THE ANATOMY, PHYSIOLOGY AND PSYCHOLOGY OF HEALTHCARE CYBERATTACKS

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

INTRODUCTION

Cyberattacks can impact anyone in any organization or market sector these days, but healthcare organizations and the people who work in them are particular targets. It is no longer a matter of "if" but "when" your healthcare organization will be targeted in a cyberattack. In fact, you may have already been hit and are not aware it is happening.

That is why awareness is a good starting point for any healthcare organization's cybersecurity strategy. The more everyone in the organization, from C-suite level executives, to the medical staff, to the receptionists, grasps the nature of cyberattacks, the more prepared they'll be to recognize attack styles and vectors, and then take measures to prevent them.

At the very least, anyone in your healthcare organization who touches a computer needs to understand the composition of cyberattacks and how they happen. This latest whitepaper in our cybersecurity series details the structure of some of the more prevalent attack methods encountered in healthcare and other industries to provide a baseline for preventing them and properly responding when they happen.

ESTABLISHING THE ATTACK SURFACE

To understand the potential types of cyberattacks, it is important to understand the human, network and software targets, collectively known as the "attack surfaces." When people in cybersecurity talk about attack surfaces they mean the sum of all "attack vectors" or points of entry for unauthorized users of a software environment or network. There are three major areas:

- **Human.** People are fallible. They are not only prone to deception, but also to mistakes caused by carelessness and a lack of cybersecurity awareness and training. They are often resistant to organizational change—including the kinds of changes that effective cybersecurity measures warrant—so they do things like leaving devices unlocked and unprotected, ignoring physical security protocols and abusing their authorization privileges.
- **Network.** The network attack surface consists of potential entry points on your network for attackers. These include network applications, cloud networks, and endpoints like computers, smartphones, and any device connected to the Internet, including medical devices.
- **Software.** All software interfaces and applications are vulnerable to exploitation.

Cyber attackers count on these factors to establish an attack surface, and once they do, they use a variety of means to attack.

SOCIAL ENGINEERING: EXPLOITING THE HUMAN ATTACK SURFACE TO GET AT OTHERS

First, let's look at what is often the most vulnerable attack surface in healthcare—humans—and the most common overall method for exploiting this attack surface, known as "social engineering."

People are vulnerable to a variety of techniques that cyber attackers use to manipulate them into witting or unwitting acts, including bypassing security protocols or giving up confidential information such as login credentials. Social engineering tactics target certain aspects of human behavior—generosity, beliefs, and emotions, for example—to create a level of trust, or curiosity, or consternation that prompts some desired action.

Social engineering can happen on the phone, online or even in person. The majority of it happens on the Web and over email. Users will often respond to an email that appears to be sent from somebody they care about, like a grandchild, or something they worry about, like the IRS, without verifying the sender, and attackers anticipate this. Some socially engineered attacks play on the user's emotions or generosity to get the targeted person to provide financial data. Others rely on pop culture and news stories to get users to click links, visit websites, or watch videos, all embedded with malware.

Social engineering is used for some of the following types of attacks:

- **Phishing.** In phishing, the attacker poses as a trusted party (called "spoofing"), and sends an email designed to persuade the recipient to reveal specific information, such as a username and password, or to download malware, or visit an infected website. Besides just generalized phishing attacks, there is also "spear phishing," which targets a certain individual or organization, and "whaling," which is similar to spear phishing, but targets top corporate leadership. Phishing scams usually have telltale signs such as misspelled words, spoofed links, or a generic salutation rather than the user's name, but users often don't notice the mistakes because they are focused on the message. That's what happened to the Wyoming Medical Center in Casper. An employee clicked on a link in a phishing email and within minutes the attackers gained control of the entire email system, which they used to send out more phishing email. They also gained access to patient health information and EHRs (Belliveau, 2016).

- **Pretexting.** This is another form of spoofing in which the attacker impersonates a trusted or known individual, such as an employee, client, or someone from tech support, and requests information in an attempt to gain access to the company network.

- **Baiting.** In baiting, the attacker dangles a promised reward, like free music downloads or store gift cards, to trick the user into providing personal information or login credentials. Another popular baiting attack is simply leaving a USB drive lying around that is loaded with malware, which someone, out of curiosity, plugs it into their computer and spreads the malware.

GETTING INSIDE THE NETWORK AND SOFTWARE ATTACK SURFACES

One very sinister and potentially damaging goal of the social engineering we outlined above is to plant "malware," a broad term used to describe any malicious piece of code or software that creates a risk to the confidentiality, integrity, or availability of data, a network, or other computer resources. Malware can be used to steal data or credentials, enable unauthorized access, log keystrokes (keylogger malware), track user behaviors and online activity (spyware), or allow takeover of a computer or network by mimicking legitimate software or functions (a Trojan horse).

Ransomware Attacks Grow in Healthcare

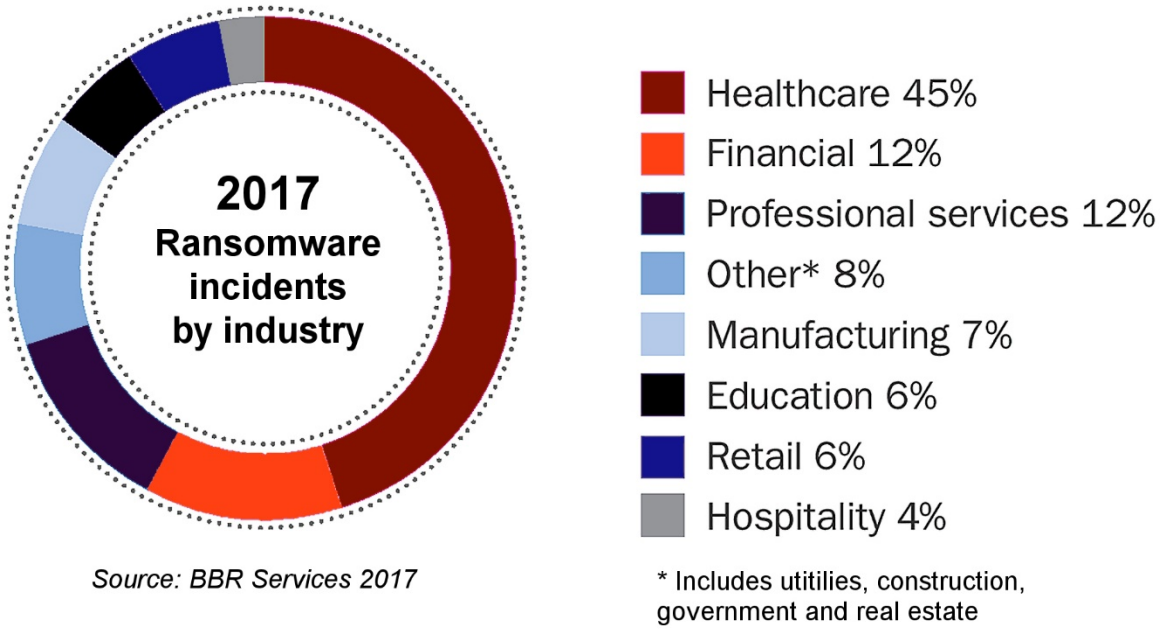
A particular type of malware is known as "ransomware" because it is used to lock users out from access to the system until a ransom is paid, also known as cyber extortion. Ransomware attacks have been around for years, but according to the FBI, they surged in popularity in 2015. They are also becoming increasingly sophisticated and harder to detect, with ransoms becoming more difficult to pay (FBI, 2016).

Ransomware is most commonly delivered through a phishing attack, and often in the form of an email attachment. When the malware is downloaded to a computer, it encrypts the computer's data, including any backup files stored on the infected computer network. The user is coerced to pay a ransom within a certain time period in order to unlock the encryption code. To remain anonymous, the cybercriminals almost always demand the ransom in e-currency such as bitcoins.

While ransomware attacks can affect any organization or individual, the healthcare industry is especially at risk because of the high value of protected health information they collect. Lives are at stake any time this information is held hostage, since hospitals lose access to medical records and interaction with patient medical devices.

A report from global cybersecurity insurance company Beazley found that healthcare suffered more ransomware attacks than any other industry in 2017 (see Figure 1). Of the more than 2,600 data incidents in 2017 across several industries, the report found that 45 percent of all ransomware attacks studied in 2017 were in the healthcare sector. The next highest industries for volume of ransomware attacks were financial (12 percent) and professional services (12 percent). The report also revealed an 18-percent increase in ransomware incidents in 2017 over the prior year (Beazley, 2018).

Figure 1: Ransomware incidents by industry in 2017



Source: BBR Services 2017

* Includes utitilies, construction, government and real estate

In early 2016, a rash of ransomware attacks shut down emergency room computer systems around the country, forcing hospital staffs to share records via fax and to document information the old-fashioned way with pen and paper (Pagliery, 2016).

An attack in February 2016 on Hollywood Presbyterian Medical Center disabled access to its network, email, and patient data. The hospital was forced to close its radiation oncology lab and had no access to CT scans or bloodwork information. In response to the attack, they transferred patients and stopped new admissions. In the end, they paid up—about $17,000. That, of course, doesn't count the cost to the hospital itself because its systems were down. One estimate put the cost of the CT system disruption at $100,000 a day (Dahany, 2016).

In healthcare, protected health information and EHR data are such hot commodities that attackers often take extra steps to extort ransoms. For example, when the Kansas Heart Hospital in Wichita was hit with a ransomware attack in May 2016, hospital leaders paid the fee, the amount of which the hospital's president refused to disclose. Instead of releasing all of the files, however, the hackers continued to hold a few bits of data hostage and asked for a second ransom. The hospital refused to pay the second ransom request (Smith, 2016).

The incident isn't unusual. In March 2016, the FBI and the Canadian Cyber Incident Response Centre issued an alert discouraging ransoms, warning that paying them doesn't guarantee that the hackers will unlock the data (Goedert, 2016). Instead, the FBI recommends education for employees, strong prevention tools, and secure backups on a secondary network, which we will detail later in this paper (FBI, 2016).

Unfortunately, many companies ignore the FBI's advice. Several 2016 studies found that most companies will pay when they are victims of an attack, and some companies are now even stockpiling bitcoins, just in case (Simonite, 2016).

The most significant global attack to date, the WannaCry ransomware attack that was attributed to North Korea, impacted at least 144 countries and had a profound impact on the National Health System in the United Kingdom (Hayes, 2017). This attack illustrated how exploits in one part of the healthcare ecosystem, such as disabling clinicians' access to critical medical information across all types of care environments, can adversely affect care and prompt a major health crisis as well as disrupt operational workflow in all other sectors of the industry (Abraham, 2018).

Denial of Service Attacks

Other examples of attacks used in cyber extortion are Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks don't use malware, but instead target computers or networks with such a high volume of network traffic that they are overwhelmed and can't respond. To legitimate users they appear to be down or inaccessible. The difference between the two is that DoS attacks come from a single source and DDoS come from many and are much harder to defend against and recover from. The extortion aspect comes in when the attacker demands payment to either stop an attack in progress, or to not initiate a full attack.

Because of the nature of these attacks, people in healthcare organizations need to be ever-vigilant for unusual activity on their computers and networks.

UNDERSTANDING STYLES AND TARGETS OF ATTACKS

It is important for everyone in the organization to understand some common cyberattack methods and targets. The following are three commonly used attack styles.

- **Pivot Attack.** During a pivot attack, the hacker uses point of least security, such as a relatively unsecure section of a Web server or a third-party connection. Once inside, the hacker is able to easily move or "pivot" around a network or targeted application, and, in some cases, compromise areas of the system that are usually untouchable. Pivot attacks are also used in penetration testing conducted by ethical hackers.

- **Privilege Escalation Attack.** Privilege is a security step meant to allow access to certain databases or areas of the network. Well-run IT departments limit access based on what an individual needs. This discourages insiders from making unauthorized changes that could compromise the network, applications or data.

In a privilege escalation attack, the attacker is able to gain access or mimic an authorized user by exploiting errors, flaws, and vulnerabilities in the system. This can include setting up a guest account on the server or stealing authentication credentials.

There are two types of privilege escalation attack: horizontal and vertical. In a vertical attack, the hacker gives himself higher privileges to gain more access. In a horizontal attack, the hacker keeps the same level of privilege but assumes the identity of other users at that same privilege access.

- **Brute Force.** The brute force attack, also known as brute force cracking, uses a trial-and-error method to find user names, passwords, and PINs to access accounts. It is one of the oldest types of attacks, and the most time-consuming to perpetrate.

  In this type of attack, software programs generate millions of combinations to guess the right authentication code. Once the program hits the right combination, the hacker gains access to the account. Simple passwords can take seconds to crack, while more complicated and lengthy passwords that use a mixture of lower and upper-case letters, numbers, and symbols, can take years before the software generates the correct combination. When conducted by an ethical hacker, brute force cracking is a useful tool because it can help recover lost passwords, access accounts locked by former employees, break encryption, or test network security.

Supply Chain Attacks

In a supply chain attack the bad actor uses a third party as an access point to an organization's network. This can be accomplished by physically tampering with electronic devices–preloading malware onto a hard drive before delivery, for example–or through a less secure vendor that has access to your network. Given the amount of information-sharing that occurs between vendors and organizations in the supply chain, this type of attack can have widespread consequences, going well beyond affecting just one organization; they can affect any company that shares servers, network connections or data.

Domain Name System (DNS) Tunneling

Domain Name System (DNS) is the naming system for anything connected to a private network or the Internet. DNS provides an identifier for the network's numerical IP address. For instance**,** the IP address for Geisinger Health System is 159.240.9.177 and the DNS is geisinger.org. The connected world depends on DNS, so exploiting it can have serious repercussions.

Domain name system tunneling is the act of coding data and applications into DNS queries and responses. Besides doing damage or stealing information, the hacker can also gain control of the server and the domain, and bypass perimeter security such as firewalls.

Negligent Insider Attacks

When we think of insider attacks we think of a malicious person with a grudge or someone carrying out an attack for financial gain. However, while these attacks do occur in organizations,

they are much less common than the threat from negligent insiders. These attacks occur when an employee or other insider accidentally exposes, modifies, or deletes corporate data.

Healthcare organizations have suffered numerous data breaches due to lost or stolen laptops or devices holding sensitive patient information. For example, when a laptop owned by Premier Healthcare in Bloomington, Ind., was stolen in early 2016, more than 200,000 patient records were compromised (Davis, 2016).

Other examples of negligent insider attacks come when the user accesses unsecured WiFi connections, shares sensitive information online, sends an email file to an unauthorized recipient, or unwittingly creates an opening for a potential hacker. In 2013, California-based Cottage Health System discovered the security system on one of its servers was accidentally disabled and files were not encrypted. Thus, data for thousands of patients was exposed and compromised after malware made its way into the network (Vaas, 2015).

In another whitepaper in this series, titled, "A Culture of Security: Turning Your Greatest Threat into an Asset," we detail the threat from your employees and what healthcare organizations can do about those threats.

Thinking Outside of the Box in Targeting

Healthcare organizations need to realize that cybersecurity threats have a much wider scope now, going beyond just computers and networks. Any part of your organization is subject to an attack, from the cafeteria and housekeeping department, to the surgical suites and financial network.

While the EHR and employee computers are obvious targets, other, not-so-obvious targets offer additional entry points for attacks. These include closed-circuit television systems, webcams, remote door controls, digital video systems, and video conferencing systems. Attackers could install malware on all security cameras then watch as an employee punches in an access code for the EHR, locked drug cabinets, or an MRI machine. Increasing the vulnerability of these systems is the fact that few of them fall under the purview of the IT security team, so they are not included in routine system scans or protections (Filkins, 2014).

Social Media Targeting

Social media is a rising attack vector and a goldmine for cybercriminals, because of the ubiquity of social media combined with the fallibility in the human attack surface. Cybercriminals exploit the high level of trust we have on social platforms to get users to click on links and open files—even users who would never be tempted to fall for a phishing email scam.

Attackers spoof known acquaintances, co-workers, business associates and other familiar people by mining social media for personal details. Also, because users want to use social platforms to connect with others or as a soapbox, they unwittingly supply an overwhelming amount of personal information about their political, religious, and other points of view. Again, this allows cybercriminals to create targeted attacks based on the recipient's strongest interests.

Cybercriminals also take advantage of trending news topics to lure users to visit malicious sites or share malicious postings. For example, in the summer of 2016 cybercriminals used Zika virus worries to spread malware in spam messages that included "instructions" on how to eliminate mosquitos or sent users to a fake "official Zika" website.

"Likejacking" is a becoming a popular social media attack; hackers embed malicious code into a "like" button on a social media platform so the user is negatively affected after responding. The attack could involve a malware dump, ransomware, or scareware that requires the user enter personal information into a new browser window.

WHAT CAN HEALTHCARE ORGANIZATIONS DO TO LIMIT ATTACKS?

The following are tips and techniques from the FBI for all types of organizations and their employees to protect against ransomware threats. However, as you can see, this advice can be extended to several other types of malware attacks, and considerations for many of the attack types and targets we have presented earlier in this whitepaper. (FBI, 2016)

Prevention Efforts

- Ensure employees are aware of ransomware and of their roles in protecting organizational data.
- Patch operating system, software, and firmware on digital devices.
- Ensure antivirus and anti-malware solutions are automatically updated and regularly scanned.
- Manage the use of privileged accounts—ensuring that administrative access is only granted when absolutely needed, and administrator accounts are only used when necessary.
- Ensure that access controls, including file, directory, and network share permissions are appropriately configured. Don't allow write access to files and directories for users who only need read-specific information.
- Disable macro scripts from office files that will be transmitted via e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, and compression/decompression programs).

Business Continuity Efforts

- Back up your data often and verify the integrity of those backups.

Secure your backups and ensure they aren't connected to the computers and networks they back up.

SUMMARY

Another general tip for cybersecurity comes from the world of Homeland Security post 9-11: "If you see something, say something." If something looks or smells "phishy," it probably is.

Always keep in mind that your healthcare organization is most likely under constant attack or in imminent danger of one. That's why it is important that you and your team understand the types of attacks that can be unleashed against your organization. The best weapons to thwart cyberattacks are awareness, education and vigilance. Never be on defense. Always take the offensive approach.

REFERENCES

Abraham, C. (2018). A comparative analysis of the cybersecurity strategies: Implications for healthcare and government. Manuscript in preparation.

Beazley Group. (2018). *2018 Breach Briefing*. Retrieved at https://www.beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf

Belliveau J. (2016, April 28). Some recent potential healthcare data breaches included cases of a phishing scam, stolen devices, and mailing errors. *Health IT Security*. Accessed at https://healthitsecurity.com/news/phishing-scam-leads-to-potential-healthcare-data-breach-in-wy/.

Dahany J. (2016, March 26) Next wave of ransomware could demand millions. *VB*. Retrieved from http://venturebeat.com/2016/03/26/next-wave-of-ransomware-could-demand-millions/.
Davis J. (2016, March 9). Premier Healthcare faces possible data breach that could affect 200,000 patients. *Healthcare IT News.* Retrieved from http://www.healthcareitnews.com/news/premier-healthcare-faces-possible-data-breach-could-affect-200000-patients/.

Federal Bureau of Investigation. (2016, April 29) Incidents of Ransomware on the Rise; Protect Yourself and Your Organization. April 29, 2016; Retrieved from: https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.

Filkins, B. (2014). *Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon*. SANS 2014. Available at: https://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735/.
Goedert J. (2016, April 4). US, Canada issue national alerts on ransomware. *Health Data Management.* April 4, 2016. Retrieved from: http://www.healthdatamanagement.com/news/us-canada-issue-national-alerts-on-ransomware/.

Hayes, J. (2017). WannaCry ransomware impact on patient care could cause fatalities. *Engineering and Technology*. https://eandt.theiet.org/content/articles/2017/05/wannacry-and-ransomware-impact-on-patient-care-could-cause-fatalities/.

Pagliery, J. (2016, March 28). U.S. hospitals are getting hit by hackers. *CNN Money.* March 28, 2016. Accessed http://money.cnn.com/2016/03/23/technology/hospital-ransomware/.

Smith, M. (2016) Kansas Heart Hospital hit with ransomware; attackers demand two ransoms. *Network World.* May 22, 2016. Retrieved from: http://www.networkworld.com/article/3073495/security/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html.

Vaas, L. (2015, May 28). We don't cover stupid, says cyber insurer that's fighting a payout. *Naked Security.* May 28, 2015. Retrieved at https://nakedsecurity.sophos.com/2015/05/28/we-dont-cover-stupid-says-cyberinsurer-thats-fighting-a-payout/.