MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

WHITE PAPER

The Deep Web and Dark Web — Illuminating Defense Strategies

Table of Contents

Executive Summary 3

The Deep Web and Darknet - A Quick Primer 5

Know the Risks to Your Organization 7

Use Cases: How Attacks Work in the Dark Web 10

Combatting Cyberattacks in the Deep and Dark Web 12

Conclusion 14

Executive Summary

Recent years have seen a surge in cyberattacks that target corporate infrastructure, and the cybercriminals that perpetrate such attacks are flourishing like never before – operating in the shadows, hidden from detection. It is here in the murky and nebulous layers of the Internet called the Deep Web and Dark Web that cybercrime and hacktivism continue to evolve.

These expansive segments of the Internet represent a fundamentally different cyber battleground for companies. Unindexed sites in the Deep Web are often hidden from view, and in the Dark Web, where identities are anonymous, cybercriminals are free to operate with impunity to buy and sell stolen credit cards and corporate network logins, exchange codebreaking tactics and plan their cyberattacks with one another. An ensuing data breach may expose a wealth of information, including intellectual property, proprietary corporate data, and personally identifiable information of employees or customers.

Corporations at particular risk include financial services and healthcare organizations, where large customer bases routinely access financial or personal information online. A substantial cache of stolen data can fetch a heavy price for cybercriminals when sold on the Dark Web. Other prime targets include e-commerce or manufacturing companies, where employees and large networks of business partners access their internal systems on a daily basis. All organizations must evolve their protection strategies to carefully monitor potential threat actors, build the necessary intelligence to minimize the damage and ensure appropriate security measures are put in place.

DIVE IN

The Deep Web and Dark Web — A Quick Primer

The Deep Web and Darknet - A Quick Primer

The Deep Web

To gain a better understanding of the full Internet landscape, picture an iceberg. Visible above the water is the surface web, comprised of traditional websites that are indexed by standard search engines. It is what most of us use every day to find information, shop and interact online, but it accounts for only about four percent of the Internet.

Most of the content in the Deep Web contains information for legitimate uses – including corporate intranets or academic resources residing behind a firewall, social media sites hidden behind a login page, online forms, pop-up ads and pages that are unlinked to any other site.[1]

But some sites in the Deep Web also represent a potentially unauthorized or suspicious content, such as phishing sites that collect user credentials, sites that disseminate malware that deliberately try to hide their existence, websites and marketplaces that sell counterfeit goods, and peer-to-peer sites where piracy often takes place. Consumers may unknowingly stumble upon these unauthorized sites through spam emails, advertisements or cybersquatted domains and are at risk of unwittingly releasing personal information or credentials to fraudulent entities.

2.5M

Number of people who access the Dark Web content via Tor daily.

The Dark Web

Dig deeper underneath the surface layer of the Internet and you come to the Dark Web, a smaller but potentially more dangerous subset of the Deep Web. The Dark Web is the collection of websites and content that exists on Dark Nets – overlay networks whose Internet Protocol (IP) addresses are completely hidden. Both publishers and visitors to Dark Web sites are entirely anonymous.

Access to the Dark Web content can only be achieved by using special software such as Tor or alternatives like Freenet, Invisible Internet Project (I2P) and Tails. Tor is free to download and use, and it enables anonymous access and communication within the Dark Net. Today 2.5 million[2] people access Dark Web content via Tor daily. It is often used by strong privacy advocates, such as journalists or law enforcement agencies, that may be searching for dangerous or sensitive information and don't want their online activity tracked.

It is the very anonymity of the Dark Web that makes it an ideal foundation for illicit and criminal activity. Vast quantities of private information, such as login credentials and banking and credit card information, are peddled with impunity on crypto-marketplaces. Cybercriminals also offer their services for hire and even provide tutorials on codebreaking and how to infiltrate corporate networks. Cybercrime itself has become a service that is offered pervasively in the Dark Web.

With Bitcoin used as the preferred currency, every transaction between buyer and seller can be conducted anonymously in the Dark Web. Bitcoin transactions are not associated with names, addresses or any identifying information, so there is no way to trace purchases, and law enforcement cannot follow a money trail to the source of the activity. Bitcoin has decentralized payment processing in the Dark Web and made it anonymous, and it has brought crypto-markets to a new level of popularity and pervasiveness.

Did you know?

The most vulnerable points of access to any network are individuals, such as consumers and employees.

Know the Risks to Your Organization

The existence of the Deep Web and Dark Web isn't new, but in recent years, fraudsters and cybercriminals have been honing their tactics in these hidden digital channels to strike at their prey more effectively and minimize their own risk of being caught. Moreover, as a higher volume of users learn the intricacies of Tor to access and navigate the Dark Web, the more difficult it is to identify a single user and track down cybercriminals.

Most organizations have implemented stringent security protocols to safeguard their IT infrastructure, but conventional security measures are designed to protect data and assets inside the firewall, not outside. Targeted attacks like Business Email Spoofing (BES), whereby an internal employee receives an email purportedly from a corporate executive or the IT team requesting login or password information, are difficult to detect with traditional email security. Much like a consumer phishing or malware scam, BES attacks use sophisticated social engineering tactics to compromise login information, which can then be distributed via the Dark Web and eventually precipitate a full-scale cyberattack and data breach.

In the end, the most vulnerable points of access to any network are individuals, such as consumers and employees. Even knowledgeable users may be duped by a BES or phishing attack. And the more people that have access to your network, the more potential lapses may occur. Companies that have large partners, distributors or affiliate organizations have a larger problem as they allow access to a greater number of individuals. The sharing of confidential data on paste sites can also become a target for theft or misuse. No amount of IT security will prevent a "back door" attack on the infrastructure where an individual unwittingly surrenders the key.

Cyberattacks that propagate in the Dark Web pose a significant threat to proprietary corporate information, trade secrets, employee network access credentials and consumer financial and personal information.

Consumers may similarly be duped by brand-associated social engineering attacks, unknowingly revealing personal or financial information that can be sold on criminal Dark Web networks. Cybercriminals move silently and quickly to exploit the valuable data before the user becomes aware.

Monitoring potential threats in the Deep Web and Dark Web gives you the intelligence to take appropriate action. Cybercriminals often communicate and interact via private, cybercriminal social media forums and chat rooms and in some cases, threat actors even boast or congratulate each other after successful attacks, which can be tracked and monitored. Threat intelligence empowers you to take action by allocating the right security resources before an attack, or the data to connect the dots between threat actors to prevent future attacks. In other cases, you can mitigate the damage of a data breach – for example when credit card numbers are stolen – by working with financial institutions to cancel the cards before they can be used fraudulently.

The stakes for companies are high. Cyberattacks that propagate in the Dark Web pose a significant threat to proprietary corporate information, trade secrets, employee network access credentials and consumer financial and personal information. It falls to organizations and their Security Operations Centers (SOC) to identify the activity in order to limit financial liability to the company and irreparable damage to the brand.

The Deep Web and Darknet - A Quick Primer

SURFACE WEB

DEEP WEB

CHALLENGES TO ORGANIZATIONS

- Content on unindexed sites is harder to monitor manually
- Phishing and malware distribution sites are unindexed since they are only active for a few hours or days
- Proprietary information distributed on paste sites

HOW TO TAKE ACTION

- Automatically monitor and detect unauthorized sites
- Pursue enforcement and shut down site or remove content when applicable
- Ongoing consumer education

DARK WEB

CHALLENGES TO ORGANIZATIONS

- Users entirely anonymous
- Confidential data leakage and circulation
- User credentials stolen and sold
- Bitcoin transactions hide audit trail

HOW TO TAKE ACTION

- Enable alerts before, during or after attacks
- Analyze and investigate attack details to determine a course of action
- Ensure appropriate security measures relevant to the attack are put in place
- Educate and inform customers to maintain trust

With a "credit card dump," cybercriminals may hack a retailer's network, use malware to infect a point-of-sale device or use a phishing attack in order to steal and sell credit card numbers, expiration dates and other user information in the Dark Web.

Use Cases: How Attacks Work in the Dark Web

Financial Services

Visibility into Dark Web activity can yield important benefits for financial institutions. Clues for an impending attack might potentially be uncovered to save millions of dollars in breaches and stop the erosion of customer trust. Improved visibility can also help companies identify a person sharing insider or proprietary information in the Dark Web and determine the right course of action to minimize the damage.

One of the most common attacks against the financial services industry is called a "credit card dump." Cybercriminals may hack a retailer's network, use malware to infect a point-of-sale device or use a phishing attack in order to steal and sell credit card numbers, expiration dates and other user information in the Dark Web. Other criminals can then use the information to create fake cards to make unauthorized purchases.

In one case, detailed intelligence and analysis uncovered a large trove of stolen credit cards, and the insight gave the organization the knowledge it needed to contact customer service, validate cards that were cancelled, and shut down and re-issue cards that were still active.[3] Actionable intelligence helped determine the right course of action to minimize the damage, and do it quickly.

Healthcare

Data breaches in the healthcare industry can be especially alarming because they expose not only the healthcare organization's proprietary data, but also a vast number of people's medical information and associated personal information. A dump of customer information, from a medical clinic in one example, included images of authorized signatures, email addresses, billing addresses and account numbers.[4]

Cybercriminals who use information like this can exploit it to compromise more data, such as social security numbers and private medical records. Credentials could even potentially lead to false identities being sold.

Identifying this type of breach provides the intelligence necessary to contact customers, banks and other impacted organizations to mitigate the damage and take corrective action. Visibility into these types of attacks also provides insight into planned or potential attacks against the healthcare network.

Engineers and Software Code

Data shared in public websites or social media forums can inadvertently lead to cyberattacks and data breaches. For example, an engineer who asks a question of fellow engineers about a coding issue might share proprietary source code within the group. Seeing how internal code is designed could help an attacker identify potential vulnerabilities and open the door to hacking or cyberattack.

Part of the solution for situations like this is advance education about the dangers of sharing code publicly. In addition to ad hoc management of individual events, group training can be conducted for an entire engineering group, for example, to remind them of the importance of protecting proprietary information.

Combatting Cyberattacks in the Deep and Dark Web

1. Monitor Threats Across Mutiple Cybercrime Zones

IT security teams should ensure they are monitoring as many digital segments as possible where cybercrime frequently takes place. These include not only Deep Web and Dark Web sites but also other digital channels where fraudster-to-fraudster interactions occur, such as social networks, Internet Relay Chat (IRC) and chat sites and data paste sites. Companies must also take an effective defensive posture, developing advanced alerts before, during or after an attack occurs, ultimately providing the vital intelligence needed to take the appropriate action.

2. Find Efficient Ways to Infiltrate Criminal Networks

Some organizations might be tempted to try their hand at infiltrating cyberthreats in the Dark Web themselves. In order to do so, however, they must first go through the painstaking process of scouring the Dark Web and trying to access cybercriminal hangouts manually to detect and identify threats. They then must find a way to "build trust" with hackers and fraudsters over time. Even a large team of security analysts cannot sufficiently achieve the coverage needed for any measurable success. Such attempts are labor-intensive, time-consuming and by no means scalable as a reliable security strategy. It is better to employ an automated approach that leverages smart technology to achieve network penetration faster and in more coordinated fashion.

3. Make Education and Awareness a Priority

Education should focus on two distinct audiences to raise awareness of threats before they can impact your company. Customer outreach is critical, in particular for companies in financial

services, healthcare and other industries where users access and exchange personal or financial information. Online consumers must be regularly reminded of the dangers of phishing scams and social engineering attacks, and that they should never provide personal information unless on the verified banking, healthcare or partner site.

Likewise, internal employees and business partner employees are increasingly being targeted for attack through BES and other spearphishing attacks. Human resources and Payroll professionals are becoming common targets for these corporate-focused attacks because of the access they have to employee and other sensitive company information. Employees who commonly receive requests from senior executives (CEO/CFO/COO) may be particularly vulnerable to these types of attacks. Internal education for the entire company and the partner channel can go a long way to mitigating the potential for attack and serious data breach.

Conclusion

As corporate cyberattacks continue to thrive, companies must boost their knowledge of how these attacks can impact their networks and customers, and learn to take effective action. In spite of heavy investments in conventional security protocols, most organizations cannot unearth the vital intelligence that can help them prepare for and respond to attacks in a meaningful way. The very nature of the Deep Web and Dark Web make monitoring, detecting and protecting their organization from attacks difficult. Breached data that ends up in these realms can cause organizations and their customers significant financial loss. The key to combatting these threats is cyber intelligence. The deeper visibility you gain, and the more cybercrime zones you can monitor, the better your chances of taking decisive action to prevent the worst in an attack.

[1] DEEPDOTWEB, The Dark Web, Deep Web and Dark Net – Terminology Hell, JUNE 8, 2015. https://www.deepdotweb.com/2015/06/08/the-dark-web-deep-web-and-dark-net-terminology-hell/
[2] Wikipedia, Tor (Anonymity Network). https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29
[3] MarkMonitor Data. 2016.
[4] MarkMonitor Data. 2016.

About MarkMonitor

MarkMonitor, the leading enterprise brand protection solution and a Clarivate Analytics flagship brand, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of advanced technology, comprehensive protection and extensive industry relationships to address their brand infringement risks and preserve their marketing investments, revenues and customer trust. For more information, visit **markmonitor.com**.

About Clarivate Analytics

Clarivate Analytics accelerates the pace of innovation by providing trusted insights and analytics to customers around the world, enabling them to discover, protect and commercialize new ideas faster. Formerly the Intellectual Property and Science business of Thomson Reuters, we own and operate a collection of leading subscription-based services focused on scientific and academic research, patent analytics and regulatory standards, pharmaceutical and biotech intelligence, trademark protection, domain brand protection and intellectual property management. Clarivate Analytics is now an independent company with over 4,000 employees, operating in more than 100 countries and owns well-known brands that include *Web of Science, Cortellis, Thomson Innovation, Derwent World Patents Index, CompuMark, MarkMonitor* and *Techstreet*, among others. For more information, visit **clarivate.com**.

More than half the Fortune 100 trust MarkMonitor to protect their brands online.

See what we can do for you.

U.S. (800) 745-9229 **Europe +44 (0) 207 433 4000** **www.markmonitor.com**

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

© 2017 MarkMonitor Inc. All rights reserved. MarkMonitor® is a registered trademark of MarkMonitor Inc., a Clarivate Analytics brand. All other trademarks included herein are the property of their respective owners. MarkMonitor solutions are protected by US patent rights, including US 7,346,605. Other patents pending. Source code: DWWP110116

LEARN MORE
MARKMONITOR.COM/DARKWEB
MarkMonitor
Protecting brands in the digital world
Clarivate
Analytics