An Introduction to the Dark Web and Cybercrime

By Nisos - The Managed Intelligence™ Company

Overview

In today's threat landscape, a range of managers need an understanding of the Dark Web. It's no longer solely the domain of cybersecurity managers. It is now crucial for each department to understand how cybercriminals, counterfeiters, and IP thieves use the Dark Web and how to address the risks associated with online interactions.

Many security practitioners understand that a preventative security strategy that is based on security controls is not enough. Companies must establish a proactive approach to collecting and analyzing threats that exist outside a company's firewalls, physical security perimeter, and automated fraud controls. However, according to a SANS Cyber Threat Intelligence Survey, only 42% of companies are gathering intelligence from closed or Dark Web sources.

In this ebook, we discuss how you can effectively monitor the Dark Web and how cryptocurrency is used to facilitate payment to criminals. We also provide best practice guidance for employees and enterprises to protect themselves from fraud and threats.

NISOS

What Is The Dark Web and How Do Criminals Use It?

The surface web is the portion of the world wide web that is available to the general public. It consists of 4.5 billion websites that have been indexed by search engines, like Google. Unknown to many is the fact that the surface web makes up only 4% of "the internet." The remaining 96% is known as the Deep Web.

The Deep Web isn't always a bad thing. In fact, a majority of consumers spend their time within the Deep Web. Here are some examples of web pages that traditional search engines won't index:

- HTTP forms
- Webmail
- Online banking
- Private or otherwise researched social media pages
- Select web forums
- Subscriptions protected by paywalls
- Videos on-demand
- Select online magazines and newspapers

The Dark Web is a subset of the Deep Web that is used by the criminal underground. The Dark Web can usually only be accessed by an anonymized browser, such as TOR (the Orion Router). It cannot be accessed by traditional browsers, such as Chrome, on the surface web.

NISOS

How Do You Access the Dark Web?

To access the Dark Web, you must use a specific type of internet browser. Here are three popular choices:

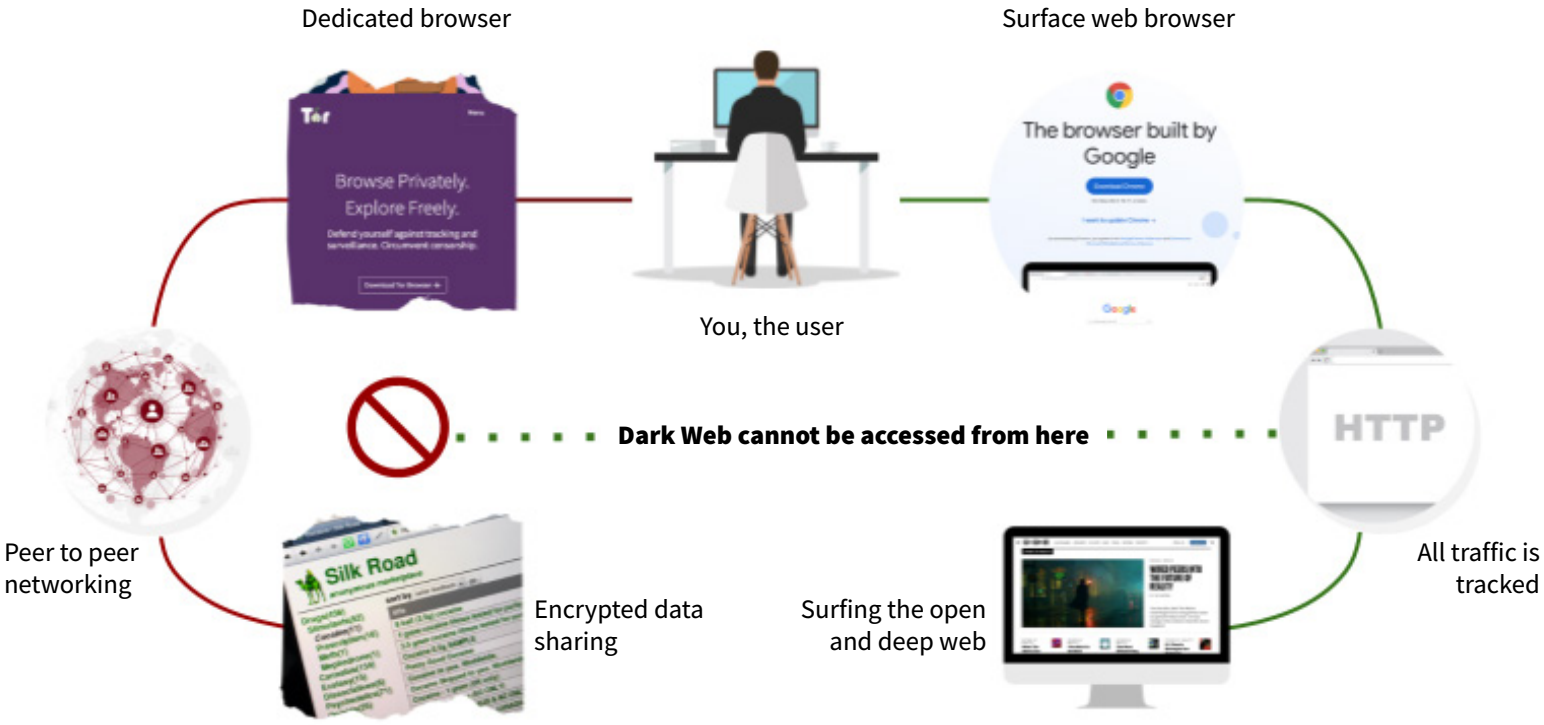
- **TOR:** The most popular anonymizing browser used to access the Dark Web.
- **Brave Browser:** An offshoot of Chrome also used to access the Dark Web.
- **i2P (The Invisible Internet Project):** An anonymous network layer that uses end-to-end encryption and anonymous connections to successfully encrypt a user's traffic. i2P sends user data through a volunteer-run network of roughly 55,000 computers around the world.

The surface web consists of an interconnected network of websites accessed in a web browser, such as Chrome, Microsoft Edge, or Firefox. When a user enters a website through a browser, it reaches a DNS server that attaches the website address to a web server and directs the user to a destination.

Any information downloaded is tracked by the browser through web cookies, which helps users to log in to websites by remembering past user activity.

On the Dark Web, an entirely different network of websites and servers are connected through a set of dark-web-only browsers. Usually, a peer-hosted networking setup is designed so users can go to TOR's website, download TOR technology, and run it on their network.

This allows other TOR users to "bounce traffic" through their computer as one of the anonymized points in the network, making it difficult to identify sources and locations of information and users. A special TOR browser is used to take advantage of the technology. This browser works to allow users to surf the Dark Web anonymously by directing traffic through a network of intermediaries (adding layers).



NISOS

The surface web consists of an interconnected network of websites accessed in a web browser, such as Chrome, Microsoft Edge, or Firefox. When a user enters a website through a browser, it reaches a DNS server that attaches the website address to a web server and directs the user to a destination. Any information downloaded is tracked by the browser through web cookies, which helps users to log in to websites by remembering past user activity.

On the Dark Web, an entirely different network of websites and servers are connected through a set of dark-web-only browsers. Usually, a peer-hosted networking setup is designed so users can go to TOR's website, download TOR technology, and run it on their network. This allows other TOR users to "bounce traffic" through their computer as one of the anonymized points in the network, making it difficult to identify sources and locations of information and users. A special TOR browser is used to take advantage of the technology.

The Role of Cryptocurrency in Facilitating Anonymized Payments

Cryptocurrency, the preferred payment on the Dark Web, is a largely decentralized and anonymized currency. Hundreds of cryptocurrencies exist, with Bitcoin and Ethereum being the most popular.

A public ledger of transactions is available for anyone to see, but wallets and their contents on the blockchain are typically run through cryptocurrency tumblers, making it very difficult to track transactions to an individual user.

It should be noted that small and large payments can be made instantaneously and do not need to be routed through centralized payment systems commonly used by the public.

Criminals often use cryptocurrency tumblers to mix potentially tainted identifiable crypto funds with legitimate sources. These tumblers are used to obscure the trail back to the fund's original source - just like traditional money laundering.

NISOS

Common Cybercrimes on the Dark Web

While the majority of Dark Web criminal activity consists of drug trafficking, child pornography, identity theft, and the sale of illegal and illicit products, other crimes take place as well. The sale of access to your organization is one such example. Whether criminals are selling credentials, exacting product fraud, stealing intellectual property, or performing ransomware extortion, the Dark Web is where you'll be able to find indicators of breaches or illegal events involving your brand.

Threat Actors Conducting Cybercrime

There are multiple types of people that interact on the Dark Web. While most of the cybercrime activities are untraceable until results appear on the surface web, there are some intervention activities you can perform based upon the results of proactive monitoring efforts. Here are the four types of roles actors play in the Dark Web.

Sellers

Initial Access Brokers

Exploit and Tool Developers

Technical Operators

NISOS

Threat Actors Conducting Cybercrime

Sellers: Sellers have low to moderate technical sophistication and possess a desirable commodity. They typically provide access to a set of product brokers, but also personally operate on public marketplaces. They will sell illicit goods, such as social media accounts, gift cards, or data dumps containing personal identities.

Generally, these sellers can get paid anywhere from hundreds to tens of thousands of dollars for their commodities. Their price is dependent upon the quantity, validity, and sensitivity of what they sell.

Initial Access Brokers: Initial access brokers lay the groundwork for more advanced technical operators who will conduct the cybercrime.

These middlemen validate initial access to networks and ensure that the commodities purchased from the sellers are valid.

As part of their work, they operate scanning tools to identify vulnerable organizations. It is not uncommon for initial access brokers to validate VPN and RDP credentials.

No industry is immune from being targeted by initial access brokers. Currently, the technology sector commands the highest prices for access, estimated at an average of $13,000 per access in 2020.

As shown with past breaches, the compromise of one company can potentially lead to the compromise of many.

Exploit and Tool Developers: Exploit and tool developers are a critical choke point in the cybercrime and fraud ecosystems. They are the technical experts who develop N-day (known vulnerability) exploits to critical services and give access to other malicious operators.

Exploit and tool developers also build malware tools, such as credential harvesters or phishing kits, used to trick victims in social engineering campaigns. And they develop scraping tools and the associated social media sock puppet accounts used to propagate disinformation.

Technical Operators: The technical operators are the “tip of the spear” in the cybercrime ecosystem. They possess the required technical sophistication to execute the crimes. Their main objectives and crimes include:

- Defrauding individuals and using social engineering to convince people to send them money.
- Purchasing initial access from brokers and moving laterally, escalating privileges, and stealing data.
- Exfiltrating data from companies to hand off to a broker or seller.
- Conducting ransomware or disinformation campaigns.
- Engaging employees to execute a malicious payload in order to gain remote code execution on a device.

After they achieve their collection objective and monetize the event, the process begins all over again. Many times there are artifacts - such as usernames and passwords from a domain controller, credit card numbers, etc. - from the “collection” that can be re-sold into the ecosystem.

NISOS

5 Business Use Cases for Monitoring the Dark Web

Cyber Threat Intelligence

- Prevent leaked credentials for privileged access
- Stop exploits to various services that allow initial access
- Build container environments to alleviate data leakage
- Filter out phishing or command and control infrastructure
- Block access to fraudulent domains
- Identify/Mitigate ransomware as a service
- Encrypt different keys and cloud access credentials to production databases found in third-party repositories

Physical Security Intelligence

- Identify Personal identifiable information (PII) that's been exfiltrated
- Monitor for leaked credentials
- Scan for fraudulent schemes, including the opening of credit cards
- Analyze and track negative public sentiment
- Track closed forums and Dark Web for the potential of threats, violence, and physical demonstration

Platform and Fraud Intelligence

- Stop Personally Identifiable Information from being used against consumers
- Analyze and prevent identity fraud
- Flag and block fraudulent bank and gift cards
- Prevent credential stuffing and other brute force attacks
- Identify stolen account purchases and account takeovers disinformation as a service

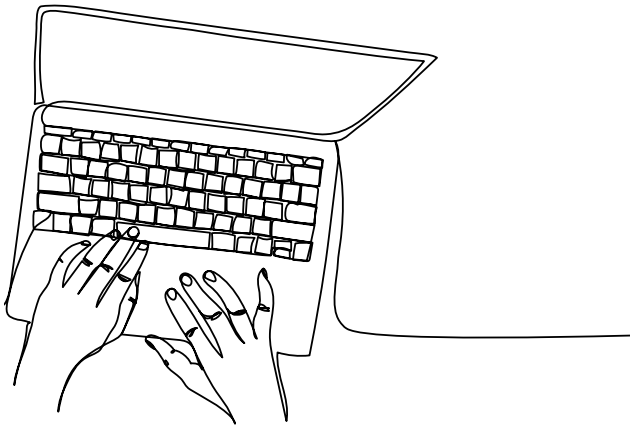
Reputation Intelligence

- Address false-placed negative sentiment
- Monitor discussions of the company or executives
- Highlight infrastructure used in the technology and network stack

Third-Party Intelligence

- Early detection of third-party supplier breaches
- Triage for credential stuffing attacks that are successful against the supplier
- Analyze data leaks to identify relevant client data

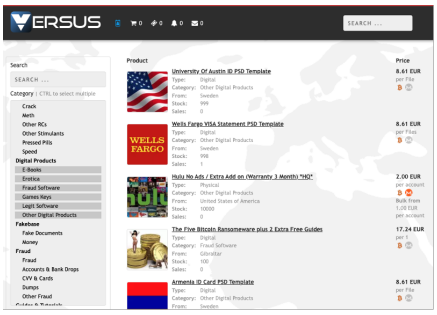
All of these intelligence domains can be used to inform clients of weaknesses and potential threats that exist in the Dark Web and closed sources.

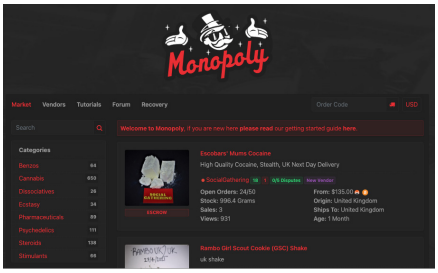


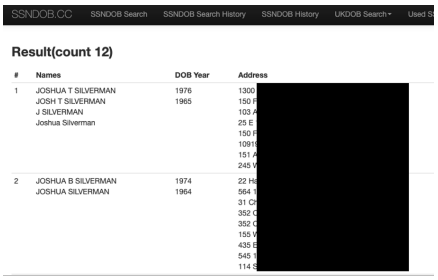
NISOS

Dark Web Marketplaces

Many Dark Web marketplaces are crowdsourced, which means anyone can sign up and sell illicit goods. Versus Market, Monopoly Market, and SSNDOB are examples of these types of illicit online marketplaces.







Commodity Goods Sold on Crowdsourced Forums

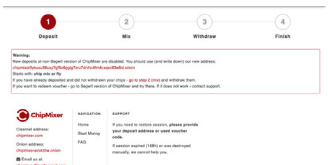
Pervasive fraud techniques available within crowdsourced forums include:

Carding: Carding includes hacked accounts or stolen credit cards for sale. Usually, threat actors will take payment cards, link to accounts or payment cards they've stolen, and sell that information. This is called "cashing out" and is done by purchasing multiple gift cards that are difficult to track.

Often social engineering attempts occur through email phishing intended to obtain credit card and personal information. Actors now even include two-factor authentication services in their social engineered events, with the hope of capturing an active session cookie and mimicking browser sessions of victims allowing them to bypass credential logins.

Tutorials: Tutorials explain the process of carding and bypassing client security, login, and account verification. A popular tutorial found in forums details the use of refund services for gig-economy applications, such as Grubhub and Postmates. Actors often sell tutorials detailing how to facilitate refunds from legitimate apps.

Money Laundering: Money laundering with cryptocurrency is usually done through "tumblers." Tumbler services receive cryptocurrency and then send several transactions through multiple wallets in different increments. This prevents the utilization of public blockchain records to follow the transactions. The return is then deposited into an actor's cryptocurrency wallet. Some examples of crypto tumblers are mixtum.io, CryptoMixer, and ChipMixer.



Fake Accounts: Often, threat actors get kicked off platforms for illicit activity. To regain access, they create sock puppet accounts (fake personas) with fake emails and burner phone numbers. The fake accounts are verified with ID and connected to Facebook or Google accounts, including SMS verification.

NISOS

Recommended Security Controls

Illicit marketplaces allow fraudsters to manipulate the security controls intended to protect employees and enterprise networks. A comprehensive and intelligent defense strategy is required to counter this manipulation.

Advice for Enterprise

- **Security Awareness Training:** Organizations should continuously educate their employees. Users need to be educated on the new and emerging fraud and phishing schemes. Education should also emphasize that self-reporting malicious activity is critical to establishing a strong security posture.
- **Anti-Malware Tooling:** Deployment of endpoint detection and response (EDR) capabilities allows security teams to monitor malicious activities on endpoints and servers and are critical to a comprehensive security program.
- **Intelligence Augmentation:** Integrating threat intelligence on stolen credentials with a two-factor authentication process will help with identifying and countering the use of compromised credentials.
- **Identity Access Management:** Implementing a system of "least privilege" allows limited users access to sensitive data. Therefore, when credentials are compromised and illicit network access is gained by threat actors it will prevent or delay their ability to steal sensitive production data.

How to Monitor the Dark Web

The use of experts to conduct Dark Web monitoring and analysis can significantly improve an organization's risk awareness and posture. In many cases, actions that take place on the Dark Web between sellers, brokers, developers, and operators are indicators of past or impending events. Threat actors can often be found discussing exploits before events take place. Properly analyzing these threats, requires specialists with access to a wide range of datasets and threat intelligence feeds. Monitoring generally takes two forms:

- **Open-source monitoring** for proprietary data, lost credentials, discussions of the company or executives, data leaks from suppliers, and details of infrastructure used in a company's technology and network stack.
- **External attack surface monitoring** of your perimeter to validate if credentials or exploits are being used against your employees or organization.

Provide Control Access at the Individual Level

- **Password Manager:** Individuals should use password managers such as 1Password and LastPass to authenticate all services on the internet. Users should never save passwords in browsers.
- **Two-Factor Authentication:** Two-factor authentication should be registered for all services including email, banking, anything sensitive, and anything that could be used to gain access to other services.
- **Credit Monitoring:** It's important to apply credit locks to prevent threat actors from opening new credit cards or mortgages.

If you would like to learn more about the Dark Web or would like assistance with Managed Intelligence™ - Nisos can help. Learn more at www.nisos.com