Significant Threats to the Healthcare Sector

The healthcare sector is a high-value target for cyber actors. Vast amounts of patient data, in addition to the critical nature of the sector within modern society, make it a lucrative target for actors attempting to profit or impose maximum harm against a population. The COVID-19 pandemic has not curbed the influx of criminal groups seeking to exploit the sector at its most desperate point.[1]

If history repeats itself, hackers will continue to take advantage of the situation. In light of the COVID-19 crisis, it is important to keep in mind that ransomware attacks—one of the biggest threats to the healthcare sector—do not take a break during the pandemic. Let's take a closer look at some of the motivations driving these threats.

Typical Motivations

DATA THEFT

A driving force for economic espionage is the availability of research or intellectual property for collection via intrusion into healthcare sector networks. Acquiring this type of information has the potential to give other nation-states key stepping stones for accelerating technological advances and bringing new products or pharmaceuticals to market more quickly than competitors.

The availability of personally identifiable information (PII) and protected health information (PHI) to use as part of the bulk collection of data utilized to track personnel (government or otherwise) presents a unique opportunity for state-sponsored threat actor targeting.

Large amounts of stored PII and PHI are a ripe target for financially motivated threat actors who can sell this information on underground markets.

OPERATIONAL DISRUPTION

Ransomware is one of the largest threats to the healthcare environment, particularly due to its potential to disrupt patient care. The impact to critical devices, systems, and human lives creates circumstances where a dire need for the restoration of services causes a threat actor to perceive that the likelihood of receiving a ransomware payment is higher within this sector.

Attacks also could be conducted with the aim of disrupting continuity of operations, without a ransomware component.

Ransomware Discussion

Several years ago, cybersecurity reporting noted a trend in ransomware moving away from targeting individuals to targeting corporations. We continue to see this in the news today as organizations present a richer target than individuals for cybercriminals motivated by financial gain. The ability to hamper critical operations increases the likelihood of larger payouts from organizations desperate to restore operations. With the move to targeting corporations comes the need for threat actors to develop operational models to support large-scale campaigns with clear distinctions between software development, malware distribution, targeted system encryption, and payment collection.

1 Gallagher, Ryan and Bloomberg. "Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus." *Fortune*, 1 April 2020, https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/.

As such, researchers have identified a Ransomware Kill Chain that clearly defines the stages of an infection. The Ransomware Kill Chain presents several opportunities for detection—and therefore interruption—of a given campaign, as described in the table below.[2]

Campaign Stage	Details	IronNet Detection Opportunity
Distribution	Downloading the dropper via an email, watering-hole attack, exploit kit, or drive-by download	Phishing analytics Suspicious file download
Malicious Code Infection	Phone home to predetermined command and control (C2) server or via use of DGA to connect to a pseudo-random domain in order to download an executable which installs the ransomware	Beaconing analytics Suspicious file download Domain generation algorithm
Malicious Payload Staging	Establishing persistence	N/A
Scanning	Searching for content to encrypt (locally and across the network)	Scanning analytics (dependent on sensor placement)
Encryption	Discovered files are encrypted	N/A
Payday	Ransom note is shown and attacker waits to collect	N/A

Detection early in the Kill Chain can lead to quicker mitigation of an attack before the actor is able to inflict more substantial damage. Targeting a corporate environment with ransomware potentially takes a significant amount of time. The extensive time it may take an adversary to map a network to determine which systems to target, as well as to encrypt files to hold for ransom, introduces more time for defenders to intervene. One of the examples below describes a real-life scenario where the threat actor had a presence on the network for more than a year before deploying ransomware.

Notable Threat Actors and Campaigns

Although some of these threats were detected a few years ago, there is no evidence to suggest that they are *not* currently active.

Ryuk Ransomware

An IT services provider that offers cloud hosting, security, and access management for more than 80,000 computers and servers supporting more than 100 nursing homes in the United States was hit with Ryuk ransomware in late 2019.[3] The adverse impacts to people and facilities included blocked access to patient medical records; inability to order medications; prevention of submission of billing to Medicaid; and blocked access to email, phone, and payroll operations.

2 Exabeam. *Threat Research Report: The Anatomy of a Ransomware Attack.* Exabeam, Inc, 2016, https://www.exabeam.com/wp-content/uploads/2017/07/Exabeam_Ransomware_Threat_Report_Final.pdf.

3 Krebs, Brian. "110 Nursing Homes Cut Off from Health Records in Ransomware Attack." *Krebs on Security*, 23 Nov. 2019, https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/.

Companies hit by Ryuk are often those that supply services to other companies, in particular, cloud-data firms. These companies are often compromised for months or years as attackers map their target's internal network to identify key resources to compromise. In this specific instance, it is believed that the service provider was initially infected in September 2018, more than a year before ransomware was actually deployed. The likely initial infection vectors were spearphishing emails with malicious attachments leading to downloads associated with Trickbot or Emotet banking Trojans.[4] This scenario demonstrates why it is imperative to stop attackers early in the Kill Chain. Other recent examples of Ryuk ransomware victims include a hospital in France, a Missouri-based healthcare system, and the government of the state of Louisiana.

Targets	TTPs	IronNet Detection Opportunities
• Cloud data firms • IT services and other service providers	• Spearphishing emails with malicious attachments • Use of Trickbot and/or Emotet Trojan malware	Phishing analytics

APT41

APT41 is a state-sponsored threat actor operating for espionage purposes on behalf of the Chinese government; it also has been identified conducting financially-motivated cyberattacks. While targeted sectors have varied throughout the years, the healthcare industry is consistently included in victim lists between 2014 and at least 2018.[5]

This group utilizes a vast array of tools, from those that are publicly available all the way to custom-developed malware—even malware used by other Chinese espionage operations. Documentation of APT41 tactics, techniques, and procedures (TTP) repeatedly point to the use of spearphishing with malicious attachments to achieve initial access into a victim network. Malicious attachments are often compiled HTML (.chm) files, but there are likely other file types utilized. Another notable TTP is the use of stolen digital certificates in order to sign malware and appear more legitimate. Finally, researchers have documented APT41's willingness to quickly stand up and move to new infrastructure when their activity is discovered.

Targets	TTPs	IronNet Detection Opportunities
Healthcare sector organizations	• Spearphishing with malicious attachments (typically .chm files) • Use of stolen digital certificates • Infrastructure is quickly built and torn down	• Phishing analytics • Domain analysis analytics

4 "NCSC Releases Advisory on Ryuk Ransomware." *U.S. CISA*, 28 June 2019, https://www.us-cert.gov/ncas/current-activity/2019/06/28/ncsc-releases-advisory-ryuk-ransomware.

5 Fraser, Nalani, et al. "APT41: A Dual Espionage and Cyber Crime Operation." *FireEye Threat Research*, 7 Aug. 2019, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html.

Whitefly

Whitefly is the group that is attributed to the SingHealth data breach that occurred in the summer of 2018. It is estimated that the personal information of approximately 1.5 million patients was stolen, including prescription information for Singapore's Prime Minister and other senior government officials that the attackers appeared to have specifically sought out.[6]

This group has been operating since at least 2017 and has targeted organizations across a wide variety of sectors with the primary goal of stealing large amounts of sensitive information.[7] Cybersecurity reporting indicates that it is highly likely that victims are compromised initially through the use of spearphishing emails that include malicious executable or DLL files disguised as documents or images. Whitefly has been observed with long dwell times in victim networks with repeated communications to command and control domains, thus presenting several detection opportunities for behavioral analytics.

Targets	TTPs	IronNet Detection Opportunities
• Healthcare • Media • Telecommunications • Engineering	• Spearphishing leading to malicious files disguised as documents or images • Usage of multiple command and control domains per target	• Phishing analytics • Suspicious file download • Beaconing analytics

Orangeworm

In 2015, a group dubbed Orangeworm was identified targeting the healthcare sector in the U.S., Europe, and Asia through the installation of a backdoor known as Kwampirs.[8] Although secondary targets at first appeared to be outside of the healthcare sector, it quickly became apparent that these targets had direct links to healthcare-related organizations, meaning that these organizations were also specifically selected for their role in the healthcare supply chain.

Although the threat actor's method of initial access was not identified in reporting, some details regarding malware behaviors were shared. Of note, at one point during execution, Kwampirs inserted a randomly-generated string into the middle of a decrypted payload to help evade signature-based detections. Orangeworm also attempts to spread by utilizing techniques that are more viable in networks running legacy systems, which may be more prevalent in the healthcare sector. This technique—plus repeated attempts to beacon to command and control servers—makes Kwampirs somewhat noisy and prone to detection by behavioral-based solutions.

Targets	TTPs	IronNet Detection Opportunities
• Healthcare sector organizations • Organizations involved in the healthcare supply chain	• File copy over network shares • Beaconing to command and control servers, likely using standard application protocols	• Beaconing analytics • Lateral movement related analytics

6 Tham, Irene, et al. "SingHealth Cyber Attack: How it Unfolded." *The Straits Times*, 20 Jul. 2018, https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

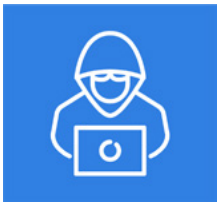
7 Critical Attack Discovery and Intelligence Team. "Whitefly: Espionage Group has Singapore in Its Sights." *Symantec*, 6 Mar. 2019, https://www.symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore.

8 Critical Attack Discovery and Intelligence Team. "New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia." *Symantec*, 23 Apr. 2018, https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia.

FIN4

FIN4 is a financially motivated threat group that was reported in 2014 as having targeted more than 100 companies since mid-2013 for the purposes of collecting insider information relevant to publicly traded companies. More than two-thirds of these targets were healthcare or pharmaceutical companies.[9] The group accomplished this by targeting the email accounts of individuals who regularly communicated about "market-moving, non-public matters" through the use of mergers and acquisitions-themed or SEC-themed lures designed to capture credentials from targets. These credentials were then transmitted to command and control servers. Another tactic employed the use of links directing targets who had been spearphished to fake Outlook Web App login pages in order to attempt to capture user credentials. The nature of this campaign makes it a prime target for detection via IronNet phishing or beaconing related analytics.

Targets	TTPs	IronNet Detection Opportunities
• Healthcare companies • Pharmaceutical companies • Users from these companies with insider financial information	• Spearphishing • Fraudulent Microsoft Outlook login pages	• Beaconing analytics • Phishing analytics



Deep Panda

Deep Panda is an advanced persistent threat (APT) purported to be working on behalf of the Chinese government. This group notably breached the network of the health insurance provider Anthem in 2014, exfiltrating 80 million social security numbers and other sensitive data.[10] One of the more striking tactics utilized by the group in this case was the work they took to stand up extensive malicious infrastructure which closely mirrored legitimate infrastructure utilized by the company. For instance, the attacker registered we11point[.]com to mimic wellpoint[.]com (a health network part of the Anthem organization) and serve as command and control for malware communications.[11] Communications with infrastructure such as this present multiple opportunities for detection via IronNet behavioral analytics. This is especially true when the infrastructure is present for an extended period of time. Deep Panda is believed to have been in Anthem's network for at least nine months prior to discovery.

Targets	TTPs	IronNet Detection Opportunities
Healthcare insurance companies (specifically Anthem)	• Mimicking legitimate infrastructure of the target • Domain name spoofing	• Domain analysis analytics • Phishing analytics

IronNet threat hunters and analysts are keeping a sharp eye on both known and unknown threats. Visit ironnet.com/blog for the latest reports and news from our Cyber Operations Center (CyOC), including our monthly IronLens CyOC report.

9 Dennesen, Kristen, et al. "FIN4: Stealing Insider Information for an Advantage in Stock Trading?" *FireEye Threat Research*, 1 Dec. 2014, https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html.

10 Krebs, Brian. "Anthem Breach May Have Started in April 2014." *Krebs on Security*, 9 Feb. 2015, https://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

11 ThreatConnect Research Team. "The Anthem Hack: All Roads Lead to China." *ThreatConnect*, 27 Feb. 2015, https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/.