RAPID7

RAPID7 RESEARCH

QUARTERLY THREAT REPORT



By Michelle Martinez, Senior Threat Intelligence Analyst, Rapid7
Kwan Lin, Senior Data Scientist, Rapid7
Bob Rudis, Chief Data Scientist, Rapid7

November 13, 2018

Wiz - EXHIBIT 1141
Wiz, Inc. v. Orca Security Ltd.
IPR2024-01190

Q3 2018

CONTENTS

Introduction 5

Key Observations: threat events 7

- Adversaries on Holiday 7
- Sizing Things Up 7
- A Plethora of Poisoned Packets 8

Key Observations: Qualified Incidents 11

- Hook, Line, and Sinker 11
- Street Cred[s] 12
- Banking [Trojan] Breakdown 13
- Top Detections 14

Key Finding: Planetary-Scale Intelligence 15

- "Previously, on Planetary-Scale Intelligence…" 15
- Eyes on the VNC/RDP Prize 16
- "I'm Not Dead Yet" 17

Our Recommendations 19

- Clean House 19
- Back to School 19
- Mind the [DNS] Details 19
- Better Watch Out! 20

Appendix 21

About Rapid7 33

WHAT IS A THREAT?

We throw the term “threat” around a lot, so it’s important to define exactly what it is we mean.

When there is an adversary with the intent, capability, and opportunity, a **threat** exists.

When two or more of these elements are present (e.g., intent and capability, but no opportunity), we call it an **impending threat**, because there is just one missing piece before it becomes a true threat.

When there is just one element present (e.g., an opportunity in the form of a software vulnerability), we call it a **potential threat**. There is the potential for it to turn into a true threat, although there are additional components that need to come to fruition before it has a real impact to most organizations.

INTRODUCTION

It's harvest time (at least here in the United States), and as we prepare to reap the bounties of the land, so too have we seen attackers make good use of the exploits they've sown and infrastructure they've co-opted. The credential compromises and remote access attempts of Q2 have ripened into suspicious service logins and lateral movement actions involving credentials, along with increases in the presence of malware on systems.

Summertime generally means vacation time[1] and as a result there's a definite slowdown in threat events involving user interaction. Other 2018 Q3 highlights include:

- Continued use of PowerShell in- and post-compromise;
- Detected Emotet/Hedeo use in 70% of malware-oriented incidents in September; and,
- The continued threat of memcached being used in amplification attacks, along with Mirai letting us know "it's not dead yet."

Plus, we'll keep you updated on the the status of EternalBlue-related campaigns and other notable characters from previous reports. So, grab a steaming mug of mulled cider and read on!

For those just discovering this resource, our quarterly threat reports cover three core areas:

1. What the raw threat event landscape looked like for our Managed Detection and Response customers (so you can get a feel for event types, volume, and velocity to compare against your own threat event logs);
2. How those raw threat events manifested into distilled/qualified incidents that required a response by security operations teams; and,
3. A review of the most critical internet-facing threats.

We're also trying something new this time around and including an appendix of all of the host-, URL-, and IP-based indicators of compromise here and over at our public GitHub repository[2], broken down by the associated incident threat category.

You can always reach out to research@rapid7.com for more information on any topic in any of our reports.

---

[1] The vast majority of our threat events involve organizations in North America

[2] https://github.com/rapid7/data/tree/master/threat-report/iocs/2018-q3-iocs

For Q3, both large and small organizations faced similar volumes (percentage-wise) of events directly involving human interaction.

KEY OBSERVATIONS: THREAT EVENTS

Adversaries on Holiday

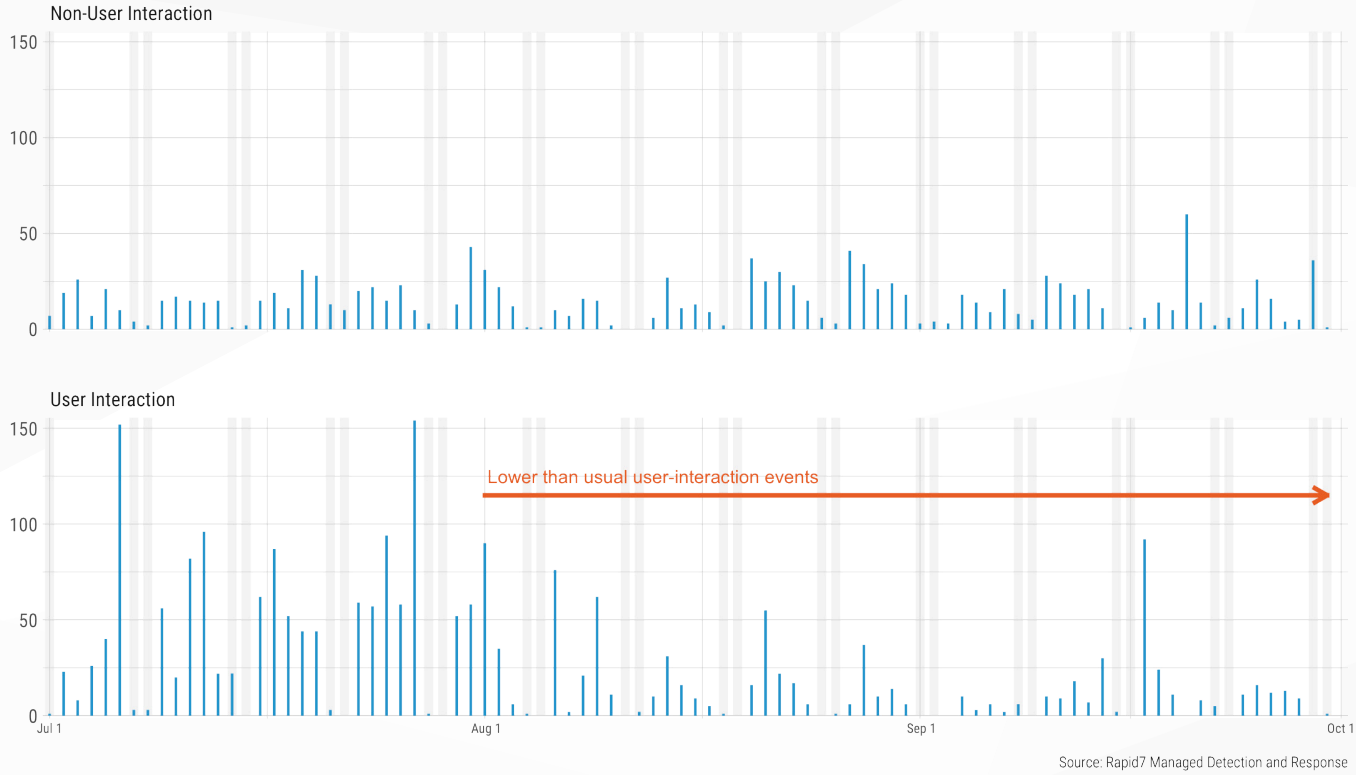
In light of the multi-year standout core pattern of threat actors attacking the human layer of organizations to gain a foothold within, we've revamped our incident event distribution charts to distinguish those involving or requiring user interaction from those that do not. The result is Figure 1, and we can glean at least two findings from this updated view.

First, user interaction events—apart from a few outliers—dropped off during August (the last major vacation month for the U.S.) and September (when Hurricane Florence and Tropical Storm Gordon hit). Our prediction for Q4 is that we'll see a return to "normal" levels, but stay tuned, since a continuation in this drop-off pattern may be a signal that attackers are indeed dramatically shifting tactics.

The second finding fits into the "Captain Obvious" category since it's just pointing out that most malicious events still require user interaction. We'll put this into more context in Q4 when we recap the year and look back on 2018 with a more detailed breakout view.

Figure 1: Q3 Incident Distributions

Across all organizations and industries. [Gray bars represent weekends.]



Source: Rapid7 Managed Detection and Response

Finally, note the maximum spikes in early August and mid-September. If you're drilling your Security Operations team based on the standard <10 threat events per day and are not throwing a mass-event curveball their way every so often, they likely won't be prepared to handle a spike to ~85 real events in a given day (which one organization did, in fact, face in Q3).

Sizing Things Up

For Q3, both large and small organizations faced similar volumes (percentage-wise) of events directly involving human interaction, and both the rattle and rhythm of more subtle attacker actions. However, they diverged significantly when it came to events that were triggered by InsightIDR's more advanced Attacker Behavior Analytics (ABA) and network-level actions.

Initially, the low percentage of Remote Entry-related events for large organizations and fairly high percentage for small organizations (Figure 2) had us scratching our heads. A typical component of this category is attackers aiming for access via external systems, and large organizations unsurprisingly offer a larger attack surface. However, digging in a bit, we noticed that the vast majority of events in both size categories were authentication attempts from multiple countries. While relying solely on IP geolocation and adopting a strategy of geofencing access to resources should not be adopted hastily, this strategy may have some immediate benefit for organizations that have a high confidence in where their employee-, contractor-, partner-, and general user-base populations originate from.

The most straightforward way to glean takeaways from this chart is to compare the differences in frequencies between large and small organizations within a given event category, then compare what we've recorded with (or "against") what you observed in your organization. As a reminder, we define a large organization as one with 1,000 or more monitored assets, and a small organization as one with fewer than 1,000 monitored assets. Appendix A has all the detail on which threat events fall into a given threat group.

Figure 2: Q3 Incident Threat Event Frequency

Percentages represent distributions of detected threat incident groupings within organization size

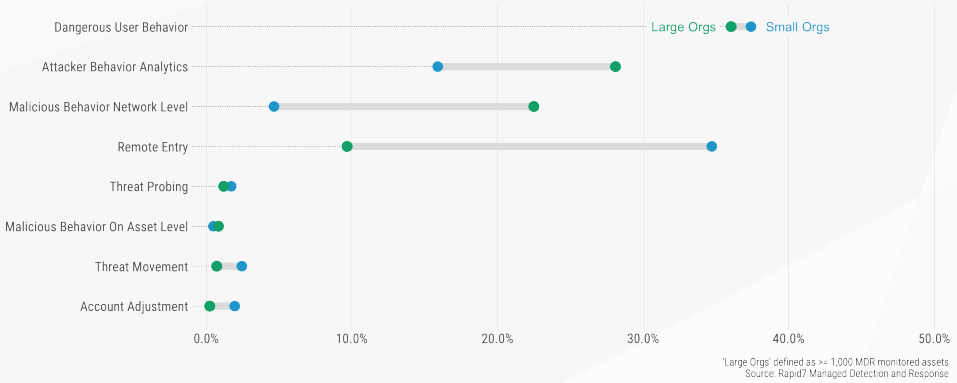
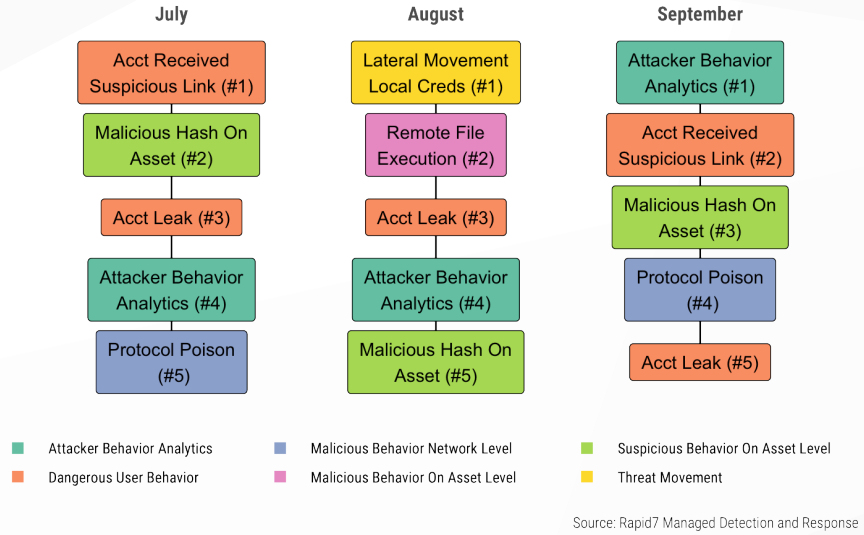


Figure 3: Top 5 Threat Events Per Month

Across all organizations.



Source: Rapid7 Managed Detection and Response

A Plethora of Poisoned Packets

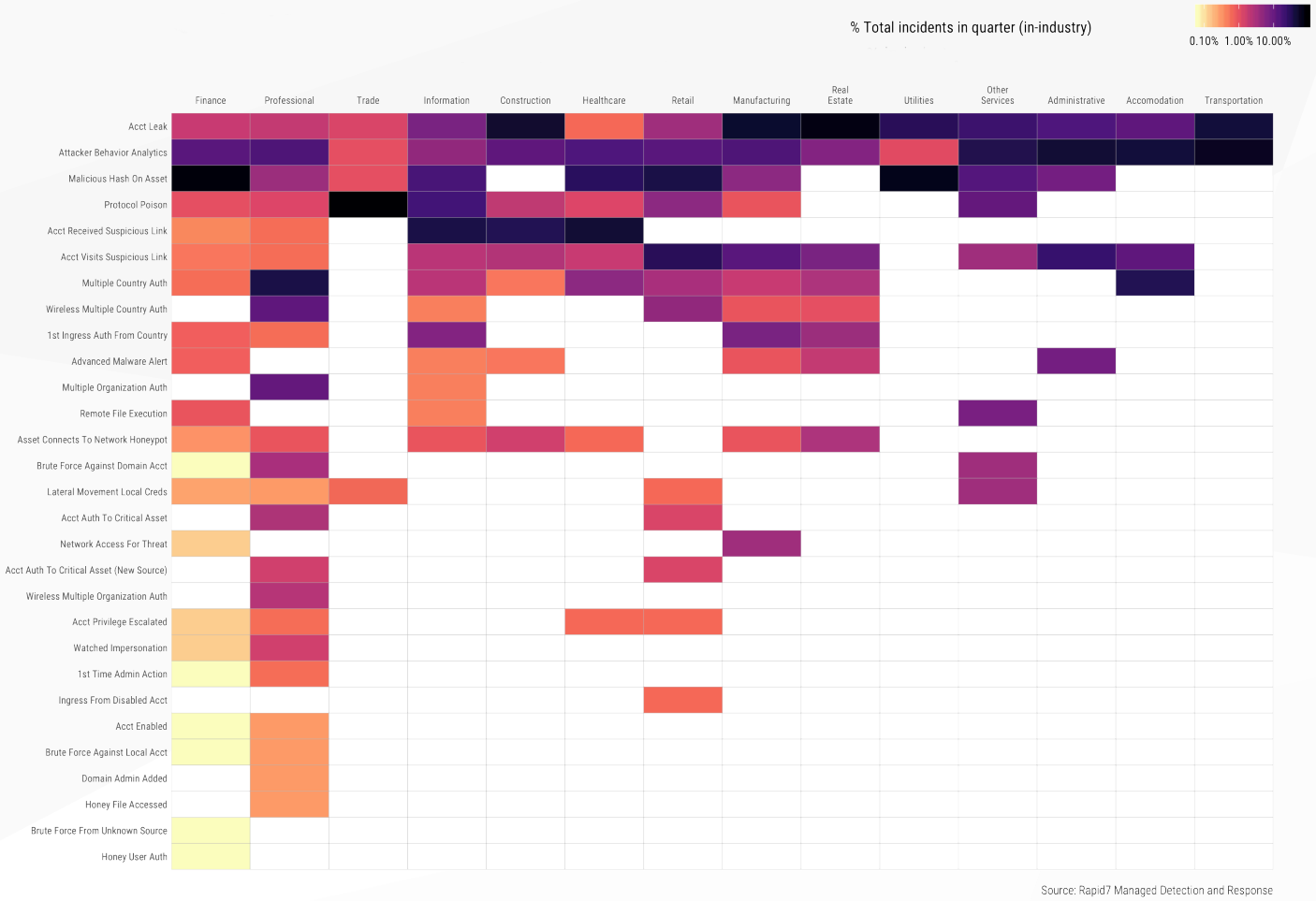
We enumerate the top five threat events per month (Figure 3) to get a feel for how attackers shift their focus throughout the year, and this quarter seems to be shaping up as the "aye, they got a foothold and are burrowing deep" quarter. An especially interesting development is "Protocol Poison" making it into the top five twice. The general principle behind protocol poisoning is to use specially crafted software placed to "confuse" nodes on a local network, and then cause them to route network data through it to facilitate the capture of credentials, hashes, and/or general data. You can find out more detailed information on how to detect and prevent this type of attack over at MITRE's ATT&CK Framework guidelines on DNS Poisoning[3], LLMNR/NBT-NS Poisoning[4], and Network Sniffing[5].

The "Top 5" lists come from our corpus of threat events that arise during the quarter. We modified the industry threat event heatmap (Figure 4) for this report just a tad by rolling up organizations in industries with a small percentage of threat events into an "Other Services" category. This was done to both reduce the complexity of the heatmap and to avoid making unsound statistical observations for those industries.

[3] MITRE ATT&CK DNS Poisoning Technique — https://attack.mitre.org/techniques/T1382/
[4] MITRE ATT&CK LLMNR/NBT-NS Poisoning — https://attack.mitre.org/techniques/T1171/
[5] MITRE ATT&CK Network Sniffing — https://attack.mitre.org/techniques/T1040/

Figure 4: Q3 Threat Event Distribution by Industry

Normalized by number of events per organization per industry for Q3 2018. Columns sum to 100% in-industry.



Source: Rapid7 Managed Detection and Response

One way to use this heatmap is to find your industry and use the event descriptions in Appendix A to benchmark your metrics with that of your aggregate peers. The Rapid7 InsightIDR "Malicious Hash on Asset" event signals that known malware was identified, and the chart shows this was a fairly major event type across all industries in Q3 (it generally is in the top 5 each quarter). The 2018 Q3 Qualified Incidents section provides a deeper-dive into what types of malware our customers encountered and also provides some context into how malware events have evolved year-to-date.

For some sectors, these pages seem like they're nonstop events across the quarter, while others only see them sparingly.

KEY OBSERVATIONS: QUALIFIED INCIDENTS

An incident is: a breach of a system's security policy in order to affect its integrity or availability; and/or the unauthorized access, or attempted access, to a system or systems; and is made up of one or more of the threat events described in the previous section. Rapid7 Managed Detection and Response (MDR) analysts take the discrete threat events observed within a customer's organization and mix them together with current threat intelligence and knowledge of the organization's business processes and policies. They then apply their crafting skills to turn them into qualified (i.e., non-false positive) incidents.

Figure 5: Phishing [Page] Hotspots

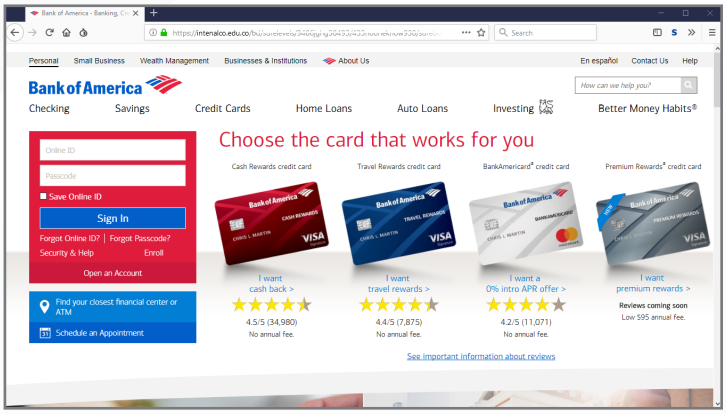
Color scale/percent-label represent percent of Q3 in-industry incidents involving a given phishing page.

	Accomo-dation	Admin-istrative	Con-struction	Enter-tainment	Finance	Health Care	Infor-mation	Manu-facturing	Mining	Other Services	Profes-sional	Real Estate	Retail	Trade
Adobe Login			1%			2%	1%						3%	
Apple Id					<1%			1%						
Bank of America		4%									<1%			
CareerBuilder					<1%									
Docusign		4%				2%	1%	3%			1%	4%		
Dropbox			1%	16%		2%						4%		4%
Exchange						2%								
G Suite Login					<1%		2%							
Generic Login		4%	5%		4%	2%	3%				<1%	4%	7%	
Maersk Shipping Login						2%								
Microsoft	12%	8%	13%		5%	2%	2%	6%		25%	<1%	4%	1%	8%
Netflix Login					<1%									
Office 365	6%	4%	23%		4%	4%	1%	3%	11%		2%	4%	3%	
One Drive			13%		8%	6%	4%	4%	11%		6%	12%	4%	13%
SharePoint Login			1%		1%			1%						
Wells Fargo								1%						
WeTransfer						2%								4%
Windows Defender			1%								<1%			

One example of such a scenario is a phishing campaign against an organization that results in one or more individuals being compromised, after which attackers drop malware onto systems and spread out on the network with lateral movement. A single-incident scenario such as this one may be made up of 10 or more InsightIDR individual threat events. In fact, we mention this scenario because it's No. 1 this time around (see "Hook, Line, and Sinker").

Hook, Line, and Sinker

Figure 5 is the Q3 catalog of "fake login" phishing pages used against the organizations in our corpus. For some sectors, these pages seem like they're nonstop events across the quarter, while others only see them sparingly. These fake login pages are often very convincing:



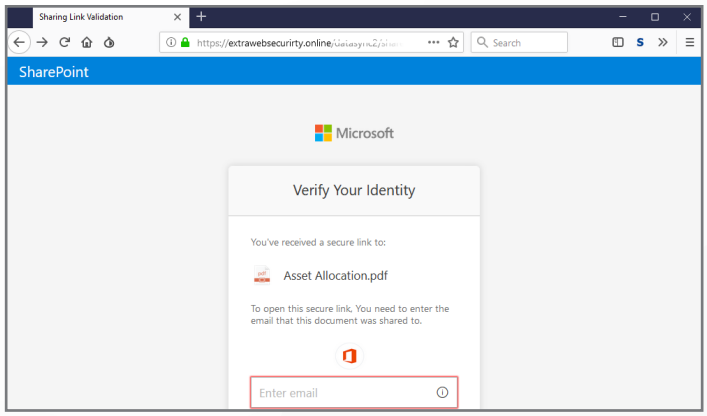


Image 1 (left):

Partial IOC[1]: https://intenalco[.]edu[.]co/PATH-READACTED

Image 2 (right):

Partial IOC: https://extrawebsecurity[.]online/PATH-REDACTED

[1] Indicator of Compromise — https://insightidr.help.rapid7.com/docs/threats

Readers with a keen eye for detail likely noticed the sketchy URLs in those screen captures, but both of those examples have "*everything's great!*" green lock icons in the address bar, meaning humans in a hurry may miss such subtle details. Furthermore, the green lock icon is with us for a while[6], despite how easy it is for attackers to obtain trusted website security certificates for free. Potentially compounding the confusion is an initiative by browser makers to do away with presenting URLs entirely[7].

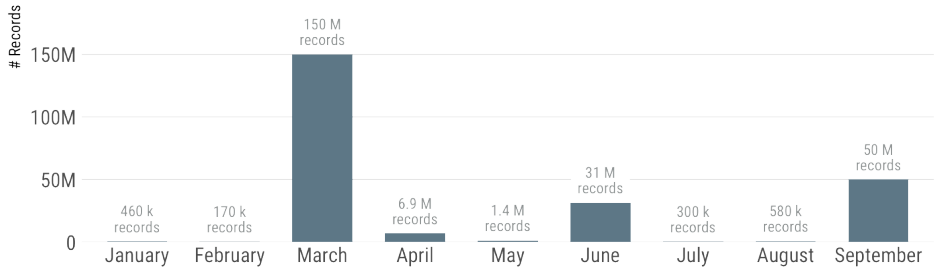
Despite the proliferation of free website certificates and forthcoming reduced opacity in what link you're actually visiting, one way to empower your front-line defenders (i.e., your entire employee and contractor base) is to show them samples of these fake login pages as your incident handlers encounter them, then give them the information and tools necessary to help distinguish good from bad. You may even want to consider ensuring your workforce is aware of any active campaigns targeting your organization. More mature organizations can explore investing in modern machine learning-based and cooperative content-oriented block list feeds/technologies, which may help reduce overall encounter rates for these types of phishing lures. Finally, most "enterprise-grade" cloud application providers support multi-factor authentication. If your organization does not use multi-factor authentication as a means of gating access to cloud resources, consider adding it into your 2019 budget and program development calendar.

Street Cred[s]

In Q2, we noted how organizations were feeling the pain due to the nonstop breaches resulting in record loss. Figure 6 shows the monthly breakdown of these events as catalogued by the Privacy Rights Clearinghouse.

Figure 6: 2018 Breached Record Count Per Month

Monthly median breach count involving record loss = 17
156 total breaches involving record loss since 2018



Source: Privacy Rights Clearinghouse <https://www.privacyrights.org/data-breaches>

If we compare this with Figure 7, which focuses on the top four qualified incidents per month since January, there's a definite pattern of increased notifications about compromised credentials in organizations shortly after each monthly spike[8]. However, attackers—armed with said credentials and new ones from direct phishing campaigns—are spinning credential straw into foothold gold as they gain access to internal systems and begin to move around. Of particular interest is the steady trend of malware being installed on systems, now surpassing the percentage of incidents involving them in previous months.

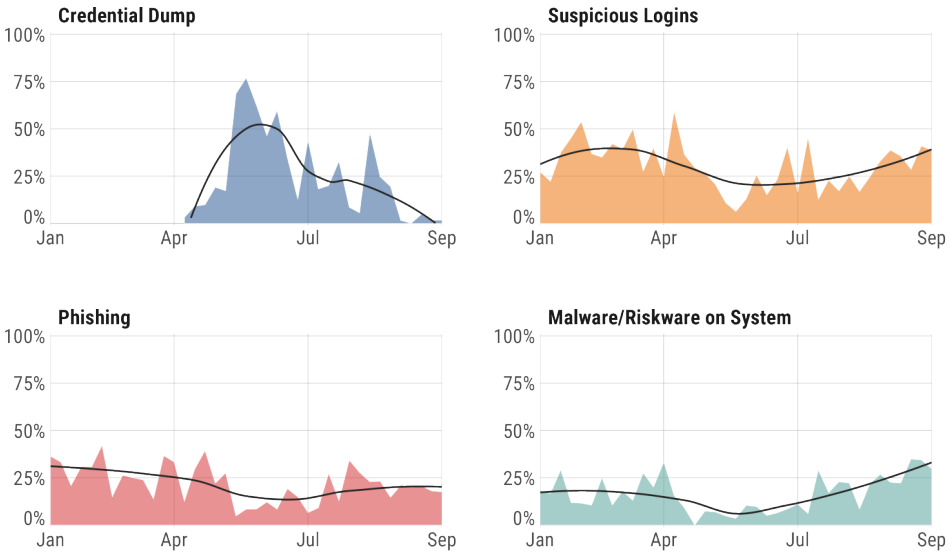
[6] Google Chrome says goodbye to green 'Secure' lock on HTTPS sites" — https://www.cnet.com/news/say-good-bye-to-that-green-secure-lock-on-google-chrome/

[7] "Google Wants to Kill the URL" — https://www.wired.com/story/google-wants-to-kill-the-url/

[8] Watch this space in the Q4 report to see if this holds true for October 2018.

Figure 7: 2018 Top Four Qualified Incidents Per Month

Organizations faced increased on-device operations and lateral movement attempts by attackers this quarter.



On the plus side, the detection technologies in these organizations are catching these malicious binaries. On the negative side, we don't have insight into the detection deficit[9] for these discrete events, so we can't say how long malware lingered before being identified.

It's important for you to capture and use these types of incident metrics in your organization to enable micro-adjustments of your defense strategies and processes as the days, weeks, and months roll on.

Banking [Trojan] Breakdown

In September, just over half of the qualified incidents involving malware were directly related to Emotet+Heodo campaigns and occurred across an array of industries (i.e., construction, finance, healthcare, information, manufacturing, professional, real estate, utilities).

In July, US-CERT issued an alert[10] about a powerful malware family known as Emotet[11] as a result of seeing elevated levels of successful attacker campaigns across a large number of state, local, tribal, and territorial governments, as well as private and public sector organizations that have seen remediation costs close to an average of $1 million (USD) per incident.

The entry point for Emotet is via malicious spam ("malspam") or phishing emails that either impersonate well-known third-party sites or even brazenly try to mimic your own organization's content/style. Once it gets on a system, it cloaks itself from traditional anti-malware solutions, embeds malicious code in otherwise benign running applications, and applies a Swiss Army knife of utilities that are capable of siphoning off emails, stored credentials, and other sensitive data. Once fully embedded on a node, this malware then tries to spread across the network.

In September, just over half of the qualified incidents involving malware were directly related to Emotet+Heodo campaigns and occurred across an array of industries

[9] In this case, the "detection deficit" is defined as the time-delta between when an attacker managed to install the malware on one or more systems and when said malware was detected and/or removed.

[10] https://www.us-cert.gov/ncas/alerts/TA18-201A

[11] https://researchcenter.paloaltonetworks.com/2018/07/unit42-malware-team-malspam-pushing-emotet-trickbot/

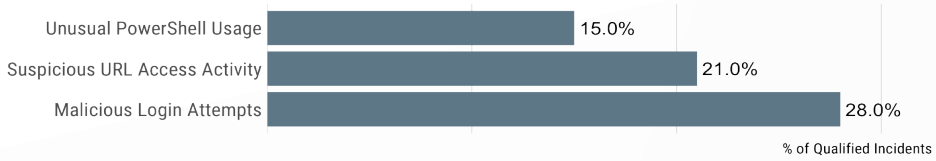
The US-CERT alert included a substantial amount of guidance to help prevent initial infections and the spread of existing ones. Key recommendations to consider prioritizing are:

- Implement Domain-Based Message Authentication, Reporting & Conformance (DMARC), and a validation system that minimizes spam emails by detecting email spoofing using Domain Name System (DNS) records and digital signatures.
- Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
- Mark external emails with a banner denoting it is from an external source. This will assist users in detecting spoofed emails masquerading as internal communications.
- Consider blocking file attachments that are commonly associated with malware, such as .dll and .exe, and attachments that cannot be scanned by antivirus software, such as .zip files.
- Adhere to the principle of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.
- Do not knowingly log in to infected systems using domain or shared local administrator accounts, even if it's just to assess the damage. Doing so gives away your password hash to any malware that cares to harvest it.
- After reviewing systems for Emotet indicators, move clean systems to a containment virtual local area network that is segregated from the infected network.
- Because Emotet scrapes additional credentials, consider password resets for other applications that may have had stored credentials on the compromised machine(s).

Top Detections

Incidents and breaches are not the result of supernatural acts performed by malicious mages. Threat actors send emails, execute code, and make network connections to achieve their goals. The quicker defenders can detect these signals, the faster they can neutralize the threat.

Figure 8: 2018 Q3 Top Detection Techniques



The most successful detection techniques for Q3 (Figure 8) were the identification of unusual Windows PowerShell[12] usage (15% of all incidents), identification of users visiting suspicious URLs (21% of all incidents), and login activity from country origins or cloud/VPN provider origins that did not fit within the traditional access patterns of the target organizations (29% of all incidents).

To make use of this newfound knowledge, your security controls must be able to record the events (and associated event metadata) that enable such detections. If any of these are blind spots in your current setup, now would be a good time to add support for additional coverage to your 2019 budget and project plans.

[12] https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6

KEY FINDINGS: PLANETARY-SCALE INTELLIGENCE

Rapid7's Project Heisenberg[13] has over 150 honeypot nodes spread across the internet, watching for signs of attacker activity and analyzing attacker behavior and methodology. Our Project Sonar[14] nodes scan the internet on a plethora of ports and protocols designed to discern service composition, configurations, and exposure[15].

"Previously, on Planetary-Scale Intelligence…"

MikroTik Madness Abated (For Now)

Regular readers will remember our deep dive into the massive MikroTik compromise back in the 2018 Q2 Threat Report. Rapid7 Labs provided a list of vulnerable systems with associated ownership metadata to the Brazil CERT[16], and through a combination of their efforts—along with reports of a "grey hat" violating[17] virtually every computer fraud and abuse bit of legislation across the globe—we can confirm that follow-up scans show the previously noted cryptocurrency miner injection campaign to be almost completely neutralized. That doesn't mean everything is fine. MikroTik equipment is inexpensive, fairly powerful, and easy to [mis]configure. A fresh crop of vulnerabilities were disclosed in August (and updated just before the publication of this report), including another remote code execution bug. This means any malicious campaign that makes use of MikroTik equipment has fresh fodder to work with.

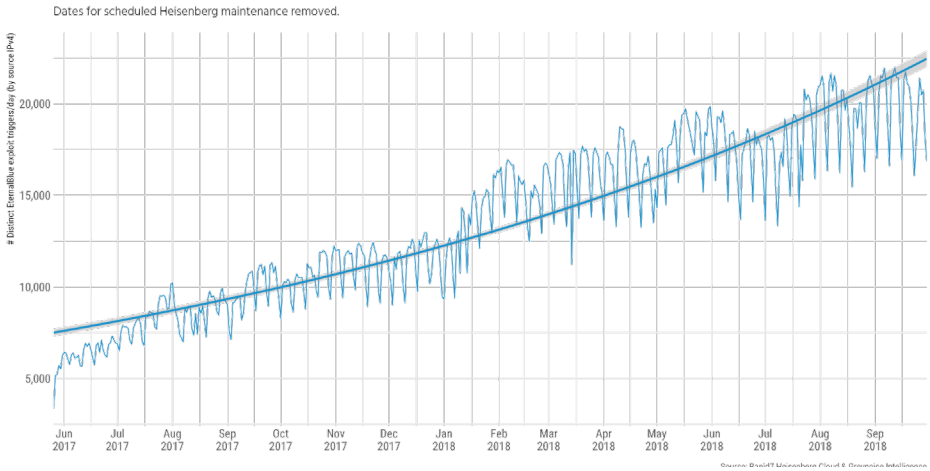
If you have been the victim of one of the campaigns, or a victim of the "grey hat" attacker, your best bet it to revert your impacted devices to base firmware levels, fully patch it to current levels, use a better base configuration, and monitor MikroTik's site for updates.

EternalBlue Campaigns Continue

Figure 9 shows a continued elevation in probes and attacks by attackers in search of vulnerable Microsoft systems on the internet.

Figure 9: Daily Unique EternalBlue Exploit Attempts

Dates for scheduled Heisenberg maintenance removed.



[13] https://www.rapid7.com/research/project-heisenberg
[14] https://www.rapid7.com/research/project-sonar/
[15] We exhaustively define what "exposure" means in our annual National Exposure Index reports — https://www.rapid7.com/info/national-exposure-index/
[16] https://www.cert.br/en/
[17] "Internet vigilante claims he patched over 100,000 MikroTik routers already" — https://www.zdnet.com/article/a-mysterious-grey-hat-is-patching-peoples-outdated-mikrotik-routers/

Furthermore, there are still hundreds of thousands of vulnerable and likely infected Microsoft file servers spread across the internet helping to keep this particular bane alive.

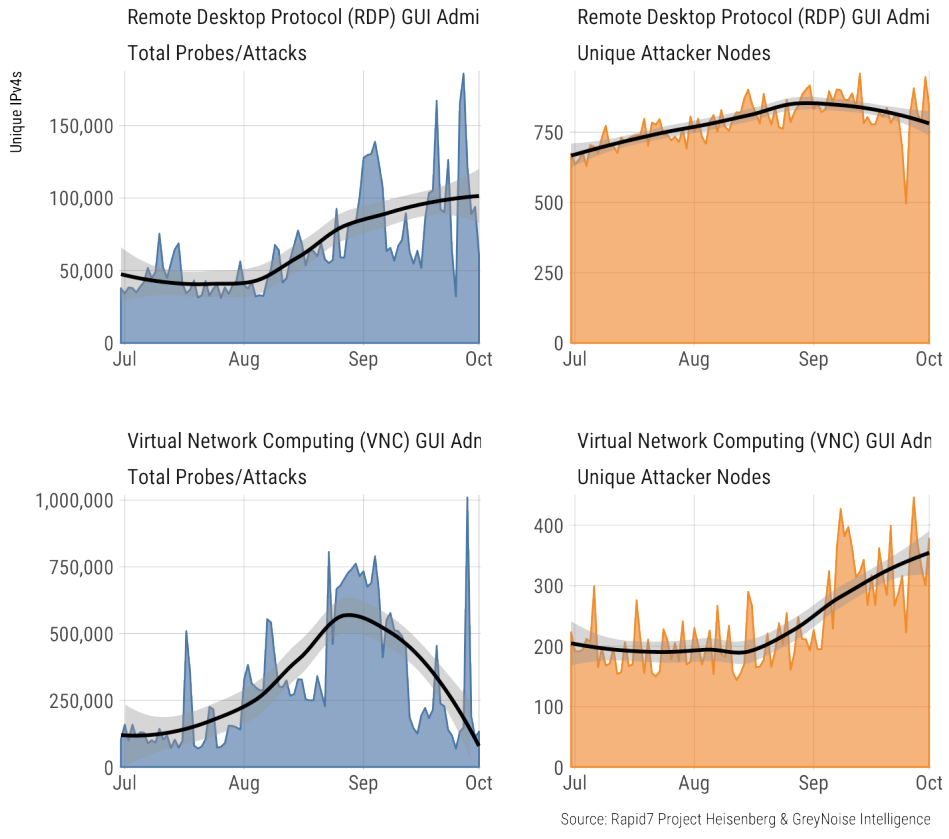
October 2018 marks the one-year anniversary of WannaMine[18], which is a cryptocurrency miner based on the exploit code in EternalBlue. Attackers are increasingly morphing this malware base to cover new ground and take advantage of organizations that still have not developed a solid defensive strategy to thwart it. Rapid7 MDR incident responders have handled customer incidents involving WannaCry[19]—yes, that WannaCry—in each and every quarter to date in 2018.

It is vital that you look in every nook and cranny for vulnerable systems and devices, including printers, embedded file servers, manufacturing equipment, and anything else that may have slipped through the cracks. The UK Department of Health & Social Care (DHSC) recently released[20] an update to its post-WannaCry attack remediation progress from back in 2017, noting that damage and cleanup efforts have cost over $100 million (USD).

Eyes on the VNC/RDP Prize

Figure 10: VNC and RDP Unique Attack Node vs. Total Probes/Attacks

Note: Free Y Scales



Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

[18] https://www.pandasecurity.com/mediacenter/pandalabs/threat-hunting-fileless-attacks/
[19] https://blog.rapid7.com/tag/wannacry/
[20] "Securing cyber resilience in health and care" — https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

The Q2 2018 Threat Report took us on a deep dive into the spate of Windows Remote Desktop Protocol (RDP) attacker activity. This quarter, our Heisenberg nodes picked up on two different patterns of elevated attacker activity to both RDP and another protocol that is used in remote administrator/user access: Virtual Network Computing (VNC).

The skinny on Figure 10 is that we're seeing an overall increase of daily malicious IPv4 attack attempts, but leveling off of the unique sources (and the number of total sources is still less than 1,000 daily). Hopefully, you've heeded the Q2 advice about shoring up your RDP defenses, as the attackers are being quite persistent in their endeavors.

The VNC picture is a bit more disconcerting. The number of daily, unique malicious IPv4 hosts has doubled since Q2, and the volume of attacks (the vast majority of which are credential attempts) has skyrocketed, with spikes of up to 1 million attempts across our array of sensors in a single day. While it may be possible to create a self-defending RDP node, one could make a good argument that all remote desktop usage should be behind a multi-factor VPN or tunneled through a highly secured bastion host. If you want a second opinion, even the U.S. Federal Bureau of Investigation had something to say[21].

We're continuing to keep a keen eye on this remote access ravaging and will provide an update on this pattern in future reports.[22]

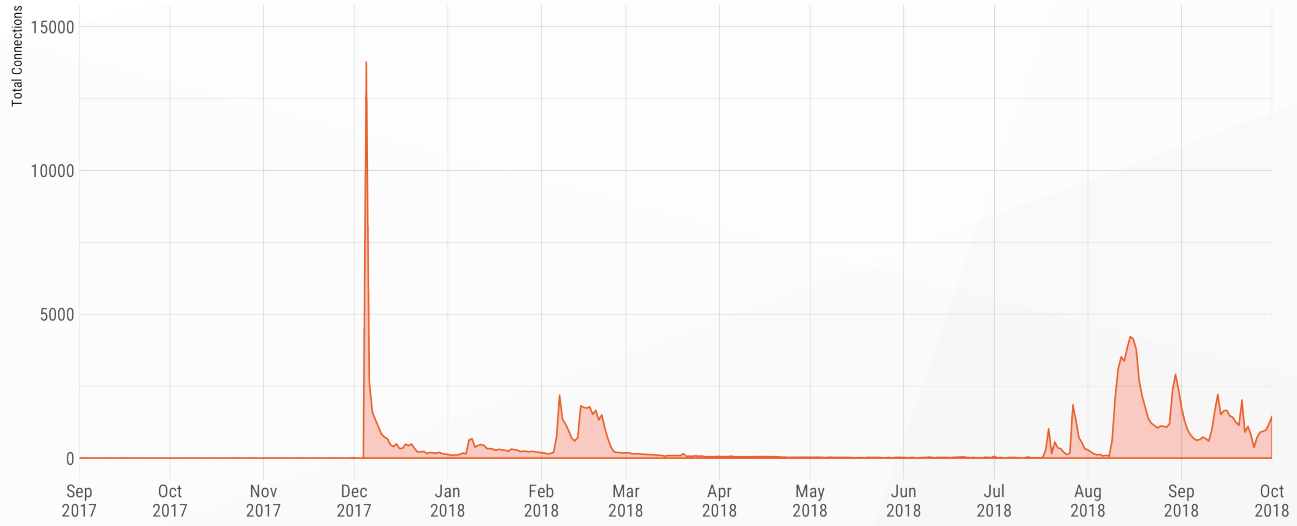
"I'm Not Dead Yet"

All Eyes on Mirai

The Mirai[23] malware/botnet has persisted as a menace for approximately two years now, reliably co-opting poorly secured IoT devices into unwitting contributors to botnets that can be wielded by nefarious command and control systems to wreak distributed mayhem. The public release of the original Mirai source code unsurprisingly resulted in a proliferation of derivatives of the malware—including spin-offs like Akiru, Sora, Owari, and Saikin, among others[24]—virtually ensuring that Mirai and its ilk will not likely fade into oblivion anytime soon.

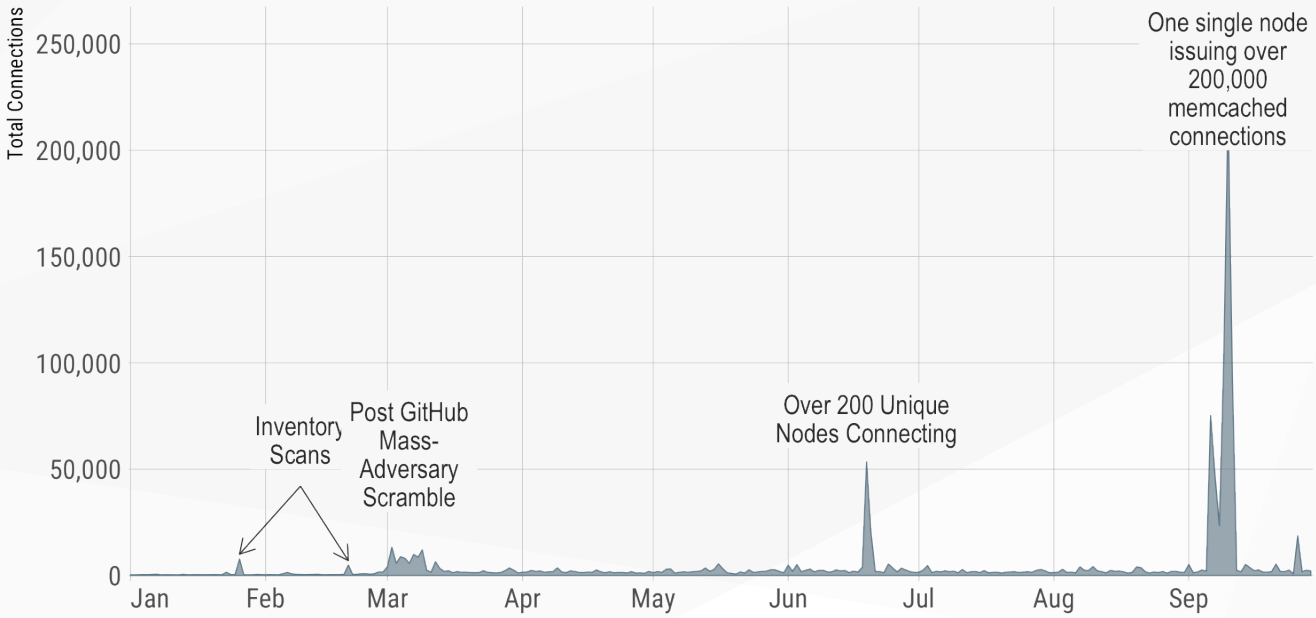
One particular Mirai derivative we have taken a closer look at is the Satori malware (Figure 11). Back in December 2017, the security researchers over at 360 Netlab[25] focused on a new variant of the Satori derivative and pointed out its targeting of ports 37215 and 52869, which turned out to be attempts to exploit Huawei HG532 home gateway devices[26] and Realtek devices[27]. After an initial dramatic spike in activity targeting those particular ports on our Heisenberg honeycloud in December 2017, connections to those ports seemed to peter out for some time, with a sudden cyclical resurgence beginning in mid-July. While recent activity has been relatively moderate, it does serve as a reminder that past threats are not necessarily gone, especially if the desired targets for compromise remain no more secure than they were in the past.

Figure 11: Satori Daily Unique Connections



[21] FBI I-092718-PSA "Cyber Actors Increasingly Exploit The Remote Desktop Protocol to Conduct Malicious Activity" — https://www.ic3.gov/media/2018/180927.aspx
[22] Rapid7 customers won't have to wait until the Q4 report, as you'll be updated in the monthly threat briefings if this continues to be a significant trend.
[23] https://blog.rapid7.com/2016/10/24/mirai-faq-when-iot-attacks/
[24] https://blog.avast.com/hacker-creates-seven-new-variants-of-the-mirai-botnet
[25] http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
[26] https://research.checkpoint.com/good-zero-day-skiddie/
[27] https://www.exploit-db.com/exploits/37169/

Figure 12: Memcached Daily Connections



Source: Rapid7 Project Heisenberg & GreyNoise Intelligence

memcached Resurgence

Back in late February 2018, GitHub became the victim of a 1.3 Tbsp amplification, distributed denial-of-service (DDoS) attack[28]. We've kept our eye on this new entrant into the short list of weaponized internet-facing services and noticed especially large/noisy spikes in September (Figure 12):

The bulk of the September spikes came from a single node in Indonesia IPv4-space that was involved with separately recorded DNS, memcached, and other amplification DDoS attacks throughout the month by organizations that specialize in DDoS monitoring.

Why are we telling you this? In 2018, attackers have been using a wider and more diverse array of tools to accomplish their goals (which has mostly been financial gain in the cases we've looked at); ransomware truly became a commodity service in 2017, adversaries are fast-turning to use exploits to gain cryptocurrency mining power vs. data theft, the Mirai botnet zombie hosts number in the millions and are available for rent at virtually pennies-per-node, and amplification DDoS has been a longstanding weapon in the arsenal of many individuals and groups.

It's easier than ever for attackers to shift from one business process to another to earn their keep, and there's virtually nothing stopping any of them from using the memcached "nuclear option" with an array of rentable attack nodes to aim their attacks at any victim they choose. If you aren't prepared for a DDoS attack that's designed to either hold you offline for ransom or distract you while the attackers are raiding the data stores, you really should be thinking of how you can go about modeling these type of risks to your organization and then developing appropriate plans to mitigate said risks.

[28] https://www.wired.com/story/github-ddos-memcached/

OUR RECOMMENDATIONS

The presence of a clear pattern in attempts to gain internal access in Q1, followed by a treasure trove of lost credentials and external network-based attacks in Q2, with subsequent overt indicators of internal malicious activity in Q3 across organizations of all sectors and sizes warrants some practical guidance on how to securely operate in the malicious-by-default world we live in.

Clean House

To clarify a familiar theme in past reports and to emphasize a topic presented earlier in this very tome: Perhaps it's time to give your network a really thorough scan. Collect as detailed an inventory as possible of what you have running on it, and how those systems and devices are configured. Attackers were clearly doing this to aid in their lateral movement journeys in Q3, and they're spinning new exploits out of well-worn toolsets like EternalBlue. Knowing what you have, and the condition those items are in, can help you map out a remediation plan before a successful attack occurs, hopefully costing you much less than the $100 million (USD) post-campaign remediation bill the UK DHSC received.

Back to School

We mentioned the MITRE ATT&CK[29] resource earlier in the report, and given the diversity and complexity of attacker behavior seen so far this year (and especially in Q3), it might be time to take a good look at it and adopt it as an internal standard. ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. You can use it as a framework during risk assessments, a cookbook for designing incident simulations, and a resource during investigations to cross-reference discrete indicators to potential end-to-end attack scenarios, which may help you stop an attack before attackers reach their goal. Using it can truly level-up your entire information security team regardless of organizational security maturity level.

Mind the [DNS] Details

If we were forced to provide only one piece of guidance that would have helped thwart a large percentage of incidents over the past three quarters, we'd have to reply with "fix your DNS configurations." DNS is the glue that binds your internal and internet network bits together. Over 20% of qualified incidents began with a URL "click." Most of those came from phishing emails. One of the best ways to shore up email defenses is by utilizing additional DNS records that work in tandem with email servers to validate the legitimacy of senders and receivers.

There's an acronym-laden bowl of alphabet soup that is needed to convey advice about shoring up DNS defenses, but we'll only cover three of them here. First, we suggest that you embark on a project to employ DMARC[30] and Sender Policy Framework[31] (SPF). Both of these are just DNS TXT records, so they're essentially "free" security tools in that you don't have to purchase anything, since you already have or use DNS.

SPF DNS records inform all email servers about the list of hosts you've authorized to send mail on your behalf. This list includes your own mail servers, but it can also include third-party services, such as newsletter or marketing cloud service providers.

Over 20% of qualified incidents began with a URL "click." Most of those came from phishing emails.

[29] https://attack.mitre.org/
[30] https://dmarc.org/overview/
[31] http://www.openspf.org/

When SPF records are utilized in combination with DMARC records (which are also free DNS TXT records), you receive two additional benefits. First, you get to specify what happens to illegitimate emails (rejecting them outright, quarantining them for inspection, or letting them pass through). Second, if you also employ one more free DNS record type known as DomainKeys Identified Mail[32] (DKIM) and configure your email servers correctly, you gain cryptographic identity and integrity checks that adversaries cannot forge (unless you were lax in how you stored your keys or certificate authority certificates).

These DNS records may be free, but it will require time and effort to identify all sources that should be allowed to send emails on your behalf and to set up the appropriate cryptographic configurations in your email systems. The good news is that you can test the waters by putting everything into "monitor mode" to see how the configurations would impact legitimate communications, make any needed tweaks to the configurations, and then implement them. Backing out of these changes is also as simple as going back to monitor mode or removing the records and email server changes.

Better Watch Out! (for the Q4 Threat Report and 2018 Year-in-Review)

That's it for this quarter, but be on the lookout for our 2018 year-in-review issue coming in Q1 of 2019. Remember that you can always reach out to research@rapid7.com with any questions about or feedback on any of the reports, or let us know what you'd like us to cover.

[32] http://www.dkim.org/

APPENDIX A: METHODOLOGY

We gathered up closed and confirmed incidents from across a representative sample of our Managed Detection and Response (MDR) customers using our InsightIDR solution for the third quarter of 2018. Where possible, we've provided full incident counts or percentages; when more discrete information needed to be provided by industry, we normalized the values by number of customers per industry. While we wanted to share as much information as possible, the precise number of organizations, industries, and organizations-per-industry is information no reputable vendor would publicly disclose.

Additionally, we also used coded-incident data provided by our MDR incident responders. Each coded incident contains one or more alerts from the raw event data along with an incident narrative. We refer to these as "significant investigations", and they help capture the stories that the discrete alerts tell.

As noted in situ, for this report we also incorporated data from both Project Sonar and Project Heisenberg. Raw Sonar scan data and limited Heisenberg data is available at no cost via httpd://opendata.rapid7.com/ and you can contact research@rapid7.com for questions regarding those data sources or any other findings/data used in this report. Known-benign traffic was filtered out of all honeypot data using feeds provided by GreyNoise Intelligence — https://greynoise.io/#rapid7.

The following table provides a full breakdown of the InsightIDR threat events and the threat event groups they belong in (as seen in Figure 6). Appendix B has the full, expanded listing of InsightIDR threat events.

IDR Threat Categories:

Dangerous User Behavior

- Account Visits Suspicious Link
- Password Set To Never Expire
- Network Access For Threat

Threat Probing

- Asset Connects To Network Honeypot
- Watched Impersonation

Threat Movement

- Account Authenticated To Critical Asset
- Lateral Movement Domain Credentials
- Lateral Movement Local Credentials
- Suspicious Authentication

Remote Entry

- Wireless Multiple Country Authentications
- Multiple Country Authentications
- Ingress From Non Expiring Account
- Ingress From ServiceAccount
- Service Account Authenticated From New Source
- Account Authenticated To Critical Asset From New Source
- New Local User Primary Asset
- Ingress From Disabled Account

Failed Access Attempt

- Authentication Attempt From Disabled Account
- Brute Force Against Domain Account
- Brute Force Against Local Account
- Brute Force From Unknown Source

Malicious Behavior On Asset Level

- Remote File Execution
- Log Deletion Local Account
- Harvested Credentials
- Log Deletion
- Virus Alert
- Network Access For Threat

Suspicious Behavior On Asset Level

- Malicious Hash On Asset

Malicious Behavior Network Level

- Advanced Malware Alert
- Protocol Poison
- Administrator Impersonation

Account Adjustment

- Account Privilege Escalated
- Account Enabled
- Account Password Reset
- Account Locked
- DomainAdmin Added

APPENDIX B: INSIGHTIDR THREAT EVENTS

EVENT	DESCRIPTION
Account Authenticated To Critical Asset	A new user authenticates to a restricted asset.
Account Authenticated To Critical Asset From New Source	A permitted user authenticates to a restricted asset from a new source asset.
Account Authenticates With New Asset	A permitted user is authenticating to an application from a new source asset.
Account Created	An account was created on a flagged asset.
Account Enabled	A previously disabled user account is re-enabled by an administrator.
Account Leak	A user's credentials may have been leaked to the public domain.
Account Password Reset	A user resets the password for an account.
Account Privilege Escalated	An administrator assigns higher level of privileges to the account.
Account Received Suspicious Link	A user receives an email containing a link flagged by the community or threat feeds.
Account Visits Suspicious Link	A user accesses a link URL identified as a threat from the Threats section or from other intel sources.
Advanced Malware Alert	An advanced malware system generates an alert.
Asset Connects To Network Honeypot	There was an attempt to connect to a network honeypot.
Attacker Behavior Analytics	A pre-built detection modeled around intrustion analysis and threat intelligence findings was triggered.
Authentication Attempt From Disabled Account	A disabled user attempts to access an asset.
Brute Force Against Domain Account	A domain account has failed to authenticate to the same asset excessively.
Brute Force Against Local Account	A local account has failed to authenticate to the same asset excessively.
Brute Force From Unknown Source	An unknown source has failed to authenticate to the same asset excessively.
Domain Admin Added	A user has been added to a privileged LDAP group.
First Ingress Authentication From Country	A user logs onto the network for the first time from a different country.
First Time Admin Action	An administrator action was used for the first time in this domain.
Harvested Credentials	Multiple accounts are attempting to authenticate to a single, unusual location.
Ingress From Disabled Account	A disabled user logs onto the network or a monitored cloud service.
Ingress From Non Expiring Account	An account with a password that never expires accesses the network from an external location.
Ingress From Service Account	A service account accesses the network from an external location.

EVENT	DESCRIPTION
Lateral Movement Domain Credentials	A domain account attempts to access several new assets in a short period of time.
Lateral Movement Local Credentials	A local account attempts to access several assets in a short period of time.
Log Deletion	A user deletes event logs on an asset.
Log Deletion Local Account	A local account deletes event logs on an asset.
Malicious Hash On Asset	A flagged process hash starts running on an asset for the first time.
Multiple Country Authentications	A user accesses the network from several different countries within a short period of time.
Multiple Organization Authentications	A user accesses the network from multiple external organizations too quickly.
Network Access For Threat	A user accesses a domain or IP address tagged in the Threats section.
New Local User Primary Asset	A new local user account was added to the primary asset of a domain user.
New Mobile Device	A user accesses the network from a new mobile device.
Password Set To Never Expire	A password of an account has been set to never expire.
Protocol Poison	Poisoning of a network protocol, such as via Responder, is detected.
Remote File Execution	Remote file execution has been detected.
Service Account Authenticated From New Source	A service account authenticates from a new source asset.
Spoofed Domain Visited	A user makes a DNS query to a newly registered internet domain.
Suspicious Authentication	A suspicious authentication was detected.
Virus Alert	A virus alert was triggered from an asset.
Watched Impersonation	A user authenticates to a watched user's account.
Wireless Multiple Country Authentications	A user logs onto the network using a mobile device from too many countries in a short period of time.

APPENDIX C: 2018 Q3 INDICATORS OF COMPROMISE

We're including a list of all host, URL, and IP address indicators of compromise (IOCs) across all the qualified incidents in Q3 2018, broken down by the threat category of the incident. You can find a CSV file of these lists at https://github.com/rapid7/data/tree/master/threat-report/iocs/2018-q3-iocs

Reach out to research@rapid7.com if another format is preferred.

Cryptocurrency Mining IOCs

ws032.authedmine[.]com

europe[.]cryptonight-hub[.]miningpoolhub[.]com

hxxp://foreground[.]me/m/3[.]ico

www.hashing[.]win

lixans[.]com

hrtests.ru

stafftest.ru

browsermine[.]com

hxxp://newage[.]newminersage[.]com:8393/

newage.newminersage[.]com

newage.radnewage[.]com

newage.minernewage[.]com

ftp.oo000oo[.]me

europe.cryptonight-hub.miningpoolhub.com

Malicious Office Document IOCs

hxxp://www[.]furnisofa[.]com/YucipclqQ4/

hxxp://www[.]marpaybiotech[.]com/IlzaSAz/

hxxp://www[.]gentiane-salers[.]com/PpsNE9P/

hxxp://www[.]bibizdevar[.]com/dNL2ZI5all/

hxxp://www[.]hotpietruck[.]com/LnhchhmDCU

hxxp://189[.]197.62.222:443/

hxxp://187[.]167.192.22/

hxxp://theneonblonde[.]com/hu[.]hu

hxxp://adultacnetreatmentreviews[.]com/hu[.]hu

hxxp://matdansunano[.]com/sotpie/8kQ6K/

hxxp://www.sayginmedia[.]com/6gOwBc/

hxxp://www.federalarmsinternational[.]com

hxxp://www.peternakan.unwiku.ac[.]id/8jPle/8jPle/

hxxp://www.mezuena[.]com/MfXlN/

hxxp://88[.]79[.]210[.]243:443/

hxxp://24[.]121[.]176[.]48:443/

hxxp://144[.]217[.]246[.]57/

hxxp://www.npi95[.]fr/YTR/

hxxp://www.showbizpro[.]ru/HI/

hxxp://www.agjas[.]org/m/

hxxp://www.altinbronz[.]com[.]tr/BCsOo/

hxxp://www.travelution[.]id/cbpGh3W/

144.217.246.57

hxxp://www.ekomaiko[.]cl/Gblamb/

hxxp://www.nevisandeh[.]info/L4GS7dj/

hxxp://www.frotista.com[.]br/Yb/

hxxp://www.planedoengenharia.com[.]br/y/

hxxp://inicjatywa.edu[.]pl//5n/

hxxp://www.alouane-organisation[.]com/Z8W/

hxxp://mironovka-school[.]ru/SrSb1/`

hxxp://www.valentinesday[.]bid/SlqoBZC/

hxxp://www.gubo[.]hu/bSGADpL/

hxxp://www.destalo[.]pt/K7Uk/

hxxp://hanking-investment[.]com/bu

hxxp://ekuvshinova.com/GqLhxQ

hxxp://ano-aic[.]ru/7Dq

hxxp://bazilevs[.]ru/lb

hxxp://frepaen[.]org/5w

hxxp://98\.163.53.175:443/

hxxp://examon[.]info/franky/skytha.exe

hxxp://alpharockgroup[.]com/HT

hxxp://adminflex[.]dk/l5TF6w

hxxp://gailong[.]net/X5AyWfJG

hxxp://shunji[.]org/logsite/TJaaB

hxxp://binar48[.]ru/OtTIVIU5

Malware/Riskware on System IOCs

hxxps://styxsaloka[.]com/beta/backup.php2

hxxps://styxsaloka[.]com/beta/page.php

hxxps://dl.dropboxusercontent[.]com/s/namkbc37wtx2mdq/reg_load_subsequent.ps1

b08fyqxb2.ru

hxxp://whitakerfamily[.]info

hxxp://rayanat[.]com

hxxp://whitakerfamily[.]info/ico.ico

hxxp://rayanat[.]com/ico.ico

hxxp://harshartcreation[.]com/microsoft.vbs

hxxp://pm2bitcoin[.]com:5000/is-ready

hxxp://lidsandjars[.]com/room[.]plo

hxxp://velsun[.]in/room[.]plo

hxxp://bibersongs[.]com/breepital27xxxger?mujejur=l&woxuaega=cimedaqibi&lezovopuco=bagalyd14ffa5b9704f119d5964781ce8913d5fgreatestcontent4yourmachinenow/./bid

disorderstatus[.]ru

differentia[.]ru

76236osm1[.]ru

gvaq70s7he[.]ru

hxxps://ossainicholasossai[.]com/wp-content/templates/kdjfs.png

hxxps://time2code[.]ch/wp-content/templates/fhdxdnq.png

hxxps://otcpress[.]aliencyb.org/wp-content/ttt/mkcxid.png

hxxps://www.dropbox[.]com/s/41zf98knyy5atko/001_01.ps1?dl=1

hxxps://www.dropbox[.]com/s/dh8flnrogfq1h1w/001.ps1?dl=1

hxxp://mgnr[.]mx/pl.ox

hxxp://handsurgeonkatytx[.]com/pl.ox

hxxp://www[.]alouane-organisation[.]com/Z8W/

hxxp://mironovka-school[.]ru/SrSb1/

hxxp://www[.]valentinesday[.]bid/SlqoBZC/

hxxp://www[.]gubo[.]hu/bSGADpL/

hxxp://www[.]destalo[.]pt/K7Uk/

hxxp://edisonnjseo[.]com/jap.plap

hxxp://longbeachcaseo[.]com/

hxxp://31[.]148.220.142/

86.105.18.236

inbound.iboe[.]com

hxxp://jandkonline[.]com/smp/B4Nxg4v/

hxxp://michaelkammes[.]com/N9vdTTT/

hxxp://www.wrightstexasnursery[.]com/1koy/

hxxp://creative-machine.net/eh0HC/

hxxp://redwire.us/rco/P5DDr/

hxxp://pixy7[.]com/Uhkt

hxxp://pharno[.]ch/h8jnf2uL

hxxp://rent360[.]co.za/EwE

hxxp://schuhversand-mueller[.]de/NiCi

hxxp://mds[.]ge/EogJiPj

192.151.158.138

hxxp://miplataforma[.]net/pdf/US/DOC/Invoice-749812

154.127.59.97

vvrhhhnaijyj6s2m[.]onion[.]top

srv1000.ru

104.239.213.7

45.77.56.53

104.100.69.37

hxxp://www.fortgibsonstorage[.]com

hxxp://henkterharmsel[.]nl/doc/En/Recent-money-transfer-details

hxxp://service-pc[.]com.ro/rog

hxxp://loucic[.]com.br/Vmr

hxxp://macrospazio[.]it/oJl

hxxp://light-estate[.]co.jp/logon/MN3

hxxp://michiganbusiness[.]us/gDuCDakW

hxxp://www.ultigamer[.]com/wp-admin/includes/Y3M2

hxxp://siamgemsheritage[.]com/career_system/backoffice/uploads/pwZ1CfJ4

hxxp://website.vtoc[.]vn/demo/hailoc/wp-snapshots/Hf2l

hxxp://barocatch[.]com/kUOtt

hxxp://muhammadiyahamin[.]com/wp-content/uploads/2018/05/NOr

hxxp://tenicoriv[.]com/Flux/tst/index.php?l=abc2.tkn

hxxp://scandryer[.]se/

hxxp://leisurecoinmachine[.]com/XxO

hxxp://santacharityevent[.]com/QKkQ

hxxp://nase-rodina[.]cz/xoV9W6

hxxp://serborek[.]com/b3eoWq

54.39.58.168

hxxp://204[.]155[.]31[.]67/bootstrap.css

hxxp://getapp.elemonopy[.]com/download/1495373619430762/PdfPro_ie.exe

hxxp://tapertoni[.]com/Flux/tst/index.php?l=ab1.tkn

ddukmql[.]com

hxxp://oligobere[.]com/Flux/tst/index.php?l=aa2.tkn

home[.]mindspring[.]com

didobanty1[.]ddns.net

hxxp://psychedelicsociety[.]org[.]au/3mw

hxxp://dolci-peccati[.]it/y7U9

hxxp://shokoohsanat[.]ir/uzCM5rrY

hxxp://kandosii[.]net/RfYza

hxxp://fractal[.]vn/oL

tunuhon[.]com

d274eq41c39r2n.cloudfront[.]net

hxxp://hertifical[.]com/tst/index.php?l=soho6.tkn

zedrevo[.]com

condonizer[.]com

vezeronu[.]com

veserans[.]com

panisodan[.]com

lambchop[.]thisplace[.]ca

hxxp://habarimoto24[.]com/Nh

hxxp://fenett2018[.]com/dObgx

hxxp://eastend[.]jp/Bl5kFA

hxxp://bemnyc[.]com/u8ERiJeq

hxxp://abakus-biuro[.]net/a9zqEmm

hxxp://zedrevo[.]com/tst/index.php?l=soho8.tkn

hertifical[.]com

hxxp://vaderstog[.]com/Flux/tst/index.php?l=aa10.tkn

hxxp://hertifical[.]com/tst/index.php?l=soho10.tkn

lambchop[.]thisplace[.]ca

hxxp://vezopilan[.]com/tst/index.php?l=soho7.tkn

baberonto[.]com

vedoriska[.]com

cimoselin[.]com

hxxp://cimoselin[.]com/tst/index.php?l=soho1.tkn

hxxp://cimoselin[.]com/tst/index.php?l=soho2.tkn

vezopilan[.]com

bidesony[.]com

hxxp://cimoselin[.]com/tst/index.php?l=soho5.tkn

hxxp://memeconi[.]com/TNT/index.php?l=anti2.tkn

fedvertisa[.]com

hxxp://memeconi[.]com/TNT/index.php?l=anti3.tkn

hxxp://vezopilan[.]com/tst/index.php?l=soho9.tkn

apatternlike[.]com

lolobec[.]website

hxxp://miafashionropadeportiva[.]com/y

hxxp://terabuild.sevencolours[.]eu/4bc2kL

hxxp://oztax-homepage.tonishdev[.]com/Lg4

hxxp://vioprotection[.]com.co/u

hxxp://test.helos[.]no/6GZ24w1

yfucgda[.]com

pgtexkd[.]com

hxxp://lementiora[.]com/YUY/huonasdh.php?l=oue2.tkn

hxxp://beriodnas[.]com/YUY/huonasdh.php?l=vbn6.tkn

nedioplina[.]com

www.lementiora[.]com

supportfilds[.]ru

hxxp://nobles-iq[.]com

hxxp://bba-es[.]com

hxxp://studio-aqualuna[.]com/UpBe

hxxp://krever[.]jp/5

hxxp://santafetails[.]com/dcz6vEs

hxxp://stolpenconsulting[.]com

hxxp://repro4[.]com/website/wp-content/uploads/MbO

hxxps://maindreamline[.]com/space/send.php2

hxxp://monwepoasdnqw[.]com/YUY/huonasdh.php?l=kuk2.tkn

hxxp://may64[.]co[.]pl/go[.]php?a_aid=5847df2ec7de8&fn=netflix

hxxp://filegenerator[.]blob[.]core[.]windows[.]net/

hxxps://intie.blob.core.windows.net/

hxxp://pexirenta[.]com/YUY/huonasdh[.]php?l=kuk2.tkn

hxxp://puntoyaparteseguros[.]com/l

hxxp://infolierepvc[.]ro/z6OFthrp

hxxp://mzep[.]ru/xGKS

hxxp://grafobox[.]com/S@

hxxp://haldeman[.]info/Zw

hxxp://bba-es[.]com/cli.nkz

hxxp://beds2buy[.]co.uk/cli.nkz

hxxp://37.59.117[.]243/indexphp?id=b3851d747c5cff6f99051aa0126fd11cd2cfc19b40bfcbf6dd7b15d815369703

hxxp://ftp.impreac.com/

hxxp://boloshortolandia[.]com/ozylgj6Z6

hxxp://ncvascular[.]com.au/69V3Cpx

hxxp://inmayjose[.]es/lB8JhFSXiV

hxxp://lalievre[.]ca/O0Pmale

hxxp://makmedia[.]ch/b5jSC1b

hxxp://201[.]146[.]211[.]106:7080/

hxxp://73[.]125[.]45[.]48/whoami.php

hxxp://thenlorefuse[.]com/4/forum.php

hxxp://thosewebbs[.]com/wp-content/plugins/prevent-xmlrpc/1

hxxp://thenlorefuse[.]com/mlu/forum.php

hxxp://thosewebbs[.]com/wp-content/plugins/prevent-xmlrpc/2

hxxp://thosewebbs[.]com/wp-content/plugins/prevent-xmlrpc/3

hxxp://smartstoragerd[.]com/MVZ

hxxp://semashur10s[.]org/FQCS

hxxp://mahdepardis[.]com/NblDl9ep

hxxp://ekositem[.]com/t

hxxp://zombieruncr[.]com/teglHp

hxxp://a4d-development[.]org/YGKX

hxxp://alanyapropertysale[.]com/OOmX2a

hxxp://tan-gho[.]com/StjB

hxxp://mahdepardis[.]com/DpTRthF

hxxp://samarthdparikh[.]com/4b9iHQ3

hxxp://tfkam38pqhsh6m[.]com/RTT/opanskot.php?l=kbnk4.tkn

hxxp://enduuyyhgeetyasd[.]com/RTT/opanskot.php?l=omg9.tkn

hxxp://tomas[.]datanom[.]fi/testlab/w0qi46LyvZ

hxxp://www[.]plasdo[.]com/MNXfUEtpo

hxxp://vinastone[.]com/m3qQf5sLVY

hxxp://vaarbewijzer[.]nl/D50JpVAsc0

hxxp://ruforum[.]uonbi[.]ac[.]ke/wp-content/uploads/afZG2WrC

hxxp://enduuyyhgeetyasd[.]com/RTT/opanskot.php?l=omg8.tkn

hxxp://ooiansyyhgeetyzxc[.]com/RTT/opanskot.php?l=omg4.tkn

zooloopil[.]fun

uuaisdnqweasd[.]com

lambchop.thisplace[.]ca

hxxp://hvyiasubeqweqw[.]com/RTT/opanskot.php?l=omg9.tkn

hxxp://laschuk.com[.]br/C7f65h8p

hxxp://jobarba[.]com/wp-content/nY7NWG7z

hxxp://familiekoning[.]net/YT9gzKUs

hxxp://www.ultigamer[.]com/wp-admin/includes/OCklr3Q

hxxp://fluorescent[.]cc/ttQoKkJ4sC

whoulatech[.]com

africategy[.]website

hxxp://apollon-hotel[.]eu/X3LVJH6

hxxp://138[.]68[.]2[.]34/wp-content/uploads/cfNP5EWD

hxxp://45[.]64[.]128[.]172/2

hxxp://5minuteaccountingmakeover[.]com/BRWYR

hxxp://alyeser[.]com/wp-content/themes/framed-redux/images/GRO

hxxp://milehighffa[.]com/Wn0Kwn

hxxp://yess[.]pl/YdJytbr

hxxp://auto-diagnost[.]com.ua/F

hxxp://silverlineboatsales[.]com/1R906A1

hxxp://miaudogs.pt/x3ZLoewB

hxxp://q0fpkblizxfe1l.com/RTT/opanskot.php?l=targa3.tkn

hxxp://t95dfesc2mo5jr[.]com/RTT/opanskot.php?l=targa2.tkn

hxxp://q0fpkblizxfe1l[.]com/RTT/opanskot.php?l=targa4.tkn

kanboard.globalsoftm[.]com

hxxp://q0fpkblizxfe1l[.]com/RTT/opanskot.php?l=targa3.tkn

hxxp://aprovadopeloshomens[.]info/NkKo

hxxp://autopricep[.]kz/HxrdY

hxxp://bazarmotorco[.]ir/X5bAi4CB

hxxp://atrakniaz[.]ir/mcm

hxxp://avangard30[.]ru/UiDWw

hxxp://bioners[.]com/X8nV8i

hxxp://otiaki[.]com/33EKwRe

hxxp://bc-cdc[.]org/x

hxxp://marienthal[.]info/gIAl3AM

hxxp://jingtianyanglao[.]com/iaM5oV8

hxxp://vagenkart[.]com/XOE/kemvopod.php?l=qily3.tkn

hxxp://familiekoning[.]net/Sw51duCIY

hxxp://website.vtoc[.]vn/demo/hailoc/wp-snapshots/JeHXbk6WzM

hxxp://librusfan[.]ru/271vNHA

hxxp://tomas.datanom[.]fi/testlab/VJ1t3ol

hxxp://altarfx[.]com/8Es5z7sVJL

hxxp://vagenkart[.]com/XOE/kemvopod.php

hxxp://3kh4te118zvms[.]com/XOE/kemvopod.php?l=xtem3.tkn

hxxp://marqets.ru/tlyJ

hxxp://7continents7lawns.com/huWJYej

hxxp://7naturalessences.com/iX

hxxp://dek-kam.ru/09XTe

hxxp://krever.jp/bvu0

hxxp://5yg65qcxsulvovz8[.]com/DAB/nerimf.php?l=jeba7.pas

hxxp://alignsales[.]com/5iTjBVHgiZ

hxxp://aquatroarquitetura[.]com.br/xqk3qb5a

hxxps://adamant[.]kz/CVjsyDag

hxxp://02feb02[.]com/d8rOmLBT

hxxp://pornbeam[.]com/B6v8OJvL

hxxp://vanieospjo[.]com/DAB/nerimf.php?l=kamax5.pas

hxxp://69.70.248.98:8443/

hxxp://96.23.80.242:50000/

13.107.4.50:80

23.217.164.198:80

191.232.80.58:443

hxxp://bcgfl[.]com/sdn.uqw

hxxp://ubeinc[.]com/sdn.uqw

hxxp://gabrielamenna[.]com/ONSxgnweAI

hxxp://danilbychkov[.]ru/QBIN69xgw

hxxp://caspianlab[.]ir/tIcXKP6

hxxp://ctiexpert[.]com/7U87CMw

hxxp://ecol[.]ru/9kgiz7sV1

hxxp://hnuk[.]net/g

hxxp://fenja[.]com/wwvvv/8S

hxxp://www.elucido[.]se/mH95fHIX

hxxp://edisolutions[.]us/U7mhh6Ks

hxxp://ecopropaganda.com[.]br/SBNPa

hxxp://ruralinnovationfund.varadev.com/lKKK1wruj

hxxp://alumni.poltekba.ac.id/9Oqgg6M

hxxp://fourtion.com/qyBf2DfGd

hxxp://emmlallagosta.cat/SxSBuh1k

hxxp://sparq.co.nz/78sA4Pii

81.177.23.178

hxxp://hadidndintligh[.]ru/d2/about.php

hxxp://bitcoinpaperstockcertificate[.]com/

hxxp://cryptocurrencypaperwalletcertificate.org/

hxxp://razerovuar.com/jzmc1naxan90.uti

hxxp://195.123.225.153

hxxp://bahiacreativa.com/drF5M4c

hxxp://02feb02.com/tLJxCef1

hxxp://johnscevolaseo.com/mxtKQr8md

hxxp://stoobb.nl/408wovgJL

hxxp://sem-komplekt.ru/GSwcxHi

llkkjjhhg[.]com

hxxp://duwyernsdjfnssla[.]com/VRE/kotner.php?l=kueta2.pas

hxxp://duwiurwoxoqwiew.com/VRE/kotner.php?l=kueta3.pas

hxxp://duwyernsdjfnssla[.]com/VRE/kotner.php?l=kueta4.pas

hxxp://iwoeiwuqyeqiwakw[.]com/VRE/kotner.php?l=kueta4.pas

duwiurwoxoqwiew[.]com

download.drp[.]su

hxxp://peekaboorevue.com/0B5WOLOKFg

hxxp://atgmail.net/Jj6SClPro

hxxp://krever.jp/njwxGImMd

hxxp://gabrielamenna.com/RLDjDvQJw

hxxp://desnmsp.com/oEdTUUscJA

24.14.188.26

hxxp://omlinux[.]com/EjgPh

hxxp://circuloproviamiga[.]com/wp-content/themes/5Db8XGz

hxxp://spectrumbookslimited[.]com/SawGapId

hxxp://www.ultigamer[.]com/wp-admin/includes/QV0VCt

hxxp://supermercadoyip[.]com/R

hxxp://wuyeqwidkxueiqqo[.]com/MXE/lodpos.php?l=rejo4.xt2

hxxp://ogxbody[.]com/EyW

hxxp://sbtasimacilik[.]com/H3PmH

hxxp://immenow[.]com/cKoJs

hxxp://r-web[.]pl/TUyiK6z

hxxp://pangeamt[.]com/a4ov

hxxp://jcstudio[.]com[.]my/EN_US/Documents/09_18

hxxp://louisianaplating.com/18Ge0wDF

hxxp://stonehouse.me.uk/AIvUfSm

hxxp://peakperformance.fit/2TfHVaCdGP

hxxp://djsomali.com/z4x6QiEr

hxxp://maquettes.groupeseb.com/Lf01Lq4ZSS

201.111.8.75

190.147.53.140

hxxp://luxeestateslifestyles[.]com/Y

hxxp://persiapet[.]net/lEu5S

hxxp://store[.]bmag[.]vn/vuy

hxxp://psdesignzone[.]com/Pw33lZ2

hxxp://paramountmemories[.]com/CDP

hxxp://luxeestateslifestyles[.]com/y

hxxp://store.bmag[.]vn/vuy

74.195.12.152

172.245.10.114

hxxp://goldenyachts.customexposure.tech/wp-content/uploads/e

hxxp://omnigroupcapital.com/poVNoK

hxxp://marindofacility.co.id/zErEGbN

hxxp://icexpert.net/bMHUCW

hxxp://puuf.it/Cv4Y2

hxxp://wuyeqwidkxueiqqo[.]com/MXE/lodpos.php?l=rejo5.xt2

45.33.90.169

getapp.elemonopy[.]com

bonefreeze[.]com

hxxp://emporioflorianopolis.com.br/multimedia/AH3dB5Y2h

hxxp://www.xianjiaopi.com/DTWn8HR6e

hxxp://ufindit.com.au/yO47HFVs

hxxp://www.lidersahtebalik.com.tr/44v1qfZlhA

hxxp://wpcouponsite.com/dttLyRtF

hxxp://201.233.81.143/

hxxp://81.134.0.41:8080/

hxxp://187.250.60.214/

hxxp://72.181.91.254:8080/

hxxp://149.202.160.202:8080/

hxxp://h2812932937292sjshskz[.]com/MXE/lodpos.php?l=yows1.xt2

hxxp://217.182.231[.]43/lodpos.php

hxxp://216.189.151.181/26p2oqu6gn[.]exe

hxxp://hollywoodgossip[.]biz/GpyDtTIIO1

hxxp://charpentier-couvreur-gironde[.]com/2Agu5kOrh7

hxxp://surprise-dj-team[.]com/2Atuefrxm

hxxp://spektramaxima[.]com/IXx8GGy

hxxp://dc.amegt[.]com/wp-content/QNhKWYE

coffemokko[.]com

lifespanfitness[.]com

Phishing IOCs

hxxp://jawaanw[.]com/wp-includes/js/office/365/gsuite/gsuite/secure/index.php

hxxps://storage.googleapis[.]com/onedrive-predistinguish-702812361/index.html

hxxps://searchurl[.]bid/messagecenter000111/finish30.php

hxxps://minamin-junko[.]info/admin/include/11/index.php

hxxp://thepeacefulmarketer[.]bid/.love/A2/

hxxp://thepeacefulmarketer[.]bid/Smileys/.file/A2/

hxxp://uncleoscar[.]com/ygsd/adobee/adobe.php

hxxp://canningvalebusinessbuilders[.]com[.]au/

hxxps://alven-sa[.]com.ar/closing/office/

hxxps://apppostpaid[.]com/

hxxps://oceanictech[.]top/languages/finished/index.php

hxxps://withuard[.]gq/

hxxps://talkmemores[.]info/tfcx/index.php?fire=works

51cf45f45-billing[.]com

hxxp://accsrequidsatsl[.]com/

hxxp://tozoleaummaires[.]com:443

hxxps://mwemaafricasafaris[.]com/wp-content/wwpp22/h8eJ5oaat/NMyBgMxeW/LCQ3LGbXJdb/vwZL58Rka/bm2aiXMjSC/Sg5imk4NjV/d5ZGdE28CDD/QnYrGchFgz/LmdwNpBHd6k/index.htm

hxxps://lannilakhacnuanhunmanhhodoa-heptahedral-roundabout.mybluemix[.]net/viaowiqo/vp4OJ-signin-5miles/9l19Ki4P

hxxps://sylykaoyaha[.]info/adadx/?mad=htmledit

hxxps://unhunena[.]info/adadx/?mad=htmledit

hxxp://www[.]cabinetdiouri[.]com/backup/2/fonctions/Outlook/index.php

hxxps://nunt2[.]usa[.]cc:443

hxxps://weevoxsound[.]com/re.php

hxxps://bawaberita[.]com/hghggk/office_micro/login/office/

hxxp://recommendedforall[.]org/freedomforme/Googledoc

hxxps://sysmark[.]com[.]br/tmp/finished/index.php

hxxps://myprevexpoogd.co[.]uk/Shoppas/Ride/archive/

hxxps://protect-us.mimecast.com/s/SopHCKrYZYC2A8kMiMMjOF?domain=bifurcate-splashes.000webhostapp.com

hxxp://aromabel[.]com[.]ar/

hxxps://efiyo[.]com/file/document

hxxps://fbaym[.]com/securemail/

hxxp://www[.]ustechsupport[.]com/

hxxps://bluestarhosting[.]net/confijjjjr/re.php

hxxps://courage2care[.]net/nnrhhjgj/office_micro/login/office

hxxp://jpchoices[.]com/auth/BOAlastest/login.php

hxxp://karphomes[.]com/wabRedo/webredo.php

hxxp://webconnect.karphomes[.]com/Maxfiles.loaded/

hxxps://bpllplawfirm[.]com/

hxxps://tuyrb[.]ml/shipping/maersk/index.php

hxxp://bodegold[.]date

hxxp://dilitang[.]date

hxxps://missbasket[.]net/ss/sw/

hxxp://forme[.]twilightparadox.com/5b5b5d9eb4d87H3d4EHrsgA

hxxps://ntyrfter[.]co[.]uk/FIRSTAMERICA/office_micro/login/office/

melit[.]biz/aerospirit/mic/processor.php

hxxp://moonmaroon[.]com/images/secure/index.php

174.127.119.210

hxxp://adminhelp[.]ulcraft.com

185.165.123.4

hxxps://xses[.]info/php/EXEL/

66.206.46.81

hxxp://boaalaw[.]com/capital/law

hxxps://www.xwes[.]info/auths/sam2.aspx

hxxps://www.kieznetz[.]info

hxxp://vigilantsys[.]co.ke/foldie/ofiice/office/login.php

162.144.67.83

hxxps://northcare[.]solutions/Thursday/ssl-v.1/

hxxps://dunlatoparoa-presufficient-exec[.]mybluemix.net/ozipao/

169.54.245.69

hxxps://help-mkjjjjjj[.]cf/

hxxps://www.redfarmacalama[.]cl/wp-includes/new/business

hxxp://andersen2018[.]com/3438934dc84b9250bf1413c4e52aecfa/

hxxps://rlamzo[.]org/cac/db

hxxp://ghoshexim[.]com/cac/db/

hxxps://keepcallingu[.]info/rtyh/

hxxps://undualpropals[.]ga/

hxxps://www.corneroffice.co[.]in/newsletter/

192.254.188.69

hxxps://dhaligroupbd[.]com/log/docc/docusi

hxxp://bonanza[.]cl/

hxxp://imqrmnczhlweqpt[.]usa[.]cc/wp-include/

hxxps://ofinsen[.]com/payout/

146.112.61.108

hxxps://aswadinvestment.co[.]ke/qazss/

hxxps://newroad[.]gq/kl/one/

166.62.45.59

hxxps://decksscholach.ga/surf3

hxxps://gst-ingenieros[.]com/rt/one/

hxxp://endtimesng[.]org/wp-update/cgibin/

hxxp://take-your-prize[.]cf/css/upgrade/

hxxps://www.liteflashhelp[.]trade/

hxxps://cdn.opendld[.]net/

hxxp://lp.boostmac[.]download/cnsn/1/

hxxp://microsoft.0ffice365.2020mode[.]com/mcroft/

civicbeatssedan[.]info/qwsa/index.php?youth=arena

93.157.63.189

hxxp://ud6j08kz3fo7h20yy2mg[.]epizy.com/

hxxp://adepafm[.]com/

hxxps://datedcodings[.]com/office/

hxxp://hmtaxrevs[.]co.uk.ref9043030spacepoint3e23.mistonedcraz.com/login/

hxxps://onedrive[.]godaddysites.com

hxxp://bookmystuff[.]co.in/invoicecopy/hdrive/DRIVE/ertyo

hxxp://jnas[.]na.am/one/onedrive/

hxxp://hooghlyonline[.]in/direct/online/12/index.php

hxxps://goabeachlife[.]info/edcx/index.php?arynews=percentage

hxxp://justyatra[.]com/txt/92511e64398856644de41dde17570294/

hxxps://sbil[.]biz/kg/@%23%25!!%23%25$

hxxp://www.trevorconnors[.]com/wp-includes/Requests/Response/

hxxps://maitlanede[.]cf/Merryshop/CBEdited/CBEdited/CBEdited/shop&earn.htm

hxxps://drayconstruction[.]com/assets/hits/arc/index.php

hxxps://kerstensantiques-my[.]sharepoint[.]com

hxxps://redscells[.]flu[.]cc/ordersecure/eimprovement/index.php

hxxps://vranwraf[.]bid/file/docusign/docusign/

hxxps://kerstensantiques-my.sharepoint[.]com/

hxxps://greens[.]nut.cc/account-verification/

hxxps://phxfreight[.]com/fumr

hxxps://xclusivedevelopers[.]com/qaz/@$@@!$

hxxps://3kreatif[.]tk/WeTransfer/vice/Office/Login/

hxxps://saisportswearltd[.]co.ke/Office365N/CD3HUD/newpage/account

hxxps://zipporehna[.]info/dfvc/

hxxps://vewbnj[.]com/admnone/onente/admnshp

shorturi[.]win

hxxps://almagdpharma[.]com/u9/login/$%25%5E&@@%23/tk/login.php

air45[.]duia[.]eu

hxxp://stolpenconsulting[.]com/QAjZrH6

hxxp://www.fps-enp[.]com/office365s/

hxxp://ysd63[.]com/xw0jDX

hxxp://exclusiv-residence[.]ro/luWn6

hxxp://leizerstamp[.]ir/zqiQcpE

hxxp://firstchoicetrucks[.]net/kCV0l

hxxp://olsenelectric[.]com/zVz4iwC

hxxp://ovstor[.]space/ZCcns6R8/upPYZXJ-5bmsQxwPi/m/h9L/g/

hxxp://ovstor[.]space/YChf/uZ/PTb/VgL/3/-evQxcHoB1/HcA

hxxps://megabasez[.]info/xcde/index.php?highway=jump

hxxps://megabasez[.]info/edcx/

hxxps://adakokosar.weltechin[.]com

hxxp://estudioalm.com[.]uy/wp-furniture1/

hxxps://gshort12[.]000webhostapp.com/new_now/

hxxps://dequpnet[.]cf/danilas/oneee

hxxps://choldengs[.]gq/scholes/oneee/

hxxps://le-cid[.]org/cgi/six/

hxxps://redcosb[.]com/create/invoice/aproval/s/shared/index/index.php

hxxp://parallelintegration[.]org/protect/protected/X3D/

hxxps://sysmark.com[.]br/bccccccccc/businessfiless/index.php

hxxps://elkgm[.]com/029092/vmnl/mvm

hxxp://dropbox.com.register.document.dropbox.com.register.document.dropbox.com.register.document.dropbox.com.register.document.ziaeco[.]com/Dropbox/doc-login/

hxxp://www[.]lyndochparish.com[.]au//wp-includes/fonts/wellsfargo.html

hxxps://accounts-serives[.]me/fm/docg/doc/filewords/index.php

hxxp://d3od.ddns[.]net/

hxxps://huyt.hopto[.]org/D3D/

hxxp://cloudserv[.]gq/

hxxps://roanus[.]ga/confirm-data/

hxxp://ddf3.ddns[.]net/

hxxps://66yyy.ddns[.]net/D3D/

hxxps://chicottada.com[.]ve/edgewater/share/

hxxp://sekretarispro[.]com/AD/index.html

hxxp://kalaniketanbalvidyalaya[.]com/js/1/login/office/

hxxps://makingoffice[.]ml/redirect.php

hxxps://dailyconnect[.]website/properties/cgi/index.php

hxxp://facebook-login[.]acrbgov.org/f/?id=muDr

hxxp://quantum9[.]kozow.com/v5oqmzs8i1efvi6jhdny

hxxps://officeservice-data365inc[.]com/*%26%23*%26*!%20%20%26!/office365/

hxxp://mrr.eddiescherries[.]com/

hxxp://zet.wenchmolts[.]com/update_flash_player.php

hxxp://interior-agency[.]de/uiopl/

hxxps://x[.]co/Urb2a67b

hxxps://intenalco.edu[.]co/bd/surelevels/

hxxp://mpnz25a922a7512aa[.]kozow[.]com/fr5h9xwgzf

hxxp://mpnz25a922a7512aa[.]kozow[.]com/9gczj8hzcs

hxxp://mpnz25a922a7512aa[.]kozow[.]com/b33zusyxxo

hxxp://manuelsuzuki[.]in.net/nsw/data/

hxxps://adobepdfclaimsshare[.]com/tgzip/tgzip/index.php

hxxps://leeraeI[.]co[.]za/protecfire/admin/login.microsoftonline.com

hxxps://cables[.]ipq[.]co/.cablesipq/.home/

hxxps://dinerkado[.]be/Office/office_micro/login/office

hxxp://www[.]dashboardonlinepro.com/read/nyt/

hxxps://extrawebsecurirty[.]online/datasync2/share

hxxps://rushberryfruitz[.]info/zxcvb/index.php?dragoon=bubblebee

hxxp://indofurnicraft[.]com/hyde/Docusign/

hxxps://ecoklimalex[.]at/index/onedri/one/index.php

hxxps://www.adarkstormiscoming[.]com/SiteSolutionsGroupLLC/OneDrive/0992/

hxxps://okunowcanordezz[.]info/yujh/index.php?xperia=lexus

hxxps://nsydkf[.]com/vm/vmailonmessage/onenewmessage/voiceroute/wavv/incorrect.php

hxxps://storage.googleapis[.]com/servingwebsitesecuredservingwebsitesecured/index.htm

hxxps://bxcszw[.]com/mmm/vmn/vmm

hxxps://wagonrcarnot[.]info/cvfds/index.php?backstreet=sports

hxxp://about-purchase-765[.]com/

hxxps://hisartgroup[.]in[.]net/Arista/Folder/Shared/OneDrive/

hxxp://www.ironwood-ind[.]com/wp-admin/js/Dcssl/docu/a/

hxxps://signsas[.]com/dr

hxxps://sooke-my[.]sharepoint[.]com/

hxxps://bkozozasairqi-unspatial-whangdoodle[.]eu-gb[.]mybluemix[.]net/bzca/

finopaos[.]ga

hxxps://phoenixplus[.]xyz/true/

hxxps://sooke-my.sharepoint[.]com/:b:/g/personal/cmccrea_sooke_ca/ETAOwyYzDq1AviQVL_uuTIUB8RISE3uyyxC1b656AGJfMQ?e=TEaNMs

hxxps://bkozozasairqi-unspatial-whangdoodle.eu-gb.mybluemix[.]net/

hxxps://grabafan[.]com/wp-accesss35/One-Drives/wp-include/One-Drive/

Suspicious Login IOCs

104.236.231.33

197.210.45.127

78.153.148.23

77.234.46.238

185.56.235.248

167.99.224.50

197.210.52.54

168.253.114.197

146.185.140.224

178.128.173.47

146.185.144.53

165.227.236.146

159.65.137.131

184.212.143.159

41.58.78.43

178.62.213.181

197.210.10.11

197.210.52.63

192.241.155.238

178.128.174.255

146.185.138.141

104.131.32.86

178.128.164.110

198.199.67.54

107.170.239.61

41.190.18.66

178.62.8.236

138.68.181.202

197.210.54.117

159.203.61.231

178.128.209.216

159.89.114.182

105.112.23.18

5.62.43.39

167.99.196.125

197.210.54.107

184.212.17.109

67.205.183.163

160.152.25.225

181.36.5.50

159.89.202.49

165.227.56.45

159.89.145.247

159.65.148.124

197.156.241.240

159.89.102.13

169.239.194.146

165.227.173.58

107.170.205.145

138.197.144.140

41.180.0.158

197.211.59.162

139.59.168.206

45.55.169.78

197.210.45.28

169.239.194.185

142.93.0.66

167.99.172.135

105.112.17.236

197.210.54.95

212.100.79.80

77.234.46.240

169.239.193.77

41.58.222.217

178.128.175.93

167.99.187.83

159.89.166.176

206.81.3.234

174.138.56.241

162.243.51.250

137.59.252.226

172.98.77.235

199.116.118.231

77.234.46.219

173.239.232.34

105.112.112.17

154.66.52.190

41.58.123.70

192.241.225.111

167.99.187.178

198.8.84.236

162.243.140.30

107.170.243.224

77.234.46.164

41.190.30.72

162.243.19.168

154.160.0.180

37.46.114.69

105.112.23.116

197.255.166.10

173.244.44.68

165.227.187.79

192.241.221.241

159.89.181.169

212.100.94.57

197.210.64.12

162.243.14.249

165.227.47.137

173.239.230.34

205.185.193.197

197.242.115.13

154.120.115.10

173.245.202.210

41.190.14.218

184.212.60.228

198.8.93.32

197.211.60.58

138.68.6.15

41.190.3.158

167.99.103.238

41.58.75.20

41.58.99.175

159.89.193.118

107.152.104.211

173.239.232.17

178.62.221.111

178.128.93.124

178.128.45.180

173.239.232.159

159.65.117.143

192.168.0.29

41.58.91.226

197.156.241.248

197.156.241.249

197.58.113.117

198.199.118.169

41.190.30.196

159.89.236.167

41.138.169.86

205.185.223.215

159.65.148.109

104.131.173.61

197.210.44.161

197.210.226.58

41.58.200.156

41.190.2.11

196.52.39.2

104.200.159.72

169.159.117.225

41.190.2.115

172.83.40.115

172.98.84.174

105.112.32.56

159.89.134.108

192.241.219.31

173.244.44.58

41.58.77.212

173.239.232.146

120.52.73.174

169.53.164.127

160.152.37.1

184.212.249.216

159.65.46.191

173.244.44.27

199.116.115.145

192.111.142.145

196.52.39.34

199.116.115.143

184.212.103.16

138.197.164.215

107.181.191.36

104.236.228.237

5.62.59.26

107.181.176.98

169.239.192.7

93.84.146.55

107.152.98.82

197.242.242.2

181.67.2.99

197.210.44.147

173.115.167.79

197.211.61.16

67.205.181.62

176.16.0.0/19

129.56.141.206

129.56.141.93

178.128.168.232

197.156.241.248

41.242.0.62

104.200.135.125

212.100.80.47

41.190.30.90

5.62.63.55

159.89.173.108

ABOUT RAPID7

Rapid7 powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response, and log management for organizations around the globe. To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

QUESTIONS?

Email us at research@rapid7.com