

Table Of Contents ^



Top 10 Dark Web and Deep Web Forums of 2025



[Home](#) » [Knowledge Hub](#) » Top 10 Dark Web and Deep Web Forums of 2025

📅 Last updated on: July 8, 2025 ⌚ 8 min read

Top 10 Dark Web And Deep Web Forums Of 2025

The internet we use daily is only a small fraction of the vast digital world hidden beneath the surface web. While most of us are familiar with search engines like Google, which index the public web, there are other parts of the internet that are not as easily accessible.

Two terms often mentioned when discussing these hidden areas are the deep web and dark web. Although they are sometimes used interchangeably, they refer to distinct parts of the internet with their own characteristics and purposes.

Among the most talked-about aspects of these areas are the deep web forums and dark web forums, which serve as gathering places for various online communities.

Understanding The Deep Web

The deep web is the part of the internet that cannot be accessed by traditional search engines. Unlike the surface web, which is indexed and searchable by engines like Google, the deep web includes content that is protected behind **firewalls** or paywalls, requires specific login credentials, or is otherwise hidden from public view. It is important to note that the **deep web** is not inherently malicious. In fact, much of the content in this part of the internet is completely legitimate, such as:

[Products](#) ▾ [Solutions](#) ▾ [Why Cyble?](#) ▾ [Resources](#) ▾ [Company](#) ▾



[Partners](#) ▾

[Medical Records](#)

- Private networks, including VPNs and intranets

This hidden content is primarily intended for **privacy and security**, catering to



Stay Ahead of
CYBER THREATS
Get Real-time
INSIGHTS

Listen on
amazon music

aws marketplace

Recent Posts



The Week in
Vulnerabilities: 717
New Cybersecurity
Flaws Rep...
August 11, 2025



Who are the Top
Ransomware Threat
Actors of H1 2025
August 8, 2025



A Region-Wise
Breakdown of Cyber
Threats: What H1

Free
Demo

IPR2025-01398

CrowdStrike EX1013 Page 1

individuals, organizations, and services that wish to keep their activities private.

Diving Deep Into The Dark Web

The dark web, a subset of the deep web, is where anonymity and secrecy intensify. It is intentionally obscured from search engines and requires special software like Tor (The Onion Router) to access it. Sites on the dark web typically use .onion domain names, which add a layer of anonymity for both users and administrators. While many users turn to the **dark web** for legitimate reasons, such as journalists or activists seeking to avoid censorship, it is also known for illegal activities.

Dark web forums, in particular, are notorious for hosting discussions on illicit topics. These include:

- Trading of stolen data (e.g., usernames, passwords, credit card details)
- Sales of illegal goods (e.g., drugs, weapons, hacking tools)
- Fraudulent schemes (e.g., identity theft, credit card fraud)

Despite its darker reputation, the dark web also provides a platform for individuals who are concerned about privacy or who seek to discuss sensitive topics without the risk of government surveillance.

Top 10 Deep Web And Dark Web Forums

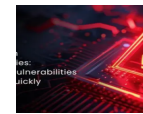
The forums on the deep web and dark web vary in terms of their focus. Some are geared towards academic, professional, or hobbyist communities, while others are havens for illegal activities. Here's an overview of some of the most well-known dark web forums and deep web forums that have emerged over the years.

1. XSS (Formerly DaMaGeLaB)

Launched in 2013, XSS is one of the longest-running forums in the dark web. Initially known as DaMaGeLaB, the forum rebranded in 2018 after the arrest of one of its administrators. XSS is primarily focused on hacking, corporate access, and data leaks, making it a hub for cybercriminals and hackers. It is heavily business-oriented, with sections dedicated to **ransomware** services and cyberattacks.

2. Nulled.to

Nulled is one of the most notorious dark web forums. Established in 2015, it is a major gathering point for cybercriminals. The forum specializes in a variety of illegal activities, including the sale of leaked data, hacking tools, and fraudulent services. Despite its focus on illicit content, Nulled has a large and active user base. In 2016, the forum suffered a data breach, exposing **sensitive user information** and heightening its notoriety.



The Week in Vulnerabilities: 1 in 5 New Vulnerabilities Expl...
August 1, 2025



Email*

☐ By submitting this form, you agree to receive marketing communications from us. You can unsubscribe at any time. For more details, please read our [privacy policy](#).

Subscribe Now

3. BreachForums

Launched in March 2022 as a successor to RaidForums, BreachForums quickly became one of the leading forums for discussing **data breaches** and sharing stolen information. After the shutdown of RaidForums, BreachForums filled the gap by hosting discussions on exploits, data leaks, and cybercrime. However, the forum has faced its own set of legal challenges, and its founder was arrested in 2023.

4. Dread

Dread, founded in 2018, is one of the largest dark web forums that exists today. The forum hosts multiple sub-communities, where users discuss everything from data leaks to illegal drug sales. Despite the predominance of illicit activities, Dread also hosts conversations related to privacy and **cybersecurity**, reflecting the diverse range of topics covered on dark web forums.

5. CryptBB

CryptBB is a highly encrypted dark web forum that caters to elite hackers and cybercriminals. Established in 2020, CryptBB utilizes advanced encryption methods, such as AES 256 CTR and RSA768-2048, to ensure the security of its communications. The forum serves as a space for both beginners and seasoned hackers to share their knowledge on a range of topics, from carding to advanced hacking techniques.

6. LeakBase

A relatively new player in the world of dark web forums, LeakBase emerged in 2023 as a response to the closure of BreachForums. Specializing in data leaks, this forum has quickly gained traction and is now considered one of the top destinations for cybercriminals looking to buy or **sell sensitive data**.

7. FreeHacks

FreeHacks, a Russian-based forum, is one of the largest hacking communities in the world. Since its creation in 2014, it has become known for providing an extensive database of hacking tools and resources. The forum primarily focuses on carding, **DDoS attacks**, and other forms of cybercrime. Due to its selective membership process, FreeHacks has earned a reputation for being a place for advanced hackers to gather and exchange knowledge.

8. Exploit.in

Exploit.in, founded in 2005, is another prominent Russian **hacker forum**. Operating on both the dark web and the surface web, Exploit.in serves as a hub for malicious **actors seeking** to buy and sell exploits, malware, and stolen data. The forum is notorious for its role in facilitating unauthorized access to networks and distributing **malware**.

9. Cracked.to

Cracked.to, established in 2013, is a deep web forum that hosts discussions

related to hacking, cracking, and data leaks. With over 3 million members

and more than 17 million posts, Cracked.to is one of the most active forums for cybercriminals. Despite its focus on illegal activities, it also features discussions on programming and **cybersecurity**, providing a mix of topics for its diverse user base.

10. Altenen

Altenen is a lesser-known but highly active dark web forum focused on credit card fraud and other forms of financial crime. Users of Altenen share techniques and tools for cracking, hacking, and committing fraud. Despite its focus on illegal activities, Altenen attracts a loyal following, with many users seeking to learn the latest methods for committing financial crimes.

Role Of Dark Web Monitoring And Threat Intelligence

Despite how big the dark web forum market is, or how many people it attracts, these forums remain a risk to both individual users and businesses. This is where **dark web monitoring** and **threat intelligence** become important.

Dark web monitoring involves tracking activity on the dark web to identify potential threats such as stolen data, leaked **credentials**, and other sensitive information that could be harmful if accessed by malicious actors. By actively monitoring **dark web forums and marketplaces**, organizations can detect early signs of a **data breach** or a compromised system, allowing them to take preventive actions. For example, if a company's private data is being sold on a dark web forum, dark web monitoring tools can notify the company in real-time, enabling them to secure their systems and mitigate damage.

Similarly, threat intelligence is another tool that involves the collection and analysis of data about potential or existing **cyber threats** to help organizations understand and prepare for future risks. This can include gathering information from various sources, including dark web forums, and analyzing trends related to cybercrime.

For example, if a specific malware variant is being sold or discussed in a dark web forum, **threat intelligence services** can provide insights into the potential risks it poses, allowing cybersecurity teams to upgrade their defenses. By leveraging both **dark web** monitoring and threat intelligence, organizations can better protect themselves from cybercriminals.

Conclusion

Dark web and deep web forums expose the darker side of the internet, often hiding illicit activities from the public eye. These platforms provide cybercriminals with anonymity, making it difficult to track and stop illegal activities. While some users seek privacy, the ease of trading stolen data and illegal services remains a major cybersecurity concern.

Dark web monitoring and threat intelligence firms like **Cyble** help mitigate these risks with advanced AI-driven threat intelligence solutions. Cyble's

these risks with advanced AI-driven threat intelligence solutions. Cyble's platforms, such as **Cyble Vision**, monitor the dark web for emerging threats, providing real-time insights to protect organizations from cybercrime. By leveraging such tools, businesses and governments can protect their data and communities from **cyber actors**.

Discover How We Help Proactively Defend Against Evolving Threats With Gen 3 Intelligence. **[Request A Demo Today!](#)**

Share Post:



Related Topics



📅 August 8, 2025

Top 15 Most Dangerous Malware Threats In 2025 (So Far)

Schedule a Personalized Demo

[Book a Demo](#)



Threat Intelligence Products & Platforms

[AmIBreached](#)
[Cyble Vision](#)
[Cyble Hawk](#)
[Cyble Odin](#)
[The Cyber Express](#)

Why Cyble?

[Compare Cyble](#)
[Industry
Recognition](#)
[Customer Stories](#)

Solutions

[Attack Surface
Management](#)
[Brand Intelligence](#)
[Threat Intelligence Platform](#)
[Dark Web Monitoring](#)
[Takedown and Disruption](#)
[Vulnerability Management](#)
[Third-Party Risk
Management \(TPRM\)](#)
[Physical Threat Intelligence](#)
[Executive Monitoring](#)
[Cloud Security Posture
Management \(CSPM\)](#)
[BotShield](#)
[Incident Management](#)

Resources

[Thought
Leadership](#)
[Blog](#)
[Knowledge Hub](#)
[Threat Actor
Profiles](#)
[SAMA Compliance](#)
[Events](#)
[Data Sheets](#)
[Case Studies](#)
[Research Reports](#)
[Whitepapers](#)
[External Threat
Assessment Report](#)
[Podcasts](#)
[Webinars](#)

Company

[Our Story](#)
[Leadership Team](#)
[Integrations](#)
[Press](#)
[Integrations](#)
[Vulnerability
Disclosure](#)

Privacy Policy

[AmIBreached](#)
[Cyble Vision](#)
[Cyble Trust Portal](#)