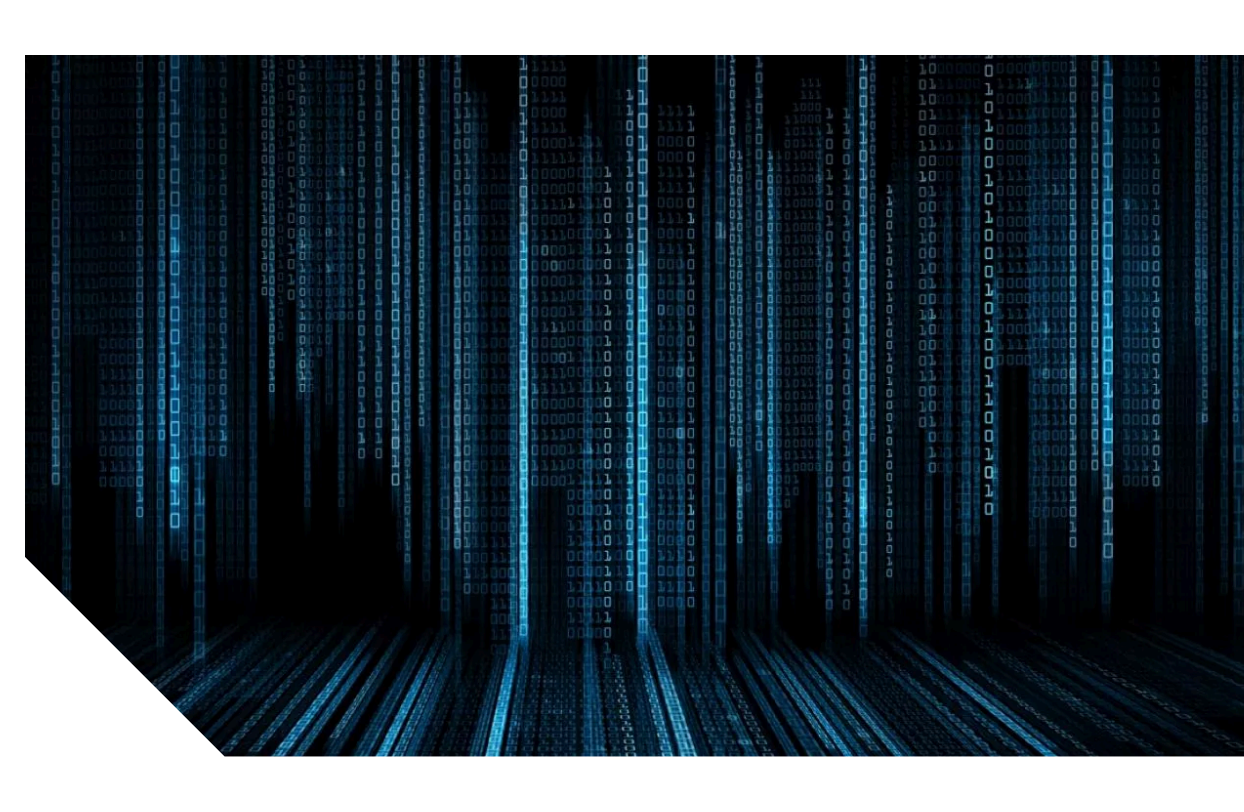
Dark Web Monitoring

January 06, 2025

Tags: Cyber Threat Intelligence



Share:

What is the dark web?

The dark web is a part of the internet that is intentionally hidden from standard search engines, making sites much more difficult to find. Data is encrypted, users' identities are protected, and URLs are not listed anywhere, requiring users to know the URL of the website to find it. Because they're designed for anonymity and privacy, many dark web locations are places where illegal goods and services are sold, where tools and information for cyberattacks are shared, and where discussions about cybercrime are hosted. This makes the dark web a rich source of threat intelligence.

What is dark web monitoring?

Dark web monitoring is the practice of tracking the activity in conversations on dark web locations to develop threat intelligence. Dark web monitoring solutions make it easier for organizations to gain access to automated, real-time information about the latest discussions concerning vulnerabilities, TTPs of threat actors, and information which has recently been exposed through data breaches.

What dark web monitoring can reveal

Because it's designed for privacy and anonymity, the dark web is unindexed, unsearchable, and not easily navigable – there are no directories telling investigators where to go to find information, nor can its content be found through search engines. Consequently, it's an ideal place for cybercriminals to go when they want to discuss, buy, sell or share the services, data and tools they use in cyberattacks. Underground forums on the dark web are the primary platform for threat actors' discussions about the latest tactics, techniques and procedures (TTPs) they're using and the unwitting victims they plan to target in an attack.

Because the dark web is such a rich source of information, sophisticated dark web cyber security investigations can reveal a great deal of critical threat intelligence.

- **Vulnerabilities**. Cybercriminals can exploit weaknesses or flaws in software to gain unauthorized access to accounts or IT systems. Threat actors will often discuss the most recently discovered vulnerabilities on underground forums, or they may share proof-of-concept or exploit kits on code repositories. This information can help teams to prioritize their patching cadence to address the most pressing vulnerabilities first.
- **Exposed credentials**. Compromised credentials accessed through techniques such as social engineering, brute-force, and infostealer botnets – enable cybercriminals to gain unauthorized access to logged-in accounts and networks, and often provide threat actors with their first foothold into enterprise systems. Monitoring this information – which is often for sale on dark web marketplaces – can help security teams understand what types of risks their users and organizations may face.
- **Data leaks**. In the wake of a cyberattack, a great deal of personal information like credit cards, Social Security numbers, and other sensitive data may be stolen and sold on the dark web or discussed in underground forums. Dark web cyber security analysts can use this information to better understand what types of attacks and TTPs have been successful so they can make plans to mitigate them.
- **Tools of the trade**. Attackers often share or sell tools and services for cyberattacks on the dark web. These include phishing kits, tools for ransomware attacks, and other types of malware and tools that can be used to successfully launch attacks. By understanding and analyzing these tools, dark web cyber security specialists can better prepare their organization's defenses against them.

What happens on the dark web?

Dark web monitoring solutions seek out and track criminal and illicit activity across a variety of sources.

Limited-access underground forums

Underground forums are established sites where reputed threat actors convene to discuss and transact the tools of their trade. These forums are arranged by thematic categories, where users post and reply to threads. Discussions can range from harmless, mundane topics to malicious cybercriminal tactics, tools and procedures, with many threat actors using these forums to transact the illicit goods and services needed to develop sophisticated cyber attacks.

Paste sites and code repositories

These are sites where users can upload large amounts of text, including compromised credentials, code, malware and data exposed during data breaches.

Illicit markets

These sites are dedicated to buying and selling illegal physical items such as weapons and drugs as well as digital items like compromised credit card numbers and corporate account credentials.

By constantly and automatically monitoring dark web sources, security teams can access a broad array of threat intelligence:

- **Chatter**: Intel derived from cybercriminal discourse, including conversations about the latest vulnerabilities and cyberattack methods, ways to carry out attacks, the latest security threats and the preferred TTPs of specific threat actors.
- **Attacks-as-a-service**: Cybercriminals turn to the dark web to hire others to carry out attacks such as network access and compromised infrastructure attacks.
- **Products for sale**: Cybercriminals can buy and sell attack methods such as ransomware or phishing kits. Data for sale can include credit card numbers, credentials and access to active systems.
- **Software-as-a-service**: Many components of a malware or ransomware attack can be purchased on the dark web.
- **Underground identities**: While the real-life identities of cybercriminals on the dark web remain anonymous, security teams can follow and track underground identities that can be helpful in building profiles of key threat actors.

The challenge of dark web monitoring

The dark web can be an invaluable source of intelligence for analysts seeking to better understand the threats against their organization. As the epicenter of cybercrime, intel extracted from the dark web can provide critical insight into the tools, tactics and procedures discussed and transacted between threat actors, the vulnerabilities they're planning to exploit and the strategies they're employing to evade current cybersecurity practices and programs.

While dark web cybersecurity monitoring is understood to be a critical component of any organization's security strategy, finding intelligence on the dark web and deriving a complete picture of the cyber threat landscape is a highly challenging task. It requires a thorough understanding of the dark web's complex ecosystem, arduous processes of infiltrating and maintaining access to heavily-guarded sources, and expertise in extracting intelligence and investigating threats.

Dark web monitoring solutions

Cybercrime is a business – and it thrives in the underground. Dark web forums, instant messaging apps and other closed sources are where various "goods" are traded: Leaked information – credentials, financial and personal. From ransomware tools and services, through malware services – all the way to insider recruitment campaigns, deep and dark web monitoring is a must for any enterprise wishing to protect against external threats.

The benefits of real-time dark web monitoring

Consider the following scenario: A threat actor has created malware and distributed it on the dark web. Traditional threat intelligence feeds will detect the new malware only once the malware is sold and weaponized, or worse, when the attack has already happened.

Bitsight dark web monitoring solves this in 3 easy steps:

1. Detect the malware when it is initially offered for sale on the dark web.
2. Extract the malware hash in the preliminary phase.
3. Block it on your firewall, trigger playbooks on your SIEM, SOAR, EPP, or VM platforms before anyone else has even downloaded it.

The impact of autonomous dark web monitoring

Your teams will combat the incoming threats faster and in a more scalable way than ever before:

- Leverage more relevant data
- Get faster, more accurate data
- Gain data that is matched with specific playbooks on your SOAR/SIEM

Features of dark web monitoring solutions

Finding valuable information on the dark web requires analysts to branch out from a small set of known dark web pages to find sites that are not designed to be easily accessible. Doing so requires time and experience in dark web analysis, which can be difficult and expensive to attract and retain in-house.

A smart approach to dark web monitoring is to use dark web monitoring tools where much of the heavy lifting in exploring the dark web has already been done. However, not all dark web monitoring tools are created equal. When selecting a solution for collecting and analyzing dark web intelligence, look for the following features.

Darknet search engines

The dark web is only accessible via the Tor browser, and no complete listing of dark web sites exists. As noted above, in order to be able to visit a particular site on the dark web, you need to know its URL. Dark web monitoring services should include a dark web search engine to make it easier to find and access sites on the dark web. With a darknet search engine, analysts can seek out keywords and other data on the dark web without needing to manually search known sites.

OSINT websites monitoring

Dark web sites can be an invaluable source of open source intelligence (OSINT). Cybercriminals commonly communicate on the dark web about successful attacks, new vulnerabilities, and the latest tools and techniques. A dark web monitoring tool should collect information from the dark web and process it to identify useful open-source intelligence. This provides analysts with invaluable contextual data about the current state of the cyber threat landscape.

Social media insights

Social media sites can be a rich source of information about their users. The dark web has social media as well in the form of forums and message boards where users communicate and post information about stolen data and illegal services. Monitoring these dark web forums can provide important information about current attack trends and the mindsets of cybercriminals operating on the dark web. Dark web monitoring tools should monitor these forums and derive analytics and threat intelligence from them.

Geofencing software

Location information can be invaluable for threat detection and incident response. Determining the source of information on the dark web can help with attributing cyberattacks and developing defenses against various threat actors. For this reason, dark web monitoring services should include the ability to geolocate the source of information on the dark web. This can help law enforcement to identify actors behind an attack and to determine the likely sources of malicious traffic on enterprise networks.

Digital risk analysis

Companies perform dark web monitoring to allow them to integrate dark web threat intelligence into their risk management strategy. Information about emerging threats, ongoing campaigns, and other threat intelligence is essential to an organization's ability to assess its risk of cyberattacks. The best dark web monitoring services should support digital risk analysis by aggregating and analyzing dark web intelligence to develop a digital risk score. This is especially important for highly-regulated businesses like the financial industry that are required to assess their cybersecurity risks and implement security controls to mitigate them.

Fighting cybercrime through dark web monitoring

Because there is no published directory of sites or hierarchy of information on the dark web, finding sources to monitor requires considerable expertise. Dark web monitoring must be done covertly, to keep security teams anonymous and to avoid exposing sensitive company information.

Bitsight offers fully automated threat intelligence solutions with powerful dark web monitoring capabilities. Collecting intelligence from 10x more dark web sources and extracting data 24x faster than our competitors, Bitsight's dark web monitoring technology lets security teams know what threat actors are planning – before they strike.

Our dark web monitoring technology collects data from the most extensive base of sources in the industry. Fully automated collection and source-infiltration gives us the ability to scrape data that is inaccessible to other vendors, including high-value sources with complex CAPCHA and posts that have since been deleted.

Using powerful NLP and OCR algorithms, we process data in all languages and formats, relying on autonomous translation and image-to-text extraction of content to deliver real-time insight into dark web threats. Leveraging advanced AI and ML algorithms, we index, correlate, analyze, tag and filter each bit of intelligence, enriching it with context about the nature, source and evolution of the threat. Along with comprehensive threat actor profiles, our dark web monitoring intelligence helps security teams protect their organizations more effectively.