

3.5 Denial of Service

3.5.1 Description of the cyberthreat

(Distributed) Denial of Services is one of the highly impactful threats in cyber landscape that has been targeting almost any business or organisation. It has been quite clear that preserving a solid defence for such threat has become extensively important for different organisations. According to Arbor Networks, the strong demand for mitigation services provided by managed service providers in this field is notable with financial services, e-commerce, cloud providers and governments on the top[205]. Also, Law enforcement activities in this realm have played a key role for fighting against such malicious activities by running operations to take down services like "webstressor.org"[206] during the first half of 2018. Although this has been a great achievement, DDoS for hire services like this are not few and still the landscape is seeing activities with similar characteristics. On the other side the increase in the number of connected services globally and their dependency on the Internet of Things (IOTs) to run and facilitate such services raised concerns over threats like DoS attacks to potentially cause nation wide failures for businesses and critical systems. One example of such services is the concept of connected hospitals and related services[207]. Yet with all the mitigation and preventative activities across the world reports and researches suggest that the number of DDoS activities are on the rise (16% increase). Although we might not be observing too many large attacks[208].

3.5.2 Interesting points

- **BCP38 and DDoS.** Activities and research[209] on Implementing ingress traffic filtering to avoid IP-address spoofing in ISPs has been seen as a positive approach from different organisations and government entities (i.e. NCSC UK). This approach prevents the ISPs infrastructure to be part of (generate) DDoS attacks which are facilitating the spoofed-IP technique[210].
- **Internet of connected Services.** More organisations are depending on technologies and accordingly higher demand for connected services and information. Multiple reports emphasise the fact that APIs are becoming a popular attack surface for malicious actor in order to interrupt services in different organisations[211]. Also, researchers in CERT-EU predicted that health organisations are at risk of denial of service due to the same concept (connected hospitals with 80.000 publicly available medical devices).
- **DDoS and geo-politics landscape.** In Mexico a presidential candidate's website (Ricardo Anaya) was under a DDoS attack while he was running a television debate. This has been attributed (unverified) to an activity of a Russian based botnet by the candidate's campaign. Similar activity has been observed targeting the website of the Ukraine president when the authorities started blocking access to Russian media. On the other hand, a large DDoS attack caused operation failure to the largest (and state-run)

---

[205] https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf, accessed November 2018.
[206] https://krebsonsecurity.com/2018/04/ddos-for-hire-service-webstresser-dismantled/, accessed November 2018.
[207] https://www.leverege.com/blogpost/iot-connected-hospital, accessed November 2018.
[208] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf, accessed November 2018.
[209] https://www.caida.org/projects/spoofer/, accessed November 2018.
[210] https://www.ncsc.gov.uk/content/files/protected_files/article_files/ACD%20-%20one%20year%20on_0.pdf, accessed November 2018.
[211] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf, accessed November 2018.

train service provider in Denmark (Services disrupted included mobile application, ticketing machines and the website). During April 2018, law enforcement agencies from the US and UK announced that they have identified a considerable number of infected devices (in EU, US and Australia) attributed and ran by Russian hackers ready to run state sponsored attacks. Just in matter of days a website owned by a Russian political party (United Russia) went down for two days by a DDoS campaign[212].

- **Largest reflection-amplification attacks – Still on the rise.** GitHub became a victim of a 1.35Tbps (126.9 million pps) amplified DDoS attack[213]. The attack was originating from different autonomous systems misusing memcached services (UDP port 11211). Five days after that incident, on 5th of March 2018 Arbor networks announced[214] a 1.7Tbps attack targeting a US service provider facilitating the same memcached technique. Interesting enough since the first incident on GitHub the number of vulnerable memcached servers was cited publicly as 17000 and only 500 were remained vulnerable by June 2018.
- **Filtering at the Service provider level will help the defenders.** Researchers at akamai believe that deploying few strategies at the telecoms or service provider lever will block a good amount of DDoS attacks at the source and prevent the ongoing infection on the customer side of ISPs. For instance, blocking DNS based C&C communication queries of a botnet (i.e. Necrus) in the provider's network can ideally prevent the complete DDoS functionality of that botnet. Other strategies like securing cloud assets and keeping residential address space clean were proposed[215].
- **One of many DDoS for hire services taken down (Operation Power-Off).** With the rise in providing such services the price for running individual DDoS attacks was found to be as small as US $5. Thus more frequent attacks leads to a better business for the malicious service provider. Not surprisingly the price varies based on different capabilities of the service such as parallel attacks, limits per day and different vectors to flood the target with[216]. April 2018, the United Kingdom's major law enforcement agency (National Crime Agency) along with the Dutch crime unit (Dutch National High Tech Crime Unit) took down a major DDoS platform known as "webstresser.org" hosting more than 136,000 users. It was reported that 4 to 6 million attacks worldwide were initiated using this platform[217].
    - **Multi-Vector DDoS attacks were observed with different characteristics.** As mentioned above, DDoS-for-hire is among the most popular services. Due to its nature, time constraint is one of the main characteristics of these services. Akamai reported a specific attack series targeting DNS servers of the organisation for almost 2 days intermittently which also included another vector (PSH/ACK - TCP based) peaking at 120 Gbps (18.6Mpps). Additionally, a young malicious actor introduced a set of traffic generators in a YouTube tutorial peaking at 170 Gbps (65Mpps). When the attack was not as effective as desired, the traffic moved from targeting a single IP to flooding the full /24 subnet using a SYN ACK flood reflected off of legitimate servers across a host of

[212] https://securelist.com/ddos-report-in-q2-2018/86537/, accessed November 2018.
[213] https://githubengineering.com/ddos-incident-report/, accessed November 2018.
[214] https://asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/, accessed November 2018.
[215] https://www.akamai.com/es/es/multimedia/documents/case-study/spring-2018-state-of-the-internet-security-report.pdf, accessed November 2018.
[216] https://securitybrief.com.au/story/it-s-an-active-buyer-s-market-for-ddos-as-a-service-netscout, accessed November 2018.
[217] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf, accessed November 2018.

geographies. Other multi vector reflected attacks misusing IKE and IPMI protocols brings back the theory that "Mirai" code is still progressing[218].

- **Looking forward in the DDoS landscape.** No Surprise to see larger and more destructive attacks, Considering the addition of empowered mobile devices (5G and more processing power) and IOTs. Relatively application level attacks are predicted to rise[219].
- **IoTs and DDoS attacks.** During the first quarter of 2018 a spike was observed over the number and duration of DDoS attacks. Researchers at Kaspersky labs believe that was linked directly to Darkai and AESDDoS[220] IoT botnets. Moreover, in Q3 Fortinet reported activity of Mirai and Gafgyt after receiving new updates in addition to Bushido IoT botnet which was mainly inspired from Mirai brute forcing through telnet and IRC enabled devices[221].

3.5.3 Trends and main statistics

- Reports suggest an increase (16%) in the total number of DDoS attacks in Summer 2018 comparing to same season in 2017[222].
- An Annual survey suggested that top motivations for DDoS attacks are: Online Gaming, attackers presenting their niche capabilities and extortion[223].
- 4% increase observed in reflection type attack and almost 16% in network type attacks (Layer 3 and 4) in 2018[224]. Bearing in mind, 99% of the recorded attacks were infrastructure related in 2017[225].
- 52% attacks were utilizing multiple vectors (at least two) in Q2 2018. These attacks were observed to target multiple services like Email and IPSEC misusing GRE and SNMP protocols[226].
- While some reports[227] suggested that "Webstreessor.org" (the biggest DDoS for hire service) take down reportedly had a dramatic impact on decrease of DDoS attacks (~60%) in Europe, others reflected that DDoS activity rose after this action in the second half of 2018[228].

---

[218] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf, accessed November 2018.
[219] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf, accessed November 2018.
[220] https://securelist.com/ddos-report-in-q1-2018/85373/ Accessed Sept 2018
[221] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2018.pdf Accessed November 2018
[222] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf, accessed November 2018.
[223] https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf, accessed November 2018.
[224] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf, accessed November 2018.
[225] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf, accessed November 2018.
[226] https://www.verisign.com/assets/report-ddos-trends-Q22018.pdf, accessed November 2018.
[227] https://www.link11.com/en/blog/number-of-ddos-attacks-significantly-declines-after-shutdown-of-webstresserorg/, accessed November 2018.
[228] https://www.informationsecuritybuzz.com/expert-comments/ddos-attacks-rose-in-2nd-half-of-april-2018-after-webstresser-take-down/, accessed November 2018.

- Linux botnet involvement in DDoS attacks increased to 71,19%[229] in 2017 and the trend continued in Q2 2018 reaching 94,47% comparing to 5,53% windows-based botnets (i.e. Xor and Darkai botnets utilizing SYN floods as their most popular attack)[230].
- China keeping the top spot with the highest number of attacks covering 59,03% followed by Hong Kong with 17,13% in second place (Q2 2018 period).
- Longest attack in Q2 2018 was lasting more than 6 days and 55,28% of the attacks were identified to last less than 90 minutes[231].
- Attacks lasting less than 90 minutes occupied 55,28% of the total, while those lasting longer accounted for 44,72%. 4,62% lasted longer than 1.200 minutes. The average duration was 318,10 minutes, while the longest attack lasted 6 days, 5 hours, and 22 minutes.
- In terms of highly targeted regions, though during second quarter of 2018, China remains the most attractive targets covering 52,36% of the total number of unique attacks since 2017. US with 17,75% and Hong Kong with 12,88% comes as the second and third attractive targets.
- The distribution of denial of service attacks on a weekly analysis presented that Tuesday and Thursdays found to be the least popular days, swapping with Sundays being the quietest to the second most popular day of the week for DDoS attacks comparing to the first quarter of 2018[232] – Figure 11.

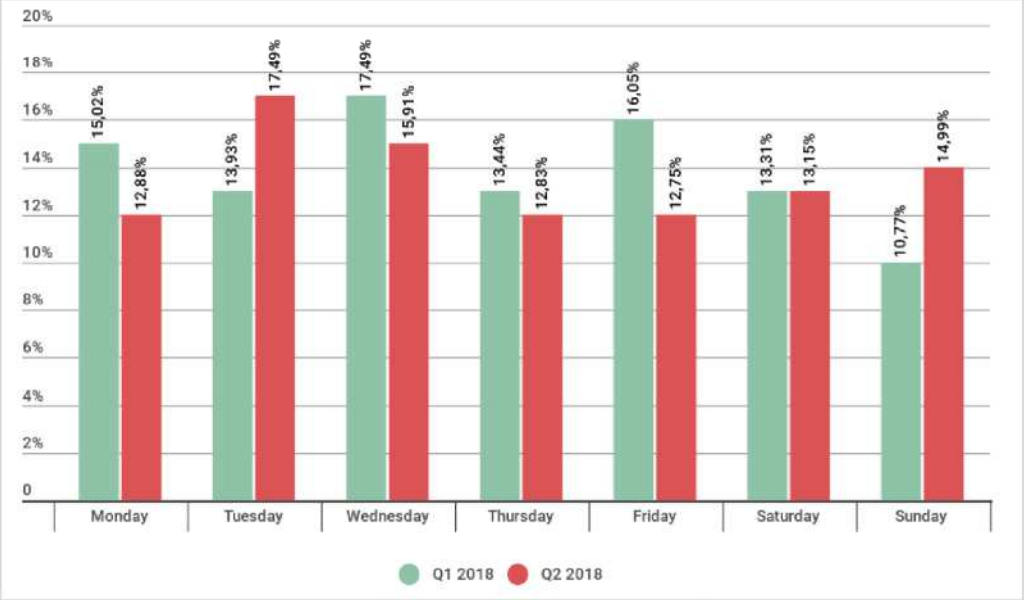


Figure 11: Distribution of attacks during[233]

[229] https://securelist.com/ddos-attacks-in-q4-2017/83729/, accessed November 2018.
[230] https://securelist.com/ddos-report-in-q2-2018/86537/, accessed November 2018.
[231] https://www.nexusguard.com/hubfs/Threat%20Report%20Q2%202018/Nexusguard_DDoS_Threat_Report_Q2_2018_EN.pdf, accessed November 2018.
[232] https://securelist.com/ddos-report-in-q2-2018/86537/, accessed November 2018.
[233] https://securelist.com/ddos-report-in-q2-2018/86537/, accessed November 2018.

According to Netscout, the maximum number of DDoS attacks observed during the first half of 2018 increased (174%) compared to the same time period in 2017[234]. The frequency though decreased by 13%.

*The overall trend of **denial of service** attacks in 2018 is **INCREASING**.*

3.5.4 Top 5 DDoS attacks

- **Memcached** (reflected) amplification attacks. A legitimate service which is developed for handling a distributed memory caching system (using UDP) can be easily exploited to reflect the traffic to target with an amplification factor of 50.000 times of the original request.
- **Multi target DDoS.** When the attackers are not seeing the desired impact on their target they tend to extend their impact to the wider network range to have a more distributed impact and potentially keep the defence teams busier. This methodology was observed by facilitating multiple DDoS vectors (i.e. SYN floods, amplification and application layer) targeting the entire /24 subnet.
- **Cache Busting DDoS.** In this type of attack the malicious actor aims to bypass the application's caching capability by sending random (or not recognizable) GET requests to flood the application server with requests to handle.
- **Persistent DDoS Attacks** (i.e. multi-day). This type of DDoS is famous for its two stages of infecting hosts and creating botnet of zombies who pretend to be a well defended endpoint and the attack phase that has been seen to take from minutes to over multiple days. The vector varies from network type attacks to application layer attacks[235].
- **Encrypted Attacks.** The rise of using encrypted services and traffic (SSL) on the web has attracted different levels of DDoS attacks. This includes attacks on the application level (flood attacks, bruteforce etc.), network level and the protocol level (i.e. SSL renegotiation or downgrade) making it harder for defenders and toolsets to recognise malicious traffic from legitimate[236].

3.5.5 Specific attack vectors

According to Nexusgaurd Q2 2018 report, most of the attacks were focused on hit-run tactics and specifically during peak times to strike their targets with UDP, TCP (SYN) and ICMP floods being the top 3 vectors. The duration of these malicious attempts were mostly recorded as lasting less than 90 minutes and the longest to more than 6 days.

[234] https://www.ipexpoeurope.com/content/download/13783/181390/file/NETSCOUT_ThreatReport_FINAL_080618b.pdf, accessed November 2018.
[235] https://www.hindawi.com/journals/scn/2018/5353060/, accessed November 2018.
[236] https://www.link11.com/en/blog/ssl-ddos-attacks-and-how-to-defend-against-them/, accessed November 2018.

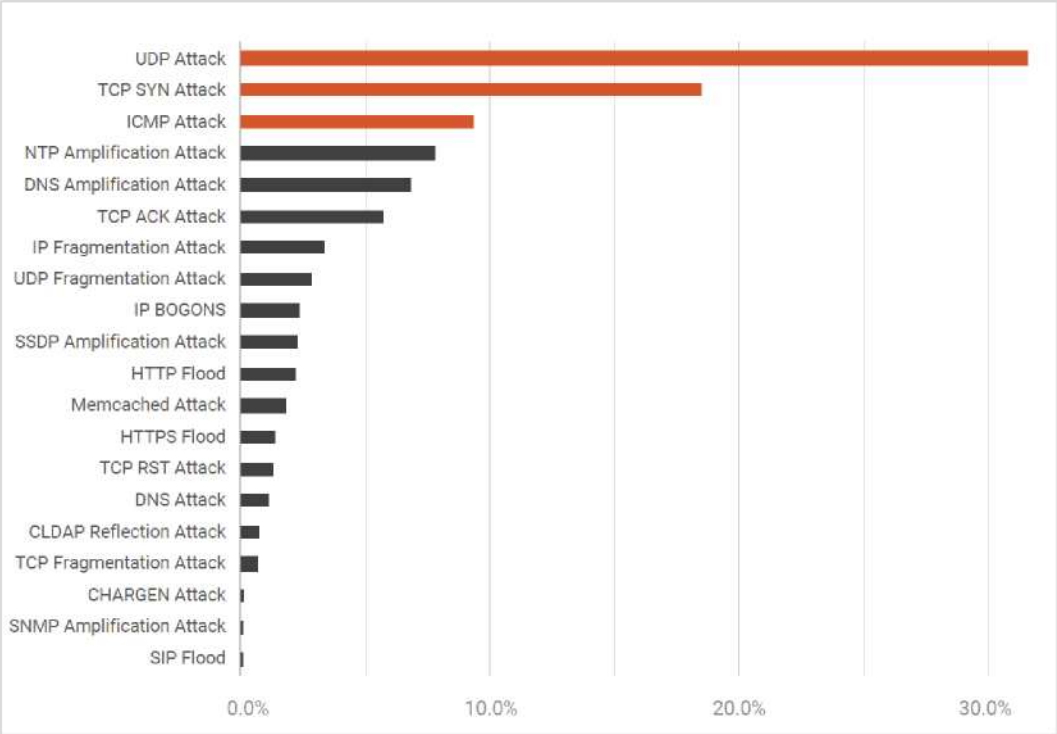


Figure 12: DDoS Attack vectors, Q2 2018[237]

3.5.6 Specific mitigation actions

- Assess the requirements for considering DDoS managed services (either through internet service provider or directly)
- Promote the appropriate use (implementation, detection, update) of different defence technologies like firewalls, web application firewalls, IPS/IDS systems, network flow, Access Control Lists and Intelligent DDoS mitigation tools or services on the network (perimeter, cloud or hybrid)[238].
- Remediate the information leakages related to the infrastructure (leak path) helping defenders reducing or even preventing a potential attack[239].
- Promote proactive activities by the provider to filter and clean their infrastructure playing a key role in preventing impactful denial of service attempts. Facilitating cache servers or dropping DNS queries at source are good examples of such proactive approaches[240].
- Identify the critical devices, processes and design by implementing and testing a service failure response and recovery plan in line with the broader Incident Response (DDoS Runbook).
- Internet Providers, carries and cloud providers play a key role in mitigating DDoS malicious attempts. Collaboration and communicating with such providers are key to a successful mitigation.

---

[237] https://www.nexusguard.com/hubfs/Threat%20Report%20Q2%202018/Nexusguard_DDoS_Threat_Report_Q2_2018_EN.pdf, accessed November 2018.
[238] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Denial-of-service-attacks-what-you-need-to-know1.pdf, accessed November 2018.
[239] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf, accessed November 2018.
[240] https://www.akamai.com/es/es/multimedia/documents/case-study/spring-2018-state-of-the-internet-security-report.pdf, accessed November 2018.

3.5.7 Kill Chain



Figure 13: Position of denial of service in the kill chain

3.5.8 Authoritative references

"Global Threat Landscape - NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report" NETSCOUT 2018, "State of the Internet – Summer 2018", Akamai 2018, "Active Cyber Defence - One Year On" National Cyber Security Centre (NCSC-UK) 2018 , "DDoS attacks in Q1-Q3 2018", Kaspersky Lab 2018, "Annual Cybersecurity Report 2018", Cisco 2018, "Verisign Distributed Denial Of Service Report – Q2 2018", Verisign 2018, "Threat Report Distributed Denial of Service (DDoS) – Q2 2018" Nexusgaurd 2018, "Quarterly Threat Landscape Report 2018", Fortinet 2018.

3.6 Spam

3.6.1 Description of the cyberthreat

Spam is the abusive use of email and messaging technologies to flood users with unsolicited messages. Spam dates back to the beginning of the Internet and is mainly distributed by large spam botnets. Although it is continuously reducing in volume, spam is still one of the major attack vectors observed in the wild. During the last years spam has evolved, (i.e. spam via social media and messengers) and it is assessed that it will continue to be used[241]. Spam is regarded a threat because of its low cost to send messages while it is time consuming and costly for spam recipients and service providers in terms of network bandwidth and storage. The good news here is that, the coordinated law enforcement activities for botnet takedowns and the advances in anti-spam technologies have resulted in lowering the spam numbers during the last years.

3.6.2 Interesting points

- **Consistent decrease in spam activity during the past decade.** During the past decade, a consistent decrease in spam activity has been observed. This could be attributed to the efforts of law enforcement as well as the changing economics for the underground spamming ecosystem[242].

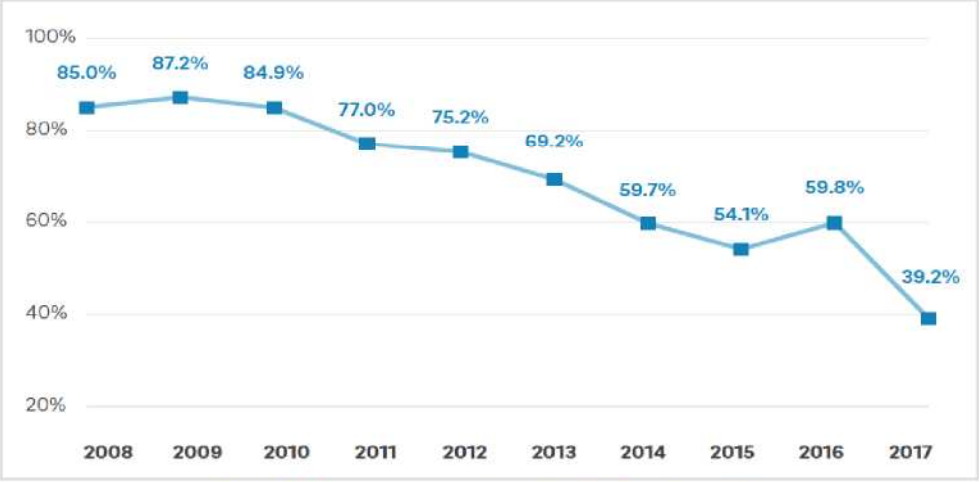


Figure 14: Spam as a percentage of total inbound email[242]

- **Stable spam rate activity during the past 12 months**. Based on the statistics of the total number of daily emails compared to the total number of daily spam emails during the past 12 months, the spam rate is almost stable as can be seen in the figure below[243]:

[241] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018, accessed October 2018.
[242] https://www.trustwave.com/Resources/Library/Documents/2018-Trustwave-Global-Security-Report/, accessed October 2018.
[243] https://www.talosintelligence.com/reputation_center/email_rep#global-volume, accessed October 2018.

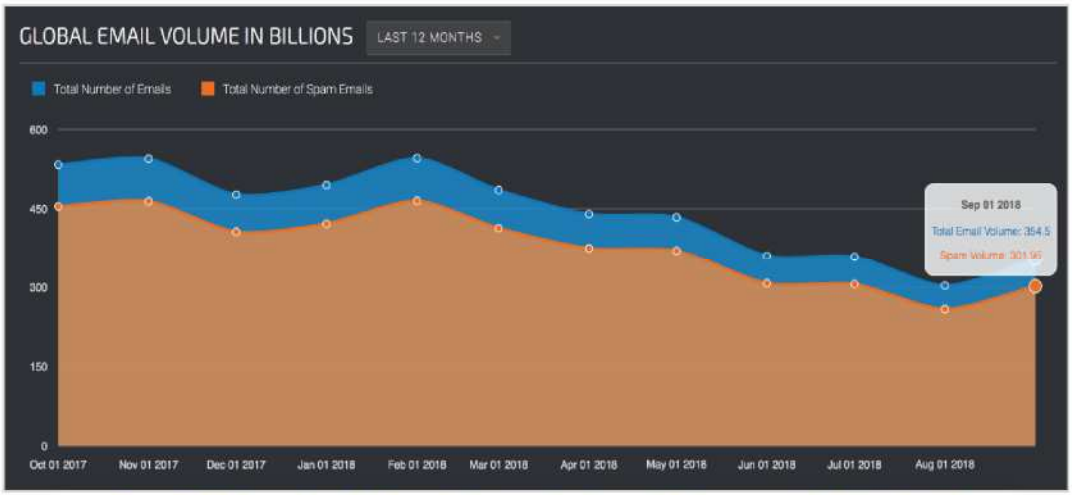


Figure 15: Total number of daily emails vs total number of daily spam emails (in billions)[243]

- **Necurs is the top spamming botnet.** 88%[249] of spam comes from botnets and the top 3 spamming botnets are: Necurs, Gamut and Cutwail[244]. During 2016 and 2017, spam-borne malware comes almost entirely from Necurs[242] and it is reported that 75%[244] to 97%[245] of total spam comes from Necurs. During 2017, Necurs has sent out almost 15 million emails in total while it has sent ca. 67.000 emails per day in the second half of 2017[248]. Necurs operates in shorts bursts of heavy spamming that are followed by dormant periods[242]. During its periods of full activity, the botnet sends spam from ca. 200.000 to ca. 4.000.000 unique IP addresses daily[242]. Although a decrease in Necurs activity has been observed, the start-and-stop nature of Necurs makes it difficult to make safe conclusions about potential decrease in the size of the botnet or actual decrease in its activity[242].
- **Spam via messengers and social networks.** It has been reported that spammers have been using WhatsApp to distribute their content (mostly fictional lotteries, airplane ticket giveaways, popular retailers, etc.)[250]. Social networks are also abused to deliver spamming content via fake celebrity and company accounts, viral threads or even via the advertising mechanisms offered by the social network[250]. A recent survey reported that 47% of social media users are seeing more spam in their feeds[246] (79% of which believe that spam content on social media includes fake news).
- **GDPR-themed spam.** A large number of GDPR-themed spam emails have been observed during the first quarter of 2018[247]. This spam activity included mostly paid seminars, webinars and workshops related to the new EU's privacy regulation.
- **Larger organisations have higher spam rates.** It has been reported that, during 2017, employees of large organisations receive more spam emails compared to the employees of smaller ones[248].

[244] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf, accessed October 2018.
[245] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2018.pdf, accessed November 2018.
[246] https://blog.hubspot.com/marketing/social-media-users-seeing-more-spam, accessed October 2018.
[247] https://securelist.com/spam-and-phishing-in-q1-2018/85650/, accessed October 2018.
[248] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf, accessed October 2018.

- **Spam is getting more "international".** While one year ago 96% of the spam was in English, the levels of spam in English have fallen to 90%[249]. This indicates a trend that spam is getting more "international" and localized.
- **Double email headers.** During the second quarter of 2018, spammers tried to tamper the email header in order to evade filtering[250]. More specifically, they used two "From" fields in the email header: a first email address from a well-known organization that has undoubtedly good reputation and subsequently, their real email address. The goal of spammers was to fool the email filters and to be perceived as legitimate. However, modern anti-spam solutions can detect spam emails not only based on the header details but also based on content.
- **Abuse of subscription forms for spamming.** Another interesting technique that spammers used during the reporting period was the abuse of the subscription forms. Spammers used a script that auto-filled subscription forms of regular websites and inserted the target email address in the "Email" form as well as a short message with a spam link in the form of the "Name". Thus, the targets received an automatic "list subscription" confirmation email that contained a spam link instead of their name. Spammers wanted to fool email filters since usually the content of "list subscription" confirmation emails is normally allowed.
- **Common spam types.** 75% of spam emails is comprised of the following 3 categories: health related spam (26,6%), spam delivering malware (25,7%) and spam for online dating sites(21,4%)[242]. Following spam types include: stock spam (4,6%), phony job offers (3,5%), phishing spam (2,1%), financial spam (1,9%), adult spam (1,5%), etc.[242].
- **Spam gangs.** It is reported that 80% of the spam targeting Internet users is coming from 100 persistent spam gangs[251]. Top spam gangs include: Canadian Pharmacy, Blaze Media Solutions, PredictLabs, Guangzhou-Seoul Information Technology Co. and RR Media.

3.6.3 Trends and main statistics

- Spam emails from webmail services are not very common as only 0,7% of spam is sent from webmail accounts like Yahoo, Gmail and Hotmail[249].
- Spam emails are small in size since 40% of spam emails were 2Kb in size[252].
- The Mining, Construction and Manufacturing sectors had the highest spam rate during 2017[248].
- The average daily spam volume is 295,62 billion, while the average daily legitimate email volume is 51,18 billion[243]. Thus, legitimate email volume is 14,76% of the total email volume while spam volume is 85,23% of the total email volume.
- The Top Level Domains (TLDs) that are the riskiest and spammy-est on the Internet are the following: .gq , .cf , .loan , .tk , .ml , .ga , .men , .faith , .top and .racing[253,254].

*The overall trend of **spam** attacks in 2018 is **STABLE**.*

[249] https://antispamengine.com/spam-statistics/, accessed October 2018.
[250] https://securelist.com/spam-and-phishing-in-q2-2018/87368/, accessed October 2018.
[251] https://www.spamhaus.org/statistics/spammers/, accessed October 2018.
[252] https://securelist.com/spam-and-phishing-in-2017/83833/, accessed October 2018.
[253] https://www.spamhaus.org/statistics/tlds/, accessed October 2018.
[254] https://krebsonsecurity.com/2018/06/bad-men-at-work-please-dont-click/, accessed October 2018.

3.6.4 Top Spam sources

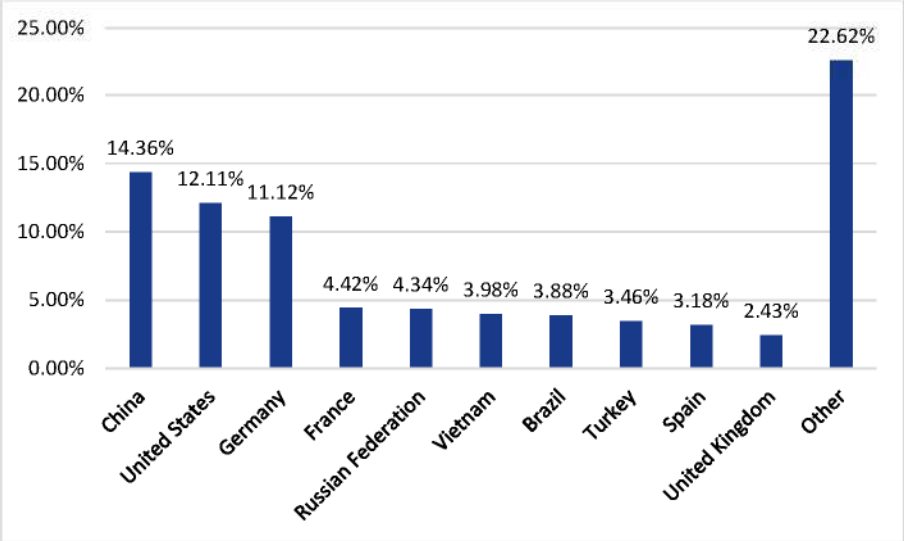


Figure 16: Top 10 sources of spam by country[250]

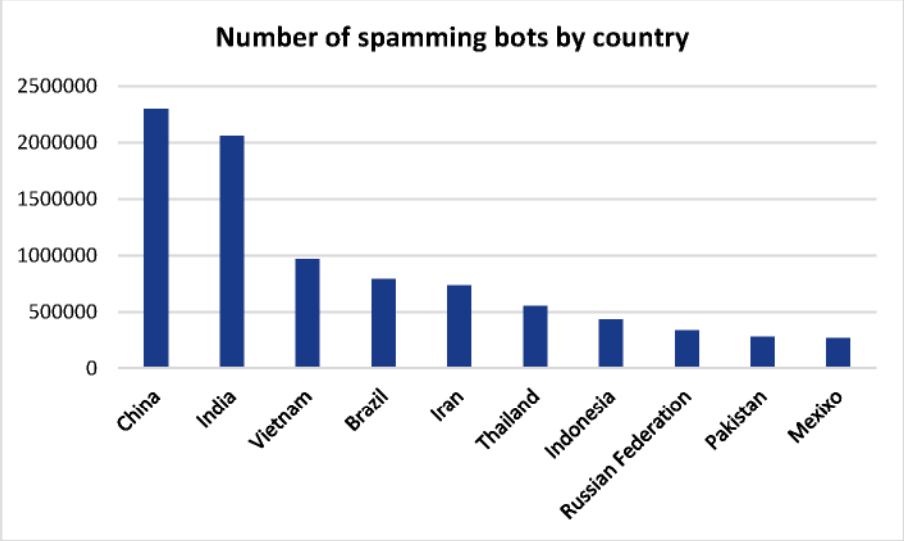


Figure 17: Top 10 countries with spamming bots[255]

3.6.5 Specific mitigation actions

The mitigation measures for spam and spam-based threats are the following:

- Use a security email gateway with regular (possibly automated) maintenance of filters (anti-spam, anti-malware, policy-based filtering).

[255] https://www.spamhaus.org/statistics/botnet-cc/, accessed October 2018.

- Disable the automatic execution of code, macros, rendering of graphics and preloading mailed links at the email clients and update them frequently.
- Implement SPF (Sender Policy Framework)[256], DMARC (Domain-based Message Authentication, Reporting & Conformance)[257] and DKIM (Domain Keys Identified Mail)[258] email security standards for the reduction of spam.
- Implement reputation filters, content filters, RBL (Real-time Blackhole List) and other measures.
- Use AI and specifically machine learning and anomaly detection techniques.
- Educate users, e.g. to ask themselves, e.g. if they know the sender, if they feel comfortable with the attachment content and type, if they recognize the subject matter of the mail, etc.
- The most important threat (impostor email) is still the most difficult to identify and mitigate as it does not rely on technical means but rather on social-engineering, and the abuse of the inherent trust in a known email partner. Therefore, user awareness and training is the first step in fighting it. In that respect, there are training services that mimic tactics used by malicious actors. Such trainings aim to identify individuals that might fall for them and essentially educate them on how to recognise and counter similar attacks.

3.6.6 Kill Chain



Figure 18: Position of spam in the kill-chain

3.6.7 Authoritative references

"Internet Security Threat Report 23", Symantec; "Spam and phishing in Q1 2018", Kaspersky; "Spam and phishing in Q2 2018", Kaspersky; "Threats Report March 2018", McAfee; "Threats Report June 2018", McAfee; "Top 10 Worst Statistics", Spamhaus; "Total Global Email and Spame Volume", Cisco Talos; "2018 Global Security Report", Trustwave.

[256] http://www.openspf.org/, accessed October 2018.
[257] https://dmarc.org/, accessed October 2018.
[258] http://www.dkim.org/, accessed October 2018.

3.7 Botnets

3.7.1 Description of the cyberthreat

During 2018, botnets were observed to be active and serving different malicious activities. From Necurs and Gamut covering almost 97% of the spam related attacks[259] to the variation of IoT related botnets, social media[260] and ads, which were driving sales for botnets[261]. On a different note, although the Mirai creators were arrested[262], its technique and source code inspired many other actors to take the same approach and build more sophisticated IoT botnets. Tori-bot is one of the good examples with 6 different persistency techniques targeting multiple architectures. Another interesting trend in 2018 was the updates and patches, which were delivered to these botnets for enhanced functionalities like VpnFilter and Hide and Seek botnets. In addition to these credential stuffing/reusing attacks saw a dramatic increase according to Akamai's September report. Below we will briefly cover interesting points and trends of 2018 followed by top attacks and mitigation techniques.

3.7.2 Interesting points

The identified interesting points for botnets are as follows:

- **Another face of Necurs**. For more than 6 years[263] since its existence, Necurs has shown different faces from delivering sophisticated banking malware to huge spam campaigns. Since September 11, IBM X-Force spamtraps caught new cyber extortion campaign from Necurs aimed at blackmailing users who are supposedly watching adult content[264].
- **Fbot tracking Crypto mining Botnets**. Since September 2018, researchers from Netlab observed a new botnet activity with three specific interesting characteristics: aimed at removing crypto mining related malware/botnets, using blockchain based DNS to resolve C2s and quite bounded to the original Satori botnet[265].
- **Torii IOT botnet**. Different from the Mirai and other Mirai-inspired botnets, Tori-bot keeps persistency by using 6 different techniques without providing any typical services like DDoS or crypto-mining (at least not yet). However, it provides a modular architecture for retrieving and executing commands and exfiltration capabilities as well as multi-layered encrypted communication mechanism. It also targets multiple computer architectures (x86_64, x86, ARM, MIPS, Motorola 68k, SuperH, PPC etc.)[266].

[259] https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/, accessed November 2018.
[260] https://www.hackread.com/hackers-selling-fortnite-accounts-botnet-on-instagram/, accessed November 2018.
[261] https://blog.trendmicro.com/trendlabs-security-intelligence/pop-up-ads-and-over-a-hundred-sites-are-helping-distribute-botnets-cryptocurrency-miners-and-ransomware/, accessed November 2018.
[262] https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/, accessed November 2018.
[263] https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/ , accessed November 2018.
[264] https://exchange.xforce.ibmcloud.com/collection/Necurs-delivers-language-targeted-porn-scams-fdb9d6b7941506807cbe56dd06e142d0, accessed November 2018.
[265] https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en/, accessed November 2018.
[266] https://blog.avast.com/new-torii-botnet-threat-research, accessed November 2018.

- **Chalubo botnet.** Sophos researchers identified the activity of another Linux-based botnet in their honeypots trying to brute-force SSH to gain access. After the infection, the bot (Lua script) seems to be focusing mostly on DDoS attacks (DNS, UDP and SYN floods).
- **Botnets Updated:** VpnFilter, a multistage and modular botnet originally developed to target the Modbus protocol, receive an update. Partially attributed to Fancy Bear[267], this botnet presents 7 new features including: network discovery, larger coverage on endpoint exploitation and obfuscating the source of the attack. Researchers found this botnet infecting Linksys, MikroTik, NETGEAR, TP-Link and QNAP NAS network devices[268]. In addition to VPNFilter updates, Hide and Seek (HNS), which was initially found targeting IP cameras[269], also received an update to cover android devices by exploiting Android Debug Bridge (ADB), similar to the Fbot botnet[270]. It is noteworthy that devices manufactured in Taiwan, China and Korea are typically distributed with this functionality enabled. For more information on multistage and modular threats, please consult chapter 5.5.
- **Botnets and credential reuse attacks.** Researchers at Akamai reported that in 2018 (between May-June) 8,3 billion malicious login attempts using automated bots were identified. The main objectives of these malicious attempts were to forge Identities, information gathering and capturing goods or money[271].
- **Botnet to Lease.** Renting out botnets was observed to be a reliable source for malicious actors to monetize their activities. Occasionally, these providers create some additional regular income by providing extra support packages with their lease options. As an example, Blow-bot was seen costing US $750 to US $1,200 based on the support and features needed[272].
- **Social Media, a platform to run and advertise botnets.** It has been reported that, different profiles on Instagram are selling access to many IoT type botnets along with stolen or compromised data. Although this trend was mostly common on fraud and money laundry activities, now it seems that malicious actors are turning to these platforms due to huge coverage of potential customers with minimal content moderation[273]. On the other hand, Proofpoint researchers investigated a botnet that was misusing an old Facebook API and a third-party app to run spam campaigns. For instance, gathering likes and followers for Facebook branded posts and pages[274].
- **Predictions made regarding botnets.** Besides the above interesting points, some predictions regarding botnets have been assessed in the reporting period. These are:

---

[267] https://blog.avast.com/vpnfilter-malware-update-and-hide-seek-botnet-targets-android, accessed November 2018.
[268] https://blog.talosintelligence.com/2018/05/VPNFilter.html, accessed November 2018.
[269] https://www.bleepingcomputer.com/news/security/new-hns-iot-botnet-has-already-amassed-14k-bots/, accessed November 2018.
[270] https://blog.avast.com/vpnfilter-malware-update-and-hide-seek-botnet-targets-android, accessed November 2018.
[271] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-2018-credential-stuffing-attacks-report.pdf, accessed November 2018.
[272] https://cdn.armor.com/app/uploads/2018/03/27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf, accessed November 2018.
[273] https://www.hackread.com/hackers-selling-fortnite-accounts-botnet-on-instagram/, accessed November 2018.
[274] https://www.proofpoint.com/sites/default/files/pfpt-uk-tr-the-human-factor-2018.pdf, accessed November 2018.

- *Swarmbots and hivenets*. Recent reports predict that the evolution of botnets could be tied closely with swarm type of attacks[275], considering that these are scalable in architecture and autonomy. The concept of sharing collected intelligence between bots is to remove the dependency on the "bot master" or "bot herder", to provide commands. This type of activity has the potential to overwhelm the defence systems and teams by not only decreasing the time needed for different stages of an attack by the attacker but, simultaneously attacking different devices or infrastructure and exploiting vulnerabilities en-mass[276]. Hide and Seek botnet enhancements providing bidirectional commands in a peer-to-peer way is a small example of such capabilities.
- *Blockchain and Botnets*. Researchers at Fortinet predicted the usage of blockchain in Command and Control (C2) communications in the near future due to the characteristics and cost effectivity of blockchain based communications. However, no sign of adoption of such methodology has been seen in the cybercriminal landscape[277].

3.7.3 Trends and main statistics

- In Q1 2018, the number and duration of DDoS attacks rose compared to Q4 2017 and Kaspersky researchers believe that can be directly linked to 2 linux-based botnets known as Darkai and AESDDoS[278].
- The percentage of Linux-based botnet decreased slightly compared to Q4 2017 (from 71% to 66%)[279].
- Regarding credential reuse in botnets, Akamai reported that each botnet is creating 300.000 malicious login attempts per hour with US, Russia and Vietnam as the top 3 sources of the attacks[280].
- According to McAfee's September report, the United States is the top country for hosting botnet control servers (36%) followed by Germany (14%) and Russia (5%) in the second and third place[281].
- Gamut botnet by far was the dominant spam botnet in Q2 2018 with 86%. Most spams were "Canada Revenue Agency" followed by bogus job offers and money Mule.
- Source code of 7 variants of Mirai was leaked via a twitter handler in first half of 2018: Akiru, Katrina_V1, Sora, Owari, Saikin, Josho_V3, and Tokyo[282].

---

[275] https://www.fortinet.com/blog/industry-trends/rise-of-the--hivenet---botnets-that-think-for-themselves.html, accessed November 2018.
[276] https://www.fortinet.com/blog/industry-trends/the-evolving-threat-landscape---looking-at-our-2018-predictions.html, accessed November 2018.
[277] https://www.fortinet.com/blog/industry-trends/the-evolving-threat-landscape---looking-at-our-2018-predictions.html, accessed November 2018.
[278] https://securelist.com/ddos-report-in-q1-2018/85373/, accessed November 2018.
[279] https://securelist.com/ddos-report-in-q1-2018/85373/, accessed November 2018.
[280] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-2018-credential-stuffing-attacks-report.pdf, accessed November 2018.
[281] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf, accessed November 2018.
[282] https://blog.avast.com/hacker-creates-seven-new-variants-of-the-mirai-botnet, accessed November 2018.

*The overall trend of **botnet** attacks in 2018 is **INCREASING**.*

3.7.4 Top Botnet Attacks

- A new botnet was created in just one day by exploiting at least 18.000 Huawei routers using the old CVE-2017-17215 vulnerability. The code of this botnet was then used in Satori and Brickerbot botnets reportedly[283].
- Necurs 2018 activity represents its multiple faces: after a typical stream of spams, in August 2018 the Necurs botnet targets more than 3.701 banking domains[284]. During the same month, the botnet was observed delivering Marap, which is a malware loader/dropper, to first fingerprint the infected device and then deliver the main malware at later stage, based on the objectives of the attack[285]. Later on, in September it was observed delivering language targeted adult-related extortion scams[286], as reported by X-Force research team, in one instance it was seen sending 3 million messages to German recipients[287]. Still one of the most dominant botnets.
- A credential reuse botnet attacked one fortune 500 financial services and made more than 8,5 million malicious login attempts in just 48 hours, with a third of the traffic originated from Vietnam and the United States[288]. Also as previously mentioned, the general credential stuffing/reusing attacks between May and June 2018 were around 8.300 million attempts.

3.7.5 Specific attack vectors

Botnets are unique in different ways when it comes to attack vectors. The infected machines (zombie networks) are created by exploiting common vulnerabilities, brute-forcing and other common infection techniques. Furthermore, the "botnet herder" facilitates and provides a platform for different malicious attacks. Examples range from distributing spam, malware infections, credential reuse, crypto-mining and most commonly DDoS.

3.7.6 Specific mitigation actions

As discussed Botnets are used in different types of attacks. DDoS attacks are a common scheme for usage of Botnets and we discussed the mitigation techniques in the chapter 3.5, describing the DDoS threat. Moreover, mitigation vectors for this threat include:

- Install and configure a network and application firewall.
- Perform traffic filtering to all relevant channels (web, network, mail).
- Install and maintain an IP address blacklist.

---

[283] https://www.zdnet.com/article/iot-hacker-builds-huawei-based-botnet-using-18000-devices-in-one-day/, accessed November 2018.
[284] https://cofense.com/necurs-targeting-banks-pub-file-drops-flawedammyy/, accessed November 2018.
[285] https://www.bleepingcomputer.com/news/security/necurs-botnet-pushing-new-marap-malware/, accessed November 2018.
[286] https://exchange.xforce.ibmcloud.com/collection/Necurs-delivers-language-targeted-porn-scams-fdb9d6b7941506807cbe56dd06e142d0, accessed November 2018.
[287] https://exchange.xforce.ibmcloud.com/collection/Necurs-delivers-language-targeted-porn-scams-fdb9d6b7941506807cbe56dd06e142d0, accessed November 2018.
[288] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-2018-credential-stuffing-attacks-report.pdf, accessed November 2018.

- Implement a botnet Sinkholing[289].
- Orchestrate and deploy regular vulnerability and patch management programs[290].
- Implement network and host level controls (i.e. AntiMalware solutions, DNS analysis)[291].
- Follow the standards for invalid traffic detection methods[292].

3.7.7 Kill Chain



Figure 19: Position of botnets in the kill-chain

3.7.8 Authoritative references

"[state of the internet] / security credential stuffing attacks", Akamai 2018, "The black market report", ARMOR 2018, "McAfee Labs Threats Report", McAfee 2018, "The Human Factor", Proofpoint 2018, "Quarterly Threat Landscape Report Q2-Q3 2018", Fortinet 2018, "Statistics for botnet-assisted DDoS attacks" Kaspersky 2018.

[289] http://la.trendmicro.com/media/misc/sinkholing-botnets-technical-paper-en.pdf, accessed November 2018.
[290] https://www.veracode.com/security/botnet, accessed November 2018.
[291] https://www.shadowserver.org/wiki/pmwiki.php/Information/BotnetDetection, accessed November 2018.
[292] http://mediaratingcouncil.org/082815_MRCDigitalRoadmapPDRF%20paper_Final_in12ptFont.pdf, accessed November 2018.

3.8 Data Breaches

3.8.1 Description of the cyberthreat

When it comes to threats and the cyber landscape, Data Breach is the only topic that does not specifically apply to a threat but reflects a successful malicious attempt, which led to an incident from the compromise or loss of data. Defined as a collective term for a successful incident from the leakage or exposure of data (including sensitive information related to organisations or simply personal details of individuals, i.e. medical information), it relates directly to the outcome from other cyberthreats.

3.8.2 Interesting points

- **Healthcare and Social Media.** Six social media breaches, including the Cambridge Analytica-Facebook incident, accounted for over 56% of the total number of records compromised[293]. The Healthcare sector continues to lead in the number of incidents (27%). The largest incident was reported by 211 LA County, disclosing the exposure of 3,5 million records from accidental loss.
- **Data is exposed or compromised every day.** According to the "breach level index report", more than 25 million records were compromised or exposed every day during the first six months of 2018[294]. In the United States alone, 22 million records were lost or stolen until July 2018.
- **Encryption is broken**. Only 1% of all the data leaked, lost or stolen was encrypted which presents a decrease compared with 2017.
- **Web Applications attacks and breaches.** Researchers suggests that web-application attacks often result in larger data breaches[295]. Not surprisingly, cloud infrastructure seems to be the most attractive target for malicious actors.
- **Costs of a cybersecurity breach**. The average cost of a cybersecurity breach increased 6,4% in 2018. Notably, the average size of a data breach is typically amplified by 2,2%. Third-party involvement and extensive cloud migration at the time of a breach increases the cost[386]. Factors such as incident response and encryption are repeatedly identified as key to reduce the costs of a data breach[296].
- **Insiders still play a big role**. Different reports suggest that 48% of data breach incidents involved outsiders and 27% were caused by human factor or negligence. This leaves 25% for system errors and glitches (business processes and IT)[297].
- **The 2018 prediction on data breaches.** The enforcement of GDPR in Europe predicted an increase in the number of extortion attacks, targeting private/personal data covered by this directive. In other words, malicious actors will increase the number of data breach attempts[298] threatening with GDPR penalties deriving from the disclosure. Furthermore, multiple reports suggest that data breaches will

[293] https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx, accessed November 2018.
[294] https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx, accessed November 2018.
[295] https://www.nttsecurity.com/gtir, accessed November 2018.
[296] https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html, accessed October 2018.
[297] http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=917, accessed November 2018.
[298] https://www.trendmicro.com/vinfo/my/security/news/threat-landscape/2018-trend-micro-security-predictions-paradigm-shifts, accessed October 2018.

cause additional problems especially to US-companies[299], due to the introduction of new data protection regulations in different countries[300]. Gemalto suggested that the implementation of Australian regulation (Notifiable Data Breach) had an impact on the number of breaches, increasing from 18 to 308 in the country[301]. Considering the number of social media breaches, this trend is expected to increase as more sectors are leveraging from these platforms to reach audiences[301].

3.8.3 Trends and main statistics

- Data Breaches compromised 4.500 million records in first half of 2018.
- Europol reported that external individual malicious actors carried out 73% of the breaches and 50% were attributed to organised crime groups. Additionally, the industry believes that state sponsored actors were involved[302] in ca. 12% of the data breaches.
- Social media ranks top for the number of records breached (56%) due to the high-profile customer data compromised from Facebook and Twitter, involving 2.2000 million and 336 million respectively.
- Healthcare continues to lead in number of incidents (27%). The largest of such incident, 211 LA County, exposed 3,5 million records through accidental loss.
- Identity theft continues to be the leading type of data breaches (56%). This has been the leading factor since 2013, according to Gemalto.
- Considering the geographic landscape:
  - North America is considered the most popular target representing 57% of the breaches and 72% of the records exposed.
  - Europe observed a 36% decrease in the number of incidents but a 28% increase in the number of records breached, with UK organizations being the most affected in Europe.
- In terms of breach costs, Canada leads in direct costs and the United States has the highest indirect costs (US $81 per compromised record in Canada and US $152 in US)[386].
- The number of incidents with data breaches declined comparing the first half of 2017 (171) with 2018 (123). However, the number of records breached increase exponentially, from 2,7 million in the first half of 2017 to 4.5 billion in the first half of 2018.[301]
- Ca. 48% of the breaches identified, used hacking techniques such as malware ca. 30-51% and email as a delivery mechanism ca. 49%[302].

*The overall trend of **data breaches** in 2018 is **INCREASING**.*

[299] http://www.experian.com/assets/data-breach/white-papers/2018-experian-data-breach-industry-forecast.pdf, accessed November 2018.
[300] https://www.prnewswire.com/news-releases/data-breach-predictions-the-trends-to-shape-2018-300569778.html, accessed November 2018.
[301] https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx, accessed November 2018.
[302] https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf, accessed November 2018.

3.8.4 Top Data Breaches

- **Huazhu Hotels Group (Chinese hotel chain)**: A total of ca. 22,3 GB of data, about ca. 130 million customers' personal data and booking information was hacked from 13 hotels operated by HHG - the data was found advertised on the Dark Web.
- **Facebook**: A weakness in the "Search" capability of the Facebook platform exposed ca. 2.000 million users' information publicly. Other Facebook related data breaches were:
  - Ca. 87 million records of user data were reportedly misused by Cambridge Analytica[303] (April 2018);
  - Ca. 14 million users were affected for a period of 4 days whereas users' privacy settings were set to public for every post generated (May 2018);
  - Ca. 30 million user data exposed on a vulnerability found in the "view as" functionality of the Facebook profile, providing access to malicious actors via "access token" and take over users' accounts (September 2018)[304].
- **Twitter (Hacking)**: A glitch in the password handling procedure potentially exposed all users' passwords in plain text before completing the hashing process. (**Ca. 330 million**)
- **Aadhaar (India) (Web):** A weakness in the system responsible for the management of Indian citizens IDs, allowed anyone to download private information from citizens including names, unique 12-digit identity numbers as well as linked applications including banking details. (**Ca. 1,100 million**)
- **Exactis (Hacking):** A database server accessible publicly allowed the theft of millions user records. The data includes phone numbers, home address and email addresses. (**Ca. 340 million**)
- **Timehop (Hacking)**: The Timehop data breach included names, email addresses, dates of birth, gender of users, country codes, and some phone numbers. An unauthorized/malicious actor logging in to the cloud server initiated the intrusion by abusing administrative user's credentials. (**Ca. 21 million**)
- **GOMO (Web)**: Users' of GOMO App had their information exposed on a publicly accessible server (backup file) on port 80 with no logins required. (**Ca. 50,5 million**)
- **Company affiliated to FedEx (Web)**: An unsecure Amazon S3 server contracted by a company affiliated to FedEx exposed data on the internet. (**Ca. 119.000**)
- **Orbitz (Hacking)**: Data related with payment cards was exposed in the internet due to an intrusion. The data accessed may have included full name, payment card information, date of birth, phone number, email address, physical and/or billing address, and gender. (**Ca. 880.000**)
- **COMCAST (Hacking)**: A software flaw in the Comcast Xfininty's login page exposed social security numbers and home addresses from costumers. (**Ca. 26,5 million**)
- **SingHealth's outpatient clinics (Hacking)**: An intrusion in the SingHealth's outpatient clinics systems resulted in a breach exposing records containing the name, addresses, gender, race, date of birth and National Registration Identity Card (NRIC) number of patients visiting the healthcare units since May 2015. (**Ca. 1,5 million**)

[303] https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data, accessed November 2018.
[304] https://www.enisa.europa.eu/publications/info-notes/another-facebook-security-breach, accessed November 2018.

- **211 LA County (Web)**: Data from 221 LA County was accidentally exposed due to a misconfigured S3 cloud server. S3 or Amazon Simple Storage Service is a "simple storage service" offered by Amazon Web Services that provides object storage through a web service interface. The records contained access credentials, social security numbers, email addresses and contacts from patients. (**Ca. 3,5 million**)
- **British Airways (Web)**: British Airways reported a breach of personal and payment data via the web and mobile app between 21st August and 5th September 2018[305]. (**Ca. 380.000**)
- **Google (Web)**: A software flaw in the Google plus platform potentially exposed user's private data between 2015 and 2018[306]. The data included age, date of birth, address, occupation and profile photos. (**Ca. 500.000**)
- **Various other data breaches**: DHS, ALERRT[307], Ticketmaster[308], Rail Europe[309] and icliniq[310] were also victims of data breach incidents with different types of personal identifiable information (PII) exposed, emphasising the growing number incidents in 2018.[311]

3.8.5 Specific attack vectors

SQL Injections Attack. This type of attack remains the most popular and commonly used web application attack. Also referred as cloud malware injection attacks[312], these are gaining popularity from an increasing demand for cloud hosting services.

Phishing Attacks. Attackers are targeting companies by trying to impersonate a partner or a vendor through an email that asks users to take an action. These emails are giving attackers an access point to critical data or information.

Insider threat. This category includes any kind of unauthorised or malicious use of organisational resources. Although most of the attacks are facilitated by external actors, insiders (with or without privileged access) are playing a key role in data breaches.

Physical theft and loss. This refers to intentional or unintentional loss of data due to physical or social engineering attacks.

3.8.6 Specific mitigation actions

Due to the wide nature of threats that can lead to a data breach, the below-mentioned mitigation controls overlap with other cyberthreats. The mitigation vector for this threat contains the following elements[313]:

---

[305] https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information, accessed November 2018.
[306] https://www.digitalinformationworld.com/2018/10/google-data-breach-api-bug.html, accessed November 2018.
[307] https://www.zdnet.com/article/a-massive-cache-of-law-enforcement-personnel-data-has-leaked/, accessed November 2018.
[308] https://help.ticketmaster.co.uk/hc/en-us/articles/360006400073-Who-has-been-affected-by-the-recent-data-security-incident-and-what-may-have-been-compromised-, accessed November 2018.
[309] https://www.raileurope.com/about-rail-europe/article/notice-of-data-breach, accessed November 2018.
[310] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-august-2018-215000000-records-leaked/, accessed November 2018.
[311] https://www.enisa.europa.eu/publications/info-notes/how-data-is-under-siege-like-never-before, accessed November 2018.
[312] https://www.globaldots.com/cloud-attack-vectors/, accessed November 2018.
[313] https://zeltser.com/malware-in-the-enterprise/, accessed November 2018.

- Perform data classification to assess and reflect the level of protection needed according to data categories.
- Implement Data Loss Prevention solutions to protect data according to their class for both in transit and in rest, especially in cases of large data transfers and use of USB devices.
- Promote the use of sensitive data encryption, both in transit and in rest.
- Reduce the access rights to data according to principle of least privileges.
- Develop and implement security policies for all devices.
- Orchestrate the patch management and updates system in line with a vulnerability management framework.
- Develop new policies to enforce the adoption of stronger passwords and two-factor authentication.
- Limit the amount of sensitive information stored on web-facing applications.
- Implement malware protection and insider threat-protection policies.
- Implement a holistic plan to cover the two distinct parts of a breach incident: assessment of the breach and development of an appropriate incident response. Organisations that plan greatly reduce their legal, reputational and financial impact.
- Enforce security awareness programs within the organization by developing and delivering training courses to users. Train employees to identify and report suspicious emails or to call the IT department if anything unusual is identified.

3.8.7 Kill Chain

Kill chain is not relevant for this threat: this is a "composite" threat consists of many cyberthreats spanning all the phases of the kill chain, just as cyber espionage.

3.8.8 Authoritative references

"Internet organised crime threat assessment", Europol 2018, "2018 Data Breach Investigations Report", Verizon, "Cost of Data Breach Study", IBM 2018[386], "2018 H1 Breach Level Index" , Gemalto.

3.9 Insider threat

3.9.1 Description of the cyberthreat

The insider threat may exist within every company or organisation. Any current or former employee, partner or contractor that has or used to have access to the organisation' digital assets, may intentionally or unintentionally abuse this access. The three most common types of insider threats are the - malicious insider - who acts intentionally - the negligent insider - who is just sloppy or does not comply with the policies and security instructions and the - compromised insider - who acts unintentionally as the means for the true attacker[314]. All these three types of insider threats must be studied in depth, as the acknowledgement of their existence and their modus operandi should define the organisation's strategy for security and data protection.

Analysis concludes that the insider threat trend decreased in 2018[315] mainly due to the infrequent publicly disclosure of incidents from inside the organizations.

3.9.2 Interesting points

The identified interesting points for the insider threat are as follows:

- **Insider threat perception changed with GDPR.** In 2018, the number of reported incidents with insider threat reduced compared with previous years. This can be justified by the way these incidents are now classified, shifting to data breaches with the introduction of GDPR.[315].
  - **The GDPR compliance rally within the EU is also changing the perception** of handling data breaches originated from insider threat incidents in the US[316]. In the realm of EU GDPR, the new California Consumer Privacy Act (CCPA) will get into effect on January 1, 2019[317].

3.9.3 Trends and main statistics

- Over half (60,8%) of the insider threat incidents impacting US Federal Organisations involved fraud, with an average financial impact between US $75.712 and US $317.551. Only in 2018, three fraud incidents (9,4%) resulted in a financial impact of ca. US $1 million[318].
- Ca. 44% of the payload for the User and Entity Behaviour Analytics (UEBA) within an organisation came from insider threats[315].
- Ca. 70% of the Chinese companies were relying on User and Entity Behaviour Analytics (UEBA) for insider threats[315].
- Ca. 50,6% of the healthcare organisations and 47,3% of medium-sized companies (up to 250 employees) rated the insider threat as their primary security concern[315].
- Ca. 77% of the companies' data breaches are caused by insiders[319].

---

[314] https://www.forcepoint.com/sites/default/files/resources/files/whitepaper_insider_threat_program_guide_en.pdf, accessed November 2018.
[315] https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf, accessed November 2018.
[316] https://insights.sei.cmu.edu/insider-threat/2018/10/how-cert-rmm-and-nist-security-controls-help-protect-data-privacy-and-enable-gdpr-compliance-part-1-.html, accessed November 2018.
[317] https://www.helpnetsecurity.com/2018/09/05/ccpa-implications/, accessed November 2018.
[318] https://insights.sei.cmu.edu/insider-threat/2018/11/insider-threats-in-the-federal-government-part-3-of-9-insider-threats-across-industry-sectors.html, accessed November 2018.
[319] https://www.forcepoint.com/sites/default/files/resources/files/whitepaper_practical_executives_guide_data_loss_prevention_en.pdf, accessed November 2018.

- Ca. 54% more organisations recorded a growth of insider threats in 2018[320].
- Ca. 48% of the companies still perceive the detection of insider threats as a great challenge for their security team[320].
- The average amount of companies' resources invested in insider threats (the average budget percentage for the Insider Threat team) was 23%[320].
- Approximately half of the companies (46%) admitted not having absolute knowledge of their sensitive data repositories[321].
- Ca. 43% of the companies' employees were confident that their data is secure against insider threats, even if their network is considered insecure[321].
- Ca. 51% of the concerned companies believed that their assets would most probably be targeted by unintentional insiders and 49% by malicious insiders[321,322].
- Ca. 90% of the cybersecurity professionals reported that the company they work for felt vulnerable to insider threats[323].
- Ca. 53% of the companies had at least one incident of insider threat in the last 12 months. Ca. 20% of them had more than six incidents in the same period[323].
- Ca. 46% of the companies noticed that the frequency of insider threat incidents was stable in 2018 and 27% responded that the frequency increased[323].

*The overall trend of **insider threats** in 2018 is **DECREASING**.*

3.9.4 Top IT and other assets vulnerable to insider attacks

A recent report[323] showed that the assets presented in figure 20 are the most vulnerable to insider attacks.

[320] https://www.alertlogic.com/assets/industry-reports/Threat-Monitoring-Report-Alert-Logic.pdf, accessed November 2018.
[321] https://safenet.gemalto.com/data-security-confidence-index/?utm_campaign=dsci&utm_medium=press-release&utm_source=&utm_content=report&utm_term=, accessed November 2018.
[322] https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf, accessed November 2018.
[323] https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, accessed November 2018.

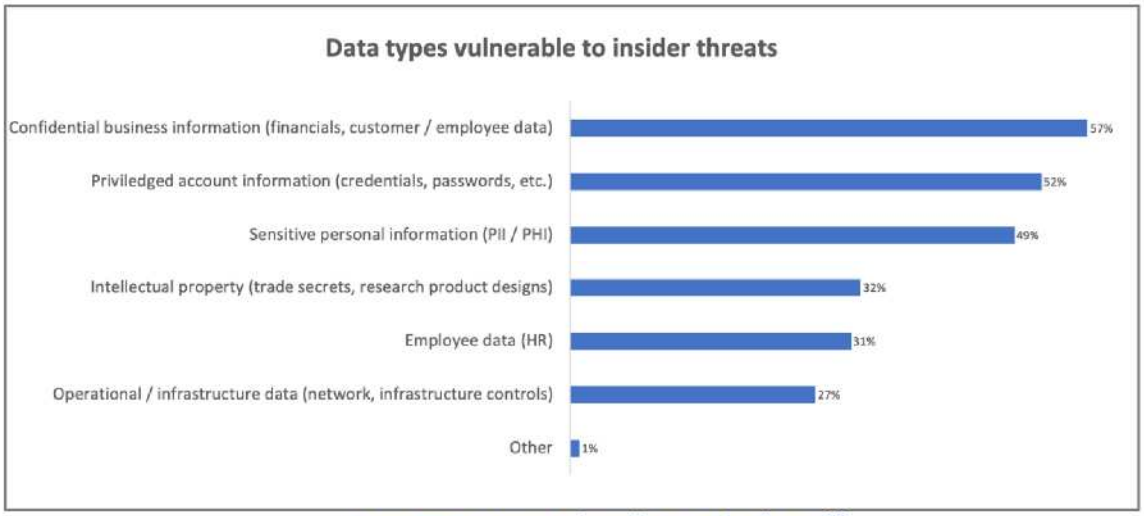


Figure 20: Data types vulnerable to insider threats[324]

The same report also focused on the IT assets that are most vulnerable to insider threats presented in figure 21.

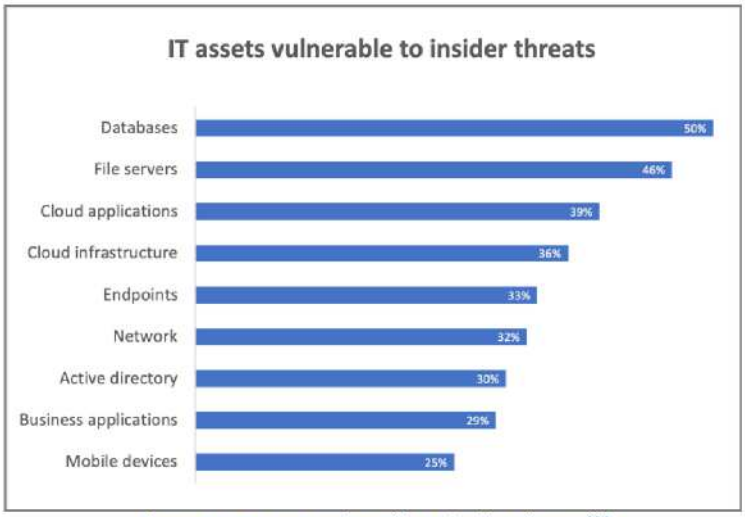


Figure 21: IT assets vulnerable to insider threats[324]

3.9.5 Specific attack vectors

A recent survey[323] revealed that the groups shown in figure 22 are the most dangerous insider threats within a company or organisation.

[324] https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, accessed November 2018.

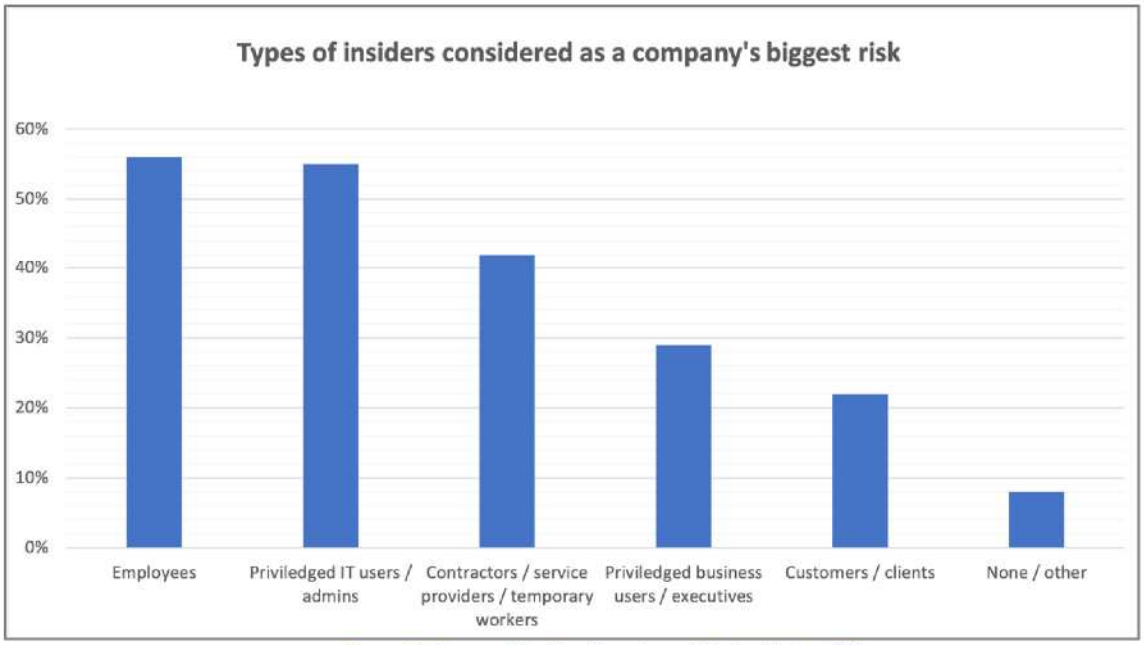


Figure 22: Types of insider threats and their risk level[324]

According to a study conducted with cybersecurity experts working for companies or organisations, phishing (67%) is the biggest weakness in the case of unintentional insider threats. Weak or reused passwords (56%), unlocked devices (44%), password sharing practice (44%) and unsecured WiFi networks (32%) were also part of the list. The study also revealed that the main reason that makes the company they work for vulnerable to insider threats, is the excessive access privileges given to many employees[323].

3.9.6 Specific mitigation actions

Specific actions for the insider threat contain the following elements:

- Implement human behaviour-driven data loss prevention (DLP) software by applying user activity monitoring, behaviour analytics and forensics in order to increase the effectiveness of a traditional DLP[325].
- Apply the 80/20 rule for the company's resources[319]. A company or an organization facing a security incident must not exhaust its available resources; a part of the resources must become available for other incidents taking place simultaneously (the case where one incident is the smokescreen for a more serious attack) or for recovery.
- Implement a Single-Sign-On (SSO) access for the company's applications[326].
- Implement a multifactor authentication method[326].
- Define a security policy addressing insider threats, particulary based on user awareness, one of the most effective controls for this type of cyberthreat.
- Use identity and access management (IAM) solutions by also implementing segregation of duties (e.g. according to defined roles).

[325] https://www.helpnetsecurity.com/2018/10/29/insider-threats-protection/, accessed November 2018.
[326] https://www.ca.com/us/collateral/solution-brief/how-can-i-counter-the-insider-threats-within-my-organization.thanks.html, accessed November 2018.

- Implement identity governance solutions defining and enforcing role-based access control.
- Implement/use security intelligence solutions.
- Use data-based behaviour analytical tools.
- Implement privileged identity management (PIM) solutions.
- Implement training and awareness activities.
- Implement audit and user monitoring schemes.

3.9.7 Kill Chain

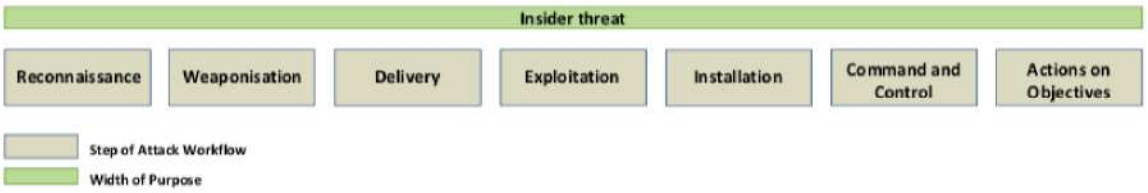


Figure 23: Position of Insider Threat in kill-chain

3.9.8 Authoritative references

"2018 Cyberthreat Defense Report", CyberEdge Group[315]; "Businesses collect more data than they can handle", Gemalto[321]; "The State of Industrial Cybersecurity 2018", Kaspersky Lab[322]; "2018 Insider Threat Report" and "How can I counter the insider threats within my organization", CA Technologies[323,326].

3.10 Physical manipulation/damage/theft/loss

3.10.1 Description of the cyberthreat

Although physical attacks are not a real cyberthreat, they are still possible within businesses today. Physical attacks may not be as popular as other types of cyberthreats, they can still lead to data breaches (even in a less subtle way). Companies are increasingly concerned about the data residing within the devices and most specifically about the loss of PII data and Intellectual Property, especially in the age of GDPR. Although storage encryption would suffice to mitigate major risks of physical attacks, the number of companies that have a consistent enterprise-wide encryption strategy is stable. Finally, physical access to a device still gives the opportunity to attackers to conduct their malicious activities, e.g. ATM fraud and POS attacks.

3.10.2 Interesting points

The identified interesting points for physical manipulation/damage/theft/loss are as follows:

- **Digital theft has overtaken physical theft with respect to corporate fraud[327].** Physical theft of assets was the most prevalent type of corporate fraud for the last 10 years. However, information theft, loss, or attack has been reported in 2017 as the most prevalent type of fraud compared to physical theft.
- **The widespread adoption of cloud storage**. A recent reported indicated that 80% of organisations are already using cloud storage and file sharing services while 16% of organisations are planning to use them in the next couple of years[328]. The aforementioned widespread adoption of cloud storage results in a limited number of reported physical thefts by major companies[329].
- **The GDPR effect.** The GDPR[330] is relevant to organisations that handle personal data in a digital as well as physical format. Recent privacy regulations have increased the compliance-driven activities and thus, taking into account the potential fines outlined, companies will be interested in investing more in information security[331]. GDPR is expected to have a direct impact on improving the physical security of organisations.
- **The slow progress in storage encryption technologies.** According to a survey[327]: establishing a storage encryption solution is one of the most effective controls in data protection, for many managers from the surveyed companies. The survey identified that only 43% of the companies currently have a consistent enterprise-wide encryption strategy[332]. The aforementioned percentage is the same as last year indicating slow progress for wider adoption of encrypted storage practices. Compliance with regulations is a significant driver for deploying encryption technologies according to half of the surveyed companies. Finally, according to a research[327], physical theft or loss of Intellectual Property is a top concern for executives. A fact that will definitely help towards a wider adoption and deployment of storage encryption technologies.

[327] https://www.kroll.com/en-us/global-fraud-and-risk-report-2018, accessed October 2018.
[328] https://community.spiceworks.com/blog/3058-cloud-storage-services-who-claims-the-top-spot-among-microsoft-google-dropbox, accessed October 2018.
[329] https://www.shreddingmachines.co.uk/pdfs/Kensington-GDPR-White-Paper.pdf, accessed October 2018.
[330] https://eugdpr.org/, accessed October 2018.
[331] https://www.viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Tietoturvan-vuosi-2017_EN.pdf, accessed October 2018.
[332] https://www.thalesesecurity.com/2018/global-encryption-trends-study, accessed October 2018.

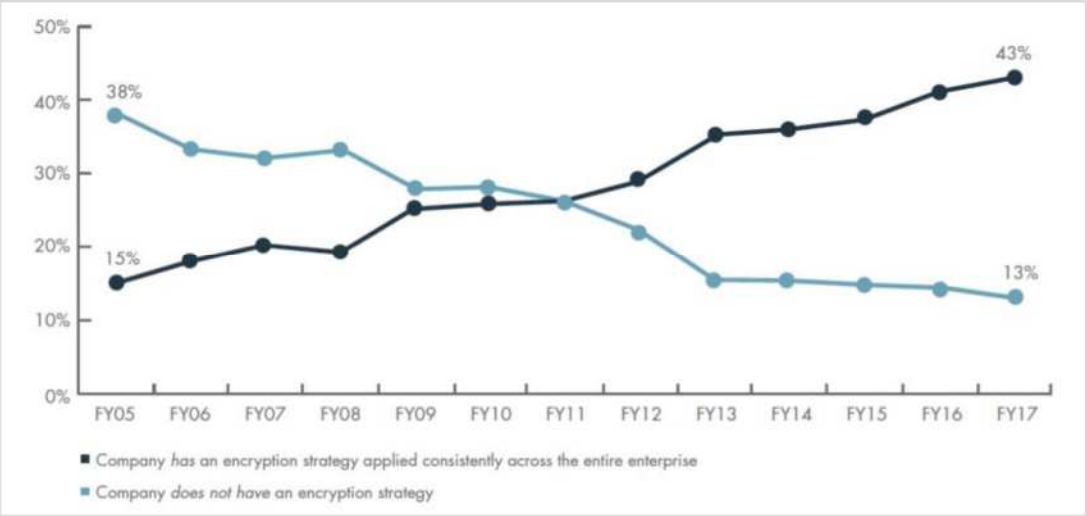


Figure 24: Trends in encryption strategy[332]

- **Consumers care more about lost data rather than lost devices.** 57% of the people that lost a personal device were mostly concerned about the data (pictures, documents, messages, etc.) residing within the gadget rather than the gadget itself[333].
- **Locations of theft.** The victim's work area or employee's private vehicles were the most common locations of theft[334] followed by theft in airports and hotels[335].
- **Assets lost or stolen.** Paper documents and laptops are the most prevalent assets found in physical theft or loss incidents[334].
- **Physical security policies and controls.** According to survey conducted by an industry player polling IT professionals across different sectors, almost one-third of the organisations lack a physical security policy to protect laptops and mobile devices[335]. It also concluded that, 42% of the organisations have fully implemented different security measures for the physical security of critical IT systems[336]. Moreover, more than half of the organisations do not utilize physical locks to secure IT equipment[335].
- **ATM physical attacks on the rise.** During 2017, almost 3.600 physical attacks against banking ATMs were reported in Europe[337]. An increase of 73% is therefore observed compared to 2012 and 20% compared to 2016. The European Association for Secure Transactions (EAST) reported that "black box" attacks in Europe increased 307% compared to 2016[338]. Finally, the increase of "ATM jackpotting" attacks in US is another indication of a trend with physical attacks against banking ATMs[334].

[333] https://mozy.com/about/news/reports/lost-and-found/, accessed October 2018.
[334] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf, accessed October 2018.
[335] https://www.theventanagroup.com/resources/kengsington-security.pdf, accessed October 2018.
[336] https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf, accessed October 2018.
[337] https://www.statista.com/statistics/419746/physical-burglary-attacks-atm-in-europe/, accessed October 2018.
[338] https://www.atmmarketplace.com/blogs/new-threats-demand-renewed-attention-to-atm-physical-security/, accessed October 2018.

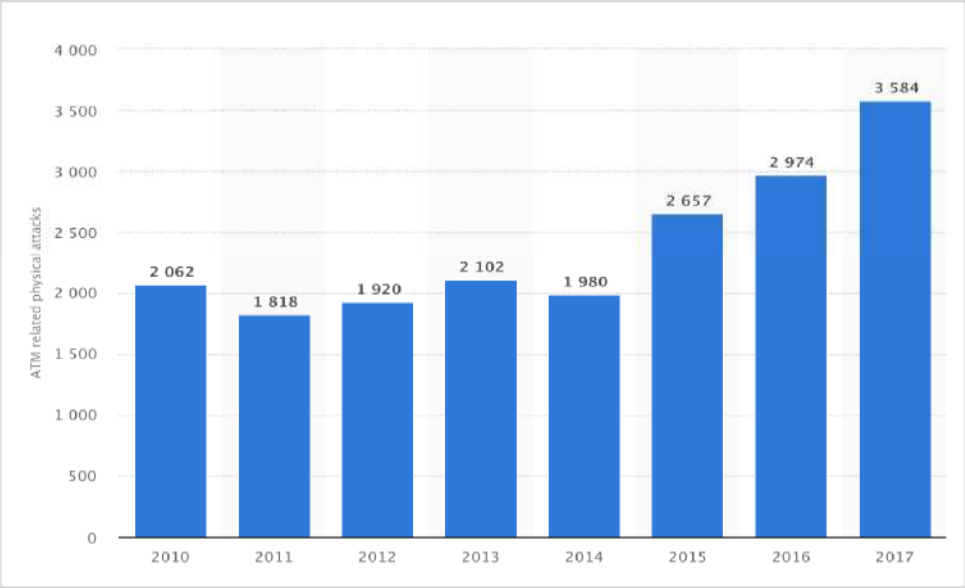


Figure 25: Physical attacks against ATMs in Europe[337]

- **Card skimming in the retail sector.** Payment card skimming attacks were responsible for one-third of the reported data breaches in the retail sector[334]. Petrol stations terminals are the major target of payment card skimmers in the retail sector (in 87% of the reported card skimming attacks)[334].

3.10.3 Trends and main statistics

- According to Verizon[334], 11% of reported data breaches involved physical actions.
- TrendMicro[339] reported that 16% of data breaches were caused by physical loss. ITRC reported that physical theft is the root cause of 4,5% of data breaches and 0,8% of records stolen within 2017[340].
- Barkly reported that the theft of information assets is the third most costly consequence of successful endpoint attacks after IT/end-user productivity loss and system downtime[341].
- Healthcare, Public and Financial sectors are the top sectors for data breaches reported, due to physical theft or loss[334].
- 25% of data breaches in the financial sector are due to the loss or theft of devices as well as the major cause for data leakages (taking into account the sensitivity of financial and customer data stored)[342].
- 46% of businesses feel vulnerable for the exposure to risks coming from mobile device loss[343].

---

[339] https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf, accessed October 2018.
[340] https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf, accessed October 2018.
[341] https://www.barkly.com/ponemon-2018-endpoint-security-statistics-trends, accessed October 2018.
[342] https://globenewswire.com/news-release/2018/10/02/1588510/0/en/Bitglass-2018-Financial-Services-Breach-Report-Number-of-Breaches-in-2018-Nearly-Triple-That-of-2016.html, accessed October 2018.
[343] https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2017/11/10083900/20170710_Report_Human-Factor-In-ITSec_eng_final.pdf, accessed October 2018.

- UK's data protection regulator, the Information Commissioner's Office (ICO) reported that 20% of data security incidents recorded between January and June 2017 were due to the physical theft or loss[344]. While the majority of the incidents resulted from the loss or theft of paperwork (14% of reported data security incidents), the loss of unencrypted devices is the cause of 5% of reported data security incidents.
- 44% of organisations find it challenging to deploy encryption technologies while 34% find it difficult to classify which are their critical data that need to be encrypted[332].

*The overall trend of **physical manipulation/damage/theft/loss** attacks in 2018 is **STABLE**.*

3.10.4 Specific mitigation actions

- Use of encryption in all information storage and flow that is outside the security perimeter (devices, networks, cloud services, etc.). This will eliminate the impact from this threat.
- Use asset inventories to keep track of user devices and remind owners to check availability.
- Limit the access to areas with sensitive information or equipment.
- Implement well-documented physical security policies and integrate physical security measures with digital devices to obtain a holistic approach.
- Consider using insurance to cover losses connected to both physical and related cyber- risks.
- Develop user guides for mobile devices (smartphones, tablets, laptops, etc.) and use good practices[345].
- Establish well-communicated procedures for the physical protection of assets, covering the cases of loss, damage and theft.
- Consider transferring the risks from this threat to an insurance.
- Put all necessary processes to reduce the time for the management of theft/damage/loss incidents.

3.10.5 Kill Chain

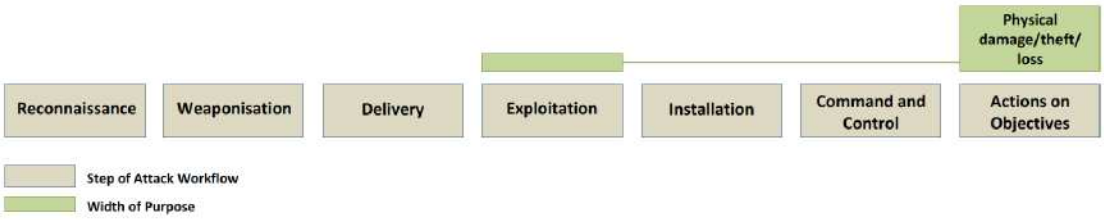


Figure 26: Position of physical manipulation/damage/theft/loss in the kill-chain

[344] https://ico.org.uk/media/action-weve-taken/csvs/2014850/data-security-incidents-csv-201718.xlsx, accessed October 2018.
[345] http://transition.fcc.gov/cgb/consumerfacts/lostwirelessdevices.pdf, accessed October 2018.

3.10.6 Authoritative references

"2018 Data Breach Investigations Report", Verizon[334]; "2018 Global Encryption Trends", Thales[332]; "Global Fraud & Risk Report 2017/18", Kroll[327]; "2017 Annual Data Breach Year-End Review", Identity Theft Resource Center[340].

3.11 Information Leakage

3.11.1 Description of the cyberthreat

Information leakage is one of the significant cyberthreats covering a wide variety of compromised information, from personal data collected by internet enterprises and online services to business data stored in IT infrastructures.

When security breaches become headlines on bulletins, blogs, newspapers, and technical reports, the focus is either on adversaries or on the catastrophic failure of cyber-defence processes and techniques. However, the indisputable truth is that despite the impact or the scope of a breach, is usually caused by an individual's action, or by a process failure inside the organisation[346]. Occasionally, a technical error or a misconfiguration may also cause a leak[347]. A recent report illustrates that unintended disclosure is the profound reason for information leakage in 2018[348].

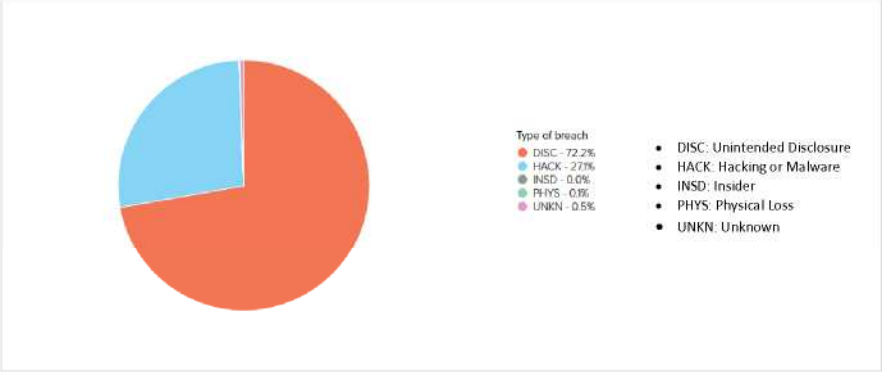


Figure 27: Annual percent of records breach by type[349]

Figure 27 shows the 10-year big picture of compromised data records as of September 2018[350].

[346] https://www.igi-global.com/dictionary/information-leakage/14421, accessed November 2018.
[347] http://projects.webappsec.org/w/page/13246936/Information%20Leakage, accessed November 2018.
[348] https://www.privacyrights.org/data-breaches/breach-type?taxonomy_vocabulary_11_tid=2436, accessed November 2018.
[349] https://www.privacyrights.org/data-breaches/breach-type?taxonomy_vocabulary_11_tid=2436, accessed November 2018.
[350] https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/, accessed November 2018.

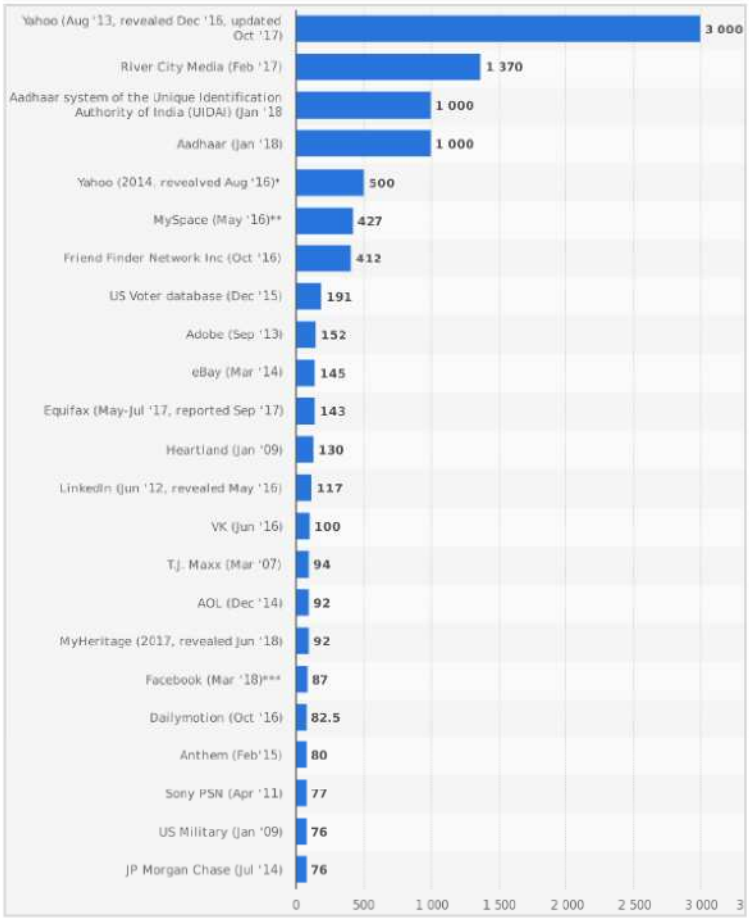


Figure 28: Number of data records in selected breaches (in millions)[351]

3.11.2 Interesting points

The identified interesting points for information leakage are as follows:

- **Geopolitics become an even stronger jigsaw puzzle**. Information leakages often drive bi-lateral agreements[352]. Targeted or nation-state sponsored attacks are multiplying resulting in information disclosures[353].
- **A busted myth.** The most reported reasons for information leakage are hacking and malware, however, device losses still count for ca. 50% of all breaches[354].

[351] https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/, accessed November 2018.
[352] https://soff.se/wp-content/uploads/2018/03/Cybersecurity_statsunderst%C3%B6dda-akt%C3%B6rer.pdf, accessed November 2018.
[353] https://cdn.sonicwall.com/sonicwall.com/media/pdfs/resources/2018-snwl-cyber-threat-report.pdf, accessed November 2018.
[354] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data, accessed November 2018.

- **Users voluntarily forget their PII ownership.** In some cases, the digital services' privacy policies drive users to waive ownership interest in their data voluntarily and, therefore, consent to data disclosures. Hence, the services operators may be able to benefit by 'monetising' this data[355,356,357,358,359].
- **Human error is the most crucial factor for data disclosure[360].**
- **Governmental organizations take the majority of data leakage incidents.** Approximately 60% of data leakage incidents take place in government and education institutions, banks and healthcare organisations[360].

3.11.3 Trends and main statistics

A recent report reveals the following trends regarding data disclosure[361].

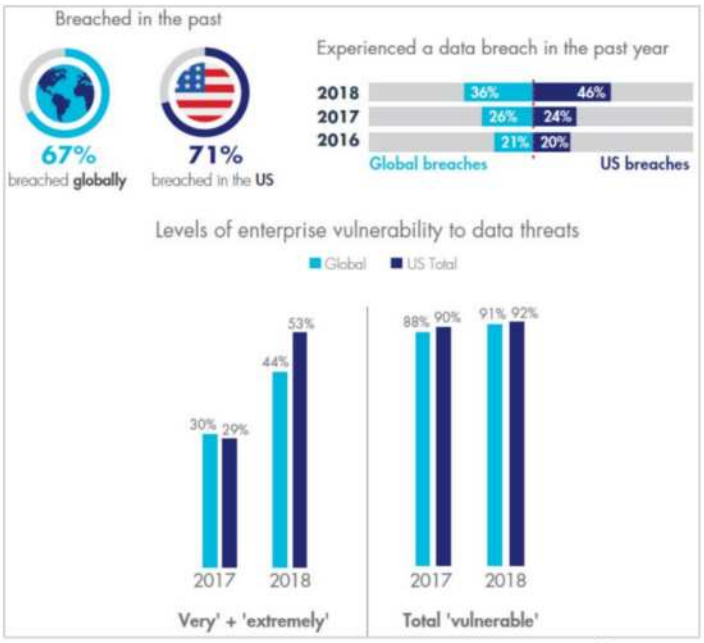


Figure 29: Recent trends for data disclosure as of 2018[361]

- As of March 2018, ca. 500.000 email accounts with passwords were priced at US $90 in the Dark Web[362].

---

[355] https://cdn1.esetstatic.com/ESET/US/resources/white-papers/ESET_Trends_Report_2018_final.pdf, accessed November 2018.
[356] https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_21.pdf, accessed November 2018.
[357] https://ieeexplore.ieee.org/document/8316392, accessed November 2018.
[358] https://inform.tmforum.org/research-reports/revenue-management-monetize-current-future-services/, accessed November 2018.
[359] http://www.analysysmason.com/Research/Content/Comments/data-monetisation-USA-Europe-RDMY0/article-pdf/, accessed November 2018.
[360] https://infowatch.com/middle_east_report_2017-2018, accessed 2018.
[361] http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf, accessed 2018.
[362] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf, accessed November 2018.

- In H1 2018, USB sticks and other removable media accounted for 2,1% of the leaks worldwide[363].
- In Q3 2018, a 20% increase in confidential data leaks compared with Q3 2017[364].
- Average total cost of data disclosure is US $3,86 million, which is a 6,4% increase[365].
- If data disclosure were to continue at the levels of 2015, fines to be paid to the European Regulators (according to GDPR) could see a 90-fold increase, from £1.4bn in 2015 to £122bn[366].
- The total amount of business data being stored is estimated to double every 12 to 18 months. Hence, the potential data exfiltration is increasing accordingly[366].
- While the forensic costs are often less when data is unintentionally disclosed, the cost to insurers can still be substantial due to the high notification and credit monitoring costs[366].
- Internal actors are 29% of those who are involved in data disclosures. In detail, 26% of the internal actors are system administrators, 22% are end-users, 12% are doctors or nurses and 22% are others[367].
- 16% of any data disclosure is due to miscellaneous errors, 13% due to privilege misuse and 7% due to lost or stolen assets[367].

*The overall trend of **information leakage** in 2018 is **INCREASING**.*

3.11.4 Top data leaks incidents

- In January, information collected by the mobile fitness tracking and sharing app Strava has highlighted the locations of secret Russia, UK, and US military bases in Syria and Afghanistan. The personal fitness tracker Fitbit, linked to the user's Strava accounts revealed the information[368].
- The marketing and data aggregation firm Exactis left about 340 million records exposed on a publicly accessible server. The trove didn't include Social Security numbers or credit card numbers, but it comprised 2 terabytes of very personal information about hundreds of millions of adults[369].
- At the beginning of May, Twitter disclosed that it had been unintentionally storing some user passwords in plaintext in an internal log. The company fixed the problem, but it wouldn't say for how long the passwords were exposed[370].
- In July, the Domain Factory, a German hosting provider, experienced a data disclosure for the full set of its customers. A former employee exploited a system's vulnerability under the assumption that the

---

363 https://infowatch.com/analytics/leaks_monitoring/100874, accessed November 2018.
364 https://infowatch.com/analytics/leaks_monitoring/100875, accessed November 2018.
365 https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf, accessed November 2018.
366 https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf, accessed November 2018.
367 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf, accessed November 2018.
368 http://nymag.com/intelligencer/2018/01/fitness-data-map-reveals-information-about-secret-bases.html, accessed November 2018.
369 https://www.wired.com/story/exactis-database-leak-340-million-records/, accessed November 2018.
370 https://www.wired.com/story/change-your-twitter-password-right-now/, accessed November 2018.

company owed him money. Data revealed include names, phone numbers, bank names and account numbers (i.e., IBAN and BIC)[371].

- In late summer, a Chinese hotel chain exposed the data of ca. 130 million customers including the information about names, phone numbers, email addresses, bank account numbers, and booking details [364].
- In September, a security researcher found an exposed database containing customer records of Veeam, a Swiss vendor of data backup recovery, and virtual infrastructure monitoring software. The database was not password-protected, constituting an easy target for any malicious actor. The compromised details included ca. 400 million email addresses and other records collected/created over a period of four years between 2013 and 2017 [364].
- Sungy Mobile Ltd., one of the world's leading mobile application developers, leaked the details on ca. 50 million consumers due to a misconfigured backup database[364].
- In mid-November, Google faced a significant incident from a routing protocol hijack which resulted in the interception of network traffic and, thus, in an information leakage (i.e., Border Gateway Protocol leak). In detail, the incident affected a Nigerian ISP (MainOne Inc.), peering at IXPN (Internet Exchange Point of Nigeria) in Lagos where Google and China Telecom are also members. The incident occurred when 212 network addresses, which aggregated more than 500 BGP announcements, were erroneously rerouted over the Russian ISP TransTelecom, to China Telecom, toward the Nigerian ISP Main One[372,373].

3.11.5 Specific attack vectors

The primary attack vector in information leakage is insiders. This term is often used to describe a person with interest to exfiltrate important information on behalf of a third-party entity. Other common attack vectors used by this threat are misconfigurations, vulnerabilities, and human errors. For more information on attack vectors, please see chapter 5 in this report.

3.11.6 Specific mitigation actions

The mitigation vector for this threat contains the following elements:

- Anonymise, pseudonymise, minimise and encrypt data according to the provisions of the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act[374,375]. Always check the regulation commitments for counterpart entities who do not come under bi- or multilateral initiatives[376,377,378].
- Store data only on secure IT assets[379].

---

[371] https://www.trendmicro.com/vinfo/in/security/news/cyber-attacks/check-your-accounts-timehop-macy-s-bloomingdale-s-domain-factory-announce-breach, accessed November 2018.
[372] https://www.internetsociety.org/blog/2018/11/route-leak-caused-a-major-google-outage//, accessed November 2018.
[373] https://www.wired.com/story/google-internet-traffic-china-russia-rerouted//, accessed November 2018.
[374] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679, accessed November 2018.
[375] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375, accessed November 2018.
[376] https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal, accessed November 2018.
[377] https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/, accessed November 2018.
[378] https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article, accessed November 2018.
[379] https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company, accessed November 2018.

- Limit user access privileges under the need-to-know principle[379,380].
- Educate and train the organisation's personnel periodically[379,381].
- Revoke access privileges to anyone who is not an employee[379].
- Utilise technology tools to avoid possible data leakages, such as vulnerability scans, malware scans and data loss prevention (DLP) tools. Deploy data and portable systems and devices encryption, and secure gateways[380,382].

3.11.7 Kill Chain

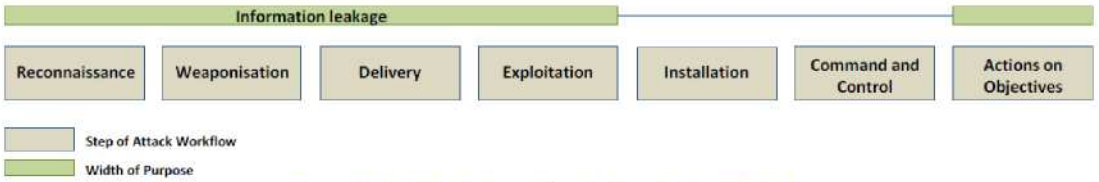


Figure 30: Position information leakage in the kill-chain

3.11.8 Authoritative references

"Trends 2018: The cost of our connected world", ESET[355]; "Data Threat Report", Thales, Cisco; "Internet Threat Report - Volume 23", Symantec[362]; "Top Leaks in Q3 2018", InfoWatch[364]; "Cost of a Data Breach Study: Global Overview", Ponemon Institute/IBM[365]; "Data Breach Investigations Report", Verizon[367]; "Annual Cybersecurity Report", Cisco[381]; "Cybercrime tactics and techniques: Q2 2018", Malwarebytes Labs[382].

[380] https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/, accessed November 2018.
[381] https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2, accessed November 2018.
[382] https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf, accessed November 2018.

3.12 Identity Theft

3.12.1 Description of the cyberthreat

Identity theft is the fraud committed from the theft of personal identifiable information strengthened by the massive digitisation of people's personal data which most of the times, include information related to their legal and civil substance[383]. Nowadays, bank accounts, home addresses, accounting records, health records and a slew of other personal information stored in own devices or organization's/companies' databases and, they are, thus, vulnerable to cybercriminal activity.

Identity theft is a procedure rather than an isolated incident; the attackers need several elements of personal information to accurately "build" a full profile of a particular person. Thus, identity theft associated with various types of data such as health records, personal web accounts, bank account information, personal information, and information of contacts. If this information "bits and pieces" is not enough for a complete profile, the data is exchanged between attackers via the Dark Web[384] , so that the identity theft may be complete in the future.

The identity theft threat is strongly associated with data breaches in companies or organisations across all industry sectors (Figure 31)[385]. Data breach attacks are in most cases targeting the company's customer records. The information leaked through these attacks may be sufficient for the next step, which is the identity fraud. Since the average number of records breached in 2018 has increased by 2,2%[386], it is safe to conclude that the identity theft trend is also increasing in the reporting period.

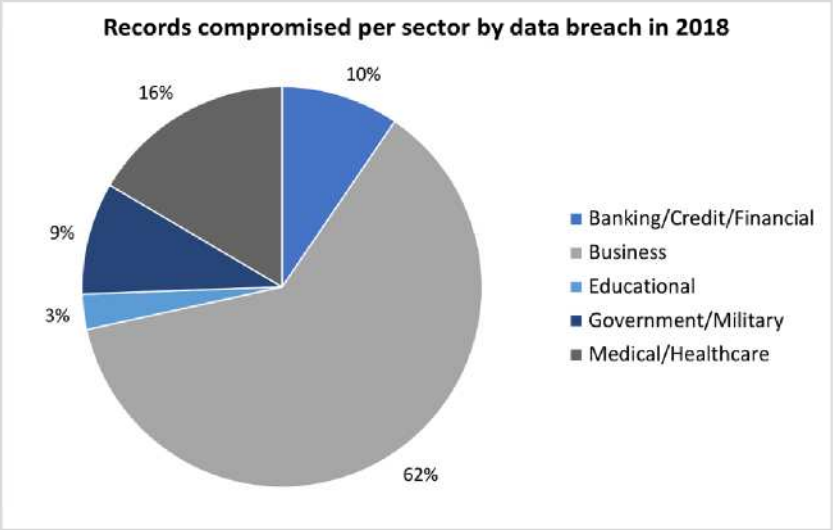


Figure 31: Records compromised by data breach in 2018, per sector[387]

[383] https://www.splunk.com/pdfs/ebooks/a-guide-to-fraud-in-the-real-world.pdf, accessed November 2018.
[384] http://www.thecommentator.com/article/6849/nhs_trusts_misplace_10_000_patient_records_in_major_security_breach, accessed November 2018.
[385] https://www.idtheftcenter.org/images/breach/2018/ITRCBreachStatsReportSummary2018.pdf, accessed November 2018.
[386] https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf, accessed November 2018.
[387] https://www.idtheftcenter.org/images/breach/2018/ITRCBreachStatsReportSummary2018.pdf, accessed November 2018.

3.12.2 Interesting points

The interesting points for this threat in the reporting period are as follows:

- **GDPR to the rescue**[388]**.** In May 2018, the General Data Protection Regulation (GDPR) was introduced for all European Union's public and private companies and organisations. The GDPR defines the rules and requirements for regulators or processors to set personal data protection policies at the Member States level and the failure of compliance may cost up to 4% of the annual company's turnover in penalties. Some of the policy elements include data encryption and the dual-factor authentication. Additionally, the GDPR dictates a formal report of any data breach of the company's assets to the regional Data Protection Agency (DPA). The basic points of the GDPR are the following:
  - Describes the frame for handling EU residents' data.
  - Enforces resident's consent regarding data collection and use.
  - Defines the types of personal data that can be stored and used by the company/organisation.
  - Enforces the use of open file formats for data transferring.
  - Allows individuals to delete or rectify their data.
  - Requires a 'liaison' officer for the collaboration between the company/organisation and the DPA.
  - Enforces the formal reporting of breaches within a few days of the event.
- **Legitimate software extensions used in campaigns.** In May 2018, the Unimania campaign[389] was revealed. It has been noticed that via popular Chrome extensions' such as the Video Downloader for Facebook (ca. 170.000 users), the PDF Merge (ca. 125.000 users) and others installed on this browser, collected personal information based on user's behaviour (i.e. posts, tweets, YouTube videos watched, user IDs and location data). These extensions, developed with attention to detail, included an End-User License Agreement (EULA). Although the developer is still unknown and more importantly, who was the recipient of the intercepted information, the EULA mentioned the company name Unimania, Inc. located in Tel-Aviv, Israel. An estimate indicates that more than 420.000 users may have been affected by this incident.

  In July 2018, the Big Star Labs campaign[390] was also revealed. The Big Stars Labs was not distributed only via Chrome but also via other legitimate software extensions, such as the Block Site (Android application and Firefox extension with ca. 100.000 users each, Chrome extension with ca. 1,4 million users), the AdBlockPrime and several more Android and iOS applications, Chrome and Firefox extensions. The Big Star Labs campaign may have infected more than ca. 11 million users, 26 times more users than the ones affected by Unimania.

  As in the case of Unimania, also in the Big Star Labs campaign, it was not clear who were the targets. However, certain parts of the embedded code pointed out the involvement of an Israel-based web analytics company.
- **Open government has exposed citizens data.** In September 2018, the US based news channel CNN reported the exposure of people's personal details (i.e. social security numbers, citizenship status, criminal records) by the public portal FOIA.gov. The Freedom of Information Act (FOIA) portal of the US Environmental Protection Agency, operating as an intermediate between citizens and

[388] https://www.pandasecurity.com/mediacenter/src/uploads/2017/11/PandaLabs_Annual_Report_2017.pdf, accessed November 2018.
[389] https://adguard.com/en/blog/unimania-spyware-campaign/, accessed November 2018.
[390] https://adguard.com/en/blog/big-star-labs-spyware/, accessed November 2018.

governmental agencies, processes personal information from applicants. A flaw on the FOIA.gov complex of servers allowed unauthorized searches on FOIA's records, without neither the agency's nor the applicant's permission. CNN alerted the US Environmental Protection Agency, which then fixed the issue and stopped the exposure. A similar situation took place in August 2016, when the Kennesaw State University, authorized to support the elections, exposed voters' registration data.

The USA is not the only country that faced this type of incident in 2018. In March 2018, a software flaw in a third-party site for the Canadian government leaked ca. 7.000 documents and in August, the UK government exposed data found by Google. In the same month, more than ca. 2,3 million Mexican healthcare records were exposed due to a database misconfiguration[391].

3.12.3 Trends and main statistics

- 10% of the UK healthcare organisations have been breached more than 10 times in the last year[392].
- 3% of the T-mobile customers' records (2,3 million individuals) were breached in August 2018[393]. The customers' personal information, such as name, billing address, and account number were stolen.
- The cost of fraud for 2018 only for the USA is estimated to exceed US $7.4 billion, a 32% growth of the recorded US $5.6 billion cost in 2016[383].
- 38% of the organisations have cloud user accounts that were compromised[394].
- More than five employee identities where spoofed in each case of the 57% of the targeted companies (10% more companies than the year before)[395].
- 30% more phishing links were detected in social media[396].
- 141% increase in North America, 22% decrease in Europe and 36% decrease in Asia, in compromised credentials[397].
- LokiPWS distribution increased by more than 300% in 2018[397].
- 28% more self-reported data breaches were recorded in 2017-2018 compared to the previous year, as a result of GDPR reporting commitment[398,386].

*The overall trend of **identity theft** in 2018 is **INCREASING**.*

[391] https://nakedsecurity.sophos.com/2018/09/06/social-security-numbers-exposed-on-us-government-transparency-site/, accessed November 2018.
[392] https://www.carbonblack.com/uk-threat-report-2018/, accessed November 2018.
[393] https://www.securityweek.com/t-mobile-data-breach-hits-over-2-million-customers, accessed November 2018.
[394] https://www.ixiacom.com/system/files/private/2018-05/Ixia-S-RP-2018-Security-Report.pdf, accessed November 2018.
[395] https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q118-quarterly-threat-report.pdf, accessed November 2018.
[396] https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q218-quarterly-threat-report.pdf, accessed November 2018.
[397] https://www.blueliv.com/blog-news/credential-theft/credential-theft-industry/, accessed November 2018.
[398] https://www.itproportal.com/news/human-error-top-cause-of-self-reported-data-breaches/, accessed November 2018.

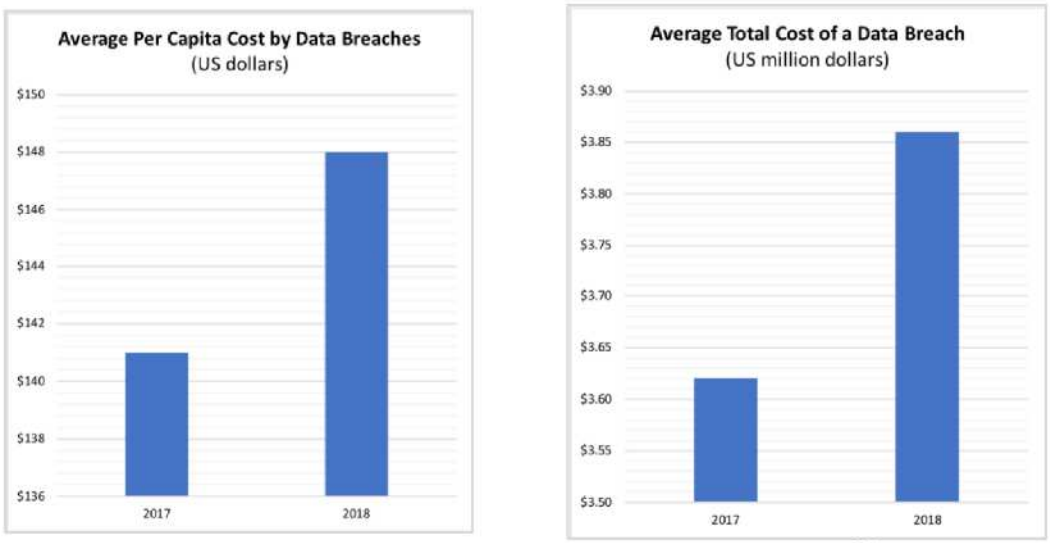


Figure 32: The cost as an indicator for the trend of data breaches in 2018[399]

3.12.4 Top identity theft threats

- **Skimmers**. An identity theft method where fraudsters place devices (known as skimmers) over card readers at registers checkout, gas stations or ATMs. Skimmers store credit and debit card information so fraudsters can use this data to make counterfeit cards, use them for online purchases or sell them on the black market[400].
- **Dumpster divers**. Fraudsters dig through trash or mailboxes, looking for bank statements, copies of tax returns and other documents that have personal information[401].
- **Telephone impersonators**. Fraudsters may contact a bank's call center many times, each time gaining a different piece of information until they have enough information to impersonate an actual bank customer and gain account access[402].
- **Network administrator impersonators**. A new form of identity theft targeting network administrators' accounts, is performed by attackers in an attempt to circumvent mitigation tools and policies and access the company's database. By the use of legitimate network tools, such as applications for remote access or remote back-ups, the attacker was able to steal the administrator's identity and operate as the legitimate administrator within the company's network. This style of attacking, namely the malwareless attacks, exceeded 49% of this year's data breach incidents. [388].
- **Phishers and spear-phishers**. Phishers use authentic-looking emails and websites to trick users to click on a link or open an attachment that will download malware onto their computers and leave confidential information vulnerable[403]. In a targeted phishing attack (spear-phishing), the attacker is

[399] https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf, accessed November 2018.
[400] https://krebsonsecurity.com/category/all-about-skimmers/, accessed November 2018.
[401] https://www.social-engineer.com/vigilant-dumpster-diving-attack/, accessed November 2018.
[402] https://www.sfpcu.org/blog/blog-detail/sfpcu-blog/2018/01/13/phone-scams-to-watch-for-in-2018, accessed November 2018.
[403] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing, accessed November 2018.

not interested in just stealing personal information, but also on taking over the control of the computer or the network that the computer is connected.

3.12.5 Specific attack vectors

- **The cloud as an attack interface for customers' data.** Although companies and organizations are accountable for the safekeeping of customers' personal information, a gap is revealed since most of the times, a part of the company's digital assets are stored in cloud services or virtual machines.
- In the case of cloud computing, the company would face financial and legal consequences even in cloud provider's data breaches. Most providers have security policies and tools, but, still, the company that hosts its digital assets in a provider's infrastructure has no control over them. It has been reported that 73% of the cloud providers had misconfigurations in their security policies that could lead to a data breach[394].
- Moreover, attacks on the cloud infrastructure are highly profitable, therefore attractive to hackers and cyber criminals, making them extremely likely.

- **Phishing tools.** The group of cyber criminals mostly focused on the theft of identity's information is the phishers. Some of the main tactics[404] that were used by phishers to intercept user credentials were:
  - ***Domain squatting***. Fraudulent domains that are similar to a valid one, for example, 0racle[dot]com.
  - ***Domain shadowing***. Fraudulent subdomains hidden in a valid domain, for example, shadow[dot]oracle[dot]com.
  - ***Malicious domains***. Domains that lure users to register and via the registration intercept personal information.
  - ***URL shorteners***. A shortened URL is used to hide the domain. Shorteners are used by valid domains, for example goo[dot]gl and the users are familiarized with this trend. This assists the phishers to pass their shorteners as valid.
  - ***Subdomain services***. A malicious site in a valid domain server, for example malicious[dot]blogspot[dot]com.

  These URLs are either intercepting random visitors or are sent via email to lure specific individuals or groups of users. For more information about phishing and spear-fishing, please refer to section 3.6.

- **W2 scam.** The W2 scam is another attack aiming at companies' records to access sensitive information. The scam starts by spoofing an executive member of finance or HR department for employees' records. These records are then used for identity theft. The scam is named after the US W2 tax form used to report employee's wages. This social engineering scam, although old (first reported in 2016 by IRS), is resurfacing with an increase of 10% more incidents than last year[395].
- **Email fraud.** In this type of attack (also known as Business Email Compromise or BEC) the sender of the email impersonates an executive member of the company or a partner organization and asks for sensitive information. It is just a query-mail, which makes it harder to detect in advance or prevent it. However, the attackers tend to use specific keywords on the mail's subject that gives a hint of the type of information they are after. The most common keywords are 'Payment', 'Request', 'Urgent', and 'FYI'. The companies and organisations that are mostly targeted by BEC are retail, healthcare and government organisations[396].

[404] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf, accessed November 2018.

- **LokiPWS.** Although LokiPWS (also known as Loki Bot) is a malware, it is also used as a password stealer. This technique also applies to other malware such as Pony, Emotet, KeyBase and AZORult[397]. For more information about the use of malware for identity theft, please refer to the section 3.1.
- **Software and hardware vulnerabilities.** Hard- software vulnerabilities may leave the user's data exposed. Some of the vulnerabilities recorded in 2018, which were associated with identity theft, are the CVE-2018-14787 of Philips IntelliSpace Cardiovascular (ISCV) devices that allowed interception of the patient's medical information[405], the CVE-2018-11776 of Apache Struts software and the CVE-2018-7445 of MicroTik RouterOS that both allowed remote code execution and several exploits have been used[406,407].

3.12.6 Specific mitigation actions

- Sensitive information such as patient records should not be stored in handwritten notes to prevent loss or misplacement[384]. It is better to give digital files a small lifespan and then to destroy them effectively.
- Apply 'threat hunting' within a company to strengthen the security plans. Threat hunting[392] is conducted by skilled members of the Security Operation Centre (SoC) team to proactively identify vulnerabilities and prevent breaches.
- Introduce policies such as velocity-based rules to mitigate identity fraud, especially for payment card transactions[383]. The machine data of valid transactions can provide sufficient information for the optimal policy definition.
- Implement Single Sign-On (SSO) authentication methods, when available, allowing a user to access several applications with the same set of digital credentials. It is highly recommended to minimize the number of user's accounts and the stored credentials[408].
- Introduce multi-factor authentication (MFA) to overcome the password hacking or loss and ensure the authentication process with multiple keys. The adaptive MFA optimizes the authentication process based on user's behaviour and context[408].
- Produce compulsory checks to URLs that are sent via email or randomly visited, before any further step is taken[404]. Checks based on IP address, the ASN that associates with the IP, the owner of the domain and the relation between this domain and others.
- Organizations that are adopting cloud services should have strong cloud security operations and prefer an architecture of on-premises storages, private cloud storages and public cloud storages simultaneously to protect their customer's personal information[394].
- Implement the use of strong and updated encryption methods for sensitive data such as TLS 1.3 (uses ephemeral keys), to prevent hacking[394].
- Adequately protect all identity documents and copies (physical or digital ones) against unauthorised access.

---

[405] https://threatpost.com/philips-vulnerability-exposes-sensitive-cardiac-patient-information/136669/, accessed November 2018.
[406] https://www.nopsec.com/blog/another-year-another-critical-struts-flaw-cve-2018-11776/, accessed November 2018.
[407] https://www.cvedetails.com/cve/CVE-2018-7445/, accessed November 2018.
[408] https://www.okta.com/resources/whitepaper/identity-driven-security/, accessed November 2018.

- Identity information should not be disclosed to unsolicited recipients and their requests by phone, email or in person.
- Password protect devices, ensure good quality of credentials, and secure methods for their storage.
- Users should pay attention when using public Wi-Fi networks, as fraudsters hack or mimic them. If one is used, it should be avoided accessing sensitive applications and data. A trusted VPN service should be used when connecting to public Wi-Fi networks.
- Transactions documented by means of bank statements or received receipts should be checked regularly upon irregularities.
- Content filtering to filter out unwanted attachments, emails with malicious content, spam and unwanted network traffic should be installed.
- Install end-point protection by means of anti-virus programs but also block execution of files appropriately (e.g. block execution in Temp folder).
- Ensure good quality of credentials and secure methods for their storage.
- Use of Data Loss Prevention (DLP) solutions.

3.12.7 Kill Chain



Figure 33: Position of identity theft in the kill-chain

3.12.8 Authoritative references

'2018 Cost of a Data Breach Study', IBM[386]; 'A Guide to Fraud in the Real World', Splunk[383]; 'Cisco 2018 Annual Cybersecurity Report - Executive summary', Cisco[404]; '2018 Security Report', Ixia[394]; '2018 - Data Breach Category Summary ', ITRC[385]; 'Quarterly Threat Report 2018', Proofpoint[395,396].

3.13 Cryptojacking

3.13.1 Description of the cyberthreat

2018 can be characterized as the year of cryptojacking[409]. Cryptojacking (also known as cryptomining) is a new term that refers to the programs that use the victim's device processing power (CPU or GPU[410]) to mine cryptocurrencies without the victim's consent. This processing power is used to solve cryptographic puzzles that are recorded in the blockchain. The Cybercrime-as-a-Service sector is always innovative and looking for new ways to generate revenue[411] and to apply the "follow-the-money" principle: cyber criminals take advantage of the victims' processing power (usually 70% to 80% unused processing power[412]) to mine cryptocurrencies and earn real world money, monetized after legal exchanges and transactions.

3.13.2 Interesting points

The identified interesting points for cryptojacking threats are as follows:

- **Shift from ransomware to cryptojacking[458].** Since the fourth quarter of 2017, a clear trend for cyber criminals to move from ransomware[413] to cryptomining as the preferred way to make profit[242] has been observed. The spike in the value of Bitcoin and the fact that cryptocurrencies became a mainstream feature of society[414], encouraged cyber criminals to target cryptocurrencies (via cryptomining or stealing users' cryptocurrency) for various reasons. First, cryptojacking is simpler and more straightforward due to the low barrier for entry (e.g. a couple of source code lines is enough for a browser based cryptominer)[244]. Second, it is less risky, stable and a less disruptive way to make money while it allows cyber criminals to fly under the user radar since the latter are not prompted to make any payment and may not notice the cryptomining activity. Third, every system can potentially be a victim (including fully patched systems)[248]. Fourth, they have attracted minimal law enforcement attention[242]. Finally, monetization is easier for the cyber criminals since no intermediary and no fraud schemes are required.
- **The prevalence of anonymity cryptocurrencies.** Bitcoin became the most popular cryptocurrency[415], however, many new cryptocurrencies have been developed[416]. Most notable of alternative cryptocurrencies are Monero[417] [418], Ethereum[419] and Zcash[420] as they provide higher levels of transaction anonymity for cyber criminals compared to Bitcoin. They can also be mineable in a distributed way, which matches with the modus operandi of cyber criminals (via infected

---

[409] https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_Threat_Trends_2018_Mid-Year_Update.pdf, accessed October 2018.
[410] https://en.wikipedia.org/wiki/Graphics_processing_unit, accessed October 2018.
[411] https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html, accessed October 2018.
[412] https://securelist.com/it-threat-evolution-q1-2018/85469/, accessed October 2018.
[413] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, accessed October 2018.
[414] https://securelist.com/mining-is-the-new-black/84232/, accessed October 2018.
[415] https://bitcoin.org/en/, accessed October 2018.
[416] https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf, accessed October 2018.
[417] https://getmonero.org/, accessed October 2018.
[418] https://www-cdn.webroot.com/6515/2168/8585/Webroot_2018_Threat_Report_US.pdf, accessed October 2018.
[419] https://www.ethereum.org/, accessed October 2018.
[420] https://z.cash/, accessed October 2018.

machines/bots)[421]. Monero has been by far the most preferred cryptocurrency as it has much lower "difficulty rate" for mining compared to Bitcoin[422]. XMRig[423] open source Monero mining software has been one of the most popular mining programs used by cyber criminals[455]. Finally, Monero miners have also been leveraged by advanced threat groups like Lazarus[424] and Iron Tiger[425].

- **The economics of cryptojacking.** During the first half of 2018, it was estimated that cryptominers have monetized for their users more than US $2.5 billion[455]. Smominru mining botnet that has infected more than 500.000 Windows machines has already mined Monero, valued between US $2.8M and US $3.6M[426]. It was estimated that an adversary controlling 2.000 victim computer systems with Monero miners could generate US $500 per day or US $182.500 per year[427].
- **Cryptocurrencies' market price and cryptojacking detections correlation.** During the past 12 months, it has been observed that the trend in cryptominers closely follows the money flow and valuation of cryptocurrency market prices[428]. The figure below presents a positive correlation between Bitcoin's market price and the detections of cryptojacking malware. One can assess (with moderate confidence) that a potential big increase or decrease in the cryptocurrencies' market price could directly influence the numbers of cryptominer detections[428].

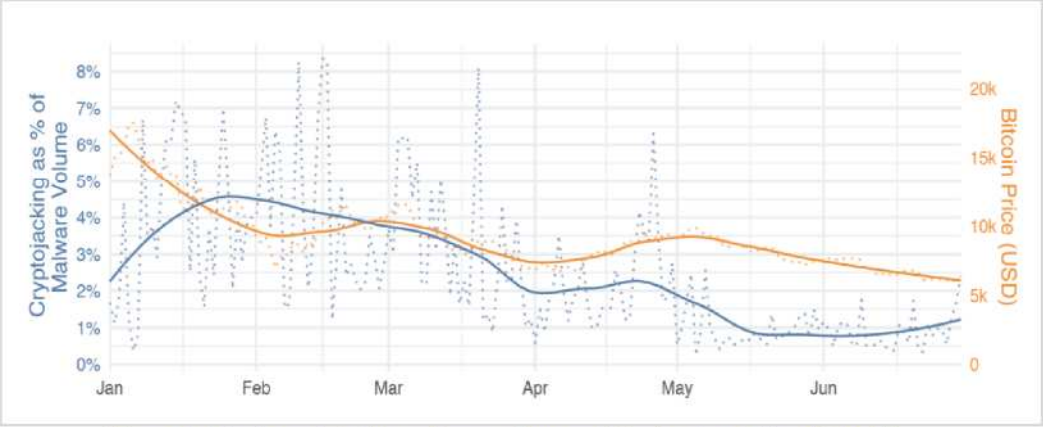


Figure 34: Bitcoin cryptojacking malware volume and Bitcoin price during 1H2018 [429]

[421] https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf, accessed October 2018.
[422] https://www.accenture.com/t20180803T064557Z__w__/hu-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf, accessed October 2018.
[423] https://github.com/xmrig/xmrig, accessed October 2018.
[424] https://www.alienvault.com/blogs/labs-research/a-north-korean-monero-cryptocurrency-miner, accessed October 2018.
[425] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/, accessed October 2018.
[426] https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators, accessed October 2018.
[427] https://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, accessed October 2018.
[428] https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf, accessed October 2018.
[429] https://www.fortinet.com/demand/gated/q2-2018-threat-landscape-report.html, accessed October 2018.

- **Drive-by cryptomining.** Cryptomining can be browser-based using technologies such as JavaScript[430] and WebAssembly[431] (a newer browser technology that is faster and more efficient than JavaScript). Since Coinhive[432] released its JavaScript based technologies in September 2017, it has been injected into thousands of websites[455] by cyber criminals and website administrators (usually this happens via 3rd party websites[435]). It is reported that 2,2% of the top 100 Alexa[433] websites have been found to use cryptomining scripts[242]. Coinhive is also marketed as an alternative way for websites to make revenue instead of using ads[248]. It is understood that many Coinhive copycats have emerged due to Coinhive's success[416]. Finally, a major advance in web-based cryptomining is a new technique for persistent mining that maintains the process running even after the browser window is closed[434].
- **Cryptomining capabilities in existing trojans and botnets.** During the reporting period, we have observed existing trojans and botnets to incorporate cryptomining capabilities[435]. Examples of such trend include TrickBot[436], Dridex[435], Neutrino[437] and CodeFork/Gamarue[438]. Malware authors can effortlessly and quickly push these cryptomining capabilities into their existing malware in order to make more profit.
- **Cryptojacking hits cloud's high-powered resources.** Cryptojacking is one of the major issues found in cloud environments as 25% of organisations have been affected[439]. The recent incident with cryptojacking activity in the cloud environments of Telsa[440], Aviva, Gemalto[441] and LA Times[442] are indicative of the trend. Moreover, cloud threats also include cryptomining via Docker and Kubernetes[443] as well as hacked serverless functions[444].
- **Cryptojacking goes mobile.** Although mobile devices do not have the processing power of PCs, cryptomining is an emerging threat with overall growth for mobile devices[458]. Cryptominers have

[430] https://www.bleepingcomputer.com/news/security/coinhive-is-rapidly-becoming-a-favorite-tool-among-malware-devs/, accessed October 2018.
[431] https://www.forcepoint.com/blog/security-labs/browser-mining-coinhive-and-webassembly, accessed October 2018.
[432] https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/, accessed October 2018.
[433] https://www.alexa.com/topsites, accessed October 2018.
[434] https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/, accessed October 2018.
[435] https://www.fireeye.com/blog/threat-research/2018/07/cryptocurrencies-cyber-crime-growth-of-miners.html, accessed October 2018.
[436] https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/, accessed October 2018.
[437] https://www.securityweek.com/jimmy-banking-trojan-reuses-nukebot-code, accessed October 2018.
[438] https://www.bleepingcomputer.com/news/security/codefork-group-uses-fileless-malware-to-deploy-monero-miners/, accessed October 2018.
[439] https://info.redlock.io/cloud-security-Trends-may2018, accessed October 2018.
[440] https://redlock.io/blog/cryptojacking-tesla, accessed October 2018.
[441] https://info.redlock.io/hubfs/WebsiteResources/RL_Cloud_Security_Trends_Oct_2107.pdf, accessed October 2018.
[442] https://www.theregister.co.uk/2018/02/22/la_times_amazon_aws_s3/, accessed October 2018.
[443] https://www.bleepingcomputer.com/news/security/coinminer-campaigns-move-to-the-cloud-via-docker-kubernetes/, accessed October 2018.
[444] https://www.theregister.co.uk/2018/06/05/serverless_functions_crypto_mining/, accessed October 2018.

managed to enter Google Play[445] and Apple's App Store[446] and thus subsequently banned by Google[447] and Apple[448]. During the reporting period, we have observed malicious multi-featured mobile apps[449] (having capabilities from DDoS, adware, banking trojan to cryptomining) that can brick mobile devices[450].

- **Cryptojacking in critical infrastructure.** In February 2018, the first incident of cryptomining malware that was found in SCADA systems of a water utility[451], connected to the Internet has been reported. This incident was not unique as the numbers in the figure below present. Moreover, this worrying overall trend for critical infrastructure can have impact on the stability and responsiveness of the operations of such systems[452].



Figure 35: Share of ICS computers attacked by cryptomining malware[452]

- **Cryptojacking and law enforcement.** Cryptojacking activity has attracted limited law enforcement attention since the beginning of the reporting period[242]. This comes as a result of the questionable legality of this activity (browser cryptomining is not illegal), the limited reporting of such crimes as well as due to the fact the victim's damages are hard to quantify and investigate[242]. It is expected that more cases of illegal cryptomining will reach to law enforcement this year, given the prevalence and exploitation of this threat[453].

---

[445] https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/, accessed October 2018.
[446] https://9to5mac.com/2018/03/13/crypto-mining-calendar-app-ios/, accessed October 2018.
[447] https://www.bbc.com/news/technology-44980936, accessed October 2018.
[448] https://mashable.com/2018/06/11/apple-bans-cryptocurrency-mining-apps/, accessed October 2018.
[449] https://www.kaspersky.com/about/press-releases/2017_new-multi-featured-mobile-trojan-loapi-discovered, accessed October 2018.
[450] https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-hiddenminer-android-malware-can-potentially-cause-device-failure/, accessed October 2018.
[451] https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility/, accessed October 2018.
[452] https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/, accessed October 2018.
[453] https://cointelegraph.com/news/cases-of-illegal-bitcoin-and-cryptocurrency-mining-chicken-farms-and-new-york, accessed October 2018.

3.13.3 Trends and main statistics

- During the 1st quarter of 2018, cryptojacking malware grew 629%[244] (from 400.000 samples in the fourth quarter of 2017 to 2,9 million samples in the first quarter of 2018)[248].
- Cryptocurrency mining continues to rise as one can observe from the figure below:

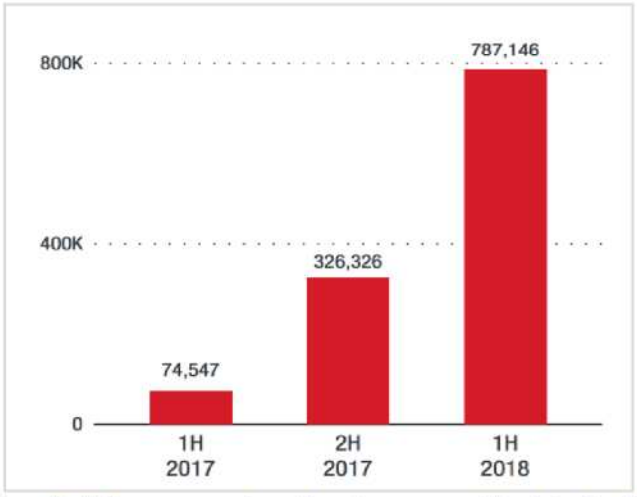


Figure 36: Half-year comparison of cryptocurrency mining detections[339]

- The distribution of cryptominers by operating system during 2017 was as follows: Windows miners (55,44%), browser miners (44,13%), Linux miners (0,25%), Android miners (0,15%) and macOS miners (0,03%)[454]. During the first quarter of 2018 the distribution of cryptominers by operating systems was: Windows miners (84,69%), browser miners (15,06%), Android miners (0,17%), Linux miners (0,07%) and macOS miners (0,01%)[454]. The above numbers show that Windows is the cryptomining platform of choice for cyber criminals.
- During the first half of 2018, cryptominers have affected 42% of organisations globally compared to 20,5% at the end of 2017[455].
- It is estimated that Bitcoin cryptomining consumes globally per year the same amount of energy as to Switzerland's total annual energy consumption[456,457].
- The amount of cryptocurrency mining is also dependent on the number of cryptojacking victims. From April 2017 to March 2018, the number of these victims were ca. 400.000 to 600.000 per month[458].

---

[454] https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2017-2018.pdf, accessed October 2018.
[455] https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf, accessed October 2018.
[456] https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/, accessed October 2018.
[457] https://digiconomist.net/bitcoin-energy-consumption, accessed October 2018.
[458] https://media.kaspersky contenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf, accessed October 2018.

- An increase in cryptominer detections has been observed on Mac computers, mostly on consumer hardware. 60% of the detections mentioned above, during 2017, have been attributed to JS.Webcoinminer variants[248].
- On the Dark Web one can purchase a cryptomining toolkit with just US $30[248].
- The rise of "insider miners" is something that is expected to come as we see more and more examples of employees using their organisations (super) computers for their own profit[459].

*The overall trend for **cryptojacking** attacks in 2018 is **INCREASING**.*

3.13.4 Top 5 cryptojacking threats

During the first half of 2018 the top cryptomining malware[455] globally is as follows:

- Coinhive[432] (30%),
- Cryptoloot[460] (23%),
- Jsecoin[461] (17%),
- XMRig[423] (7%) and
- Authedmine[462] (6%).

It is interesting to see that apart from XMRig, that is file-based cryptominer, all the others are browser-based.

3.13.5 Specific attack vectors

Cyber criminals have used the following techniques to deliver cryptominers:

- by incorporating cryptojacking capabilities in existing malware[435] and botnets[463] [464];
- via drive-by cryptomining[465] and compromised websites[248];
- via browser extensions[466];
- via spam[467].

---

[459] http://fortune.com/2018/02/09/russia-arrests-nuclear-scientists-bitcoin/, accessed October 2018.
[460] https://bitcoinexchangeguide.com/crypto-loot/, accessed October 2018.
[461] https://jsecoin.com/en/home/, accessed October 2018.
[462] https://authedmine.com/, accessed October 2018.
[463] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign, accessed October 2018.
[464] https://www.fortinet.com/demand/gated/q2-2018-threat-landscape-report.html, accessed October 2018.
[465]https://www.reddit.com/r/thepiratebay/comments/70aip7/100_cpu_on_all_8_threads_while_visiting_tpb/, accessed October 2018.
[466] https://www.bleepingcomputer.com/news/security/chrome-extension-embeds-in-browser-monero-miner-that-drains-your-cpu/, accessed October 2018.
[467] https://www.fireeye.com/blog/threat-research/2018/01/microsoft-office-vulnerabilities-used-to-distribute-zyklon-malware.html, accessed November 2018.

- via social networks[468];
- via mobile apps and app stores[469];
- via exploit kits[470];
- via ad networks and malvertising[471];
- via removeable media[472];
- via wormable cryptominers (mostly using NSA's Eternal Blue exploit)[473].

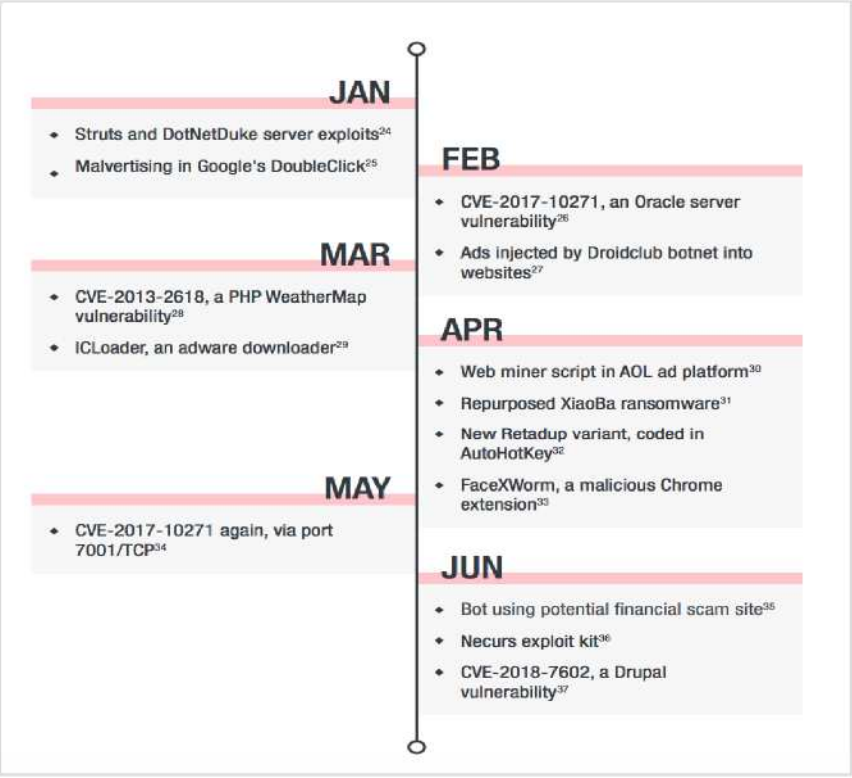


Figure 37: Different techniques used to distribute cryptominers during 1H2018[339]

The majority of the devices targeted by cyber criminals are endpoint devices (laptops/desktops), enterprise servers and cloud infrastructure, IoT devices, websites, mobile devices and ICS systems.

[468] https://blog.barkly.com/crypto-currency-mining-malware-digmine-monero, accessed October 2018.
[469] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-coinminer-and-other-malicious-cryptominers-tpna.pdf?la=en, accessed October 2018.
[470] https://www.fireeye.com/blog/threat-research/2018/06/rig-ek-delivering-monero-miner-via-propagate-injection-technique.html, accessed October 2018.
[471] https://www.bleepingcomputer.com/news/security/coinhive-cryptojacker-deployed-on-youtube-via-google-ads/, accessed October 2018.
[472] https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/, accessed October 2018.
[473] https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/, accessed October 2018.

3.13.6 Specific mitigation actions

- Implement content filtering to screen out unwanted attachments, emails with malicious content and spam.
- From a network perspective, organisations should implement filtering of the Stratum mining protocol as well as blacklisting the IP addresses and domains of popular mining pools[435].
- Install end-point protection by means of anti-virus programs but also blocking execution of files (e.g. block execution in Temp folder).
- Conduct regular security audits on corporate networks looking for anomalies.
- Implement robust vulnerability and patch management.
- Use whitelisting to prevent unknown executables from being executed at the end-points.
- Invest in user awareness especially with regard to secure browsing behaviour.
- Identify your external exposure; Internet connected systems should have proper access control for management ports, should be fully patched and continuously monitored for abuse/misuse.
- Less obvious targets, such as queue management systems, POS terminals, and even vending machines can be hijacked to mine cryptocurrencies. Make sure they are patched at least against Eternal Blue exploit.
- Implement process monitoring and blacklisting of common cryptomining executables.

3.13.7 Kill Chain

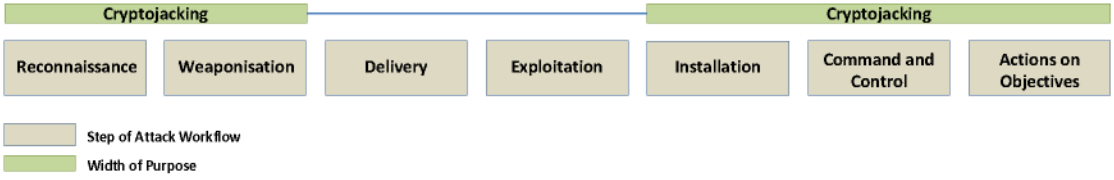


Figure 38 - Position of cryptojacking in the kill-chain

3.13.8 Authoritative references

"Internet Security Threat Report 23", Symantec; "Threats Report March 2018", McAfee; "Threats Report June 2018", McAfee; "Ransomware and malicious cryptominers 2016-2018", Kaspersky; "Cyber Attack Trends 2018 Mid-Year Report", Checkpoint; "IT Threat Evolution Q1 2018 ", Kaspersky; "Cyber Security Assessment Netherlands 2018", NCSC-NL; "Internet Organised Crime Threat Assessment (IOCTA) 2018", Europol; "2018 Mid-Year Security Roundup"; Trend Micro

3.14 Ransomware

3.14.1 Description of the cybe-threat

Ransomware attacks have been committed against a vast variety of organisations every year by financially motivated attackers for more than a decade[474]. The ransomware attacker gains ownership of files and/or various devices and blocks the real owner from accessing them. To return the ownership the attacker demands a ransom in cryptocurrency[475].

Ransomware attacks are nowadays evolving from stand-alone to cyber-adversary campaigns. This morphing is mostly due to the level of sophistication of attackers, often elevated by leaked or stolen classified tools developed by government agencies[476]. The victims of these attacks not only suffer certain financial losses, but they also lose their credibility. This motivates the existence of an accurate and updated prediction and prevention plan within every organization.

According to several security researchers groups, there has been a decrease in ransomware incidents this year, while an increase in cryptocurrency mining attacks has been observed[475]. In cryptocurrency mining, the attacker is more focused on assuming the control of the machine's computational power and producing currency units indefinitely, than being paid a ransom amount once. For more information about cryptojacking, please consult chapter 3.13.

Even though the ransomware landscape is changing, many sectors still suffer from these attacks. For example, over than 85% of the malware targeting medical devices in 2018 was ransomware[477]. Additionally, 973 out of a total of 30.362 security breach incidents (3,2%) in all sectors was due to ransomware[478]. This keeps ransomware as a threat that cannot be ignored.

3.14.2 Interesting points

The identified interesting points for ransomware are as follows:

- **From ransomware to cryptojacking**. In early 2018, a trend towards cryptojacking rather than ransomware attacks has been observed. In cryptojacking, the intruders invade a computer in a way similar to ransomware, but instead of demanding a ransom, they install malicious software to start cryptocurrency mining without the computer owner's noticing. The first indication was that, although the coin mining software (coin miners) known samples were approximately 400.000 in Q4 2017, they grew to more than 2,9 million in Q1 2018. Only in the first half (H1) of 2018, the cryptocurrency mining detections increased by 96% compared to the total detections recorded in 2017[479]. Cryptojacking is simpler and less risky for the attackers who begin to monetise on the victim's system without any delay or without risking the victim's denial. In Q1 2018, Lazarus, an international

---

[474] https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/white-papers/RansomwarePreventionIsPossible.pdf, accessed November 2018.
[475] https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf, accessed November 2018.
[476] https://www.dimensiondata.com/insights/-/media/dd/corporate/pdfs/gtir-executive-guide-2018.pdf, accessed November 2018.
[477] https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/white-papers/MedicalTechDeviceWhitePaper.pdf, accessed November 2018.
[478] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf, accessed November 2018.
[479] https://www.helpnetsecurity.com/2018/08/29/cybercrime-tools-tactics-procedures/, accessed November 2018.

cybercrime group responsible for several ransomware attacks since 2016, deployed a cryptocurrency scheme called HaoBao[480].

- **Ransomed medical devices**: **an ongoing threat.** As predicted in the past[478], this year more than 85% of all the malware that affected healthcare organizations was ransomware. Unfortunately, the healthcare sector provides an easy target to attackers due to the usual lack of integration between IT policies and the core hospital operations. Additionally, the nature of such organisations in many cases forces them to give in to ransom demands, putting a swift end to the attack. These reasons make the healthcare organisations appealing to ransomware attackers.
- **Ransomware 'DIY' is now available for everyone**. In most ransomware attacks, such as Cerber[481], the use of Remote Desktop Protocol (RDP) as a backdoor allows the attacker to gain access to the victim's computer. The sophistication of the criminal community on the use of RDP has reached a point that criminals develop a 'ransomware interface' named WYSIWYE[482]. This interface allows users to select a network computer to attack, a specific set of folders in a computer to lock, any email address to contact or hack within the network, etc. Thus, it also allows someone to become a ransomware criminal with minimum technical skills. This indicates that in the future, many more people with considerably less sophistication will unleash ransomware attacks.
- **The Dark Web is recycling**. Security Intelligence experts have shown that there is a trend of 'open' use of malware by multiple threat actors. Their analysis counted more than 3 million registered Dark Web users in 25 sites that are offering access to tools and information for attacks. The content shared was considered sufficient for any wannabe attacker, regardless the technical knowledge or experience. Noteworthy that, 12% of the available Dark Web material was ransomware-related. Moreover, the cost for accessing the material is extremely low. This environment allows anyone with just a small amount of money to be able to conduct attacks using already developed tools and methods[483]. This trend of "sharing" malicious tools via the Dark Web has shifted the nature of ransomware attacks from individuals to global groups of attackers. Such coordinated attacks provided the tools used to target the Ohio Police and Fire Department and the Minnesota Psychiatric in June 2018[479], where both critical and personal services were compromised.
- **Nations are getting involved**. The ransomware attack campaigns WannaCry and NotPetya, organized by nation-state actors, were initiated in 2017 and continued throughout 2018. In both cases, the main goal of the attacks was the destruction of information or just causing a distraction rather than receiving a specific ransom. This demonstrates that in nation-state attacks the recovery may not be a possibility for the victims. Although the attacks were allegedly orchestrated by a state, in many cases the actor was a malicious individual or a group - the Lazarus group delivered the WannaCry campaign organized by the North Korean state[479]. This use of ransomware may indicate a future trend where governments or regimes get actively involved in the cyberwarfare.

3.14.3 Trends and main statistics

- A 30% drop in the number of ransomware victims and 22,5% less attacks to mobile users comparing Q1 2018 and Q1 2017[475].

---

[480] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf, accessed November 2018.
[481] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport, accessed November 2018.
[482] https://www.pandasecurity.com/mediacenter/src/uploads/2018/07/Whitepaper-rasomwareEN.pdf, accessed November 2018.
[483] https://www.theregister.co.uk/2018/07/26/dark_web_cybercrime_sitrep/, accessed November 2018.

- Ransomware decreased to 2,80% of the total Q1 2018 malware attacks[475].
- 44,5% more users encountered miners in Q1 2018[475].
- Coin miners' development and use increased to 4% of the total Q1 2018 threats; was 3% in 2017[475].
- The mobile miners' use percentage over the total threat incidents increased by 9,5% in Q1 2018[475].
- The most common ransomware targets were payment card information (34%) and Personally Identifiable Information (PII) (36%)[478].
- 39% of the global malware-related data breaches were ransomware[484].
- 17% of the total UK healthcare data breaches were ransomware[485].
- 58,8% of the respondents to a security incident were using tools for ransomware prevention and 83% of them claimed that these tools were helpful[486].
- 64% of the major incidents targeting industrial control systems or networks were ransomware[487].
- 93% of phishing emails were related to ransomware[488].
- 36% of all malicious email in Europe and Japan was related to ransomware[489].
- 65% of the ransomware attacks were delivered via email and 35% via malicious URLs[489].
- Nearly 70% of the cybercrime incidents targeting educational institutions were ransomware[489].
- 5,4 billion WannaCry attacks were blocked[490].
- Although 66% of the companies agreed that ransomware is a serious danger, less than 13% of them were prepared for a ransomware attack[491].
- Roughly 1,0% of the infected endpoints were attacked by ransomware[492].
- Ransomware hit 15% of businesses in the top 10 industry sectors: education, IT/telecom, entertainment, financial services, construction, government, manufacturing, transport, healthcare and retail[493].

---

[484] https://www.techrepublic.com/article/new-blackberry-workspaces-platform-could-help-businesses-quickly-recover-from-ransomware/, accessed November 2018.
[485] https://www.carbonblack.com/wp-content/uploads/2018/09/uk-threat-report-sept-2018.pdf, accessed November 2018.
[486] https://www.dflabs.com/wp-content/uploads/2018/08/Survey_SOC-2018_DFLabs.pdf, accessed November 2018.
[487] https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf, accessed November 2018.
[488] http://www.intelligentcio.com/me/wp-content/uploads/sites/12/2018/03/Cybercrime-by-the-Numbers-Scale-Vulnerability-Infographic.pdf, accessed November 2018.
[489] https://www.proofpoint.com/sites/default/files/pfpt-us-wp-human-factor-report-2018-180425.pdf, accessed November 2018.
[490] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf, accessed November 2018.
[491] https://www.proofpoint.com/sites/default/files/pfpt-us-g-ransomware-survival-guide.pdf, accessed November 2018.
[492] https://www.darkreading.com/endpoint/fileless-attacks-jump-94--in-first-half-of-2018/d/d-id/133268, accessed November 2018.
[493] http://invenioit.com/security/2018-ransomware-statistics/, accessed November 2018.

- The most common ransomware attack was WannaCry, with 53,92%. The second one was GandCrab with 4,92%[494].
- The computers of 158.921 unique users were ransomware attacked in the Q2 2018[494].
- More than 20.000 installations of mobile ransomware Trojans were detected in the H1 2018[494].

*The overall trend for **ransomware** attacks in 2018 is **DECREASING**.*

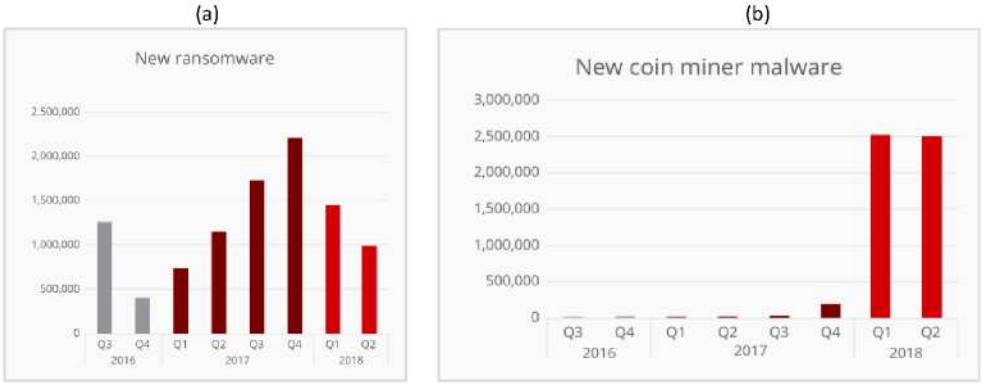


Figure 39: New ransomware (a) and coin miner malware (b) in H1 2018[495]

3.14.4 Top ransomware threats

- **WannaCry** is a ransomworm that is based on the combination of technically simple exploits namely the EternalBlue (developed by the NSA[496]), the DoublePulsar and cryptocurrency miners. WannaCry is replicated without any human interference and spreads from one computer to others on the same network. A global WannaCry attack targeting healthcare organisations started in May 2017 and managed to infect more than 200.000 computers spread in 150 countries[474], including systems of the National Health Services of Great Britain[496]. It was estimated that more than 312 ransom payments were made for WannaCry attacks[497]. The Boeing aircraft manufacturing company suffered a WannaCry attack in March 2018[498]. In many cases, WannaCry has been used by regimes in search of funding in foreign currency or in cryptocurrency [490].
- **GandCrab** was used for the first time in January 2018 and infected more than 50.000 systems in less than a month. Since then, GandCrab is taking the lead on ransomware attacks; it was the second-highest detected ransomware globally from March to July 2018[499]. It operates similarly to Locky[481] and Jaff[481], as it is based on malicious macros hidden in files which in turn are delivered as email

[494] https://securelist.com/it-threat-evolution-q2-2018-statistics/87170/, accessed November 2018.
[495] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf, accessed November 2018.
[496] https://searchsecurity.techtarget.com/definition/WannaCry-ransomware, accessed November 2018.
[497] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf, accessed November 2018.
[498] https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_Threat_Trends_2018_Mid-Year_Update.pdf, accessed November 2018.
[499] https://threatpost.com/gandcrabs-rotten-eggs-hatch-ransomware-in-south-korea/136689/, accessed November 2018.

attachments. However, the GandCrab ransom payments are done on Dash rather than on Bitcoin cryptocurrency[480]. GandCrab has been developed based on the Ransomware-as-a-Service (RaaS) model and allows the developers and criminals to share the profit[500]. GandCrab targeted mostly Scandinavian and English-speaking countries[501].

- **NotPetya** or Nyetya first arrived in June 2017. It is a combination of the EternalBlue and the EternalRomance exploits and it also includes a credential harvesting code[476]. NotPetya was first unleashed in the Ukraine infecting more than 1 million computers in 2.000 different companies[497]. NotPetya in most cases was used as a disk wiper after stealing data, disguising the attacker's true motive: the data[490].
- **SamSam,** a highly sophisticated ransomware that first appeared in 2015, is still used with high amounts of money stolen as ransom. The attackers using SamSam are specifically keen on hiding any digital trace of their actions and avoid investigation. The SamSam encryption tool renders thoroughly the victim's data files and in most cases, the recovery is impossible even by reimaging or reinstalling the software. More than US $6 million where lost due to SamSam in India during these past three years[502]. SamSam incidents affected healthcare and government organizations in 2018 such as the city of Atlanta (US $17 million damage in recovery cost), the LabCorp. and the Colorado Department of Transportation (US $1,5 million damage in recovery costs)[503].
- **Lokibot** is a banking Trojan and info-stealer targeting smart mobile devices with Android OS. However, Lokibot is also used for ransomware on mobiles because it allows the attacker to lock the device. Lokibot was among the three 'most wanted' mobile malware in the first half of 2018[504].
- **PyLocky** first appearance in August 2018, delivered via spam email, targeting European countries[505]. PyLocky has certain similarities with Locky[481], for example, the same ransom note. However, the main difference is the programing language (Python) used in writing the packaged executables. PyLocky features advanced capabilities such as anti-machine learning.
- **BlackRuby** is a new attack that combines ransomware and cryptojacking and was first used in February 2018. The attacker locates the victim's position by utilizing API to achieve better decryption pricing and initiates XMRig CPU miner at the same time[506].
- **CryptoWall** first appeared in late 2015 victimizing hundreds of computers of a major South East Asian company[490]. CryptoWall has so far more than 36.000 victims who paid more than US $18 million in ransoms[488]. CryptoWall was being delivered via existing drive-by downloads in compromised websites and not via an emailed attachment.

---

[500] https://www.fortinet.com/demand/gated/q2-2018-threat-landscape-report.html , accessed November 2018.
[501] https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf, accessed November 2018.
[502] https://cio.economictimes.indiatimes.com/news/digital-security/samsam-ransomware-raked-in-6-million-sophos-report/65228580, accessed November 2018.
[503] https://blog.barkly.com/ransomware-statistics-2018, accessed November 2018.
[504] https://blog.checkpoint.com/2018/07/05/junes-most-wanted-malware-banking-trojans-crypto-mining/, accessed November 2018.
[505] https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-the-locky-poser-pylocky-ransomware/, accessed November 2018.
[506] https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Q1-2018-Threat-Landscape-Report.pdf, accessed November 2018.

3.14.5 Specific attack vectors

One of the reasons why individuals, companies or organisations are vulnerable to ransomware attacks is the use of outdated or unpatched software and operating systems[474]. The vulnerabilities of the OS or the software, if not treated, may be exploited in a ransomware incident.

The most recent vulnerabilities with an association to the ransomware threat are the CVE-2018-8174[507] that was exploited by the GandCrab[508] and the Magniber[505], the CVE-2018-14787 of Philips IntelliSpace Cardiovascular (ISCV) that may leave exposed critical patient's clinical information[509], the CVE2018-7600 that is exploited by the XMRig CPU miner in the BlackRubby ransomware[510] , the CVE-2018-4878 exploited by the GandCrab[511] and the CVE-2018-1010, CVE-2018-1012, CVE-2018-1013, CVE-2018-1015, CVE-2018-1016 vulnerabilities of the Flexera Software[512].

3.14.6 Specific mitigation actions

Specific actions for mitigating a ransomware attack are the following:

- Implement the use of network segmentation, data encryption, access control, and policy enforcement for minimum exposure of data[476].
- Implement the use of methods such as monitoring for fast identification of infections[476].
- Monitor the access and status of the public infrastructure used[497].
- Assure the existence of a Security Operation Centre (SOC) manned with skilled security staff within every organisation or company[486].
- Implement the use of appropriate and updated tools for ransomware prevention[486].
- Define and implement a minimum set of user data access rights in order to minimize the impact of attacks (i.e. less rights, less data encrypted).
- Introduce a reliable back-up off-line scheme that is tested and is in a position to recover user data in a timely manner.
- Implement a robust vulnerability and patch management system.
- Implement a content filtering solution to filter unwanted attachments, emails with malicious content, spam and unwanted network traffic.
- Install an end-point protection solution by means of anti-virus programs but also blocking execution of files (e.g. block execution in Temp folder).
- Introduce policies to control external devices and port-accessibility.
- Implement whitelisting to prevent unknown executables from being executed at the end-points.
- Invest in user awareness especially in the promotion of secure browsing behaviour.

---

[507] https://nvd.nist.gov/vuln/detail/CVE-2018-8174, accessed November 2018.
[508] https://www.securityweek.com/researchers-discover-new-fallout-exploit-kit, accessed November 2018.
[509] https://threatpost.com/philips-vulnerability-exposes-sensitive-cardiac-patient-information/136669/, accessed November 2018.
[510] https://www.scmagazine.com/home/news/cryptocurrency/cryptomining-campaign-targeting-web-servers-vulnerable-to-drupalgeddon-2-0-nets-11000/, accessed November 2018.
[511] https://blog.malwarebytes.com/threat-analysis/2018/07/magniber-ransomware-improves-expands-within-asia/, accessed November 2018.
[512] https://www.beyondtrust.com/blog/ransomware-another-new-attack-vector/, accessed November 2018.

- Follow recent ransomware developments and prevention solutions.

In the fight against ransomware, additional mitigation actions need to be considered. Please find the full list of mitigation actions in the malware chapter.

3.14.7 Kill Chain

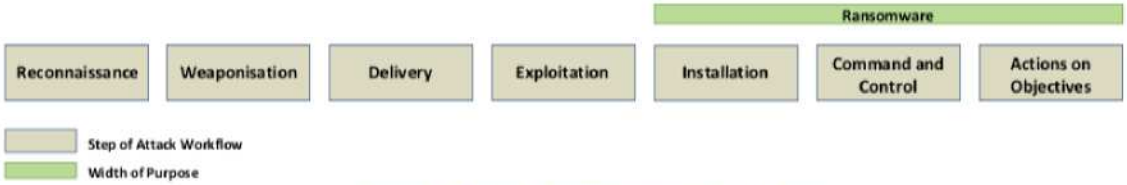


Figure 40: Position of ransomware in the kill-chain

3.14.8 Authoritative references

'KSN Report: Ransomware and malicious cryptominers 2016-2018', Kaspersky Lab[475]; 'McAfee Labs Threats Report 2018', McAfee[480,495]; 'Threat Landscape Report 2018', Fortinet[500,506]; 'The Human Factor 2018 Report', Proofpoint[489]; 'Internet Security Threat Report - Volume 23', Symantec[490]; 'IT threat evolution 2018'; Kaspersky Lab[494].

3.15 Cyber Espionage

3.15.1 Description of the cyberthreat

During the reporting period, various reports from global security research organisations revealed that cyber espionage (or else "nation-state-sponsored") is becoming increasingly popular among certain nation states[514]. This threat typically targets industrial sectors, critical and strategic infrastructures across the world including government entities, railways, telecommunication providers, energy companies, hospitals and banks[513,514,515]. Cyberespionage focuses on driving geopolitics, stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields. It also mobilises actors from the economy, industry, foreign intelligence services, as well as actors who work on their behalf[516,517,518,519,520,521]. In a recent report[517], threat intelligence analysts were not surprised to learn that 71% of the organizations are treating cyber espionage and other threats as a "black box" and are still growing and expanding their knowledge over them.

During the reporting period, the number of nation-state-sponsored cyberattacks that focused primarly on the economy has grown, and is likely to continue this way. In detail, nation-state-sponsored and other adversary-driven attacks on Industrial Internet of Things (IIoT) are increasing in the utilities, oil and natural gas (ONG), and manufacturing sectors. Furthermore, advanced persistent threat (APT) cyberattacks indicate that many financial attacks are motivated by espionage. Using tactics, techniques and procedures (TTPs) akin to their espionage counterparts, groups such as Cobalt Group, Carbanak and FIN7 have allegedly been targeting large financial institutions and restaurant chains successfully.

3.15.2 Interesting points

The identified interesting points[516,517,522] for cyber espionage are as follows:

- The European Parliament's Committee of the Foreign Affairs calls the Member States to establish a cyber defence unit[523] and to jointly work on their common defence[524]. The US President Trump calls on "proactive offensive tactics" regarding the Homeland security[544].

---

513 http://wef.ch/risks2018
514 https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf, accessed November 2018.
515 https://www.blackhat.com/docs/us-18/black-hat-intel-where-cybersecurity-stands.pdf, accessed November 2018.
516 https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf, accessed November 2018.
517 https://www.accenture.com/t20180803T064557Z__w__/us-en/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf, accessed November 2018.
518 https://www.nytimes.com/2018/11/06/opinion/midterm-elections-russia.html?rref=collection%2Ftimestopic%2FCyberwarfare&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=collection, accessed November 2018.
519 https://www.theguardian.com/technology/2018/oct/17/theresa-may-to-urge-eu-leaders-to-take-action-on-cyber-attacks, accessed November 2018.
520 https://www.wired.co.uk/article/china-hacking-cyber-spies-espionage, accessed November 2018.
521 https://www.politico.eu/article/europe-raises-red-flags-on-chinas-cyber-espionage/, accessed November 2018.
522 https://www.ncsc.gov.uk/content/files/ncsc_2018-annual-review.pdf, accessed November 2018.
523 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0492+0+DOC+PDF+V0//EN, accessed November 2018.
524 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-625.376+01+DOC+PDF+V0//EN&language=EN, accessed November 2018.

- Cyber espionage groups and tools are becoming increasingly attractive among government officials forming a new open-market area[525].
- Vulnerabilities introduced by emerging technologies, such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) generate interest among nation-states to support cyber-espionage activities through exploitation. A recent report disclosed a letter from the Israeli government addressed to US-based exploit developers inquiring about "advanced Vulnerabilities R&D and zero-day exploits for the use of its law enforcement and security agencies for a wide variety of target platforms and technologies"[526].
- Nation-states use various means to anonymise attacks making attribution extremely difficult.
- Threat actors motivated by financial, political, or ideological gain will increasingly focus attacks on supplier networks with weaker cybersecurity programs. Cyber espionage adversaries have slowly shifted their attack patterns to exploiting third- and fourth-party supply chain partners.
- Software supply chain infiltration threatens the critical infrastructure sector and is poised to threaten other sectors.
- Weak foreign laws could enable Intellectual Property theft. For example, when US companies do business in China then valuable company data is stored in China and government approval is required prior to transferring this data outside China. Another example is Russia who demands source code reviews for all foreign technology being sold inside the country.
- According to the UK's National Cyber Security Centre (NCSC), state-sponsored hackers employed by hostile nations carry out most of the attacks. They are also tackling several phishing sites targeting British consumers.
- The UK has developed a new categorisation framework to ensure that the appropriate handler manages an incident: C1 attacks are national emergencies; C2 attacks can have a serious impact on a large portion of the population, economy or government; C3 attacks can have a serious impact on a large organisation or wider government; C4 attacks could threaten a medium-sized organisation; C5 attacks include threats to a small organisation; C6 attacks on individuals and the response would be led by law enforcement agencies, such as the local police force.
- The United States is projected to be a net oil and gas exporter by 2022 and if this projection comes to fruition, the United States will directly compete with Russia in the European market. Russian state actors could sponsor disruptive or espionage-related cyber operations or support hacktivists in the name of protecting the environment to contain this new competition in one of the largest energy market.
- Newly imposed sanctions on Iran are likely to push the country to intensify state-sponsored cyberthreat activities in pursuit of its geopolitical and strategic objectives at a regional level, particularly if Iran fails to keep its European counterparts committed to the Joint Comprehensive Plan of Action (JCPOA) agreement.

---

[525] https://motherboard.vice.com/en_us/article/gy8gmb/area-surveillance-tech-european-police-congress, accessed November 2018.
[526] https://motherboard.vice.com/en_us/article/neqkgm/israel-zero-days-letter-to-american-hackers, accessed November 2018

3.15.3 Trends and main statistics

As figure 41 illustrates, cyber espionage decreased overall by ca. 2% in 2018[527].

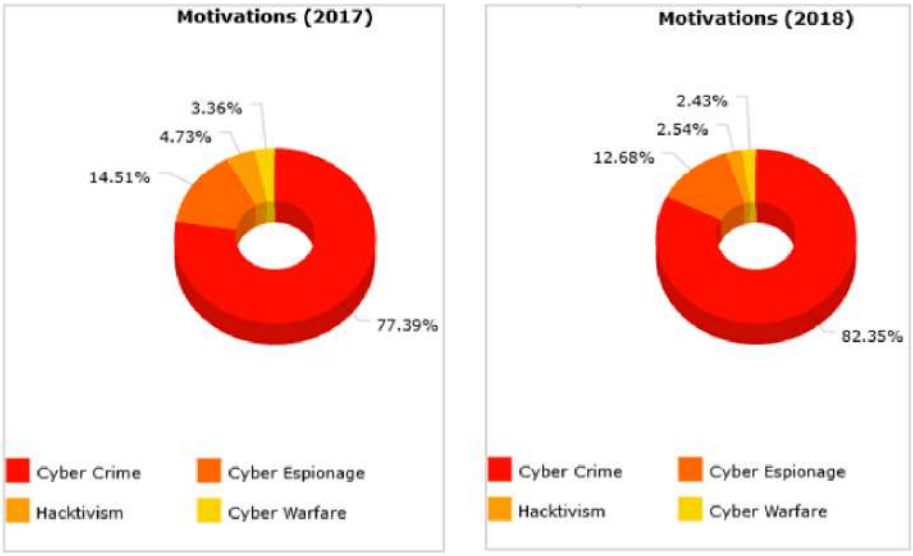


Figure 41: Distribution of attack motivations (2017-2018)[528]

- 66% of the oil and natural gas (ONG) IT managers said digitisation has made them more vulnerable to espionage compromises[517].
- China, Russia, and Iran stand out as 3 of the most capable and active cyber actors tied to economic espionage[516,517].
- 87% of the security professionals believe that recent activity emanating from Russia, China, and North Korea has made U.S. enterprise data less secure[515].
- 43% of the security professionals believe that a potential attack by large nation-states is the greatest threat to US critical infrastructure[515].
- The time spent by security professionals preventing attacks from cyber espionage or surveillance by foreign governments or competitors decreased from 6% (2017) to 3% (2018)[515]. For the same threat, the professionals' concern has also decreased from 11% (2017) to 9% (2018)[515].
- Operational technology (OT) networks of industrial enterprises is a field of glory for espionage threat actors. These actors use remote administrator tools (RATs) which are already installed in the industrial control systems (ICS). A recent report[529] reveals the top 20 countries in which RATs were used at least once on espionage incidents during the H1 of 2018.

[527] https://www.hackmageddon.com/2018-master-table/, accessed November 2018.
[528] https://www.hackmageddon.com/2018-master-table/, accessed November 2018.
[529] https://securelist.com/threats-posed-by-using-rats-in-ics/88011/, accessed November 2018.

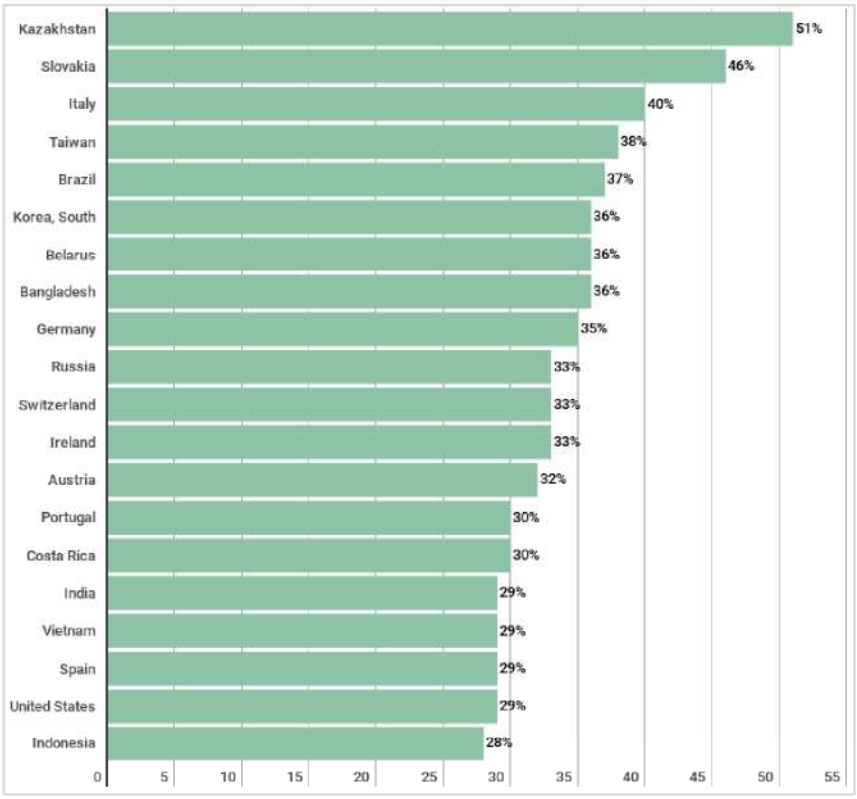


Figure 42: RAT on ICS computers vs. total computers (top 20 countries in H1 2018)[530]

*The overall trend for **cyber espionage** in 2018 is **DECREASING**.*

3.15.4 Top cyberespionage attacks

- **ZooPark** is a cyber espionage operation which targets Android users in Asia and Middle East. ZooPark can perform keylogging, steal GPS location and clipboard data (incl. audio, photos, text and data from messaging apps). Several generations of this espionage malware are active since June 2015. ZooParck incidents during the reporting are associated with the independence referendum in Kurdistan and focused on victims in Egypt, Jordan, Morocco, Lebanon and Iran[532].
- **FIN7** (also known as, Carbanak group and Cobalt) cyber espionage threat-group continues to innovate, but it has been less active in 2018 compared with previous years. However, there are new incidents of the Bateleur, HALFBAKED, BELLHOP malware, Meterpreter and Cobalt Strike BEACON in 2018[517].

[530] https://securelist.com/threats-posed-by-using-rats-in-ics/88011/, accessed November 2018.
[531] http://www.verizonenterprise.com/verizon-insights-lab/dbir/tool/, accessed November 2018.
[532] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/05/24122414/ZooPark_for_public_final_edited.pdf, accessed November 2018.

- **POWERSTATS** malware family activity is on the rise and continuously evolving, as seen in targeted attacks that have been dubbed "Muddy Water". This threat group continuous to focus in West and Southwest Asia, North Africa, and the Middle East, most prominently in Saudi Arabia[517].
- **PIPEFISH (aka OilRig)** cyber espionage threat-group continues to be active and advancing its toolset. This threat group has been mostly targeting Middle Eastern entities for surveillance and espionage objectives in the energy sector[517]. Also, the PRB Backdoor, which targets companies in Egypt, matching previous threat-actor interest in civil aviation organizations in the region. The OopsIE trojan has the ability to execute remote commands and to upload and download files from the victim system[517]. New ISMDoor variants appeared in early 2018; these variants included an information stealer and a remote administration tool (RAT)[517].
- **Unofficial** Android marketplaces, such as Myket, use malware families to attack using update lures. These have been mostly targeting users of messaging and social media platforms (such as Telegram, Twitter, and Facebook). It is an Iranian espionage campaign discovered in 2018[517].
- **TEMP.Periscope** (or else "Leviathan") cyber espionage group escalates its detected activity targeting engineering and maritime entities, especially those connected to South China issues during March 2018. This advantage includes the utilisation of a large library of malware including AIRBREAK, BADFLICK, PHOTO, HOMEFRY, LUNCHMONEY, MURKYTOP, China Chopper, and Beacon[533].
- **Operation Parliament** attackers' acts involve gaining access to top legislative, executive and judicial bodies, military and intelligence agencies and large trading companies around the world, especially the Middle East and North Africa. This targeting seems to have slowed down since the beginning of 2018[534,535].

[533] https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html, accessed November 2018.
[534] https://securelist.com/operation-parliament-who-is-doing-what/85237/, accessed November 2018.
[535] https://blog.talosintelligence.com/2018/02/targeted-attacks-in-middle-east.html, accessed November 2018.

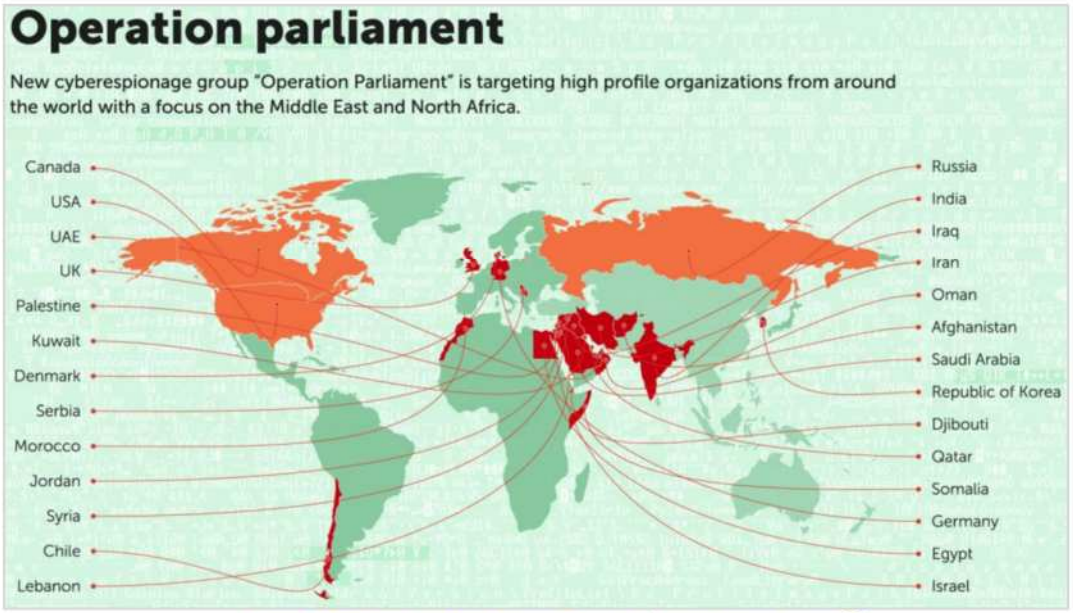


Figure 43: "Operation parliament" victims/victim organisations[536]

- **DustSquad** is a Russian-language cyber espionage group. In April 2018, Official authorities demanded the demolish of Octapus, a malicious Windows program that pretends to be a Telegram, against diplomatic entities in Central Asia[537].
- **APT27** (also known as, Emissary Panda and LuckyMouse) is a Chinese cyber espionage group. In June 2018, a national campaign is detected targeting governmental data centres and other resources[538].
- **APT28** (also known as, Fancy Bear, Pawn Storm, Sofacy Group, Sednit, STRONTIUM and Tsar Team) is a cyber espionage group most probably sponsored by the Russian government. During 2018, the Fancy Bear group targets the US Senate, the German Elections, the Emmanuel Macron campaign, the Turkish and Montenegro Parliaments, as well as Foreign Affairs Agencies and Embassies in Europe and Russia[539,540]. In August 2018, researchers exposed the fact that for many years, Fancy Bear had been targeting the email correspondence of the officials of the Ecumenical Patriarchate of Constantinople[541]. This espionage activity is also correlated with the Ukraine amid efforts to disassociate Ukraine's Orthodox church from its association with the Russian church[542]. Researchers also attributed this year spread of VPNFilter malware and Lolajack attack to this group.[543]

---

[536] https://securelist.com/operation-parliament-who-is-doing-what/85237/, accessed November 2018.
[537] https://securelist.com/octopus-infested-seas-of-central-asia/88200/, accessed November 2018.
[538] https://securelist.com/luckymouse-hits-national-data-center/86083/, accessed November 2018.
[539] https://www.databreachtoday.com/fancy-bear-targets-us-senate-security-researchers-warn-a-10586, accessed November 2018.
[540] https://researchcenter.paloaltonetworks.com/2018/02/threat-brief-sofacy-group-targeting-european-north-american-diplomats/, accessed November 2018.
[541] https://www.bloomberg.com/news/articles/2018-08-27/unholy-hackers-orthodox-clergy-targeted-by-russian-spies
542 https://risu.org.ua/en/index/monitoring/72403/, accessed November 2018.
[543] https://www.enisa.europa.eu/publications/info-notes/vpnfilter-a-nation-state-operation

- The **US Cyber Command** announced in September 2018 that they officially[544] launched a "proactive and warning cyber-attacks" against Russia and other adversaries to prevent their interference in November's midterm elections[545].

3.15.5 Specific attack vectors

In cyber-espionage attacks, threat agents often use complex pieces of malware and repurposed ransomware. In most cases, common spreading and infecting methods, such as phishing, are used. For more details about attack vectors, please see chapter 5.

3.15.6 Specific mitigation actions

Due to the comprehensive nature of this threat, several mitigation measures found in other threats of this report could be employed. The following advice[517,546,547,548] proposes baseline mitigation controls for this threat:

- Hire talented individuals to manage and support AI-based technologies at the upstream level.
- Identify mission critical roles in the organisation and estimate their exposure to espionage risks. Espionage risks are being evaluated based on business information (i.e. business intelligence).
- Create security policies that accommodate human resource, business and operational security controls to cater for risk mitigation. This will include rules and practices for awareness raising, corporate governance and security operations.
- Establish corporate practices to communicate, train and apply the developed rules and keep operational parts up and running.
- Develop an evaluation criterion (KPI) to benchmark the operation and adapt it to upcoming changes.
- Implement whitelisting development for critical application services, depending on the risk level assessed.
- Conduct regular vulnerability assessment and patching of used software, especially for systems that are in the perimeter.
- Implement a need-to-know principle for access rights definition and establish controls to monitor misuse of privileged profiles.
- Implement a content filtering solution for all inbound and outbound channels (e.g. email, web, network traffic).

3.15.7 Kill Chain

Kill chain is not relevant for this threat: this is a "composite" threat consists of many cyberthreats spanning all the phases of the kill chain, just as data breaches.

---

[544] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, accessed November 2018.
[545] https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?utm_term=.4e24594c7ab2, accessed November 2018.
[546] www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf, accessed November 2018.
[547] http://www.verizonenterprise.com/resources/rp_data-breach-digest-2018-cloud-storming_xg_en.pdf, accessed November 2018.
[548] http://www.verizonenterprise.com/resources/rp_data-breach-digest-2018-credential-theft_xg_en.pdf, accessed November 2018.

3.15.8 Authoritative references

"Internet Security Threat Report", Symantec[514]; "Where Cybersecurity Stands", Blackhat[515]; "Foreign Economic Espionage in Cyberspace", National Counterintelligence and Security Centre[516]; "Cyber Threatscape Report", Accenture[517]; "Annual Review", National Cyber Security Centre[522]; "Suspected Chinese Cyber Espionage Group Targeting U.S. Engineering and Maritime Industries", FireEye[533].

3.16 Visualising changes in the current threat landscape

This chapter provides a visualization of the changes assessed in 2018's landscape in comparison with the previous year (see table 4). Besides the changes in ranking, the table also displays the trends identified for each threat. The interesting phenomenon of having some threats with stable or decreasing trend remaining in the same ranking (i.e. Insider Threat, Physical manipulation/damage/theft/loss, Cyber Espionage), is mostly due to the fact that, albeit stagnation, the role of this threat in the total landscape was maintained (through volume of infections, identified incidents, breaches attributed to the threat, etc.).

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 4 - Overview and comparison of the current threat landscape 2018 with the one of 2017

4. Threat Agents

4.1 Threat agents and trends

Threat agent matters have been one of the most interesting areas of the 2018's threat landscape. Albeit until the middle of 2018 developments in this area advanced, they did so in analogy to the increasing maturity of CTI practices. Around the end of the year, however, we have seen some quantum leap results in attributions[549,550]. These developments were mostly caused by increasing efforts to tackle terrorism[551], but also by the increasing preparedness to politically and diplomatically thematise subliminal activities of countries towards cyber-warfare and cyber-espionage. Numerous politically motivated initiatives came to amplify the appetite of governments in looking into underground operations of opponents and use them within international diplomacy campaigns to accomplish their objectives[552,553].

As in other domains of CTI, the developments observed in the area of threat agents are due to a widening of the scope of cyberthreat intelligence to other related areas such as threat intelligence and generic intelligence. Definitely, the role of LEAs within cybersecurity operations but also the increasing role of National Cyber Security Centres has contributed towards enhancing CTI's scope. Moreover, it became apparent that the impact of cyber-incidents affects the physical space. This has led inevitably to the manifestation of the importance of attribution. Hence, the identification of threat agents has become a central element in cyberthreat mitigation.

By looking at the trends/advancements in the areas of threat agents from the defenders point of view, it is noticeable that:

- In 2018 we have seen approaches aiming at a better understanding of the "attacker perspective"[554]. Such approaches are based on the visualisation of the motives and identification of methods (TTPs) and modus operandi encountered in series of attacks[555]. Given the existence of recurring threat agent behaviours (methods, tools and tactics), this approach leads to good rates of recognition of kind and origin of threat agents.
- In 2018 there have been increasing efforts to penetrate the infrastructure of threat agents. By using intelligence, some actors try to create trustful personas allowing them to enter into hacker fora[556]. Moreover, various nation state organisations try to hack back to be in the position to monitor actions

[549] https://edition.cnn.com/videos/world/2018/10/05/russia-spies-chance-pkg-sitroom-vpx.cnn, accessed October 2018.
[550] https://www.reuters.com/article/us-norway-russia/moscow-protests-russians-arrest-in-oslo-norwegians-seal-off-room-in-parliament-idUSKCN1M41F6, accessed October 2018.
[551] https://thehill.com/opinion/national-security/370748-new-defense-strategy-requires-paradigm-shift-in-us-counterterrorism, accessed October 2018.
[552] http://www.spiegel.de/netzwelt/netzpolitik/russland-und-die-hacker-die-zeit-der-diplomatie-ist-vorbei-a-1232006.html, accessed October 2018.
[553] https://www.theregister.co.uk/2018/10/11/obamaera_cyber_detente_with_china_is_well_and_truly_over/, accessed October 2018.
[554] https://blog.barracuda.com/2018/09/10/gaining-the-attacker-perspective/, accessed October 2018.
[555] https://www.orange-business.com/en/blogs/hacker-personas-inside-mind-cybercriminal, accessed October 2018.
[556] https://www.delltechnologies.com/en-us/perspectives/spy-on-spy-hacking-into-the-darknet/, accessed October 2018.

of threat agents and/or disrupt their infrastructures[557]. Finally, through the combination of cyberthreat intelligence and intelligence skills, some impressive successes regarding unveiling of state sponsored agents have been achieved[558,559].

- Efforts to simulate threat agent tactics have been assessed in 2018. Via a series of tools, cybersecurity companies try to enhance awareness and preparedness of their customers in defending a cyber-attack[560,561]. Though not directly related to threat agents, this approach may contribute towards less successful threat agent activities.
- Cyberthreat Intelligence experts have underlined inefficiencies of defending strategies based on the kill-chain[562]. In particular, defender activities are mostly triggered at a late stage of the kill-chain[563], that is, after the adversaries have performed the infiltration of the target. In other words, defence is based on the late phases of the kill-chain (i.e. command and control, action on objectives), while defence in the early phases are often neglected in the defence strategies (i.e. reconnaissance, weaponization, delivery, exploitation and installation).

2018 has also brought quite a few new developments from the side of threat agents:

- It is assumed that traditional state sponsored threat agents are currently repositioning themselves in the changing geopolitical space[564]: though activities of some groups seem to decrease, new types of campaigns assigned to new actors may stem from known actors who have changed tactics and targets, but they are using similar tools, malicious sites and vulnerabilities.
- In 2018, attack tactics have shifted to malware-less attacks with email and impersonation attacks being the main infection vector[565]. In the enhanced threat agent capabilities belong time related attack tactics (e.g. kind of phishing according to week days), selective phishing via refined social engineering tactics, payload installed via remote access tools (e.g. Remote Desktop Protocol (RPD) interfaces)[566], targeted attacks tailored to sectors, etc.[567].
- Just as in 2018, the discovery of vulnerabilities continues increasing[568]. Until first half of 2018, vulnerabilities have reached an all year high and it is expected that 2018 in total will top all other

[557] https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back, accessed October 2018.
[558] https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions, accessed October 2018.
[559] https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/, accessed October 2018.
[560] http://pentestit.com/adversary-emulation-tools-list/, accessed October 2018.
[561] https://cyberstartupobservatory.com/how-a-breach-and-attack-simulation-bas-platform-can-help-financial-organizations-to-be-better-protected/, accessed October 2018.
[562] https://nis-summer-school.enisa.europa.eu/, accessed October 2018.
[563] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, accessed October 2018.
[564] https://securelist.com/apt-trends-report-q2-2018/86487/, accessed October 2018.
[565] https://www.itproportal.com/news/two-thirds-of-email-sent-in-2018-is-infected/, accessed October 2018.
[566] https://diepresse.com/home/karriere/karrierenews/5388590/Ransomware_Hacker-haben-Vorgangsweise-geaendert?from=rss, accessed October 2018.
[567] https://www.trustwave.com/Resources/Library/Documents/2018-Trustwave-Global-Security-Report/, accessed October 2018
[568] https://meterpreter.org/risk-based-security-vulnerability-report/, accessed October 2018.

years. This trend has also positive effects[569]: in 2018, patching of vulnerabilities from software vendors has grown. Moreover, concepts such as vulnerability taxonomy are useful tools for end users to perform vulnerability-based mitigation[570].

- Threat agents introduce new methods for evading attribution and detection of attacks. File-less and memory-resident threats as well as use of common attack tools seem to be efficient ways in achieving objectives, while at the same time effectively hide their traits[571]. This a generic trend that is manifested in various attack patterns on the one hand and the decline of activities of known threat groups.
- Threat actors, especially advanced ones, are making progress in using the supply chain to achieve their objectives[572]. In 2018, a hardware attack has made headlines[573] and led to controversial discussions[574]. Despite this single incident, numerous supply chain attacks are assumed to take place, mainly launched by high capability agents[575]. Assessments hereto have led to the conclusion that supply chain attacks are to be considered as a "key threat".

Some of the above points are taken up in the conclusions of this report (see chapter 6).

4.2 Top threat agents and motives

In this chapter, we present an outline of top threat agent groups. It includes observations about their motives and main trends assessed with regard to their capabilities. This is a complementary view to the threat assessments (including tools, methods and tactics) presented within the top cyberthreats (see chapter 3) and the attack vectors (see chapter 5).

Before going into the developments in each particular threat agent group, it is necessary to explain the complex dynamics in this field. Increasing maturity in threat agent profiling demonstrates that the characteristics of the threat agent groups are in a permanent flow[576]. Albeit ideological matters may be the main motives to let a person enter to whatever hacker group, personal developments, political environment, skills and monetary ambitions may be the drivers causing people to change their minds over time. These forces may affect the motives of threat agents and make them change their group. Criminal profiling may be the necessary tool to understand these shifts/changes. Though not applied in understanding cyberthreat agent group dynamics, these techniques start penetrating the threat landscape[577]. It is expected that this trend will persist in the coming years and will further facilitate attribution.

---

[569] https://nvd.nist.gov/vuln/search/statistics?adv_search=false&form_type=basic&results_type=statistics&search_type=all, accessed October 2018.
[570] https://www.edgescan.com/wp-content/uploads/2018/05/edgescan-stats-report-2018.pdf, accessed October 2018.
[571] https://securityaffairs.co/wordpress/77041/apt/gallmaker-apt-emerges.html, accessed October 2018.
[572] https://www.cisco.com/c/en/us/products/security/security-reports.html, accessed October 2018.
[573] https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-the-software-side-of-china-s-supply-chain-attack, accessed October 2018.
[574] https://www.zdnet.com/article/dhs-and-gchq-join-amazon-and-apple-in-denying-bloomberg-chip-hack-story/, accessed October 2018.
[575] https://www.bbc.com/news/technology-44941875, accessed October 2018.
[576] https://blog.malwarebytes.com/cybercrime/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime/, accessed October 2018.
[577] https://pylos.co/2018/08/19/threat-profiling-and-adversary-attribution/, accessed October 2018.

Just as in previous threat landscapes, we consider the following threat agents' groups: cyber-criminals, insiders, cyber-spies, hacktivists, cyber-offenders, cyber-fighters, cyber-terrorists and script-kiddies. It should be noted that the sequence of mentioning these actors is according to their engagement in the threat landscape[578,579].

The assessed cyberthreat agent groups are as follows:

In 2018, **Cyber-criminals** remained the most active threat agent group in cyber-space. The activity of this threat agent group increased from the previous year, being responsible for over 80% of the incidents[578]. The economics of cybercrime estimate that ca. 0,8% of the gross domestic product is impacted by this threat agent group[580]. Overall, the activities of cybercriminals have demonstrated an increase in complexity and sophistication. On the top of used TTPs resides the propagation of malware through emails[581]. Over 60% of email traffic contained malicious content. Email was involved in more than 90% of the cyber-attacks. Business email compromise (BEC) is responsible for a loss of over US $12 billion since 2013[581]. A further new development regarding monetization in 2018 is the use of cyptojacking/cryptomining malware[579] and cryptocurrencies attacks[582]. In 2018, ca. US $880 million losses have been attributed to cryptocurrencies attacks[583]. Although the losses are not attributed to cybercriminals only, there is a clear trend in 2018 of cybercriminals targeting cryptocurrencies. While cryptojacking/cryptomining has risen in 2018 to replace ransomware from the top of malware[584], the monetisation achieved is not very high[585]. Another clear trend in cybercrime attacks in 2018 has been the refinement of phishing by using social engineering techniques[586]. Remarkable are the trends towards attacking Software-as-a-Serice (SaaS), the rates of phishing using social engineering (tripled in 2018) and the continuous innovation towards persuading users for the originality of phishing scams[587]. As regards to geographical issues, cybercriminals still target mostly USA users with phishing attacks[586] with ca. 86% of registered incidents. Despite the increase in attack complexity, simple/classic scams are still a popular method, since even low success rates allow penetration in targeted infrastructures. As a final element of the dynamics of this threat agent group, one should mention the innovation trend of Cybercrime-as-a-Service platforms[579]. Besides improvements of offered services, these developments lead to a higher usability and popularity of these services. This may lead to more efficient attacks by all other threat agent groups.

---

[578] https://www.hackmageddon.com/category/security/cyber-attacks-statistics/, accessed October 2018.
[579] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018, accessed October 2018.
[580] https://www.computerweekly.com/news/252435439/Economic-impact-of-cyber-crime-is-significant-and-rising, accessed October 2018.
[581] https://brica.de/alerts/alert/public/1229120/malware-less-email-attacks-increasingly-common-fireeye-finds/, accessed October 2018.
[582] https://cio.economictimes.indiatimes.com/news/digital-security/crypto-thefts-drive-growth-of-global-coin-money-laundering/64881793, accessed October 2018.
[583] https://securityaffairs.co/wordpress/77213/hacking/cyber-attacks-crypto-exchanges.html, accessed October 2018.
[584] https://www.bankinfosecurity.com/cryptojacking-displaces-ransomware-as-top-malware-threat-a-11165, accessed October 2018.
[585] https://www.theregister.co.uk/2018/08/30/cryptojacking_pays_poorly/, accessed October 2018.
[586] https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf, accessed October 2018.
[587] https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/, accessed October 2018.

The insider threat (see also description as cyberthreat) is attributed to the threat agent group **insider**. This group consists of malicious and negligent insiders. Insiders may be users, privileged users and service providers/contractors. According to reports analysed in 2018, this group is the second source of compromise in the threat landscape after cybercriminals[567,588,589]. Breach statistics show that around 25% of incidents are attributed to insiders[588] in corporate environments. Yet, businesses perceive the insider threat as being the most prevalent one, with 64% of them investing in deterrence measures against insiders[590]. The difference in perception between the actual impact of actual insider misuse is causing non-proportional security expenses to organisations w.r.t. the effect of the implemented controls. Assessments found in 2018 regarding insiders reveal that privilege misuse is the second source of incidents and miscellaneous errors are at the 6th [591]. For the breaches resulting from these incidents, however, the sequence is inverted, that is, errors are leading to a higher number of breaches than privilege misuse. This might be due to the higher exploitation of errors by adversaries of all types. While monetization is the main motive of this threat agent group, most of the damage seems to be caused by unintentional actions of employees[592]. These being accidental disclosure of data (e.g. use of wrong email addresses), failures in recognising phishing attacks or misconfiguration errors[593]. Finally, it is worth mentioning that insider threat may directly or indirectly materialize in supply chain attacks[594,595].

In 2018, the activity of **Nation States** in cyberspace has been encountered multiple times in the international headlines. Undoubtedly, this was due to geopolitical developments/tensions among various countries, such as China, USA, North Korea, Russia, Germany and UK, just to mention the most important ones[596]. Hence, 2018 is the year where it becomes evident that cyberespionage has to be analysed by taking into account diplomatic, military and geopolitical developments. Moreover, by further advancing their capabilities, nation states will continue bridging their cyber activities with all other affairs of national relevance both within and outside the country. In 2018, we have seen these bridges being established by coupling intelligence capabilities with threat and cyberthreat intelligence[559]. As regards the activity of this threat agent group, 2018 has brought some noticeable changes. Firstly, it has been assessed that in 2018 the activity of some known threat agent groups has declined[578]. Yet, a comprehensive analysis of nation-sponsored threat agents indicated that this inactivity may be explained as a step back towards reorganizing their infrastructures and tactics[597]. Given the high level of investments in this area and the need to stay under the radar, this assumption seems to be plausible. Another interesting development in 2018 was the attempt to increase impact of attacks. This has been manifested via high capability campaigns aiming at destroying critical infrastructures[598]. An increase of attacks in the Industrial Control

---

[588] http://www.isaca.org/chapters1/puget-sound/education/Documents/2018%20Emerging%20Trends%20in%20Cybersecurity%20-%20EY%20ISACA%20Presentation%20-%2020MAR.pdf, accessed October 2018.
[589] https://isaca.nl/images/Presentatie_Raef_Meeuwisse_19-4-2018.pdf, accessed October 2018.
[590] https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, accessed October 2018.
[591] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf, accessed October 2018.
[592] https://www.doxnet.com/2018/04/insider-use-and-abuse-identifying-internal-threats-and-how-to-mitigate-them/, accessed October 2018.
[593] https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017, accessed October 2018.
[594] https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks, accessed October 2018.
[595] https://www.wired.com/story/supply-chain-hacks-cybersecurity-worst-case-scenario/, accessed October 2018.
[596] https://www.infosecurity-magazine.com/news/infosec18-nation-state-hacking/, accessed October 2018.
[597] https://securelist.com/apt-trends-report-q2-2018/86487/, accessed October 2018.
[598] https://www.independent.co.uk/news/long_reads/cyber-warfare-saudi-arabia-petrochemical-security-america-a8258636.html, accessed October 2018.

Systems (ICS) may be interpreted as indicative of this trend[599],[600]. Another trend of 2018 are attacks of state sponsored agencies to banks, until now typical cybercrime targets[583]. It is assumed, that with such attacks nation states try to avoid the negative impact of sanctions restricting their access to international currencies[601]. Concluding the developments of this threat agent group, one has to mention a trend that has been identified in 2018 regarding outsourcing of surveillance to foreign partners[602]. This trend may weaken governmental oversight over surveillance activities, thus causing additional, difficult to mitigate privacy risks. As a final note, one should consider **corporations** using almost the same techniques as nation state agents. This is due to the vicinity of commercial organisations with strategic role in a country to state sponsored resources in order to obtain competitive knowledge from competitors[603].

Hacktivists continue their activity in 2018 at a similar pace as in the previous year[578]. They continue defacement campaigns based on target web sites and are using DDoS attacks to victims web services to draw the attention of media. Driven by protest actions against political/geopolitical decisions affecting national and international matters, hacktivists had in 2018 sufficient reasons to unfold their activities. Women rights and gun violence have been some remarkable events that triggered protests[604]. Hacktivists still perform cyber-activism as independent, loosely associated cells[605]. A comprehensive resource on hacktivists activities provides sufficient information on defacement techniques used[604,606]. According to this report, the main defacement technique used is web site hacking. Through an extensive analysis of hacktivist activities over the last 18 years, the main techniques identified are SQL injection, unpatched system vulnerabilities and password stealing. Linux and Apache have been the main web platforms compromised[607]. However, monetization is not the main motive behind hacktivist attacks, their access to compromised web sites (ca. 10 Million) may be misused for this kind of motive. Similar incidents have been identified in the past[608]. This potential may create links to other threat agent groups aiming at profit-driven activities. Besides defacement, hacktivists are still active in disclosing confidential information found in hacked web sites. Moreover, they are extensively using DDoS at tacks, especially due to the wide availability of this attack vector in underground markets. Hacktivism was the second motive as regards the use of DDoS related attack vectors[609].

In 2018 we have not found sufficient reports on the motive **Cyber Fighters** per se, that is, on religiously motivated groups. It seems that this motivation is currently being assumed to belong to **Cyber Terrorists**

---

[599] https://www.darkreading.com/risk/take-(industrial)-control-a-look-at-the-2018-ics-threat-landscape/d/d-id/1332754, accessed October 2018.
[600] https://gbhackers.com/ics-systems-attacks/, accessed October 2018.
[601] https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report-2018, accessed October 2018.
[602]https://www.theregister.co.uk/2018/04/24/state_agencies_outsource_surveillance_to_foreign_partners_says_campaign_group/, accessed October 2018.
[603] https://www.cnbc.com/2018/10/05/chinas-cyber-spying-keeps-a-lot-of-us-tech-ceos-up-at-night.html, accessed November 2018.
[604] https://blog.trendmicro.com/graffiti-in-the-digital-world-how-hacktivists-use-defacement/, accessed October 2018.
[605] https://www.pwc.com/m1/en/publications/a-practical-method-of-identifying-cyberattacks.html, accessed October 2018.
[606] https://blog.trendmicro.com/trendlabs-security-intelligence/hacktivism-web-defacement/, accessed October 2018.
[607] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/web-defacements-exploring-the-methods-of-hacktivists, accessed October 2018.
[608] http://www.indiandefensenews.in/2016/10/patriotic-indian-hackers-lock-pakistani.html, accessed October 2018.
[609] https://www.netscout.com/report/, accessed October 2018.

and in some particular cases to state-sponsored actors[610]. This evidence has led us to merge Cyber Fighters and Cyber Terrorists to a single group under the name of **Cyber Terrorists**. This decision is also seconded by the fact that the term Cyber Fighters is now associated with cyber defence groups that are mandated with the development of tactics related to cyber warfare defence[611]. Having said that, in 2018 cyber and terrorism continue their convergence: terrorists continue using legitimate services to perform propaganda w.r.t. their efforts to recruit new members and perform fund rising to finance their operations. Together with the motive of performing cyber-attacks, monetisation and recruitment are the main aims of this threat agent group[579]. It seems that defending cyber terrorism will require a tighter cooperation among law enforcement agencies, as well as public and private companies. The main concern will be a better the scrutiny of social media (for recruitment and fund raining) for the identification of rogue actors[612]. Another important element is the observation of money flows, especially the ones regarding cryptocurrencies[579]. As regards cyber terrorist capabilities in performing cyber-attacks, it is believed that despite the existence of malicious tools in dark market, this threat agent group still maintains low capabilities. Apparently, their ability to access cyber-attack knowledge remains at a low level[613]. Despite the assessed low level of capabilities, several states have put counterterrorism protection on the agenda of state defence[614,615,616]. Given the availability of Crime-as-a-Service and the potential to recruit hackers for their objectives, it is indicative that assessments show cyber terrorism picking up significantly in the years to come[617]. If seen in relation to weaknesses in industrial control systems (ICS) systems, this predictions sound rather plausible[599,618].

The threat agent group **script kiddies** has been maintained in 2018's assessments for a variety of reasons. Firstly, some incidents emanating from this threat agent group have been encountered in 2018[619,620]. Though these incidents are just a minor part of the threat landscape, they clearly demonstrate the potential impact this threat agent group could may create. Secondly, the large amount of available tools

[610] https://www.recordedfuture.com/iran-hacker-hierarchy/, accessed October 2018.
[611] https://www.icann.org/news/blog/engaging-with-the-new-generation-of-cyber-fighters, accessed October 2018.
[612] https://www.thenational.ae/world/europe/eu-plans-new-laws-to-target-terror-on-social-media-sites-1.762013, accessed October 2018.
[613] https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html, accessed October 2018.
[614] https://www.justice.gov/ag/page/file/1076696/download, accessed October 2018.
[615] https://www.defense.gouv.fr/english/actualites/articles/les-manipulations-de-l-information-un-defi-pour-nos-democraties, accessed October 2018.
[616] http://www.basicint.org/publications/stanislav-abaimov-paul-ingram-executive-director/2017/hacking-uk-trident-growing-threat, accessed October 2018.
[617] https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf, accessed October 2018.
[618] https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h1-2018/87913/, accessed October 2018.
[619] https://www.theregister.co.uk/2018/06/20/bitcoin_baron_gets_20_months/, accessed October 2018.
[620] https://www.telegraph.co.uk/news/2018/01/19/british-15-year-old-gained-access-intelligence-operations-afghanistan/, accessed October 2018.

and source code leakage bear the risk of misuse by minors[621,622,623,624]. Such tools may become a powerful instrument in the hands of low capability groups. Moreover, when trying to quantify the available knowledge and striking power of script kiddies, one may have a look at various cyber security challenges[625]: young individuals having some guidance may become very efficient in hacking. If taken as a mirror of capability levels that can be acquired by "entry level" hackers, these events are a clear indication at what levels a teenager may arrive when utilising existing tools. Though cyber-security challenges are definitely the right instruments to engage talented individuals, one should assume that not all hacking minors will be engaged in such events. These assumptions are funded by similar assessments in the cyber-security community[626] and should be taken seriously by the cyber-security community.

4.3 Threat Agents and top threats

The involvement of the above threat agents in the deployment of the identified top cyberthreats is presented in the table below (see table 5). The purpose of this table is to visualize which threat agent groups are involved in which threats. This information is targeted towards stakeholders who are interested in assessing possible threat agent involvement in the deployment of threats. This information might be useful in identifying the capability level can be assumed behind the top threats and thus support in decisions concerning the strength of the security controls that are implemented to protect valuable assets. The table below is very similar to the one of ETL 2017[627], apart from some minor changes/adaptations based on the engagement of threat agents in 2018's incidents.

The table visualizes the various capability levels of various threat agent groups: threat agents who are the source of many primary threat actions are the ones with higher capabilities, while with ones with more secondary or no cyberthreat assignment are possess lower capabilities.

[621] https://wccftech.com/new-tool-hacking-script-kiddies/, accessed October 2018.
[622] https://blog.newskysecurity.com/script-kiddie-nightmare-iot-attack-code-embedded-with-backdoor-39ebcb92a4bb, accessed October 2018.
[623] https://medium.com/bugbountywriteup/subfinder-how-not-to-be-a-script-kiddie-567839e6ef55, accessed October 2018.
[624] http://www.securitynewspaper.com/2018/02/03/new-tool-automatically-finds-hacks-vulnerable-internet-connected-devices/, accessed October 2018.
[625] https://www.enisa.europa.eu/events/european-cyber-security-challenge-ecsc-2018, accessed October 2018.
[626] https://www.uscybersecurity.net/script-kiddie/, accessed October 2018.
[627] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, accessed October 2018.

	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

Table 5: Involvement of threat agents in the top cyberthreats

In this table, we differentiate between threats that are typically deployed through a group (primary group of a threat) and threats that are secondarily deployed by a group. This differentiation is being graphically through the colours of the check symbols in the table (see also Legend in table 5).

5. Attack Vectors

The deployment of the different cyberthreats assessed in the previous chapters is done by the use of one or more attack vectors.

*"Specifically, an **attack vector** is a path or means by which a threat agent can gain access to a computer or network server, abuse weaknesses or vulnerability on assets (including human) in order to achieve a specific outcome"*[628].

The description of an attack vector is essential in order to understand the various tactics, techniques and procedures (TTP) used by threat agents described earlier. It gives a structured way for threat analysts to describe a threat agent's behaviour and defenders to implement appropriate defences, following a "Course of Action".

In this ETL report, the primary attack vectors identified in various security incidents have been categorised in a taxonomy presented in topic 5.1. Attack vectors analysed in previous ENISA Threat Landscapes are still valid. To this extent, the current chapter provides additional vectors that have been encountered in the reporting period.

Out of the sum of encountered attack vectors, three attack vectors are analysed in this report, namely "*Misinformation/Disinformation*", "*Web and browser-based attack vectors*" and "*Fileless or memory-based attacks*". The last section of this chapter reviews current trends with attack vectors encountered in modular and multi-staged threats.

5.1 Attack vectors taxonomy for this year's threat landscape

The list below provides a categorization of the most predominant and noteworthy attack vectors observed by ENISA throughout the year. A full knowledge base of cyber adversary behaviour and taxonomy for adversarial actions maintained by MITRE is available at ATT&CK website[629].

- **Attacking the human element**
  - Social engineering
  - Phishing/spear-phishing/business email compromise(BEC)/whaling/spam through email/social media/online services
    - Malicious attachments in emails
    - Malicious URLs in emails and social media
    - Microsoft office attack vectors (macros etc)
    - Social media messaging services
  - Scams
    - Customer/tech support scams
    - Phone scams (Vishing)
    - SMS scams (Smishing)
- **Web and browser based attack vectors**
  - Drive-by downloads
  - Drive-by mining (cryptojacking)
  - Malicious scripts/URLs

[628] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, accessed November 2018.
[629] https://attack.mitre.org/, accessed November 2018.

    - Exploit-kits
    - Malvertising
    - Web application attacks (SQL injection)
    - Browser based attacks
        - Malicious browser add-ons (updates)
    - Watering hole attacks
    - Mouse hovering
- **Internet exposed assets**
    - Unprotected assets exposed on the internet
    - Default/weak service credentials
    - Password reuse
- **Exploitation of vulnerabilities/misconfigurations and cryptographic/network/security protocol flaws**
- **Supply-chain attacks**
    - Software manipulation or third-party API/software
    - Hardware manipulation
- **Network propagation/lateral movement**
- **Active network attacks**
    - DNS attacks (DNS hijacking/poisoning)
- **Privilege or user credentials misuse/escalation**
    - Access token manipulation
    - Sticky-keys
    - Account manipulation
- **Fileless or memory-based attacks**
    - Malicious PowerShell and XSL scripts
- **Misinformation/Disinformation**
    - Online trolling
    - Spread of fake news online
    - Abuse of social media and search engines algorithms
    - Illegitimate use of social bots

5.2 Misinformation/Disinformation

The alleged inference by foreign nation states in the US and French Presidential elections, in an organized fashion, constitute the hybrid threats of the 21st century[630]. The range of methods used includes propaganda, deception, misinformation/disinformation and other non-conventional tactics that have long been used to destabilise adversaries in the physical space. What is new about the attacks seen in recent years is their transposition to cyberspace, hence their speed, scale and intensity, facilitated by rapid technological change and global interconnectivity.

This type of attacks has highly targeted business and individuals. Every day, unscrupulous characters publish hundreds of made-up stories online to gain a financial advantage, sway opinion or cause damage. More than 2,000 identified online news sources publish false, outlandish, extremist, extremely slanted or

[630] https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf, accessed November 2018.

satiric information each day. Most fake news stories that appear on social media originate from those fake news sites[631].

The analysis of attack vectors used in misinformation/disinformation campaigns highlights the growing importance that this cyber capability plays in the threat landscape.

Online trolling – The definition of online trolling is the practice of behaving in a deceptive, destructive or disruptive manner using internet platforms (social media, messaging and blogs) with no apparent instrumental purpose.

The online spread of fake news – Online fake news consists of deliberate disinformation or hoaxes spreading via online platforms. Attackers can amplify their content and messages using social media, clickbait, and advertising. Furthermore, access to data and analytics on content performance and visitor demographics enable the accessibility of targets and hone the viral nature of the launched messages.

The abuse of social media and search engines algorithms **-** Algorithms are processes in (computational) calculations and/or operations. Social media and search engines use various algorithms to predict what users are interested in seeing and generate user engagement. Based on a user's habits and history of clicks, shares and likes, algorithms filter and prioritise the content that the user receives. When used maliciously, algorithms have the power to amplify the impact of misinformation/disinformation campaigns, in a more precise and effective way.

Illegitimate social bots - A social bot is an automated account programmed to interact like a user in particular on social media. For disinformation purposes, illegitimate social bots can be used to push certain narratives, amplify misleading messaging and distort the online discourse.

Example security incidents related to this attack vector:

- In May 2018, a social media user shared a warning about a popular brand for makeup-remover disposable cloths, claiming that the product caused a violent allergic reaction. Within a few days, the post[632] was shared tens of thousands of times, making it impossible for the company to contest the claim and stop the spread.
- The smartphone messaging application WhatsApp was used as a tool to target millions of Brazilian voters ahead of the October 2018 presidential election, deluging political messages. The missives, spread through the country by the millions, targeted voters before the election. A study[633] of 100,000 WhatsApp images found more than half, containing misleading or flatly false information.
- When data from 87 million Facebook users[634] (including that of 2.7 million EU citizens) were improperly shared with the political consultancy company Cambridge Analytica, data about sexual orientation, race, and intelligence were gathered by algorithms and used to micro-target and mobilise voters in the US presidential election and the UK referendum on EU membership[635].

Related cyberthreats:

---

[631] https://www.business2community.com/crisis-management/why-businesses-need-to-monitor-fake-news-sites-02095163, accessed November 2018.
[632] https://www.facebook.com/jaimie.potts.9/posts/10211895194040169, accessed November 2018.
[633] https://www.independent.co.uk/news/world/americas/brazil-election-2018-whatsap-fake-news-presidential-disinformation-a8593741.html, accessed November 2018.
[634] https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data, accessed November 2018.
[635] http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/628284/EPRS_ATA(2018)628284_EN.pdf assessed November 2018, accessed November 2018.

Cyber espionage

5.3 Web and browser based attack vectors

The high number of incidents with malicious cryptomining in 2018 requires revisiting and complementing what was described in last year ETL report about "compromising the web and browsers" attack vector. With the first introduction of JavaScript cryptocurrency miners running directly from browsers, it was quickly exploited by cyber-criminals. Since then, malicious cryptomining has been considered as a top threat, added into the top 15 in this year's ETL report. Cryptomining refers to a process in which, each time a cryptocurrency transaction is made, a miner is responsible for ensuring the authenticity of information and updating the blockchain digital ledger, in return of a financial reward. Basically, cyber-criminals use their victims' resources such as computing power, connectivity, and electrical power by exploiting their web browser to perform mining operations. More information about cryptojacking can be found in chapter 3.13.

A simple cryptokacking attack is illustrated below:

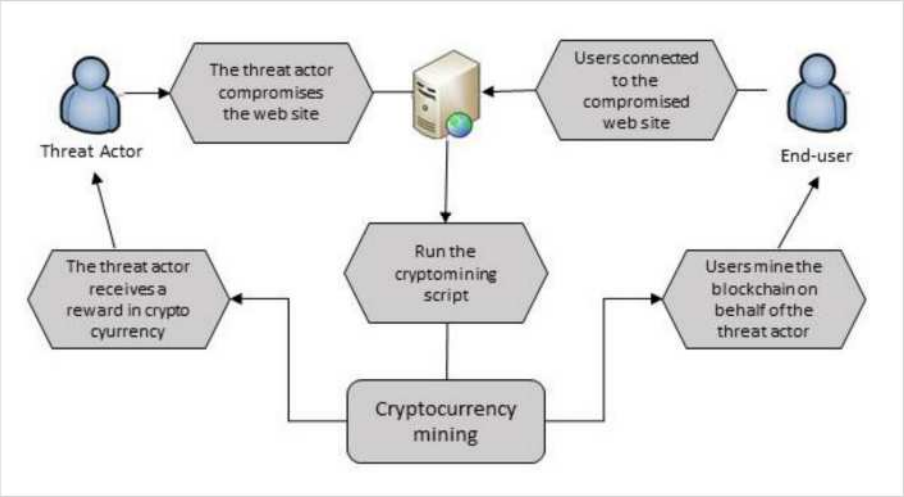


Figure 44: A cryptojacking attack

Example security incidents related to this attack vector:

- Researchers discovered[636] a new Linux crypto-miner botnet dubbed PyCryptoMiner spreading over SSH. The Monero miner botnet is based on Python and leverages Pastebin as command and control server when the original C&C isn't available. If all C&C servers of the botnet are not accessible, all newly infected bots are idle, polling for the botmaster's Pastebin page.
- The Blackberry Mobile site was hacked exploiting a vulnerability of Magento. The attackers install a Monero miner using the Coinhive library[637].

[636] http://securityaffairs.co/wordpress/67408/breaking-news/pycryptominer-botnet-miner.html, accessed November 2018.
[637] http://securityaffairs.co/wordpress/67503/hacking/blackberry-mobile-website-hacked.html, accessed November 2018.

- A report[638] published by the SANS Technology Institute reveals that attackers are exploiting a critical Oracle WebLogic flaw (CVE 2017-10271) to inject Monero cryptocurrency miners on victim's machines.
- A security researcher revealed the details of a RIG exploit campaign distributing malware coin miners delivered via drive-by download attacks from malvertising, exploiting the RIG Exploit Kit[639].
- Researchers revealed the details of a new campaign distributing a malware dubbed RubyMiner, turning outdated web servers into Monero miners[640].
- Researchers discovered[641] a newly malicious URL redirection campaign that infects users with the XMRig Monero cryptocurrency miner. The campaign has already victimized users between 15 and 30 million times.

Related cyberthreats:

Malware, ransomware, web application attacks, phishing, data breaches and drive-by-download attacks.

5.4 Fileless or memory-based attacks

Also known as "living-off-the-land"[642], fileless or memory-based attack is one in which an attacker uses existing software, allowed applications and authorized protocols to carry out malicious activities. Fileless attacks are capable of gaining control of computers without downloading any malicious files.

Characteristics of a fileless attack:

- Has no identifiable code or signature that allows typical antivirus tools to detect it. It also does not have a particular behaviour; therefore, heuristics scanners cannot detect it.
- Lives in the computer's RAM.
- Uses processes that are native to the operating system in order to carry out the attack.
- Can be paired with other malware.
- Able to circumvent application whitelisting. Fileless malware takes advantage of approved applications that are already in the system.
- May include a "dropper" or a script used in early attack stages for malware installation and for a wide variety of post-exploitation activities.

A simple fileless attack is illustrated below:

[638] https://isc.sans.edu/forums/diary/Campaign+is+using+a+recently+released+WebLogic+exploit+to+deploy+a+Monero+miner/23191/, accessed November 2018.
[639] https://www.scmagazine.com/researchers-spotted-malware-coin-miners-in-malvertising-campaigns/article/736315/, accessed November 2018.
[640] https://www.bleepingcomputer.com/ news/security/linux-and-windows-servers-targeted-with-rubyminer-malware/, accessed November 2018.
[641] https://www.scmagazine.com/millions-of-machines-download-xmrig-cryptominer-after-users-click-on-devious-links/article/739594/, accessed November 2018.
[642] https://www.symantec.com/blogs/feature-stories/your-next-big-security-worry-fileless-attacks, accessed November 2018.

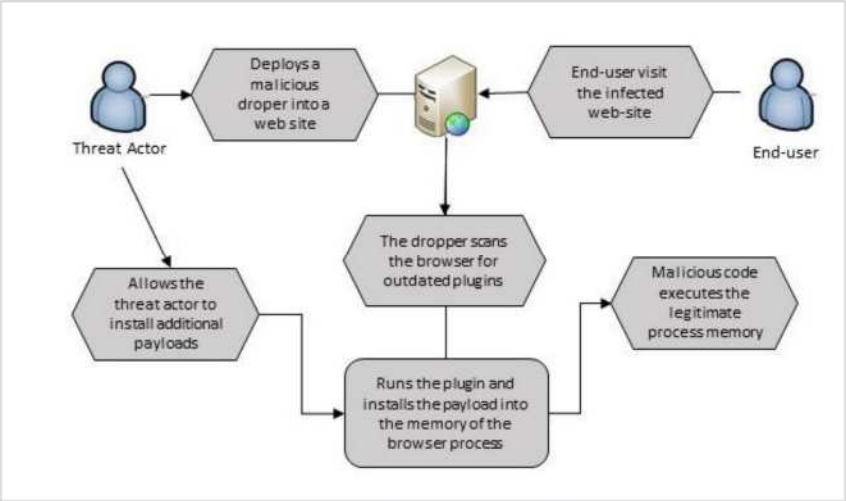


Figure 45: A fileless attack

Example security incidents related to this attack vector:

- In January 2018, security researchers uncovered[643] a campaign, dubbed Operation PowerShell Olympics, targeting organizations involved in the South Korea winter games, with the aim to control the infected machines. The researchers noted that the attacks used an open source stenography tool, to embed the PowerShell script into the image file, allowing the attackers to implant additional malware from a remote server.
- A security researcher identified[644] fileless attacks targeting servers and workstations, using PowerGhost and CactusTorch malware. PowerGhost, an obfuscated PowerShell script, plants itself in the targeted system's random access memory. Uses the WMI tool and the Mimikatz data extraction tool to escalate privileges and set up its mining operation. The CactusTorch fileless malware executes and loads malicious .NET files straight via the memory.

Related cyberthreats:

Malware, ransomware, malicious scripts and data breach.

5.5 Multi-staged and modular threats

Recent trends in multi-staged and modular malware attacks reveal how this type of attack is becoming increasingly sophisticated, versatile and persistent. VPNFilter, BlackEnergy, and CobInt are good examples of this type of attack. It uses different vectors, depending on a pre-assessment conducted to the victim's infrastructure, to initiate the attack. The VPNFilter, for example, is able to support the collection of intelligence about the victim and from the analysis, download additional malware to shape the attack dynamically.

List of known capabilities for multi-staged and modular threats:

- Self-propagates,

[643] https://www.zdnet.com/article/hackers-target-winter-olympics-with-new-custom-built-fileless-malware/, accessed November 2018.
[644] https://securitynews.sonicwall.com/xmlpost/powerghost-a-stealthy-miner-with-eternal-blue-component-for-spreading-further/, accessed November 2018.

- Self-destructs,
- Communicates anonymously,
- Behaves persistently,
- Obfuscates the origin,
- Downloads payloads and
- Installs in memory.

In July 2018, security researchers described VPNFilter as a sophisticated malware affecting 500,000 networking devices.[645]. The malware - initially affecting Ukrainian hosts - spread over 54 countries at an alarming rate. Researchers attributed this malware to a Russian state-sponsored hacking group Sofacy (also known as Fancy Bear and APT28).

The versatile and persistent behaviour of this malware on networking devices generated great concern among security professionals and authorities around the world. In its multi-stage and modular capabilities, it is able to support the collection of intelligence, misattribution and destructive cyberattack operations. Moreover, it has a range of capabilities including data exfiltration, spying on traffic and ultimately rendering the infected device unbootable. According to the researcher, the malware code overlaps with versions of the BlackEnergy malware, which was responsible for multiple large-scale attacks that targeted devices in Ukraine.

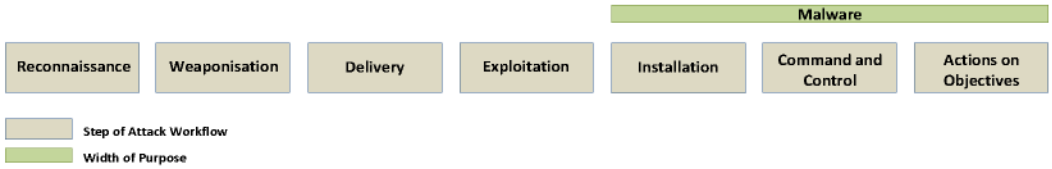


Figure 46: VPNFilter kill-chain

- **Installation** – The attacker injects malware into devices running firmware version based on Busybox and Linux. The main purpose is to gain a persistent foothold and enable the download and deployment of additional malware in a persistent way.
- **Command & Control** - Utilizes multiple redundant C2 mechanisms to discover the IP address of deployment servers, making this malware extremely robust and capable of dealing with unpredictable C2 infrastructure changes.
- **Actions on Objectives** – The attack is executed using a variety of capabilities such as file collection, command execution, data exfiltration, device management and firmware overwrite among others. Additionally, the malware introduces multiple modules serving as plugins providing additional functionality. The researcher identified two plugin modules: a packet sniffer for collecting traffic that passes through the device including theft of website credentials and monitoring of Modbus SCADA protocols and a communications module over the TOR network.

Typical attack vectors used:

1) Network propagation/lateral movement.
2) Exploitation of vulnerabilities.

[645] https://blog.talosintelligence.com/2018/05/VPNFilter.html, accessed November 2018.

3) Attacking the human element – Phishing.

Related cyberthreats:

Malware, phishing, data breaches, denial of service, exploit kits and cyber espionage.

6. Conclusions

6.1 Main CTI-related cyber-issues ahead

This chapter summarizes the CTI-related issues that have been identified during the 2018's threat assessments. They are either related directly to the assessed threats or they are consequences of those assessments. Moreover, some of those issues arise from experiences from the state-of-the-art in CTI, as they have been communicated/discussed within various interactions with CTI-practitioners. As opposed to some potentially interesting/valuable sources of threat predictions[646,647,648,649], this chapter does not provide any predictions per se. Instead, it consolidates identified needs that have to be performed in order to enhance efficiency of CTI. These activities are a consequence of the current threat landscape and the current CTI practices. Although some causality may be evident in the sequence of the points below, they are not listed according to any priority scheme, nor having any a weighting factor in mind. The issues mentioned below imply the conclusions provided in the forthcoming chapter (see chapter 6.2). They have been categorised according to their relevance with policy, business and technical matters.

In the reporting period, it has been assessed that **state-sponsored agents are allegedly changing attack practices**. They shifted their modus operandi towards lower levels of infrastructure components. This is being implemented through both hardware abuse and compromise of general-purpose components that are often outside the protection zones of organizations, such as ISPs, information brokers, cloud providers, network management services, etc. Just this year, several governments[650,651] introduced a ban and campaigned against the involvement of tech-giants such as Huawei and ZTE in building their 5G infrastructure, under the pretext of posing serious risks to their national security. Another element of their novel attack tactics includes targeted attacks at the user level: through social engineering, effective spear phishing attacks are being crafted. These changes in attack methods render sophisticated and expensive network intrusion methods obsolete and can be implemented with commonly available techniques and procedures. At the same time, their operations are difficult to spot, as they fall into the vast mass of attacks originated from other threat agents such as cybercriminals and hacktivists. These developments make evident that detection and mitigation methods for these types of attacks need to be accordingly adapted.

Non-targeted threats spreading contagiously in the cyberspace tend to last longer (or not to disappear at all). This is mainly due to the reduced adoption by individuals and organizations of cyber hygiene practices (cryptographic keys and user credentials protection, etc.), adherence to good security practices (revised security policies, two face authentication (2FA), etc.) and systems still operating without any security updates, to name a few. The same is valid to justify the lengthy time taken by many organizations to acknowledge and respond to an incident**. This situation urges organizations to include cybersecurity into their risk management functions** and identify clear strategies to anticipate and/or respond to crises.

---

[646] https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878/, accessed November 2018.
[647] https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html, accessed November 2018.
[648] https://www.boozallen.com/s/insight/blog/cyber-threat-predictions-2018.html, accessed November 2018.
[649] https://www.fortinet.com/blog/industry-trends/the-evolving-threat-landscape---looking-at-our-2018-predictions.html, accessed November 2018.
[650] https://techcrunch.com/2018/08/22/australia-bans-huawei-and-zte-from-supplying-technology-for-its-5g-network/, accessed November 2018.
[651] https://www.engadget.com/2018/11/24/us-huawei-warning-5g/, accessed November 2018.

Due to increased automation of many attack vectors, **end-users are under permanent exposure to a vast number of attacks**[652]. Given the weak protection in many end-user systems, it is likely that targeted individuals may experience a successful attack. The existing gap in cybersecurity knowledge and CTI in particular, makes affected end-users feel left alone with the mitigation of impact from successful attacks. It is imperative to close this gap by disseminating related knowledge to all intermediate elements in the delivery of services. CTI is definitely an important missing element in the protection of the entire chain of service delivery. New models of CTI knowledge delivery and automated means of cyberthreat mitigation are necessary in order to bridge this gap. Otherwise, the trust of end-users is at risk, especially when monetary impact is caused by successful attacks. An increasing number of such incidents have been encountered in the reporting period[653,654].

The above is also true for SMEs: the complexity of cyberthreats is raising with the combination of multiple payloads and stages, scalable architecture and a combination of a variety of delivery vectors in one single attack. Cyber criminals are also combining technical and non-technical attack vectors to make their campaigns more effective. **The diversity of profiles, skills and competencies required to formulate and implement a complete end-to-end cyber security strategy goes beyond the capabilities of the great majority of small and medium organizations**. Novel and affordable solutions will be required to automate many of the time-consuming manual tasks. Such solutions may be implemented via threat intelligence driven Managed Security Services or via seamless integration of threat intelligence services into end-device security solutions (i.e. CTI-as-a-Service).

Cybersecurity awareness and knowledge flows are often failing in the transitions between domains of responsibility. Variations in terminology, understanding of requirements and variating speed of relevant management cycles are the most common grounds for these failures. Numerous techniques have been identified to avoid such failures. These include the better interconnection among the various cybersecurity stakeholders, the better identification of "crown jewels", the use of horizon scanning activities and the use of scenarios as basis for cybersecurity assessments. Other factors enabling better knowledge flows are sectorial cybersecurity assessments, more targeted reporting and better sharing practices of relevant information. Nonetheless, in cases of distributed governance[655] it is necessary to implement measures that allow for the formulation of coordinated incentives, common understanding of strategic objectives and strategic requirements. It is clear that in those cases, the effort of connecting to stakeholders and anticipating the multiple perspectives involved in decision-making processes is key to success.

Cybercrime is reportedly originated from geographies with less restrictive laws/regulations to combat and prevent illegal activities outside their countries. The future protection of the digital economy, of a free and open Internet and transnational cybercrime reduction will require more effort for **coordinated cyber-diplomacy, LEA and defence cooperation, enforcing the international law in cyberspace and create homogeneous regulatory geographies**. Current activities in this direction are indicative of the importance of this issue. Yet, the abstention of some key cyberspace actors from those initiatives is a source of

[652] https://www-05.ibm.com/dk/think-copenhagen/assets/pdf/Koncertsalen_Abning_5_SteveCowley_Presentation.pdf, accessed November 2018.
[653] https://www.cshub.com/attacks/news/incident-of-the-week-phishing-scam-at-pa-bank-exposes-50k-accounts, accessed November 2018.
[654] https://www.channelnewsasia.com/news/singapore/phishing-scam-dbs-posb-customers-fake-sms-police-10957456, accessed November 2018.
[655] https://irgc.epfl.ch/risk-governance/page-139716-en-html/, accessed November 2018.

concerns towards the achievement of this goal[656]. Moreover, because cybersecurity is considered to be a utility, governments need to guarantee its continuous availability for all citizens. To this extent, CTI capability constitutes a common good that will need to be delivered to all interested parties, at least at a baseline level. Last but not least, **differences in legal frameworks are a burden in collecting cyberthreat intelligence**. In some countries, assessing the weaknesses of publicly available services is considered to be a criminal act. In order to facilitate the collection and maintenance of CTI, it will be necessary to remove such regulatory barriers.

While building CTI capabilities is a mainstream activity worldwide, **European bodies/organisations and member States are still at a low level of CTI maturity**. This fact is manifested by weak or missing references to CTI within policy documents and by the limited level of investments in relevant infrastructures and services. With most CTI sources being developed outside Europe (e.g. US), European organisations are significantly dependent on capabilities maintained mainly outside the continent. This is a threat to its sovereignty and its ability of self-determination with regard to the assessment of the cyberthreat landscape and the establishment of appropriate protection measures. And although some approaches to European CTI capabilities do exist[16,657,658,659,660], Europe lacks an overall strategy for the development of such capabilities and the enhancement of relevant skills. The establishment and further development of such capabilities is therefore seen as a high priority topic at the European level. Europe needs independent CTI capabilities based on self-collected data from the EU space. Moreover, response to CTI events has shown that **there is a high demand for bonding activities among European and international CTI providers**; and the exchange of information/experience on CTI good practices is very high in the wish list of various types of organisations.

Attacks to the supply chain have dominated the headlines for some time in 2018[573]. Supply chain attacks are happening in the transition phases of the development of complex systems and are targeting the weakest link in the chain. Though not new, these attacks have attracted the interest of cybersecurity experts due to their detection difficulty and efficiency[661]. The mounting pressure to have shorter time-to-market, to meet the demand and be cost effective, may lead to compromises during the initial stage of product research and development. But production phases are also at stake, especially due to globalisation of industrial production to geographic areas that are outside the political and diplomatic influence of western high developed industrial nations. The uncertainty about the successful implementation of cybersecurity and quality standards will persist, especially due to the emergence of IoT that connects cyber and physical spaces. **The threat landscape emerging from supply chain attacks is a major cybersecurity concern, especially for low-cost devices**.

Just as other cybersecurity disciplines, **CTI has not yet been properly "synchronised" to other important management cycles in organisations**, such risk management, corporate governance and data protection. Although asynchronous cycles are the root of problems in the communication of surfaced risks, it is also

---

[656] https://www.thenational.ae/world/europe/breakthrough-in-paris-as-51-states-agree-to-regulate-cyber-warfare-1.791103, accessed November 2018.
[657] https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cert-eu-presentation/, accessed November 2018.
[658] https://www.deutsche-systemhaus.eu/umbrella/?lang=en, accessed November 2018.
[659] https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf, accessed November 2018.
[660] https://www.cyberthreatalliance.org/, accessed November 2018.
[661] https://www.axios.com/homeland-security-supply-chain-task-force-6cf608ff-e180-4cfb-a308-c0fa35e73ead.html, accessed November 2018.

natural in all technology driven activities: often, technological projects develop own lives within organisations and may easily evade the attention of decision makers[662]. This shortcoming has been recognised among CTI experts. The mobilization of multidisciplinary stakeholders seems to be the right way for its resolution. Yet, a discussion forum where these stakeholders can voice their concerns needs to be created. Again, this is an opportunity for Europe to create such a forum and deliver a competitive advantage for the European internal market.

Cyberthreat intelligence has evolved in the last 7-8 years from the need to follow up on a rapidly changing cyberthreat landscape. This rapid development was purely technology driven and narrowly scoped. **Its relevance highly matured traditional intelligence has been recently recognized**. The advantages that can be materialised when coupling traditional intelligence and cyberthreat intelligence have not yet been implemented. Individual events in the reporting period[549] have demonstrated the increases in efficiency when combining these two disciplines. Though the deployment of cyberdefence practices may facilitate mutual fertilization between these two disciplines, public and private organisation will need to benefit from these synergies too. This is yet another opportunity for Europe - but also for international players -to implement a synergy that will boost cybersecurity to new quality and maturity level.

6.2 Conclusions and recommendations for this year's ETL report.

In this section, the conclusions of this year's ETL are being presented. They are divided into three categories, namely policy, business and research/education. This differentiation is indicative for the type of actors that would need to take up actions to cope with the points made below. Though there is a large variety of organisations matching each of these categories, they are not further specified in this report. This would go beyond the scope/purpose of this document. We believe, however, that it is quite straightforward for interested readers to understand what type of organisation would be relevant for the points made in each category, especially when national, sectorial and educational peculiarities are being taken into account. This year's conclusion are not overlap-free to the ones of previous years. However, new developments have helped us to make them more specific/targeted.

Policy conclusions

- Governments, EU Member States and EU Institutions need to facilitate training of CTI staff. Moreover, due to the increased market needs for this skill and the competitive packages offered by industry, administrations will need to develop employment conditions that can attract talents and lead to staff retention.
- EU and EU Member States will need to invest in CTI capability building by means of skills development and infrastructure (technical, human). Such activity will contribute towards the necessary improvement of European CTI capabilities and will increase independence. This will enhance the level of CTI knowledge quality and turn it to a more effective resource towards successfully managing critical events within Europe, especially the ones targeting critical infrastructures.
- The quality of CTI knowledge heavily depends on the ingested information. Several barriers do exist in Europe and worldwide that hinder access to such information: the existence of diversified regulatory spaces, the unavailability of reliable incident information and deficiencies in information sharing. A Policy should enable better ingestion of information to produce CTI by removing legal and regulatory barriers.

[662] http://www.spiegel.de/netzwelt/netzpolitik/apple-und-der-boersensturz-weg-von-hardware-hin-zu-software-a-1239605.html, accessed November 2018.

- To a certain extent, CTI is considered a public good. Administrations will need to subsidize the creation of CTI knowledge centres and support the development of good practices and tools for various types of organisations. This will be a direct contribution to enhance the protection of critical assets.
- Currently, many players join cyber-activities in the cyberspace. Administrations will need to take proactive measures to avoid distortions that may be caused by overlapping activities and responsibilities[663]. Such actions should contribute towards CTI information sharing and avoidance of duplication of work among states.
- Administrations will need to make efforts to close the gap between end-users and high-end CTI operators. This will require the availability of CTI knowledge and services in a form that is digestible by non-expert users.
- High-level horizon scanning activities that are based on emerging cybersecurity challenges and emerging threats need to be introduced and taken into account when policy decisions are being made. Such activities should be based on scenario development and may provide valuable insights for impact assessments made in the framework of regulatory activities.

Business conclusions

- Businesses will need to develop viable CTI services to cover a wide range of enterprises that possess low to no CTI skills. Such services may be oriented towards various maturity levels and provide seamless automation for the protection of assets based on CTI information.
- Businesses will need to define processes for CTI knowledge management. Such processes need to be in sync with other cybersecurity processes and in particular with risk management. They aim at enhancing the agility of processes is to follow the agility of CTI knowledge management.
- Businesses need to respond to the trend of cyber-attack automation. The developed solution should consist of tools that automate the adaptation of controls based on CTI-feeds. Such solutions will be tailored to the needs of enterprises with low security budgets.
- Businesses should estimate the risks emerging from potential cyber-attacks to their customer base by extrapolating their impact. By taking into account potential losses that can be experienced by users, they will reduce attack surfaces and help end-users protecting their assets. Such an approach will enhance user trust and remove barriers to technology deployment. This is particularly important in areas such as IoT, eHealth and mobile computing.
- Businesses should be aware of supply chain threats. Such threats are prevalent in complex product development processes involving multiple providers. While the development of qualitative criteria for the various development phases may help, it is important to assess the end-to-end characteristics of used components. Light certification processes of the components used may be a further option for the reduction of exposure to such threats.

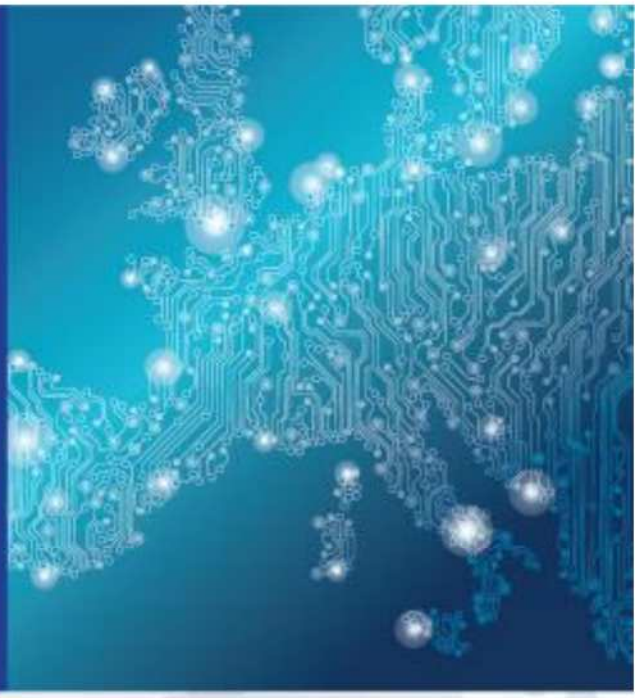
Technical, Research, Educational conclusions

- Developing threat assessments on a sectorial basis will be necessary. Such assessments will be oriented towards specific technology areas and will help users of these sectors managing threats on those environments.

[663] http://www.egmontinstitute.be/cyber-diplomacy-making-international-society-digital-age/, accessed November 2018.

- Cyber-crime evolves towards professionalization in various verticals. Moreover, cyber-criminals combine their skills to increase automation and efficiency of attack vectors. Defenders will need to better understand these developments and provide new methods for detection. Novel disruption methods need to be developed. Such methods will need to take into account defences for all phases in the kill-chain, as opposed to current practices that are triggered mostly after exploitation has been detected.
- There is a pressing need for common vocabulary in the area of CTI. Currently available threat taxonomies[664] and common frameworks[91], however, they are often side-products of threat assessment projects and are not systematically maintained/updated and/or consolidated.
- Efficiency of cyber-attacks depends on the existence of vulnerabilities in targeted systems. Vulnerability management practices need to be part of defence strategies. This is manifested through a large number of vulnerabilities in end-user systems and services and the long time-windows for patching known vulnerabilities. The cyber-security community will need to develop better means for the detection and removal of vulnerabilities by also covering geographical viewpoints (e.g. the European space).
- There are many improvements necessary at the ingestion level of CTI knowledge. Better sharing schemes and better analysis of known incidents are major avenues to achieve this goal. It is necessary to combine incident reporting and CTI processing. This will enhance the quality and accuracy of CTI.
- CTI needs to be combined with related disciplines to enlarge scope and include additional sources. In 2018, the combination of CTI and traditional intelligence has shown a great potential towards threat mitigation. Yet, mutual fertilisation from the combination of these two areas is at an initial development stage. The development of methods combining these areas needs to be enforced.

[664] https://www.sans.org/reading-room/whitepapers/threatintelligence/evaluation-comprehensive-taxonomies-information-technology-threats-38360, accessed November 2018.



ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-250-9
ISSN: 2363-3050
DOI: 10.2824/967192