

The Ransomware Assault on the Healthcare Sector

Malcolm Harkins & Anthony M. Freed*

PREFACE

While advanced persistent threats and malware continue to plague organizations across multiple industry verticals, it is the threat from ransomware that is still gaining real traction in today's cybersecurity landscape.

The continued evolution of ransomware altered the threat landscape for both organizations and individuals because it is an inexpensive yet very impactful attack method that can be employed in a wide array of attacks, ranging from phishing, drive-by, and watering hole attacks, to targeted attacks that focus on high-value subjects.

The gamechanger with ransomware is the very real threat of data destruction, whereas before, malware may have been used to steal sensitive data that is ostensibly still accessible by the victim. Ransomware goes further than traditional malware by threatening the complete and utter loss of such sensitive data, creating a new level of threat to both individuals and organizations alike—everyone is a target with ransomware.

* *Malcolm Harkins* is the Cylance Chief Security and Trust Officer. He is responsible for all aspects of information risk and security at Cylance®, as well as public policy and customer outreach to help improve understanding of cyber risks. He spent 23 years with Intel, most recently as its first Chief Security and Privacy Officer.

Anthony M. Freed is the Cylance Director of Industry Relations and was formerly an infosec journalist who authored numerous feature articles, interviews, and investigative reports which have been sourced and cited by dozens of major media outlets.

This article will provide an overview of what ransomware is, describe the rise of ransomware-as-a-service in the criminal underground, and how the move to electronic records has made the healthcare sector a prime target for potentially costly attacks.

INTRODUCTION

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009¹ was designed to be a \$31 billion, nationwide transformation of personal health information (PHI) into electronic health records (EHRs).² Yet, one unintended consequence of the landmark legislation is the historic number of assaults launched by cybercriminals on the healthcare industry since its enactment. As part of the U.S. Government's 2009 economic stimulus package,³ HITECH established payment incentives to facilitate the healthcare industry's transition from patient data as paper files locked away in doctors' offices, to electronic records stored on the information superhighway, accessible from anywhere in the world.⁴

¹ Health Information Technology for Economic and Clinical Health (HITECH) Provisions of American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII, Pub. L. 111-5, 123 Stat. 115 (2009) (codified as amended in scattered sections of 42 U.S.C.).

² CONG. BUDGET OFFICE, COST ESTIMATE: AMERICAN RECOVERY & REINVESTMENT ACT OF 2009 (Jan. 26, 2009), at 16–17; *see also* Rob Girling, *The Elusive Promise of Electronic Health Records*, MEDCITYNEWS, (Jan. 20, 2014, 1:00 PM), <https://medcitynews.com/2014/01/elusive-promise-electronic-health-records/?rf=1>.

³ American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. 111-5, 123 Stat. 115 (signed into law on Feb. 17, 2009 by President Obama).

⁴ *See* Standards for the Electronic Health Record Technology Incentive

In theory, EHRs would provide patients and their caregivers with a single source in which to house their medical history and timely data on any current treatments. They would eliminate many of the patient care mistakes that occur due to human error, such as illegible handwriting.⁵ They would also supply more efficient patient care by giving healthcare administrators easier access to a holistic picture for each patient.

Unfortunately, one of the worst side effects of EHRs has been the movement of personal and critical patient data from paper records that were never very secure to easily accessible digital files. What was intended to create accessibility for the benefit of the patient has resulted in accessibility for the benefit of cybercriminals with nefarious intentions, which can include reselling the information online, holding it ransom for vast sums of money, or committing identity theft for the purpose of obtaining free medical procedures and prescription medications.⁶

With patient data available to hackers on hospital and healthcare provider networks, cyberattacks in the healthcare

Program, 42 C.F.R. § 495.2 (2010) (establishing payment incentive programs for hospitals and healthcare providers that can demonstrate “meaningful use” of certified EHR technology); *see also HITECH Act Enforcement Interim Final Rule*, U.S. DEP’T OF HEALTH & HUMAN SERVICES (June 16, 2017), <https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html>.

⁵ Electronic Prescriptions for Controlled Substances, Interim Final Rule with Request for Comment, 75 Fed. Reg. 16236, 16238 (Mar. 31, 2010) (finding that EHRs and electronic prescription applications “may reduce medical errors caused by illegible handwriting”)

⁶ Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals*, 40 SEATTLE U. L. REV. 937, 937–41, 951–58 (2016).

industry have skyrocketed.⁷ The growth in ransomware attacks, in particular, has been a scourge on the U.S. healthcare system. The impact has taken multiple forms, including system and operations downtime, as well as patient care disruptions.⁸

I. WHAT IS RANSOMWARE?

Ransomware is a type of malware that is typically delivered via a phishing email, which is designed to look like a legitimate email received from a trusted sender. The email will contain an attached file, such as a Microsoft Word document, which when opened, will launch a piece of ransomware. The attachment itself may look and act normal, so as to delay the victim from noticing the behind the scenes deployment. Meanwhile, the ransomware will seek out and encrypt critical files on the user's machine, as well as those found on any connected devices.

Once encryption is complete, the ransomware will display an image on-screen with instructions for how the victim can remit a ransom to obtain a decryption code.⁹ This ransom is typically paid in bitcoins, which provides the malware author with an untraceable form of instant

⁷ U.S. GOV'T INTERAGENCY GUIDANCE DOCUMENT, HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE, <https://www.justice.gov/criminal-ccips/file/872771/download>; see also Khizar A. Sheikh, *Ransomware, Social Engineering and Organization Liability*, N.J. LAW., Dec. 2016, at 34 (2016).

⁸ Farringer, *supra* note 6, at 951–54.

⁹ *Id.* at 937–41 (“On the morning of March 28, 2016 . . . a nonprofit hospital system with ten hospitals in Maryland and Washington D.C. were greeted with a pop-up message stating: ‘You have 10 days to send us the Bitcoin. . . . [A]fter 10 days we will remove your private key and it’s [sic] impossible to recover your files.’”).

payment.¹⁰

A. *Ransomware-as-a-Service*

While some ransomware attacks may be launched by highly skilled programmers with a portfolio of successful attacks, thanks to the proliferation of ransomware-as-a-service (RaaS), novice cybercriminals are often finding success now as well. To expand their reach and operations, ransomware specialists offer their code and expertise to novice hackers online for a nominal fee, for no fee at all, or with a cut of any ransom obtained.

RaaS is quickly becoming one of the most popular forms of cyberextortion. It has been around for many years, but lately there has been a significant increase in the number of variations of the ransomware employed. Due to its notoriety and potential for a high payout, ransomware is quickly evolving, and cybercriminals are developing new ways to distribute malware to make money.

In years past, expert malware authors would package up their know-how into costly exploit kits and sell them on the underground market. Cybercriminals would pay a hefty upfront cost before ever infecting a victim's machine and realizing a profit. One such RaaS is known as Satan Ransomware (Satan).¹¹

Satan's developers have posted the ransomware online, making it available for free to the public. Any would-be cybercriminal with absolutely no programming skills can download and deploy *Satan* in just three easy steps, while

¹⁰ *Id.* (demanding a ransom of 45 bitcoin, which was equivalent to approximately \$19,000).

¹¹ *Threat Spotlight: Satan RaaS*, CYLANCE (Feb. 6, 2017), <https://www.cylance.com/threat-spotlight-satan-raas>.

also managing their ransomware campaigns in a central console hosted on the *Satan* developer page. Instructions on payload delivery, translation services, and customer support are even provided to would-be cybercriminals. Then, when *Satan* is successful in an attack, the downloader pays the developer 30% of the ransom obtained, while pocketing the rest.

These are examples from just one industry vertical and three ransomware variants, but they provide real-world lessons on how enterprises can be easily infected, causing great harm to operations, brand reputation, customer relationships, and even the critical infrastructure that organizations all over the world rely upon. The true tragedy of the consequences of ransomware is that they are completely and wholly avoidable with the right endpoint security product.

II. WHY TARGET THE HEALTHCARE SECTOR WITH RANSOMWARE?

The typical healthcare environment forms a perfect storm when considering the vulnerabilities that attract ransomware attacks: the value of personal health information (PHI). The goal of a healthcare ransomware attack is often either to hold prized PHI hostage in the hopes of receiving payment, or to sell the information to third parties.¹²

Today, PHI data is more valuable on the black market than personal information from financial institutions. In some industries, the ability to access data from prior system backups is sufficient to return the business to an acceptable state of operational effectiveness. However, the

¹² See Farringer, *supra* note 6, at 951–58.

fluid nature of healthcare settings requires the immediate and dependable availability of real-time data. Backups even a few minutes old can put patients at risk.

PHI is also valuable to cybercriminals in creating a market for multiple secondary transactions. As published by the FBI Cyber Division, cybercriminals sell personal health information on the black market at a rate of \$50 for each partial electronic health record, compared to \$1 for a stolen social security number or credit card number.¹³

The Lack of Preparation

There is a quote that circulates frequently amongst enterprise workers: “A lack of planning on your part does not constitute an emergency on my part.” In the case of healthcare cybersecurity prevention, nothing could be further from the truth. The industry’s lack of focus on cybersecurity prevention, and the resulting emergencies, are well documented by both the media and HHS.¹⁴

A 2015 study conducted by ABI Research states that the healthcare sector is ill prepared for the new cyberge. Hospitals, clinics, trusts, and insurers are constantly under attack from malicious online agents. Medical identity theft and fraud are on the rise, and healthcare providers are struggling to cope, with the past few years seeing hundreds of instances of data breaches leaking millions of personal

¹³ FED. BUREAU OF INVESTIGATION, HEALTH CARE SYS. & MED. DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FIN. GAIN (2014), <http://www.illumweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf>.

¹⁴ See U.S. DEP’T OF HEALTH & HUMAN SERVS., FACT SHEET: RANSOMWARE & HIPAA, (July 11, 2016), <http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>; see also Farringer, *supra* note 6, at 941–51.

records. And yet the industry spends very little on cybersecurity, in comparison to other regulated critical industries.

ABI Research calculates cybersecurity spending for U.S. healthcare protection will only reach \$10 billion globally by 2020, just shy of 10% of total spending on critical infrastructure security.¹⁵ Examples of these gaps in cybersecurity risk management include the continuing presence of deceptive phishing emails and fake website URLs, which can entice employees to unknowingly disclose login information or download malware. Additionally, without the appropriate patches, servers can be vulnerable to threats. Without proper protection, medical devices and industrial control networks can also be accessed, with potential impacts to life-saving systems.

The Lack of Security Awareness Training

A 2015 survey conducted by the Healthcare Information and Management Systems Society revealed that 64% of 297 respondents—each with some responsibility for information security—had experienced a security incident within their healthcare organization caused by phishing.¹⁶ Healthcare professionals, while highly specialized in their clinical disciplines, are generally not well trained in security awareness. The report indicates that otherwise savvy people click on links found in phishing emails due to sophisticated impersonation techniques.

¹⁵ ABI RESEARCH, *Healthcare Cybersecurity a Massive Concern as Spending Set to Reach Only US \$10 Billion by 2020* (Feb. 25, 2015), <https://www.abiresearch.com/press/healthcare-cybersecurity-a-massive-concern-as-spen>.

¹⁶ HEALTHCARE INFO. AND MGMT. SYS. SOC'Y, HIMSS CYBERSECURITY SURVEY (2015).

For instance, a healthcare phishing attack might involve an email that looks as if it's coming from a familiar vendor such as LabCorp, with the subject of 'Patient Results Available.' The email will look exactly like a LabCorp email. But the link found in the email will take the recipient to a perfectly "spoofed," identical copy of the login page from LabCorp.com. When the recipient tries to log in, his or her credentials will be stolen. Now, the hacker can log into LabCorp and access PHI directly from the healthcare organization's patient rolls.

Impact on the Medical Industry

There is certainly no shortage of threats to write about these days when it comes to ransomware, and the recent surge of activity involving high profile attacks and their victims. It is deeply concerning to hear about the high-profile medical entities that have been targeted as of lately. In this scenario, the price paid for the attack is not limited to the money paid as the ransom. A ransomware attack on a health center has proven to cause delays in patient care, which can even lead to a loss of human life.

Large health systems are particularly vulnerable to attacks on less secure parts of their systems, given the siloed nature of the systems and technologies created using software from various independently managed vendors. A number of high-profiled ransomware attacks on hospitals have resulted in some of the victims paying out tens of thousands of dollars in ransom money to cybercriminals. Consequently, such payouts have led to multiple new attacks on these very same organizations, and the success of these attacks has emboldened the cybercriminal community as a whole.

Ransomware attacks can lead to dramatic losses for

hospitals, healthcare providers, and other healthcare-based enterprises, including:

Financial:

- Amount of the ransom, if paid
- Regulatory investigations, security audits, fines
- Breach notifications
- Civil litigation and reparations to impacted patients
- System upgrades and restoration
- Revenue Loss

Operational:

- System downtime, loss of productivity
- Loss of new patient admittance
- Cancelled procedures and treatment
- Billing and reimbursement delays

In a highly publicized example of such an attack, forty hospitals that are part of the U.K.'s National Health Service (NHS) were hit simultaneously by the WannaCry Ransomware.¹⁷ Reports of canceled surgeries, medical appointments, and lab results on hold due to the attack flooded the local news, and the public outcry escalated the incident to the global news stage.

The *WannaCry* infection highlighted the outdated and vulnerable infrastructure and security of the NHS. In the weeks following the attack, the hospital network was slow

¹⁷ Ian Sherr, *WannaCry Ransomware: Everything You Need to Know*, CNET (May 19, 2017, 12:29 PM), <https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know>.

to recover and restore functions back to each of the forty affected hospitals.

WannaCry: Anatomy of a Ransomware Attack

WannaCry leveraged the *EternalBlue* vulnerability, which took over the news in May 2017 as a result of its inclusion in data leaked by the criminal syndicate known as The Shadow Brokers—a hacking group that has published several leaks of sensitive hacking tools originally developed by the National Security Agency (NSA).¹⁸ Utilized in multiple attacks alongside the also-released *DoublePulsar* exploit, and the cryptocurrency miner malware *Adylkuzz*, these exploits represent just the tip of the cyberwarfare tools that The Shadow Brokers claim to have in their arsenal.¹⁹

The latest *EternalBlue* and *DoublePulsar* based attacks, delivering the *WannaCry Ransomware*, have been extremely damaging to healthcare organizations, while also impacting over 200,000 endpoints in 150 countries.²⁰ *WannaCry-WanaCryptor 2.0* was coupled with the *EternalBlue* exploit, allowing it to automatically propagate itself to vulnerable machines across the Internet. While not technically advanced, the use of *EternalBlue* and *DoublePulsar* created a ransomworm that spread much faster than any other previously reported ransomware

¹⁸ *Id.*

¹⁹ *Threat Spotlight: The Shadow Brokers and EternalPulsar Malware*, CYLANCE (Aug. 15, 2017), https://www.cylance.com/en_us/blog/threat-spotlight-the-shadow-brokers-and-eternalpulsar-malware.html

²⁰ Rohit Langde, *WannaCry Ransomware: A Detailed Analysis of the Attack*, TECHSPECTIVE (Sept. 26, 2017), <https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack>.

outbreak.

This attack exploits a flaw in the *Server Message Block (SMB)* in Microsoft Windows, which can allow for remote code execution upon proper and successful exploitation. The flaw was patched in Microsoft's March 2017 update cycle (MS17-10).²¹ However, many network environments are still behind on these patches and for various reasons—such as computers running on legacy operating systems like Windows XP, which are no longer updated/supported with security patches, leaving their systems entirely exposed and vulnerable to attack.²²

Leveraging this exploit, the attackers can fully execute arbitrary code. In the case of the *WanaCrypt* issue, we are dealing with a ransomware executable that includes additional worm functionality. It has the ability to scan and locate other machines, and propagate itself to other adjacent and exposed hosts via the *EternalBlue* vulnerability. Due to the nature of the flaw, machines that are propagated via the worm functionality do not require interaction from the user on the victimized host.

The worm/ransomware binary handles the remote execution. In most confirmable cases today, stage one is a malicious phishing email. This includes an attachment that the victim executes, which infects them, while simultaneously kickstarting stage two—the worm-type functionality and internal propagation/pivoting.

Ransomware has been around for well over a decade, but traditional antivirus solutions still require every single

²¹ MICROSOFT, SEC. UPDATE FOR MICROSOFT WINDOWS SMB SERVER (4013389) (Mar. 14, 2017), <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>.

²² Farringer, *supra* note 6, at 957 (noting critics see an industry-wide culture that is unwilling to adapt to, and more importantly invest in, the advancing technological landscape).

piece of malware to be discovered by its execution on an endpoint, meaning that these solutions cannot stop ransomware until it infects its first victim. If your organization is the “sacrificial lamb” that traditional antivirus providers need, you could be faced with an extremely costly ransom, which may or may not yield the ability to decrypt your locked data.

The Sense of Urgency

The obligation of healthcare organizations to maintain the integrity of patient care environments and the accuracy of medical records is a powerful incentive to return the environment to its original state. But this sense of urgency held by healthcare providers to return to normal operations as quickly as possible also provides a strong advantage to the perpetrators of ransomware attacks.²³

When hospitals lose control of their data, they risk being in violation of HIPAA regulations as outlined in the HIPAA Breach Notification Rule.²⁴ The rule requires HIPAA-covered entities and associates to provide notification following a breach of unsecured PHI. Older and less sophisticated strains of malware wrap or encrypt the PHI data, never moving it from the server or desktop environment. A party who does not have the proper authorization cannot view it. A current list of a list of breaches of unsecured protected health information affecting 500 or more individuals is available.²⁵

However, more sophisticated malware variants are

²³ *Id.* at 951–58.

²⁴ HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414 (2009).

²⁵ U.S. DEP’T OF HEALTH & HUMAN SERV., BREACH PORTAL: NOTICE TO THE SEC’Y OF HHS BREACH OF UNSECURED PROTECTED HEALTH INFO. (2018), https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

able to access the data, and some sit dormant for long periods of time before creating the breach. In such a case, the burden of proof is on each healthcare organization to have solutions in place that can clearly determine whether or not the ransomware viewed or accessed any PHI data, potentially enabling the ransomware author to download or view it.

III. CONCLUSION – AN OUNCE OF PREVENTION

In February 2016, the Ponemon Institute released the results of its 2016 State of Cybersecurity in Healthcare Organizations study.²⁶ According to its researchers:

- Healthcare organizations average one cyberattack per month;
- 48% of respondents stated that their organizations have experienced a security breach involving the loss or exposure of patient information data in the last 12 months; and
- Only half of the respondents indicated that their organization has an incident response plan in place.

With findings like this, the answer seems obvious. Benjamin Franklin said, “[b]y failing to prepare, you are preparing to fail.” With the current opportunity for healthcare decision makers to hardwire their enterprises with next-generation endpoint protection solutions, the industry could potentially begin to see reports of cyberattacks drop significantly within the coming twelve months.

²⁶ PONEMON INST., THE STATE OF CYBERSECURITY IN HEALTHCARE ORGS. IN 2016 (Feb. 2016), https://cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf.

The responsibility to take appropriate steps toward the right solution now lies in the hands of board members, C-level executives, and IT security specialists. In parallel, employees must be trained to identify phishing events, and to address them in a way that reduces security risk.

Cyberattacks are planned and delivered in nearly the same manner, seldom straying from a high-level process map known as the Cyber Kill Chain. The only variable is the amount of technical or personal resources cybercriminals spend on the different stages of an attack. No matter where your current internal infrastructure lies on the spectrum of cybersecurity preparedness, understand that there are emerging next-generation solutions available that can stop malicious files before they ever execute, with no “sacrificial lamb” required.

The problem with legacy security solutions is that adversaries can continually evolve their techniques and tactics to bypass them, leaving enterprises vulnerable to attacks. This means that traditional solutions are reactive in nature and rely on a constant stream of “signature updates” to tell them what type of files to look for after an attack was successful on some other system, known as “zero-day” attacks. Traditional security solutions are built around a basic set of rules and signature files that are costly and high risk because they require many “sacrificial lambs” before they can create the ability to block an attack—meaning it is not possible to identify a new threat until after some damage is done. This is what is occurring in the health care industry, as well as in other sectors. It is time for us to innovate and take action faster than we currently have. We need to implement new security architectures that will provide significant improvement in our ability to mitigate and manage our growing information risks.

Any future security architecture to be implemented

must provide for better prevention, and it also must be more flexible, dynamic, and more granular than traditional security models. A new architecture also needs to greatly improve threat management. We need to do this in the upfront design, development, and validation during the creation of technology to reduce vulnerabilities well before the technology gets deployed. And as new attacks appear, we need a security system that is able to recognize the good from the bad in milliseconds, so that it can stop the bad and allow the good. For any attack that gets past these preventive controls, we need to be able to learn as much as we possibly can without compromising the user's computing performance or privacy. This information enables us to investigate exactly what occurred, so we can take immediate action to mitigate the risk, whilst also learning how to prevent similar attacks in the future.

A control architecture should assume that attempts at compromise are inevitable—but we should also understand that it is possible to achieve real prevention for 99% or more of the risks that could occur, including that of malicious code and zero-day attacks caused by mutated malware. Should a piece of malicious code attempt to execute, we can then instantly apply artificial intelligence and machine learning to analyze the features of files, executables, and binaries to stop the code dead in its tracks, before it ever has a chance to harm the environment. For the remaining attacks—representing less than 1% of malware—we need to focus heavily on survivability.

JFK once said: “The problems of the world cannot be solved by skeptics or cynics whose horizons are limited by the obvious realities. We need men who can dream of things that never were and ask why not.” When we innovate and implement a new security architecture focused on prevention of risk at the core, coupled with AI based detection and

response, we can achieve a dramatic reduction in risk and an equally dramatic improvement in our health care system.