FIREEYE™

Beyond Compliance:

Cyber Threats and Healthcare

EXECUTIVE SUMMARY

The healthcare vertical faces a range of threat actors and malicious activity. Given the critical role it plays within society and its relationship with our most sensitive information, the risk to this sector is especially consequential. In some cases, criminals seek to monetize personally identifiable information (PII) and protected health information (PHI); nation states carry out intrusions to steal valuable research and mass records for intelligence gathering purposes; and disruptive threats like ransomware have the potential to wreak havoc among hospital networks and impact the most critical biomedical devices and systems. To move beyond compliance with current regulations and address the everchanging threat landscape, organizations in this sector should utilize threat intelligence to understand these threats continue to evolve, and minimize risks appropriately.

Based on FireEye's observances of threat activity across this vertical, the threats facing healthcare organizations can be grouped into the following:

Theft of Data

- Financially motivated threat activity represents a high-frequency, high-impact threat to healthcare organizations. Cyber crime actors may conduct focused intrusions into specific targets that house or have access to valuable patient records and data, or carry out opportunistic targeting of poorly secured organizations and networks.
- In comparison to cyber crime activity, cyber espionage campaigns pose a lower frequency but still noteworthy impact risk to healthcare organizations, particularly those in some subsets of the industry. Much of what FireEye has observed from such threat actors—particularly those with a nexus to China—appears to driven by an interest in acquiring medical research and collecting large data sets of information, potentially for the purposes of fostering intelligence operations.
- In our 2018 M-Trends report, FireEye observed that healthcare was the third-highest industry to be retargeted following an incident

Disruptive and Destructive Threats

- Disruptive threats driven by extortionist cyber criminals and nation state actors continue to present a threat to continuity of operations for healthcare providers and others in this space.
- Both targeted activity such as ransomware delivered post-compromise, and less frequent but widespread nation-state-originated threats like WannaCry can pose threats to poorly secured infrastructure.
- Similar to operational technology networks within critical infrastructure, security organizations within healthcare providers face difficulties in maintaining visibility of threats targeting these systems.

Looking forward, the increasing number of biomedical devices used for critical functions within hospitals and healthcare providers presents a growing security challenge. Furthermore—given their importance and value—a growing willingness by cyber crime, or, in a period of heightened geopolitical tensions, nation state actors—to deploy disruptive and destructive tools may significantly increase the impact from these threats we have observed to date.

THREAT ACTIVITY BY MOTIVATION

Cyber Crime

- Financially motivated threat activity almost certainly poses a high-frequency, high-impact threat to healthcare organizations. Common targets include PII, PHI, and access to critical systems.
- Observed activity includes credential theft malware distribution, cryptomining, sale of compromised access to healthcare systems, encryption of hospital systems through ransomware, and extortion campaigns.
- A wide variety of cyber criminals from many regions target the healthcare sector. Observed tracked groups include TEMP.Demon, and thedarkoverlord.

Cyber Espionage & Nation State Threats

- Moderately frequent espionage activity targeting the healthcare sector can have a noteworthy impact.
- Actors observed targeting the healthcare sector include China-nexus APT10 (Menupass), APT41; Russia-nexus APT28 (Tsar) and APT29 (Monkey); and Vietnam-nexus APT32 (OceanLotus).
- There is a potential for significant to catastrophic impacts should destructive or highly disruptive campaigns target the sector, particularly targeted against healthcare providers.

Hacktivism & Information Operations

- FireEye Intelligence assesses with moderate confidence that hacktivist campaigns are an uncommon threat to most organizations in the healthcare sector and may only have a negligible or minor impact on targeted organizations.
- Information operations affecting the healthcare sector are almost certainly a low-frequency threat that typically causes low- to moderate-severity effects.
- Actors observed propagating healthcare-related messaging in recent years include the Russia-nexus operators CyberBerkut and @pravsector.

THEFT OF DATA

Within any industry, threat actors will often gravitate to the least secured points in the ecosystem to obtain the data or access they are seeking. Beyond insurers, cyber criminals will often gravitate to poorly secured healthcare providers to obtain PII and PHI. Cyber espionage actors can leverage this data for intelligence collection purposes, to further target high-profile individuals or those who may have access to valuable information. Additionally, organizations involved in research and development, whether for treatments, medical devices, biotechnology, or other subsets of the industry, have valuable intellectual property that is a driver for economic espionage. Notably, China's strategic "Made in China 2025" plan includes a push for increased domestic development of medical technologies and devices, which may drive threat activity against IP holders and producers of these technologies.

Cyber Crime Threats

FireEye Intelligence assesses with high confidence that financially-motivated cyber threat activity poses a frequent threat with significant impacts due to compromise of large volumes of highly sensitive personal identifiable information (PII), PHI, and financial data.

Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common, and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures.

- Between Oct. 1, 2018 and March 31, 2019, FireEye Threat Intelligence observed multiple healthcare-associated databases for sale on underground forums, many for under $2000. Notably, according to the vendor descriptions, the timing of these database advertisements did not typically correlate with the timing of a breach. Many of the observed advertisements were for databases that had been compromised in previous months or years:

	Price
March 19, 2019, actor **InfoMerchant** – Unspecified amount of data associated with an unnamed "health card" company that contains PII and healthcare information.	N/A
Feb. 21, 2019, actor **NetFlow** – 4.31 GB of data associated with a U.S.-based healthcare institution that contains patient data, including driver's licenses, health insurance, and ZIP Codes.	$2000
Feb. 12, 2019, actor **specfvol** – 50,000 records associated with a U.S.-based healthcare institution that contain medical records, PII, and health insurance information.	$500
Feb. 2, 2019, actor **fallensky519** – 6,800,000 records associated with an Indian-based healthcare website that contains patient information and PII, doctor information and PII, and credentials.	$1700
Jan 28, 2019, actor **x999x** – Unspecified amount of records associated with a Canadian-based healthcare website that includes access to the domain admin, access to the network, and includes the server name, IP address, and platform information.	$5500
Jan 22, 2019, actor **emoto** - 58,000 records associated with a U.S.-based healthcare institution that contain PII.	$480
Jan 16, 2019. actor **ping** advertised 100,000 records with personally identifiable information (PII). According to the advertisement, the actor obtained the data from a server used by more than 270 U.S. hospitals.	$500
Dec 15, 2018, actor **emoto** – 19,000 records associated with a U.S.-based healthcare institution that contain financial data, email addresses, and information on employees.	$300
Nov 15, 2018, actor **Lavanda** – 20,000 records associated with U.S.-based medical universities that contain employee data and PII.	N/A
Nov 4, 2018, actor **Merky** – 180,000–200,000 records associated with a UK-based healthcare institution that contain PII.	$200

In addition to directly selling data stolen from healthcare organizations, cyber criminals also often sell illicit access to these organizations in underground markets. This access can enable other actors to perform post-exploitation activity such as obtaining and exfiltrating sensitive information, infecting other devices in the compromised network, or using connections and information in the compromised network to exploit trust relationships between the targeted organizations and other entities to compromise additional networks.

- TEMP.Demon has, since at least July 2018, conducted intrusion operations impacting multiple industries including the health care sector, using publicly available tools to compromise and move through victim environments.
- On Feb. 6, 2019, on a popular Russian-language forum, "Jendely" advertised access to a U.S.-based medical institution. According to the advertisement, the actor obtained the domain administrator's access to the network consisting of 3,000 hosts. The access is being auctioned for$9,000–$20,000 USD. In November 2018, the same actor advertised accesses to networks of multiple U.S.-based companies with over 600 hosts for $15,000 USD.

Activity by "thedarkoverlord" was initially associated primarily with targeting the healthcare sector by selling access to records and attempted extortion. While thedarkoverlord later diversified targeting to include other sectors, healthcare was still a primary target through the 2017 arrest of several purported members of the group. A limited degree of underground activity by thedarkoverlord resumed in late 2018; however, it is not clear how active thedarkoverlord remains at this time as only a small amount of activity has been observed in 2019.

HEALTHCARE DATABASES (BY REGION) SOLD BY "THEDARKOVERLORD" IN 2016

Location of Healthcare Provider	Total Number of Records	Price
Atlanta	396,459	300 bitcoins
Central/Midwest	207,572	170 bitcoins
Farmington, Missouri	47,864	60 bitcoins
Bronx, NY	34,621	25 bitcoins
United States	9,278,352	300 bitcoins
Fairview, Illinois	23,565	35 bitcoins

CYBER ESPIONAGE THREATS

Continued Focus on Medical Research by Chinese APTs

FireEye continues to witness a concerted focus on acquiring healthcare research by multiple Chinese APT groups. In particular, it is likely that an area of unique interest is cancer-related research, reflective of China's growing concern over increasing cancer and mortality rates, and the accompanying national health care costs. Open source reports indicate that cancer mortality rates have increased dramatically in recent decades, making cancer the nation's leading cause of death.

As the PRC continues to pursue universal healthcare by 2020, controlling costs and domestic industry will surely affect the PRC's strategy to maintain political stability. Another probable motivation for APT activity is financial: the PRC has one of the world's fastest growing pharmaceutical markets, creating lucrative opportunities for domestic firms, especially those that provide oncology treatments or services. Targeting medical research and data from studies may enable Chinese corporations to bring new drugs to market faster than Western competitors.

- In early April 2019, suspected Chinese cyber espionage actors targeted a U.S.-based health center—with a strong focus on cancer research—with EVILNUGGET malware. One of the lure documents references a conference hosted by the targeted organization. In alignment with a trend we continue to witness affecting healthcare, this same organization has been targeted by multiple Chinese threat actors in the past.
  - » A year prior in 2018, China-nexus APT41 used CROSSWALK malware to spearphish individuals at this entity.
  - » APT22—a Chinese group that has focused on biomedical, pharmaceutical, and healthcare organizations in the past, and continues to be active—also targeted this same organization in prior years.
- Over the years, APT41's interest in healthcare-related entities has extended to numerous compromises.
  - » Between July 2014 and May 2016, APT41 targeted a medical devices subsidiary of a large corporation. Although APT41 initially targeted the parent company, 30 percent of the victimized hosts were related to a subsidiary specialized in manufacturing medical devices. Password strings and spoofed domains leveraged in the operation signify a narrow tasking to target the subsidiary instead of the parent corporation. We have some indication based on the nature of hosts targeted that APT41 was interested in information technology employees and software used by the medical device subsidiary. A keylogger dubbed GEARSHIFT was first deployed at the medical device company. Additionally, a digital certificate from the victim was compromised and used to sign malware used in other operations against the sector, detailed below.
  - » Concurrent to some of these operations, a biotech company undergoing acquisition was targeted by APT41 in May 2015. Highly sensitive information about corporate operations, including human resources data, tax information, and acquisition-related documents, were targeted. Notably, clinical trials data of developed drugs, academic data, and R&D funding-related documents were also exfiltrated. The time frame, use of the same GEARSHIFT sample, and a digital certificate from the aforementioned medical device company provide some indication that these two campaigns were conducted by the same operator concurrently.
- In late 2017, as part of a spearphishing campaign, China-nexus APT10 distributed three healthcare-themed documents were deployed against entities in Japan likely associated with the industry. Two of the documents were related to cancer research conferences.
- Since at least 2013, APT18 (Wekby) has targeted biotech- and pharmaceutical-related organizations, as well cancer-specialty research organizations. In one incident investigated by FireEye at a healthcare manufacturing company, APT18 was believed to be active in the organization's network for at least 60 days prior to detection. During this time, the actors used or accessed approximately 14 user accounts and accessed or installed backdoors on more than 450 systems. They also collected several gigabytes of medical imaging equipment files into compressed archive files in an attempt to exfiltrate the information from the manufacturer's network.
- Similar to other examples we have witnessed, cyber-enabled theft of medical data and research is likely one component of a broader strategy by China at acquiring key innovations and technology. In April 2019, several researchers at the MD Anderson Cancer Research were dismissed following concerns over theft of medical research on behalf of the Chinese government.

One theme FireEye has observed among Chinese cyber espionage actors targeting the healthcare sector is the theft of large sets of PII and PHI, most notably with several high-profile breaches of U.S. organizations in 2015. We assess that the theft of bulk data appears to remain a tactic employed by Chinese cyber espionage actors in targeting certain groups of individuals, as evidence by the breach of SingHealth in 2018.

- The malware and TTPs described in the 2018 Singaporean Health breach most closely match a cluster of China-nexus cyber espionage activity known publicly as "Mofang." FireEye Intelligence has previously reported on Mofang campaigns deploying this malware, which we track as QUASIFOUR and DUOBEAN, against Southeast Asian entities in government, media, transportation, construction, and telecommunications verticals.
- A China-nexus cyber espionage actor associated with several intrusions that we believe were intended to gather bulk sensitive data on U.S. persons, has carried out targeting of healthcare organizations holding PII, in addition to aviation, and the sensitive data of U.S. Government employees. We believe this actor is collecting data to identify, track, and even exploit targeted personnel. The government data alone could be used to identify undercover agents operating in China; to recruit informants and double agents in the U.S.; or to identify and harass or threaten the family members of Americans with security clearances.

Beyond Chinese-nexus groups, FireEye Intelligence has observed a wide variety of other cyber espionage and nation state actors involved in targeting the healthcare sector, including:

- Russia-nexus APT28 has been linked to targeting of a global sports regulatory agency and other organizations associated with international sports competitions and athlete drug testing.
- In August 2017, CyberBerkut, a hacktivist group that we are moderately confident is linked to Russia-nexus espionage actors including APT28, made a post containing unsupported claims that US authorities, Ukrainian authorities, contractors, and health-focused non-governmental organizations (NGOs) were conspiring to test biological weapons in Ukraine. A similar claim was made in August 2016 by the Russia-linked false hacktivist persona @pravsector, asserting that leaked documents from an Ohio-based clinic proved that US military organizations were testing biological weapons in Ukraine.
- APT29 has conducted phishing against healthcare and health policy-related individuals during at least one campaign.
- Vietnam-nexus APT32 used lure documents identified at a healthcare organization in the UK.

DISRUPTIVE AND DESTRUCTIVE THREATS

Ransomware or extortion campaigns are likely perceived as especially useful against this sector, as they could limit access to patient or health information or disrupt critical care, potentially leading to an increased success rate and higher payouts for actors. Future activity could cause significant to catastrophic effects should actors undertake destructive or high-impact disruptive attacks, as evinced by the WannaCry and EternalPetya attacks.

Ransomware

Ransomware infections pose a more significant risk to healthcare organizations than entities in many other sectors due to the need for consistent, near real-time access to patient data and the potential for harm to patients should organizations lose access to important files, systems, and devices. While this increased criticality is likely known by ransomware operators, there is a reticence among some actors to carry out ransomware attacks on hospitals fearing it could lead to increased law enforcement scrutiny, particularly should it lead to an accidental loss of life. However, with the growth of targeted, post-compromise ransomware campaigns, some criminal actors may be willing to assume more risk in carrying out operations against healthcare providers in the belief that they have the means and willingness to pay.

- In November 2018, FireEye responded to a breach at a U.S. hospital that involved GandCrab—a ransomware family whose operators recently announced it was shutting down after claiming to have made more than $2 billion USD.
- Texas-based Altus Brown Hospital (ABH) acknowledged that is suffered a Dharma ransomware attack in November 2018 that infected the hospital's systems and encrypted hospital records, including patient information.
- In September 2018, FireEye responded to a Samas ransomware incident at a U.S. healthcare provider in which 93 work stations were impacted.
- In early January 2018, a U.S. hospital paid a four bitcoin ransom (around $55,000 USD at the time) to unlock their IT systems, despite having backups. While hospital employees detected the ransomware quickly, it was too late to prevent the spread of infection to the hospital's email system, electronic health records, and internal operating systems.
- Multiple other healthcare organizations have reported being affected by ransomware campaigns in the last several years. Responses have varied from paying a ransom or accepting data loss and associated costs to having limited effects due to effective security implementations that allowed rapid remediation.
- In some cases, threat actors have purposely avoided targeting healthcare. In a 2019 post in an underground forum advertising bitpaymer ransomware services, actor dihlofoss specifically noted, "we don't work against hospitals, educational and gov. institutions."

To reduce the impact from ransomware infections, organizations, particularly those that require high availability like hospitals, should have not only robust backup policies and implementations, but also redundant and properly segmented isolated networks and systems. This could assist in cases where one segment of a network or one set of devices has become compromised, as it could potentially allow other systems and data to remain protected and able to operate in at least a limited capacity during remediation efforts.

Cryptomining Malware

In late 2017, we also confirmed multiple healthcare organizations were affected by cryptomining operations. This is consistent with the growth in popularity of cryptomining malware among cyber criminals over the last several years; however, the effect on healthcare organizations from this type of activity may be elevated due to the possible impact of cryptomining malware on critical systems through increased processing and network load, decreased system stability, and possible decreases in infected device lifespan.

Nation State Disruptive and Destructive Attacks

Use of ransomware or wiper malware to disrupt or destroy healthcare capabilities in a given region or country could be advantageous in periods of conflict or heightened tensions, particularly when combined with false criminal or hacktivist personas claiming credit to give the attack sponsors plausible deniability.

- Many healthcare organizations were reportedly affected by the widespread EternalPetya wiper and WannaCry ransomware campaigns in 2017, demonstrating the damage that can be done by these types of campaigns.

Targeting of Medical Cyber Physical Systems (MCPS)

A particularly concerning target for disruptive and destructive threats within healthcare is medical cyber physical systems (MCPS) or biomedical devices. These devices, including implanted devices such as pacemakers and insulin pumps, are increasingly connected to networks to allow for remote management by physicians and reduce the need for invasive procedures. These features provide advantages, but also introduce the risk of impact from malicious cyber activity targeting these devices.

FireEye Intelligence is not aware of any malicious activity against personal medical devices in the wild; however, research about threats and vulnerabilities affecting these systems is abundant.

- Since 2016, the ICS-CERT has released thousands of medical advisories for products from major vendors such as Philips, Roche, Medtronic, Smiths Medical, General Electric, and Abbot Laboratories. Despite the outburst in medical vulnerability disclosures, regulation and guidance for protecting cyber-physical networks is still in the early stages of development.
- Even though vulnerabilities in MCPS have been disclosed since at least 2010, during the past two years we have seen multiple disclosures related to products from major vendors. For example, in 2017 and 2018, Abbott Laboratories, St. Jude Merlin, and Medtronic faced the challenge of remediating a series of vulnerabilities affecting pacemakers, programmers, and patient monitors.

We speculate that the existence of networking features and remote access will eventually be used to harm individuals or groups, whether intentionally through a targeted attack or inadvertently through unexpected interactions between device software and activity during access to devices.

- As critical medical devices that individuals rely on to stay alive are increasingly networked and accessible remotely, the potential for a well-resourced malicious actor to carry out a highly targeted campaign designed to injure, sicken, or kill a device user also increases. Such an attack could theoretically be conducted remotely, though possibly requiring close proximity to the device or associated hardware, and would represent a significant escalation in cyber threat activity.
  - » Additionally, actors targeting a device for surveillance, curiosity, or testing could potentially interact inadvertently with a device in such a way that they cause it to malfunction or stop working, causing a similar result to an intentional attack.
- Healthcare-focused Internet of Things (IoT) devices such as inventory-tracking "smart" storage, remote patient monitoring and tracking systems, and remote data access devices similarly increase the theoretical attack surface for healthcare organizations. Compromise of these devices could be used for a variety of purposes, such as to sow confusion by creating false patient alerts, facilitate theft by changing inventory data, and move laterally through a network to conduct further compromises after breaching an insecure device.
- Developers of medical devices have multiple factors to balance in their designs, including power consumption, reliability, and cost; however, we previously assessed that some devices are insecure by design in order to increase access to data for healthcare providers and reduce barriers for physicians to access devices implanted in patients. We suspect that other types of medical devices have similar security shortfalls.

While there is currently no standard network architecture for MCPS. However, the National Institute of Standards and Technology (NIST) special publication (SP) 1800-8B provides a useful baseline to understand the structure of these networks. Following this approach, segmentation plays a key role to enable the implementation of security controls across health care networks.

CONCLUSION

Healthcare organizations must contend with a range of cyber threat actor motivations and behavior. Because of the wealth of data they hold, healthcare breaches and compromises can have far reaching consequences for consumers. The valuable research being conducted within some of these institutions continues to be an attractive target for nation states seeking to leapfrog their domestic industries. Looking forward, as biomedical devices increase in usage, the potential for them to become an attractive target for disruptive or destructive cyberattacks—especially by actors willing to assume greater risk—may present a more contested attack surface than today.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.