Advanced Persistent Threats: Healthcare Under Attack

Summary

Despite ongoing efforts to strengthen their security posture, healthcare companies are still largely deficient in managing security. In fact, according to a recent Ponemon institute research study, 96 percent of healthcare providers had at least one data breach in the past two years, with patient billing data and medical records representing some of the most vulnerable data types.[1] A key contributor to this trend has been a lack of effective policies and controls to detect and respond to breaches.

To complicate matters, a recent HIMSS study of healthcare providers found that 58 percent of the respondents had no staff members dedicated to security, and 50 percent spent 3 percent or less of their organizational resources on security.[2]

The external threat landscape in healthcare data security is a force with which to be reckoned, and presents a unique set of challenges for the IT security professional. Recent attacks against many industries are highly sophisticated, well organized, and often connected to nation-state activities or cyber-crime organizations around the globe that are motivated by financial, political and ideological objectives.

One of the most insidious types of attacks is Advanced Persistent Threats (APTs), a genre with generally malicious intent that greatly compounds the risks inherent in EHRs. This type of attack represents an evolving threat to healthcare organizations' intellectual property, financial assets, and ultimately, their reputations. APT actors (the adversaries guiding the attack) target specific organizations for a singular purpose, and attempt to gain a foothold in the target's environment, often through tactics such as targeted emails, or "spear phishing", that contain malicious web links or attachments designed to compromise a particular computer. The attackers then typically use the compromised systems as a conduit into the target network and as a method to deploy additional tools that help fulfill their primary objectives.

In recent months the Dell SecureWorks' Counter Threat Unit has found that the healthcare industry is particularly vulnerable to advanced threats, with many of the most prevalent malware tools used by APT groups affecting the healthcare industry at a rate comparable to or greater than its peers in the banking, retail and manufacturing industries. Most malware subtypes are represented in the attacks that healthcare organizations have experienced. This may be partially due to the attackers' strategy of using healthcare organizations as a "testing ground" for malware, before deploying it on targets in other industries. Healthcare organizations are viable testing platforms for "proof of concept" attacks, due to the general lack of effective controls and high state of vulnerability throughout their networks.

Organizations can protect against advanced threats by gaining situational awareness, and forming defensive strategies around the risk posture that exists. Although a foundation for this awareness starts with risk assessments, implementing effective network architecture, along with penetration testing and continuous monitoring are also necessary components of a security program. Planning for these events and the organization's anticipated response on a continual basis makes it much more difficult for APT actors to conceal their actions, and will make incident response efforts more effective, both for internally- and externally-based threats.

[1] Second Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, December 2011
[2] Fourth annual HIMSS Security Survey

Background: Who, not what

Advanced Persistent Threat (APT) attacks happen when someone or some organization decides you specifically have something they want and they are willing to invest resources and time to get it. You are not a generic target. You have been singled out for a specific reason. Understanding this is fundamental to combating APT. Individual malware can be detected by antivirus solutions and vulnerabilities targeted by mass exploit kits can be patched. However, the fact that a person or group and all of the cognitive abilities and resources at their disposal are being applied with the singular goal of obtaining your assets changes the game. It means the threat actors can and will adapt to specific situations until the actors achieve their objectives, or until the cost of the operation outweighs the perceived value of those objectives.

The hallmarks of advanced threats are that they are *organized*, *efficient*, and *tenacious*. Organizations can be plagued by a single APT campaign for months or years, even after they become aware of the efforts against them. The incident response drags on as the actors continue to adapt to defensive measures and look for new weaknesses in the target's security posture that will allow them to achieve their goals. In most cases, the actors can dedicate as much time as needed to focus on the target, while IT and security staff have competing priorities and experience fatigue as the intrusion efforts drag on.

According to a recent report published in *PC World*, malicious attacks increased 81 percent from 2010 to 2011, with a particular increase in advanced targeted attacks.[3] Lack of role-based access management in many industries has made the targets of these attacks particularly vulnerable. Such vulnerabilities led to the exposure of over 187 million identities in 2011, according to the Norton Cybercrime Index.

The healthcare industry, in particular, has been particularly vulnerable to many of the prevalent tools used by attackers (Figure 1). The entry points for attackers have expanded through a rapid increase in the use of mobile devices in healthcare and life sciences settings.

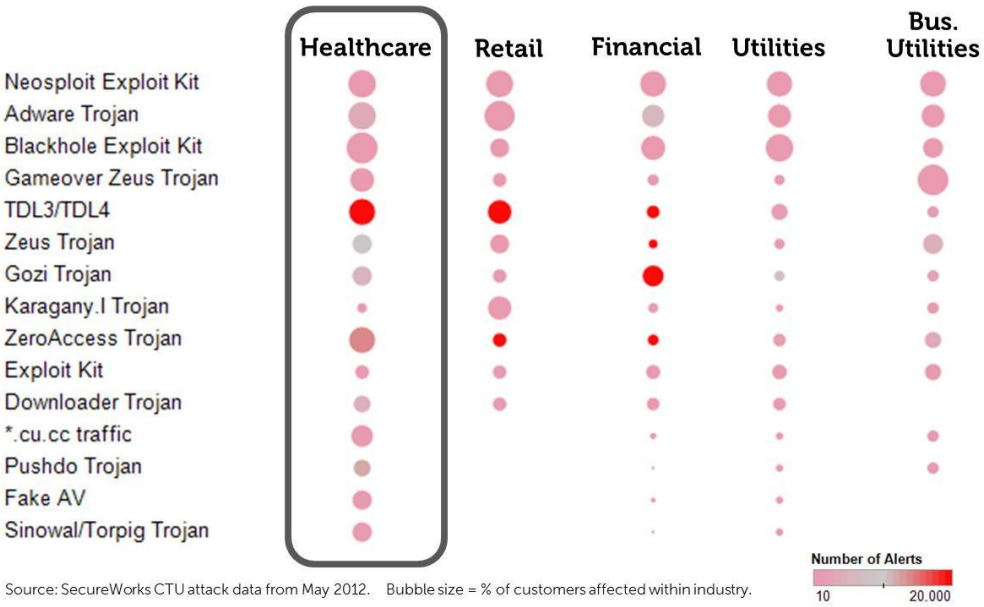

Figure 1: Healthcare is a frequent target for advanced attackers

[3] www.pcworld.com/printable/article/id,254730/printable.html

Advanced Threats: Stages of attack

Actors behind APT intrusions focus on a specific target and are able to customize and adapt their Tactics, Techniques and Procedures (TTP). They may run multiple campaigns in parallel, each consisting of one or more operations. These targeted operations can be dissected into a series of phases. Phases such as preparation and gaining the initial entry point are prerequisites. Figure 2 diagrams the basic operational phases commonly observed in a single APT intrusion.

Figure 2: Lifecycle of an Advanced Persistent Threat.

Preparation and Initial Intrusion

Advanced threats typically pursue a course consisting of several phases, including *preparation*, *initial intrusion*, and *achievement of the primary objective*.

Initially, APT attacks and exploitation typically involve a high degree of preparation. Highly complex operations may be required before executing the exploitation plan against the primary target(s). In the preparation phase, actors enumerate the components necessary to execute their plan and begin their efforts to collect the components. These components commonly include infrastructure, tools, data, information on the targets' environment and other required assets. Actors also collect intelligence on security controls and procedures they are likely to encounter to create evasion and response plans.

After the attacker completes preparations, the next step is an attempt to gain a foothold in the target's environment. An extremely common entry tactic is the use of spear phishing emails containing a web link or attachment. Email links usually lead to sites where the target's web browser and related software are subject to various exploit techniques or where the APT actors attempt to social engineer information from the victim that can be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer.

Gaining a foothold in the target environment is the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is commonly a simple downloader, basic Remote Access Trojan or a simple shell.

Primary Objective

After the requisite steps of preparation and gaining control of a system in the target environment, the APT actor can use the infected system as a conduit into the target network and as a deployment mechanism for additional tools that will facilitate the fulfillment of their primary objectives.

Once the APT actors possess the target's account credentials, movement through the network can become more difficult to track. When users use patterns in their passwords and change them in a predictable way, the APT actors may be able to use the data they obtained to gain access even after account changes have taken place.

APT actors also perform expansion efforts to support other phases of the operation. These phases include gaining access to systems that host or can retrieve targeted data during the search and exfiltration phase, systems that make good locations for the installation of persistence mechanisms, and systems with good network locations that can be leveraged to exfiltrate data or serve as proxies in and out of the network.

Persistence

The "Persistence" phase spans numerous aspects of the lifecycle. Overcoming a target's perimeter defenses and establishing a foothold inside the network can require substantial effort. Between the time APT actors establish a foothold and the time when there is no further use for the assets or existing and future data, APT actors employ various strategies to maintain access. In some instances, actors may prepare for being completely ejected from an environment by maiming the target's network and system defenses, crippling the victim's ability to repel or detect future intrusion attempts. This course of action is a highly premeditated component of preparation.

Search and Exfiltration

The ultimate target of network exploitation is generally a resource that can be used for future exploit(s) or documents and data that have financial or other perceived worth to the intruder. In many cases, the APT actors have a specific document or type of data in mind before the attack is launched. In other cases they know it is likely that valuable data exists in the target's network and systems, but are unsure where the valuable data is stored.

A popular approach to search and exfiltration is to take everything from the network that might be of interest. This includes every document, email and other types of data discoverable on the network. Some frequently examined locations include the infected user's documents folder, shared drives located on file servers, the user's local email file and email from the central email server. To avoid detection, some actors take a more focused approach: searching documents at the target's site for keywords and metadata that indicate the document may be of interest to the actors.

In cases where the actors only have access to the user's account, and therefore their access level, collection may be limited to the infected computer and the victim's files on several file servers. With an individual's user account password, the APT actor can collect the local email stores, such as the PST (personal folder) files used by Microsoft Outlook. If the APT actor gains access to the administrative level account, they may be able to install malware on the central mail servers that can monitor all incoming and

outgoing messages. This visibility lets the actors monitor all email within the organization, and may also let the actor read faxes and listen to recorded voicemails.

All of this data is collected and sent to a location where the actors can retrieve it. To circumvent data loss prevention (DLP) technologies that look for keywords or patterns in documents leaving the network, the stolen data is often placed in an encrypted or otherwise coded archive format. Modern APT capabilities also include the ability to exfiltrate data regardless of proxies, firewall rules or other border control measures.

Cleanup

Cleanup efforts during an intrusion are focused on avoiding detection, removing evidence of the intrusion and what was targeted and eliminating evidence of who was behind the event. Sometimes cleanup involves planting or manipulating data in the environment for the purpose of misdirection. The better the APT actors are at covering their tracks, the harder it will be for victims to assess the impact of the intrusion.

Conclusion

APT actors interested in your data are focused on acquisition of crucial information, and they adapt to failures and continue to hunt for security weaknesses and blind spots in monitoring. When they are able to slip past defenses, they can make rapid lateral movements for persistence and data collection. Once they locate data, they can move it out of the network for offline review. That data is used for future intrusions on you or related targets, to eliminate technical advantages over the actors' customer or country, to provide advantages in business dealings or for other real-world purposes that can have significant economic and strategic impacts on targeted entities.

Considering security and the mindset of the actors behind the threats when planning network and system architectures can yield better designs that make the task of network instrumentation and system monitoring easier. Good architecture can help with controlling data flows. Segmentation of network resources either by access requirements, services offered or other strategies compatible with organizational needs makes policy development, enforcement and auditing possible. A log retention and monitoring strategy is also important. Planning these considerations ahead of time will make it much harder for APT actors to cover their tracks and will make incident response efforts more effective and efficient.

A well-developed communications plan that helps users understand the threats and how to identify them will help mitigate social engineering attempts. Maintaining the IT environment through vulnerability assessment and efficient patch management is an important step to eliminate opportunities for initial intrusions. Removing local administrative privileges from users' workstation accounts and limiting access to only what is necessary helps prevent privilege escalation and access expansion efforts.

Modeling the threat through penetration testing and training exercises that emulate APT actor TTP are also a valuable self-assessment and training tools for management and defense staff.

Good situational awareness is critical to forming effective defense strategies. Without a thorough understanding of the threat, defensive strategies and spending will be inefficient at best and ineffective at worst. In the case of APT, security controls must be developed that account for the actors, their ability to adapt and the resolve they have towards obtaining your assets.

About Dell SecureWorks

Should you have any questions about how Dell SecureWorks can help your organization prepare for or respond to advanced, targeted attacks, contact your account manager, visit our website, email info@secureworks.com or call (877) 905-6661.

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.