ThreatSTOP

Learning from Three Healthcare Cyber Attacks

(that could have been prevented)

Medical Records are Cyber's New Goldmine

Leading cyber security experts claim that medical records have become one of the most sought after data types, worth 10 times more than credit card information. As stated by Forbes, a single medical health record could be worth hundreds or even thousands of dollars, while the going rate for social security and credit card numbers is 10 and 25 cents consecutively.[1] The $3 trillion U.S. healthcare industry is continuing to headline as a desirable cyber attack target, while many healthcare computer systems and networks are still not up to date with the necessary security technology and procedures.

The Value of Medical Records

Medical records are relatively easy for cyber criminals to access. Many healthcare companies and hospitals have weak security measures, with records stored on outdated and unpatched servers. Cyber threat actors, on the other hand, are constantly developing new malware variants, evasion techniques and attack vectors.

Once stolen, medical records can be sold in bulk, reeling in major profits. In some cases, the data is used for medical fraud, including the creation of fake IDs for the purchase of medical equipment and drugs that can be resold. The compromised patient data can also be used to file fake insurance claims.

Medical data has extreme operational importance as well, posing another incentive for threat actors to block access and lock systems down. Continuous access is critical, and the healthcare sector heavily relies on IT systems for storage and operation of medical information.

2019 Healthcare Threat Landscape

Over 13 million patient records were compromised in 2018, in a total of 351 data breaches.[2] Heading in to 2019, healthcare breaches still remain the most expensive to recover from, costing even more than the global cross-industry average of $3.86 million.[3]

It's clear that while the healthcare industry continues to be attractive to cyber criminals, they are not going to cease enhancing their methods in achieving patient information and seizing hospital networks for ransom. The healthcare sector needs to improve security awareness and technology, and learn from reported breaches.

This paper outlines three major malware campaigns that hit the healthcare sector in the past year.

1. https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-tohackers/# 449b286150cf
2. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/
3. https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/

SamSam Ransomware Holds Hospitals Hostage

Since 2015, SamSam ransomware has been attacking victims by and large, with an estimated $6 million raked in from its victims so far, in addition to $30 million in victim losses.[4] While most ransomware attack groups deploy mass infections, attempting to bank as much ransom money as they can, the criminals behind SamSam have become experts at deploying targeted attacks, making them all the more dangerous to organizations. In 2018 healthcare was SamSam's most targeted sector

In January of last year, Allscripts was hit by SamSam, causing a week-long system outage.[5] Hancock hospital was also plagued by the ransomware, which locked the hospitals' patient data and forced them to pay a $47,000 ransom.[6]

Erie County Medical Center was hit by a similar variant in April 2017, taking six weeks for the organization to recover and costing them nearly 10 million dollars.[7]

SamSam's main attack vector is targeted attacks on vulnerable, public-facing servers. In its initial campaigns, the attack group utilized JBoss, Microsoft IIS, FTP and RDP vulnerabilities. In 2018, the SamSam attack group's focus shifted to acquiring single-factor external access to RDP/VNC servers in an attempt to compromise them.[8]

Ransomware poses a triple threat to healthcare organizations – from the encryption or blockage of access to crucial operational data, to the extortion of confidential patient information, and of course, the financial burden of both ransom payment and remediation costs.

4. https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks
5. https://www.healthcareitnews.com/news/allscripts-sued-over-ransomware-attack-accused-wanton-disregard
6. https://www.healthcareitnews.com/news/hancock-health-pays-47000-ransom-unlock-patient-data
7. https://blog.barkly.com/10-million-dollar-ecmc-hospital-ransomware-attack
8. https://www.csoonline.com/article/3263777/security/samsam-explained-everything-you-need-to-know-about-this-opportunistic-group-of-threat-actors.html

Orangeworm Target Anyone Related to Healthcare

An attack group dubbed "Orangeworm" was exposed by Symantec in April of last year. While their motives aren't entirely clear yet, it seems that Orangeworm is attacking large international corporations in an attempt to access critical organizational and customer information. The attack group, who have previously conducted targeted attacks against organizations in various industries, is now primarily targeting the healthcare sector in the U.S., Europe, and Asia.

Orangeworm have deployed targeted attacks on a variety of victims in the healthcare sector, such as healthcare providers and pharmaceutical companies. Targets from seemingly unrelated industries have also been attacked, probably in order to achieve a point of entrance to healthcare companies. These include medical imaging manufacturers selling devices to healthcare firms, IT organizations providing support services to medical clinics, and logistical organizations delivering healthcare products.

Once Orangeworm has infiltrated a victim's network, they deploy Trojan.Kwampirs, a backdoor trojan that provides the attackers with remote access to the compromised computer. Kwampirs Trojan serves as a backdoor and provides Orangeworm with remote access to machines they have compromised.

The trojan first establishes persistence on the machine by confirming the main payload is loaded upon system reboot. Kwampirs then collects information about the compromised machine to determine its value. If it deems the information valuable, the trojan propagates throughout the network, copying itself over network shares and infecting as many machines as possible. Kwampirs then connects to its control and command servers, most likely to exfiltrate the victims' information.

In recent attacks, Kwampirs malware has been used to control X-RAY and MRI machines, as well as machines containing patients' personal information. Additionally, Orangeworm was observed to have an interest in machines used to assist patients in completing consent forms for required procedures.[9]

9. https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Wannacry Freezes Healthcare Devices

The WannaCry epidemic of May 2017 was deemed by Avast "easily the worst ransomware attack in history".[10] The ransomware was able to reach over 250,000 computers in 116 countries, utilizing its self-propagating capabilities to spread like a worm.

The widespread attack propagated using EternalBlue, an exploit developed by NSA. EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol, and the patch for this vulnerability was released nearly two months before the attack. After propagation, WannaCry tries to access a hard-coded URL, and if it is unable to reach the URL, the ransomware encrypts the files on the victim's computer, asking for a ransom payment in order to retrieve them.[11]

In England, the biggest victim of the May 2017 attack was the National Health Service, or NHS.

It is estimated that around 20,000 appointments were cancelled,[12] including over 130 urgent referrals for cancer patients.[13] The ransomware also blocked access to critical medical equipment such as MRI scanners and devices used to test blood and tissue samples, with a total of more than 1,200 pieces of diagnostic equipment affected.[14] Recovery costs and compensation payments to customers amounted to a loss of over 90 million pounds for the organization.[15]

Even a year later, after both the NHS and government put in an enormous effort to secure the organization's systems, all 200 NHS trusts failed the cybersecurity assessment by NHS digital.[16] Many of these trusts are said to have failed because their systems were not patched – the very reason they were infected with WannaCry in the first place.

10. https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html
11. https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
12. https://www.zdnet.com/article/wannacry-ransomware-report-nhs-is-still-not-ready-for-the-next-big-attack/
13. https://www.bbc.com/news/technology-41753022
14. https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/
15. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
16. https://www.healthcareitnews.com/news/nearly-year-wannacry-and-all-200-national-health-service-trusts-failed-cybersecurity

Preventing the Next Healthcare Attack

Understanding the healthcare industry's unique security challenges is crucial to providing the best possible protection from cyber attacks. First and foremost, healthcare organizations need the flexibility to run distributed environments over which highly regulated information can be securely shared only to authorized parties. In addition, medical devices critical to patients' health are becoming increasingly connected to IT systems, which can easily be attacked if not properly secured. A combination of heightened awareness, strong security technology, and the implementation of common security practices can help healthcare organizations ensure thorough protection.

We would like to recommend three actions we believe every healthcare organization should implement:

Patch, Patch, Patch

Unpatched public-facing servers are a cyber attacker's dream. So many healthcare servers are not being patched often enough, leading to awful consequences (such as in the WannaCry attack on NHS). Updating your servers with the latest patches will minimize the risk of your servers being exploited.

Impliment Geo-based Traffic Restriction

Most healthcare organizations and hospitals do not need their devices to communicate with a wide variety of countries, especially countries that are leaders in cybercrime. Blocking both inbound and outbound traffic based on geographic IP data will help minimize communication with unwanted destinations.

Use Network Segmentation

Some healthcare network devices, especially those that come in contact with patients, cannot be patched regularly due to certification restrictions. Another way to reduce threat exposure and spreading is network segmentation – splitting the network in to separate subnetworks, each with its specific security needs and restrictions.

Educate About Phishing

Phishing is an effective infection vector for attackers attempting to infiltrate computer systems, and it works best when the victims are tired, distracted, busy, or need to act quickly. This makes Healthcare workers especially vulnerable to phishing attempts, which usually come in the form of spoofed emails, document files and URLs. Educate workers about various phishing types, how to recognize a phishing attempt, and how to contact your security team if they think they may have fallen victim.

Block Malicious Traffic - Both Ways

Blocking inbound malicious traffic should be at the top of any security operations practices list. With the enormous amount of known threat indicators out there, using a security platform integrated with various threat intelligence sources will give you crucial coverage, barring attackers from reaching your machines. On top of that, blocking outbound traffic based on known indicators gives your systems an additional layer of coverage. For example, if a malware downloads itself but cannot contact its control and command servers, it may not be able to exfiltrate data or download other malware components.

What is ThreatSTOP?

ThreatSTOP is a cloud-based automated threat intelligence platform that transforms the latest threat data into proactive enforcement. The ThreatSTOP platform blocks unwanted traffic and attacks by preventing connections, both inbound and outbound, with threat actors. This approach enables ThreatSTOP to neutralize a broad range of threats and malware including ransomware, DDoS, Angler Kits, phishing and botnets. Enforcement policies are automatically updated and delivered to firewalls, routers, DNS servers and endpoints in the network to stop attacks before they become breaches. The ThreatSTOP platform also includes industry-specific policies, ensuring optimal coverage for each industry's unique security needs.

Tailored Security for Every Operation

The ThreatSTOP platform provides the ability to tailor a security policy to meet specific operational objectives. ThreatSTOP users can customize policy components, as well as create and apply User Defined Lists. Active policies block both inbound and outbound malicious traffic, and can be used to identify malicious activity already in the network. ThreatSTOP DNS Firewall, for example, can be used to identify machines infected by Wannacry ransomware that are currently latent due to successful access to its “kill switch” domains.

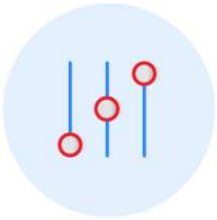
Continue reading here

PREVENT

Move from detection and response to intelligent proactive defense

AUTOMATE

Continuously update network with new threat defense, without manual methods

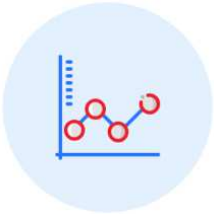


CUSTOMIZE

Defense tailored to specific architecture, policy needs, and reporting requirements

OPTIMIZE

Reduce network load, free up analyst time, dramatically lower incident response costs



Optimal Protection for Healthcare Organizations

ThreatSTOP uses the latest threat intelligence to protect healthcare organizations from IT and IoT threats.

"We have plenty of other systems in place, but ThreatSTOP prevented an ultrasound machine attack and gave us visibility into a large number of DNS queries that were being blocked. It also enabled us to quickly track down the infected ultrasound making the calls. That sold the product."

- Geisinger Health System, ThreatSTOP Customer