WHY THE DARK WEB MATTERS TO HEALTHCARE CYBERSECURITY

Authored by:
Colin Konschak, FACHE, Divurgent
Shane Danaher, MBA, Divurgent

www.divurgent.com © Divurgent 2017-2018

INTRODUCTION

By now people in every business sector have heard about, and learned to fear the Dark Web, whether or not they truly understand what it is or why they should be afraid of it. Credit monitoring and financial management companies take advantage of this fear by offering Dark Web threat detection services, promising to scan the Dark Web for individuals' sensitive information.

Despite all of this concern and activity, the Dark Web—unlike other issues we have covered in this cybersecurity whitepaper series—is not something like ransomware, phishing, denial of services attacks, or other threats The Dark Web is where all cybercriminals can communicate with each other – it is an online black marketplace for stolen information that provides a great degree of anonymity for cyber criminals.

What it does in terms of its relationship to healthcare is incentivize these other nefarious activities and make healthcare a particularly lucrative target for those crimes because of the usefulness of its information. That's why the Dark Web is important to consider in keeping sensitive information safe in healthcare. In this latest whitepaper in our cybersecurity series, we explore the Dark Web and present some methods for securing your information , starting with a few definitions.

WHAT IS THE DARK WEB?

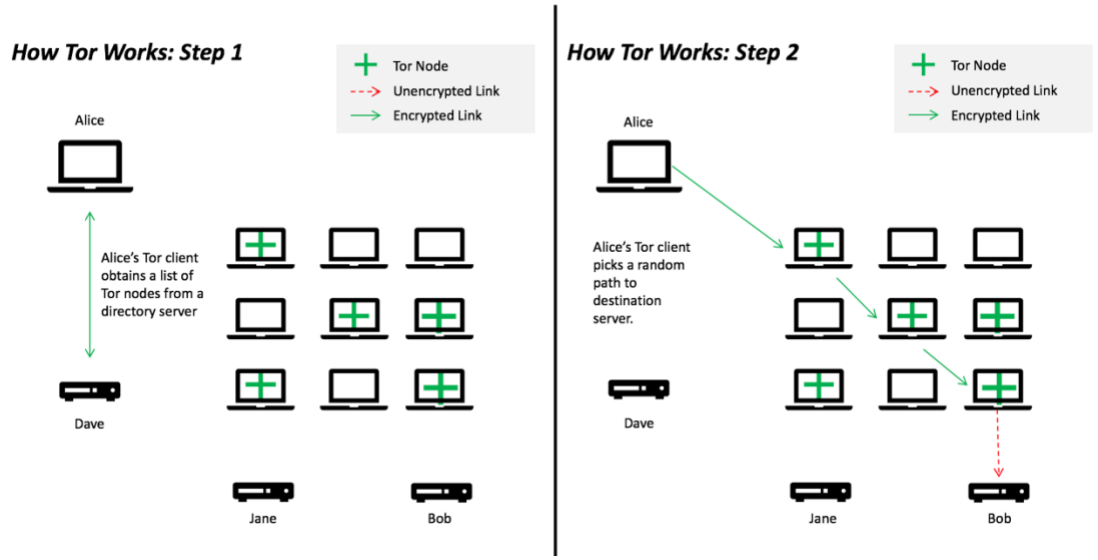
Understanding the Dark Web starts with familiarity with the internet's structure. The internet most people are familiar with—where they go on Facebook or Twitter, buy things on Amazon, or use search engines like Google—is called the "Clear Web" or the "Surface Web." But no matter how unfathomably vast it may seem to most people, the part of the internet that is visible to the general public makes up only about 4 percent of what is actually there. The other 96 percent is known as the "Deep Web" because it can't be accessed by searching with Google or any other common Web browser.

Despite its slightly sinister name, most of the Deep Web is above board and not used for nefarious activity. The Deep Web is internet content that, for various reasons, can't be indexed by search engines like Google. The Deep Web can only be obtained by searching strictly within a website, and includes dynamic web pages, unlinked sites, non-HTML/-contextual/-scripted content, limited-access networks and blocked sites (which require access through CAPTCHA- a program or system that distinguishes human from machine input, thwarting bots, spam, etc.)

The Dark Web is a different matter. Contrary to what many believe, the Dark Web is not a dark part of the internet, or one that simply allows cyber-crime. It was not created by design to enable criminal activities. Its major differentiation from other parts of the internet is that it can only be accessed using specialized browsers, the most popular of which is The Onion Router, or Tor (Ciancaglini, 2016). Tor and other browsing software of its type were created to secure communications and, in many cases, became platforms for good, facilitating free speech in repressive nations where censorship of the press and authoritarianism are the norm. For example, the mobilization of the Arab spring protests was facilitated by the Dark Web. But like any other tool, the Dark Web may be used in criminal pursuits, depending on a user's intent (Ciancaglini et al, 2016. P.3).

According to the Tor Project (at http://torproject.org), Tor is free software that is used on an open network designed to protect users against traffic analysis. Users are routed through a network of servers operated by volunteers, making users' traffic untraceable and creating greater privacy. Even though the Dark Web does not anonymize activities, users often navigate through such directories as the "Hidden Wiki," which organizes sites by category (Finklea, 2017 p.2).

Figure 1: How Tor Works



On the Dark Web, people communicate via email, web chats, and the Tor personal messaging platform. Although the Dark Web is used for legitimate purposes, the ability to host intentionally concealed content on it also creates an ideal environment for hiding criminal or otherwise malicious activities including guns, counterfeit money, contraband and illicit drugs. Tor has been used to circumvent censorship, access classified contents, and disrupt sensitive government communications. A range of malicious activities, from terrorism to cyber-ambushing of prominent individuals, is being carried out on the Dark Web. It is uncertain how much of the Dark Web is committed to serving a particular illegitimate market at one time, or how much traffic is flowing to any given site.

Healthcare information is among many offerings on the Dark Web. Research has shown that account information and free passwords for sites like Netflix, Hulu and Spotify are all available for pennies on the Dark Web. In addition, the Dark Web has become a digital hub for child pornography.

HEALTHCARE INFORMATION AND THE DARK WEB

One of the best starting points for developing an effective cybersecurity plan in any business sector is understanding who is targeting you and why. An underground network of criminals has been growing in the Dark Web, employing continually morphing strategies and technological abilities that the healthcare system's IT infrastructure and culture has not been able to match. They have preyed on financial institutions and their customers, stealing credit card numbers and other data to perpetrate fraud in the black market. They have now launched attacks on the healthcare system in a range of cyber-attack strategies for stealing health records, forcing hospitals to pay ransom, and making patients prove their innocence over identity fraud charges.

So what healthcare information is out there on the Dark Web, how does it get there and why is it so attractive to cybercriminals?

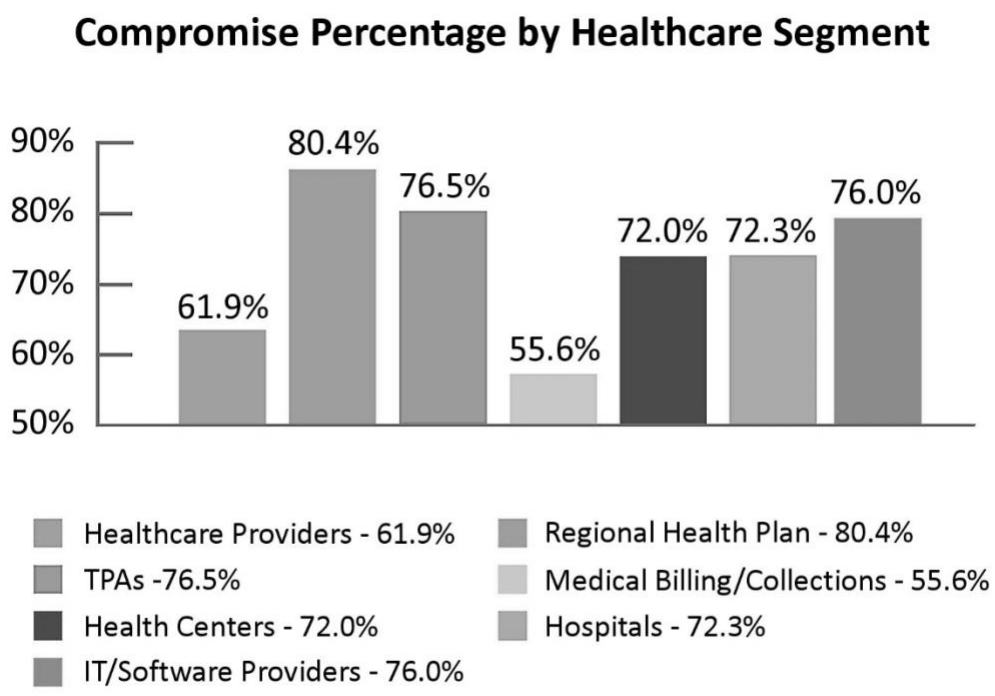
When we think of stolen information available on the Dark Web we often go immediately to personally identifiable information (PII) or protected health information (PHI), which cannot only compromise individuals, but can get healthcare organizations in hot water with violations of the Health Information Portability and Accountability Act (HIPAA).

But there is other, potentially more dangerous information out there in the form of compromised email credentials from healthcare organizations, which can be used to commit further cyber breaches of those organizations.

Compromised email credentials from healthcare bought and sold on the Dark Web can be used to study targeted organizations, gain access to their networks and systems, gain greater access privileges, and move around the organization in a pivot attack, extracting data and controlling access. Having this information can make brute force and social engineering attacks easier for cybercriminals (Evolve IP, 2017).

In a 2017 Dark Web analysis conducted jointly by cloud services company Evolve IP and threat intelligence firm ID Agent, 1,000 different healthcare companies across a range of business types and sizes were reviewed. The study found that an average of 68 percent of the companies have compromised email credentials that are "visible and available" on the Dark Web. Depending on the market segment, those numbers range from 55.6 percent to 80.4 percent (see Figure 2 below).

Figure 2: Email Credential Compromise in Healthcare



Source: Evolve IP. (2017). *Email Vulnerability in Healthcare*.

The study found that 76 percent of the hacked healthcare email records reviewed on the Dark Web had passwords associated with them, and of those, 23 percent had passwords that were fully visible. The authors state that even if the passwords are outdated, the information is still valuable because other studies show that people use the same or similar passwords in all of their activities online, and cyber criminals can use algorithms or simple logic to figure out how a user's password will evolve over time (Evolve IP, 2017).

Still, the value of PII and PHI stolen from healthcare organizations and sold on the Dark Web creates a great incentive for criminals to find new and more ingenious ways to get it. The electronic health record is a great source of PHI and PII. Medical records can be much more valuable to identity thieves than financial records because along with the usual information like credit card numbers, the typical healthcare record has at least 18 protected personal health identifiers, including name, social security number, address, phone number, and other financial information. Health records also contain health insurance information that criminals can use to create fake insurance credentials, giving them access to medical care and prescription drugs. The cybercriminals then turn around and sell those drugs on the Dark Web.

A 2016 report from the Institute for Critical Infrastructure Technology states that cybercriminals are breaching healthcare systems looking not only for personal identity information, but also are sometimes targeting specific high-profile patients or trying to find potentially harmful information about healthcare providers (ICIT, 2016).

Much has been made about the high value of healthcare information, but on the Dark Web is where the issue of price comes in. Even though there is high demand for the data, the sheer amount of hacked healthcare records on the Dark Web means the price is dropping, though it is still high compared to other types of information offered there. From 2016 to 2017, the value of an individual record dropped from an average between $70 and $100 to an average $20 to $50 (Richard, 2017).

Much of this Dark Web-marketable material can be found in electronic health records (EHRs). The complexity of the EHR systems ensures that no one person in a healthcare organization has a holistic understanding of how the system works. Technological evolutions occur within IT infrastructures in health organizations as they merge, acquire, or add services with a plethora of vendors who can introduce even more cybersecurity vulnerabilities as the attack surface expands. These software vulnerabilities are exploited as part of the attack strategy.

The EHR, which serves as a data repository, communication, and information exchange platform among physicians, patients and the general care system has become the primary target for cybercriminals seeking multi-institutional patient data they can sell on the Dark Web. Let's look at how some of the attacks work in stealing this data.

A BIG BUSINESS ATTACK METHODOLOGY

As we have mentioned throughout this series, cybercrime is no longer about some young hacker sitting in his basement trying to find a way into your computer. Cybercrime is big business. Although they may work anonymously through underground computer channels on the Dark Web, they run as smoothly as any corporation in a skyscraper, vetting "employees" and collaborators. They have marketing departments, programming experts, and business managers. And, just like any other business, they know their audience and target their attacks accordingly.

During the intelligence-gathering stage, they look not just for strategic information about the target, but also the organization's overall IT infrastructure. They learn about the target's applications and software and how they're used, including the organization's hierarchy.

This can be a lengthy process, especially when large corporations are the targets. Organizations with superior security systems can create some barriers, but the intelligence-gathering stage helps cybercriminals create an attack plan that can avoid those systems.

Once the threat actors have enough intelligence on their specific target, they can then evaluate the optimum point of entry. It could be as simple as deciding which employees are most susceptible to a phishing campaign, or as complex as targeting a specific third-party vendor to dump an advanced persistent threat (APT) through the supply chain.

After the network perimeter is breached and the attack mode downloaded and activated, the hackers use Command and Control communication (C&C) to maintain contact with the now-compromised system. They install back doors to allow for easy access into the network. The idea is to lurk around the system for as long as possible to scope out the locations of the most sensitive and valuable data.

When those files are located, the cybercriminals begin the process of relocating them outside of the host organization's network, then disappear without leaving a trace. Some cybercriminals keep the back door in place so they can return and steal more information.

Targeted attacks are so well-executed and so difficult to detect that it takes, on average, 150 days after the breach and data theft occurs to discover them (Lennon, 2016).

Cyber extortion through ransomware attacks is an increasing threat in healthcare organizations, as we covered in the previous whitepaper in this series, but often, the criminals steal the information in the same attack that locks users out of their systems or leave a back door to go back and get it later. In these cases, if the hospital or other healthcare organization pays a ransom to regain control of the system, the cybercriminals get a double payoff when they post the information for sale on the Dark Web.

A hacker in June 2016 claimed theft of about a million patient records from three U.S. healthcare organizations, and demanded $500,000 in bitcoin or the hacker would put the records up for sale. Similarly, a Los Angeles Hospital paid ransom in bitcoin to hackers who disabled its digital security systems. There are lots of malware strains, some in email campaigns, and others directed towards medical vendors who either supply pharmaceuticals or are the third party to patients. The Massachusetts General Hospital attack on over 4,300 patients' dental records in 2017 showed how the Dark Web can also attack vendors (Seals, 2016).

Most hackers know hospitals don't have a robust anti-malware strategy, and therefore exploit this weakness. The story of hospitals' willingness to pay ransoms is spreading among attackers, letting them know their attacks are successful and showing their victims' vulnerability. Healthcare organizations are slow to educate employees about the dangers of the Dark Web, and to manage employee access to sensitive data. Cyber hackers know this, and through critical system dark nets, exploit the nonchalance of health workers. Defending against ransomware is said to be simple, through backup restoration, yet the Dark Web users are becoming more sophisticated. There are reports that hackers have deployed a phishing attack against Amazon users, disguising as shipping confirmation emails. Hackers are also able to hide ransomware links in ways that appear legitimate when a patient or health worker hovers the cursor pointer over them. Healthcare operators must know that attackers are thinking light years ahead, and continuously are looking for loopholes in areas they don't know exist.

HOW IS STOLEN INFORMATION USED BY THE DARK WEB AND CYBERCRIMINALS?

Identity Theft

A study by the Ponemon Institute in 2014 found there were 500,000 victims of medical identity fraud that year. The number rose by 22% in 2015, and more than 65% of victims had to pay an average of $13,500 to resolve crimes and prove their innocence. The data contained in medical records lives forever, so it is easier for cybercriminals to reuse information for a variety of purposes (Ponemon, 2015).

Tax Fraud

The number of tax fraud cases has also increased, due to theft of EHR data. The tax returns are sold, and the original user gets into legal convolutions with the tax systems. This problem prompted the American tax preparation program TurboTax to temporarily suspend state tax filings to investigate tax fraud increase.

Medical Insurance

Medicare insurance ID numbers can be used to obtain medical insurance, and hackers can also sell the profiles that have approved prescriptions. Even though the information may be outdated, the vendor assures buyers that the medical information is still active. At only 50 cents per profile, cybercriminals can buy multiple profiles and perform several test purchases.

Drug Procurement

The Dark Web is notable for sales of prescription drugs, using the information on stolen medical data. A significant increase in underground prescriptions has been noticed, with the real owners of the medical ID being completely unaware of any drug receipt when they receive medical bills. By having a medical ID, hackers create an address on a profile they have purchased, and send the medication to their homes, using the credit card information of the EHR user. These medicines are later sold on the Dark Web for massive profits, through mail-order programs provided by health insurance providers. Electronic drug prescription increased for controlled substances by almost eight times between 2014 and 2015. About 10% of drugs were diverted because of forged and stolen paper prescriptions, and there is a growing number of digital prescription thefts happening on the Dark Web since 2016 (Pittman, 2016).

Surveys show prescription medication abuse continues to rise. For example, more than 500,000 people in the U.S. currently abuse Ambien prescriptions through untraced channels (Addiction Center, 2016).

CONCLUSION

The internet has become a crucial part of the care system, and must be considered when making healthcare decisions. In 2015, it is estimated that 100 million records were proliferated on the Dark Web, with attack victims not receiving due protection from the government as consumer protections on the cyberspace were not yet well-defined. The FBI confirms that the resilience toward the Dark Web by the healthcare sector is very low, increasing cyber-attacks. Vulnerability also increases in the system as the experiences of attacks are not documented, leaving other members without adequate information on breaches and recognition of suspicious activities. The FBI wants health organizations to share experiences even though business models differ. It is hoped such cooperation will help strengthen the interconnections on the health supply chain. The demand for medical information increases in the underground marketplace, and causes financial and reputational losses to healthcare organizations, as the lack of sharing attack experiences makes for longer periods of time before attacks are realized, thereby allowing proliferation. To protect the healthcare sector from Dark Web criminals, education agendas that uphold the access and availability of affordable care treatments in the conventional market could help dissuade people from going to the Dark Web.

The bottom line in disincentivizing the Dark Web is that the healthcare sector needs to become much better at curbing cyber-attacks. It needs to better control who has access to various technology systems and how much access they have to utilize them. The healthcare sector must strive to keep patient data out of sight by limiting the people who have access to it, and limiting those people to only the information they need.

Other measures include:

- Implementing improved password strength and security standards to make it more difficult for cyber attackers to gain access credentials.
- Consulting with security experts to manage and monitor consistently; this includes collecting an inventory of devices accessing their network, patch management, up-to-date antivirus and anti-malware, performing security risk assessments, and encrypting patient data and patient data transmissions.

All in all, every healthcare provider will need to be in a proactive, threat-defensive posture in order to successfully fight off cyber-attacks that incentivize Dark Web criminals. However, this requires taking a comprehensive risk management strategy that includes cybersecurity as a primary and sufficiently funded component, and a top organizational priority.

Think of taking the incentive away from the Dark Web threat actors in these terms: Your home is burglarized and all your valuables are stolen, and weeks later they show up at a pawn shop a few towns over from you for sale. Both the burglar and the pawn shop owner are criminals, but if everybody in your neighborhood creates adequate security measures to keep the burglar way from your valuables, you put both the burglar and the pawn shop owner out of this nefarious business.

REFERENCES

Addiction Center. (2015). Ambien Addiction and Abuse. Available at: https://www.addictioncenter.com/sleeping-pills/ambien/.

Ciancaglini, V., et al. (2016). Below the Surface: Exploring the deep web. Trend Micro. Available at https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

Evolve IP. (2017). Email Vulnerability in Healthcare. Retrieved at: http://www.evolveip.net/wp-content/uploads/2017/03/email-vulnerability-in-healthcare.pdf

Finklea, K. (2017) Dark Web. Washington, D.C.: Congressional Research Service. Available at https://fas.org/sgp/crs/misc/R44101.pdf

Institute for Critical Infrastructure Technology (ICIT). (2016). Hacking Healthcare IT in 2016: Lessons the Healthcare Industry Can Learn from the OPM Breach. Available at: https://icitech.org/hackinghealth16/

Lennon, M. (2016, February 25). Breach detection time improves, destructive attacks rise: FireEye. Security Week News. http://www.securityweek.com/breach-detection-time-improves-destructive-attacks-rise-fireeye.

Pittman, D. (2016, August 18). Politico. E-prescribing controlled substances skyrockets. Politico. Available at: http://www.politico.com/tipsheets/morning-ehealth/2016/08/e-prescribing-controlled-substances-skyrockets-215922.

Ponemon Institute (2015). Medical Identity Fraud Alliance. Fifth Annual Study on Medical Identity Theft. Available at: http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

Robinson, E. (2017). The future of cyber security in healthcare. Konnecktis. Available at: http://www.konnektis.com/new-gallery/2017/9/19/nx4s0fn3otvf49pavmh2lriovnr498