GLOBAL BIOSECURITY

Branch LE, Eller WS, Bias TK, McCawley MA, Myers DJ, Gerber BJ, Bassler JR. Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. Global Biosecurity, 2019; 1(1).

RESEARCH ARTICLES

Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017

Lauren E Branch[1], Warren S Eller[2], Tom K Bias[1], Michael A McCawley[1], Douglas J Myers[1], Brian J Gerber[3], John R Bassler[4]

[1]West Virginia University, Morgantown, WV, USA
[2]The City University Of New York, New York, USA
[3]Arizona State University, Tempe, AZ, USA
[4]University of Alabama at Birmingham, Birmingham, AL, USA

Abstract

Introduction: The healthcare industry has begun seeing a new hazard develop against them- the threat of cyberattack. Beginning in 2016, healthcare organizations in the United States have been targeted for malware attacks, a specific type of cyberattack. During malware incidents hackers can lock users out of their own network to gain access to information or to hold the organization for ransom. With the increase in medical technology and the need for access to this information to provide critical care, this type of incident has the potential to put patient lives and safety at risk.

Methods: A content analysis was conducted to assess the trend of attacks on healthcare organizations. U.S. Healthcare IT News and Becker's Hospital Review were used to collect all publicly reported malware attacks against U.S. healthcare organizations between 2016 and 2017. A logic diagram was also developed to illustrate how hackers gain access to a healthcare network using malware.

Results: There were 49 cases of malware attacks against U.S. HCOs identified. The attacks occurred across 27 states, and they took place during 18 out of 24 months. Six of the organizations reported paying ransom, whereas 43 organizations did not pay or did not report payment to the press. Impacts of these attacks range from network downtime to patient and staff records being breached.

Discussion: Malware attacks have the potential to impact care delivery as well as the healthcare facility itself. Even though this study identified 49 malware attacks, we know this number is significantly higher based on data from HIMSS and the FBI. A reporting loophole exists in that hospitals are only required to report attacks in the case of breached protected health or financial data. For HCOs to fully understand the risk cyberthreats pose, it is important for attacks to become public information and for lessons learned to be shared. Future research reviewing identified attacks could help identify best practices for the healthcare industry to better prepare for cyberattacks.

Introduction

Recently, the healthcare industry has been facing a new type of hazard; bad actors have started targeting hospitals and other healthcare facilities for cyberattacks. This industry is particularly vulnerable to cyberattacks because healthcare providers depend on up to date information from electronic health data. This information includes patient histories and test results, which is often needed at a moment's notice to provide critical patient care. Approximately 95% of hospitals in the United States use health information technology, such as electronic medical records (1). Many other health technologies, including glucose meters, IV pumps, and implanted medical devices, are also connected to and dependent on the hospital's network. With patient safety on the line, hospitals may be more willing to pay for restored access to their network. Healthcare organizations (HCOs) have become much more reliant on health information technology over the past decade. Another vulnerability that makes hospitals susceptible to cyberattacks are the out of date cybersecurity systems at many facilities and limited training for staff on safe cyber practices (2). These characteristics combined make HCOs good targets for attack (1, 3).

The cyberthreats that HCOs now face are complex and can come both internally and externally to the network (4). In a survey conducted by the Healthcare Information and Management Systems Society (HIMSS) of healthcare organizations, 37.6% of respondents said their most recent security incident was caused by an online scam artist, whereas 20.8% reported a negligent insider and 20.1% reported a hacker as the cause (5). There are also many points of entry in to a healthcare network, which have the potential to make them extremely vulnerable (See Figures 1 and 2). A point of entry is a way for bad actors to gain access to a hospital computer or network in

order to achieve something malicious, whether that be stealing data or delivering a payload virus (6). Some points of entry identified in the HIMSS Cybersecurity Survey include email, infected hardware or software, compromised medical devices, third party website, and a provider or a service linked to the network via the cloud (5). Some additional points of entry include internet access, a wireless network, removable media (i.e. USB drive, laptop), or theft of equipment (6). In the 2018 HIMSS Survey, 61.9% of participants identified e-mail (e.g. phishing e-mail) as the point of entry in their organization's most recent significant security event. Another way that hackers attack is through backdoors or unpatched vulnerabilities, which are essentially access points left open across the network.

Figure 1 displays a sample hardware network of an HCO. Each switch on the diagram represents multiple devices connected to the network, and each device presents their own multiple points of entry via e-mail, the internet, or USB connections. Depending on the level of network cybersecurity, an infected phone being connected to a system computer or an infected link from an email being clicked can potentially transfer a virus to the network and spread. Figure 2 shows an example of a software network within an HCO. In this example, there is a virtual interface with a corporate office with its own clinical and administrative management software. There are also interfaces with many different applications used around the organization, including imaging, labs, pharmacy, payroll, and patient scheduling. Each of the applications represents potential points of entry for bad actors to break in to the organization. HCOs must rely on their corporate interfaces as well as third party vendors to keep their products secure with up-to-date protections. With so many different points of entry in to the HCO hardware network, these networks have become extremely intricate and therefore highly susceptible to unauthorized access. This complexity also serves to make the networks hard to secure. Figures 1 and 2 are based on small hospital network, but the connectivity displayed in each diagram, a central hub that interacts with many different devices and applications, is a set-up seen in the typical U.S. hospital.

Hackers use different attack techniques to take advantage of HCO vulnerabilities and gain access to the network. A common type of attack is a phishing scam conducted over email. Hackers send an authentic looking email to hospital staff and include a link or attachment that unsuspecting users open or click. Once that content is activated, the hacker gains access to the network and can get information or activate a malicious virus (6). Phishing scams are on the rise; there was a 789% increase in phishing e-mails from the last quarter in 2015 to the first quarter in 2016 (7). A second type of attack is a malware attack, which is when malicious code or virus is dispatched within a computer network (4). One example of malware attack that is of growing concern for healthcare organizations is ransomware. In the HIMSS 2018 Cybersecurity Survey, respondents ranked perceived threats and ransomware is now second on the list (11.3%), whereas natural hazard (i.e. fire or flood) was eleventh on the list (8.3%) (5).

During a ransomware attack, bad actors will lock users out of a network and demand a ransom payment to restore access. The first ransomware attack took place in 1989 when an AIDS researcher, Joseph Popp, sent 20,000 floppy disks to AIDS researchers in 90 countries. The floppy disks were said to contain a questionnaire to help determine patient's risk of contracting AIDS. When inserted, these disks infected the computer with a virus that lay dormant until the 90th time they were turned on. Once the computer was booted for the 90th time, a note would appear on the screen asking for licensing fees to be paid while locking the user out of the computer (3). Since 1989, ransomware attacks have continued and are now categorized as one of two types: scareware and crypto ransomware. Scareware will inform a computer user there is something fatally wrong with their machine and offer a solution for a small payment. Crypto ransomware is much more complex, in that it will encrypt computer files so that they need a certain decryption key to be opened. These crypto-viruses have become a lot harder, and many times impossible, to break even by experts (3).

Similar to the first ransomware attack, hackers have again shifted their targets to the healthcare industry. In healthcare, this type of attack can essentially shut down an organization's ability to operate and lock providers out of essential data needed to provide patient care (8). In May 2017, a global ransomware attack known as WannaCry was perpetrated by the North Korean government (9). Hackers utilized a stolen National Security Agency (NSA) tool that highlighted a vulnerability of Windows Operating Systems to gain access to 300,000 computers across 150 countries (9-10). During this attack, 36 health organizations, including hospitals, ambulance services, and physicians' offices, in Great Britain were locked out of their systems (11). WannaCry forced the National Health Service to send patients away from certain facilities in order to receive the care they needed (11). Homeland Security experts have said this attack directly put patients' lives at risk (10).

This type of cyberattack against organizations has become more frequent in occurrence (12). In April 2016, there was a 159% jump seen in ransomware attacks from the month before. This was a huge rise from the normal 9-20% monthly increase that had previously been seen (13). In 2015, across all industries, the Federal Bureau of Investigation (FBI) reportedly received more than 2,500 ransomware complaints, which cost the victims $214 million (14). A 2016 IT report stated 93% of phishing emails now contained ransomware (7). In 2018, the city of Atlanta

fell victim to a ransomware attack and lost many of its critical municipal systems. This attack alone cost the city $2.7 million to recover (15).

In February 2016, an outbreak of ransomware attacks against United States hospitals began at Hollywood Presbyterian Medical Center in Los Angeles, California. The hospital was offline for over a week before deciding to pay the ransom (16). Approximately $17,000 was paid and the hospital regained access to its operating systems (17). Since this initial attack, there has been a surge in reported malware attacks of healthcare providers across the United States. These attacks can be extremely costly for HCOs (18). A hospital in New York was attacked in 2017 and it has been estimated that their recovery cost was almost $10 million, including hardware, software, extra staff hours, overtime hours, and loss of business costs (19). The on-going fixes and upgrades to the hospital system are estimated to be an additional $250,000 to $450,000 a month (19). In the most recent HIMSS Cybersecurity Survey, 75.7% of respondents reported a significant security incident in the past 12 months (5).

The best way for hospitals to protect themselves is to be proactive and take steps to strengthen their potential vulnerabilities and weaknesses. Hospitals need to conduct risk assessments to better understand how large the risk malware attacks pose to their organization, as well as how big an impact successful attacks can have on operations. Once they have a risk analysis of malware attacks, HCOs can decide which fixes to their system make the most sense financially to offer the most protection.

Lack of reliable reporting on frequencies and impact of this type of attack make it difficult for the healthcare industry to better secure their systems. The risk reports that do exist do not expand on the nature and scope of these successful attacks. Some of these incidents only affect a few computer terminals, whereas other incidents have a more significant impact on the organization and have the potential to affect patient care and safety. Due to the inherent nature of hospitals and the initial ransom payment made by Hollywood Presbyterian Medical Center, these types of incidents are only expected to continue to grow in frequency.

Currently, there are popular media reports on these attacks, but there is no methodology for consistently tracking hospital attacks over time. This study seeks to address this gap by assessing the trend of malware attacks on HCOs over time. This objective will be achieved by reviewing publicly-reported, successful attacks on healthcare organizations within the United States between 2016 and 2017. The final product of this analysis will be a timeline of reported ransomware attacks on hospitals, as well as a summary of what data is being reported with each attack. A logic diagram will also be developed to show the process of a malware attack on an HCO. Without a better understanding of this type of threat, healthcare organizations cannot adequately protect their organization or their patient's safety (4).

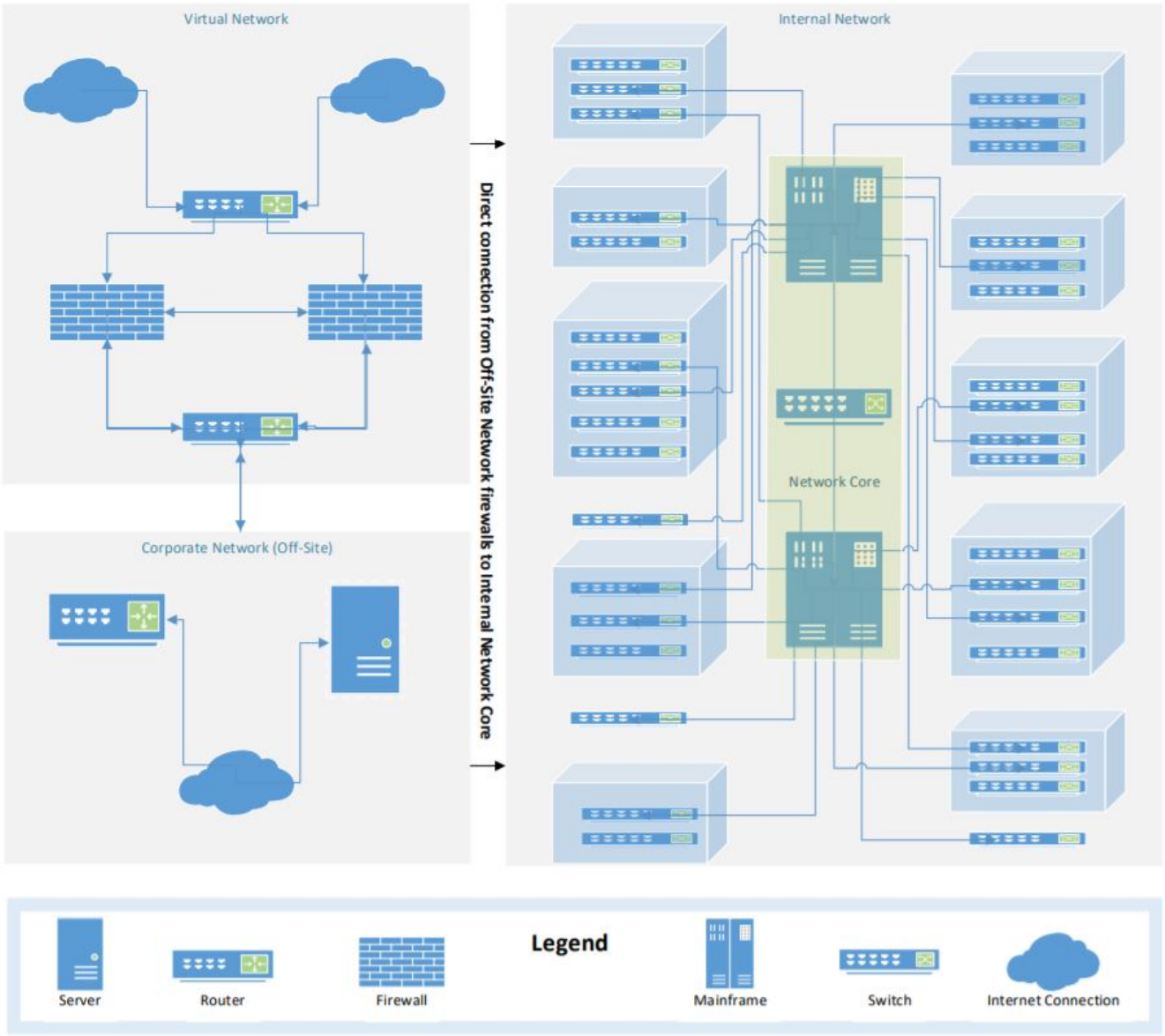
Methods

A content analysis was conducted of news articles related to hospital malware attacks. The new sites Healthcare IT News and Becker's Hospital Review were used as data sources. Healthcare IT News is a site published by Healthcare Information and Management Systems Society (HIMSS) and is one of the most comprehensive news sources for information on healthcare information technology. Becker's Hospital Review is another well-known and reputable source of information related to information technology in the field of healthcare. A search of these databases was conducted using a combination of the keywords "hospital" or "healthcare", "malware" or "ransomware" and "attack". These articles were reviewed for relevance to the research question. Inclusion criteria for articles were references to malware or ransomware attacks on hospitals or healthcare facilities within the United States during 2016 and 2017. Articles that discussed data breaches caused by hackers or misplaced hardware, as well as articles that discussed phishing scams, were excluded from this analysis.

The included articles were analyzed to identify cases, which were then were formatted into timelines to summarize the number and locations of reported malware attacks. Upon further investigation and research, each case was also reviewed for date of attack, name of facility or organization, location, how many facilities were affected, what the impact on the facility was, and if any outcome was disclosed. If the articles referenced a data breach, that information was cross referenced with the U.S. Department of Health and Human Services Office of Civil Rights Breach Report Database. The HITECH Act requires that all data breaches impacting 500 or more individuals be reported in this database. This data was put in to a table to summarize the extent of publicly-reported malware attacks on United States hospitals between 2016 and 2017, and to identify trends within this dataset.

A logic diagram was also created to illustrate a malware attack on a hospital network through a phishing attempt. This diagram walks through the steps of a phishing ransomware attack in which a hacker gains access to the network. The logic diagram was created using data collected during qualitative interviews with subject matter experts, including a Chief Information Officer, a Chief Information Security Officer, a Senior Network Administrator, and a Healthcare IT Manager. It uses a hypothetical hospital to show the extent of a successful phishing attack, and the breadth of access to data and applications a hacker could potentially gain in to a secure network.

Figure 1. Hardware Network Diagram



Note: Below are brief explanations of the purpose each hardware device in this figure. A server is a computer that either provides information to other computers or stores files which can be access from other computers. A router is the director of communication traffic between devices (e.g. computers). A firewall is a form of security used to keep unauthorized users out of a network. A mainframe is a computer where large organizations store their critical applications that are access through the network. A switch is a networking device that connects multiple computers to the network. The internet connection is the organizational connection to outside networks.

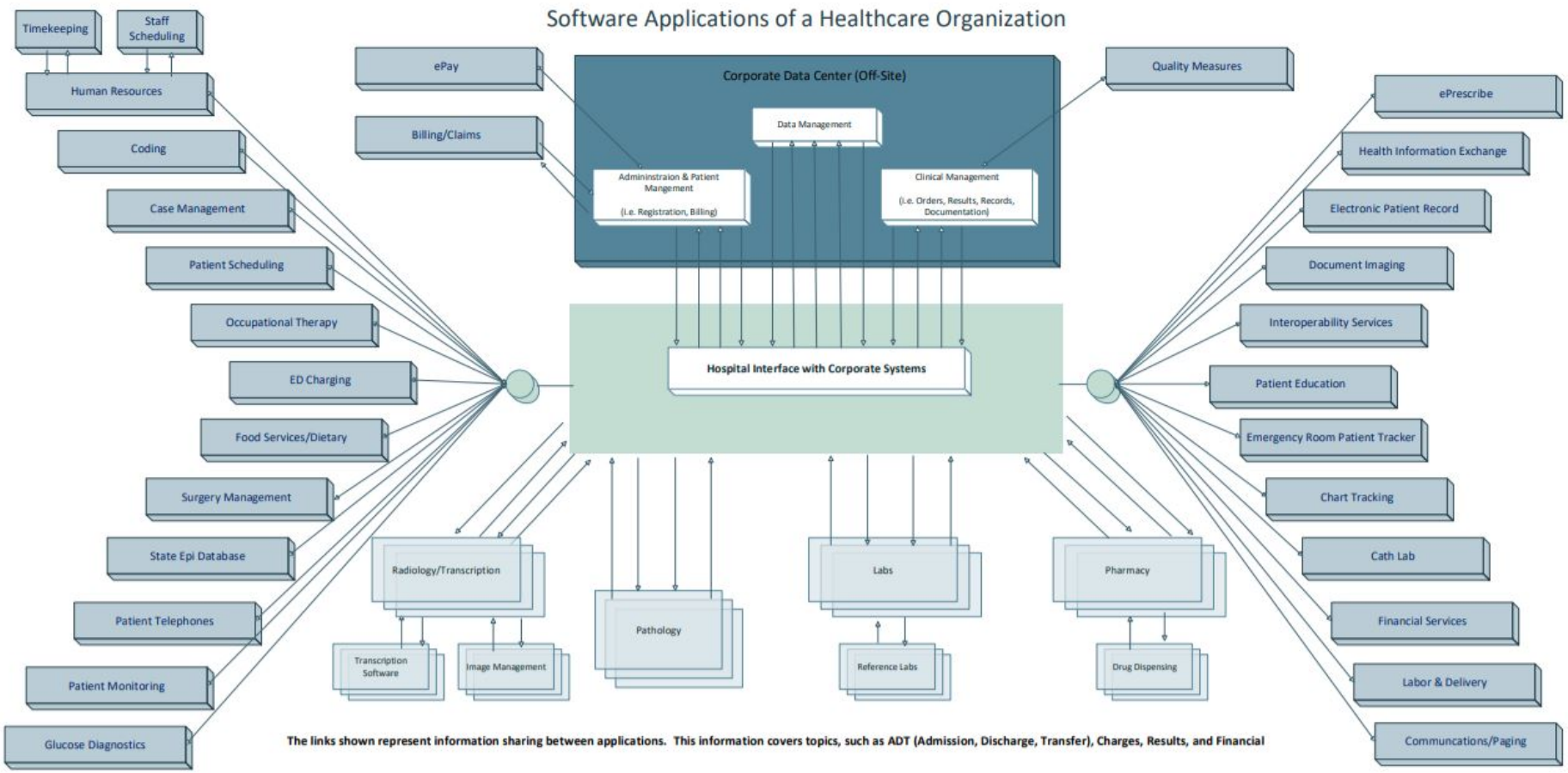
Results

Malware Attacks, United States 2016-2017

Overall, this study discovered 49 reported cases of malware attacks on U.S. Healthcare Organizations during 2016 and 2017. There were 22 malware attacks in 2016 and 27 malware attacks in 2017. Figures 3 and 4 present these healthcare attack cases, respectively. This analysis has shown attacks occur all over the country and take place all year long. The data collected showed there were malware attacks on HCOs in 13 states in 2016 and 20 states in 2017. A map of the United States displaying frequency of malware attacks for both years is shown in Figure 5. The state with the most attacks was California with 9 attacks across both years. There were 16 states that saw one attack across both years. Both years had attacks reported in 9 different months. The attacks are affecting more than just hospitals across the country. One attack against a health system impacted 10 hospitals and 250 outpatient clinics in the D.C./Maryland region. Another attack against a health system saw impacted hospitals across state lines. Some of the attacks only impacted one facility, but often that facility lost access to its medical records.

Each of the 49 identified cases did not have the same impact to their respective healthcare organization. Tables 1 through 4 present impact details of the identified malware attacks. Forty-one of

Figure 2. Software Network Diagram



Note: This diagram is an example software network, which is typical for HCOs. There is a central network hub that interacts with the numerous software applications, and in this example also is connected to an outside corporate network.

Figure 3. Timeline of Hospital Malware Attacks in the United States, 2016

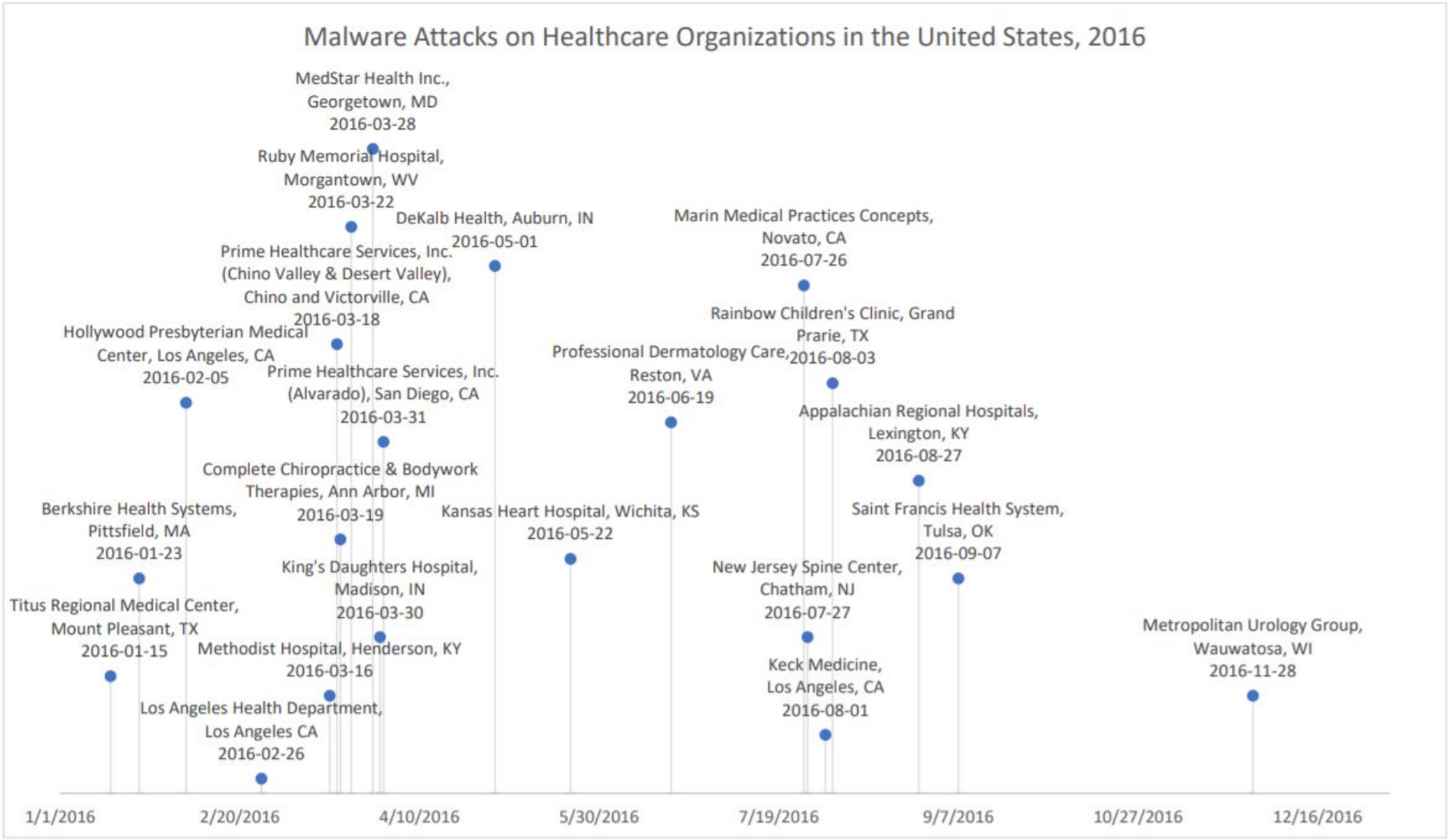
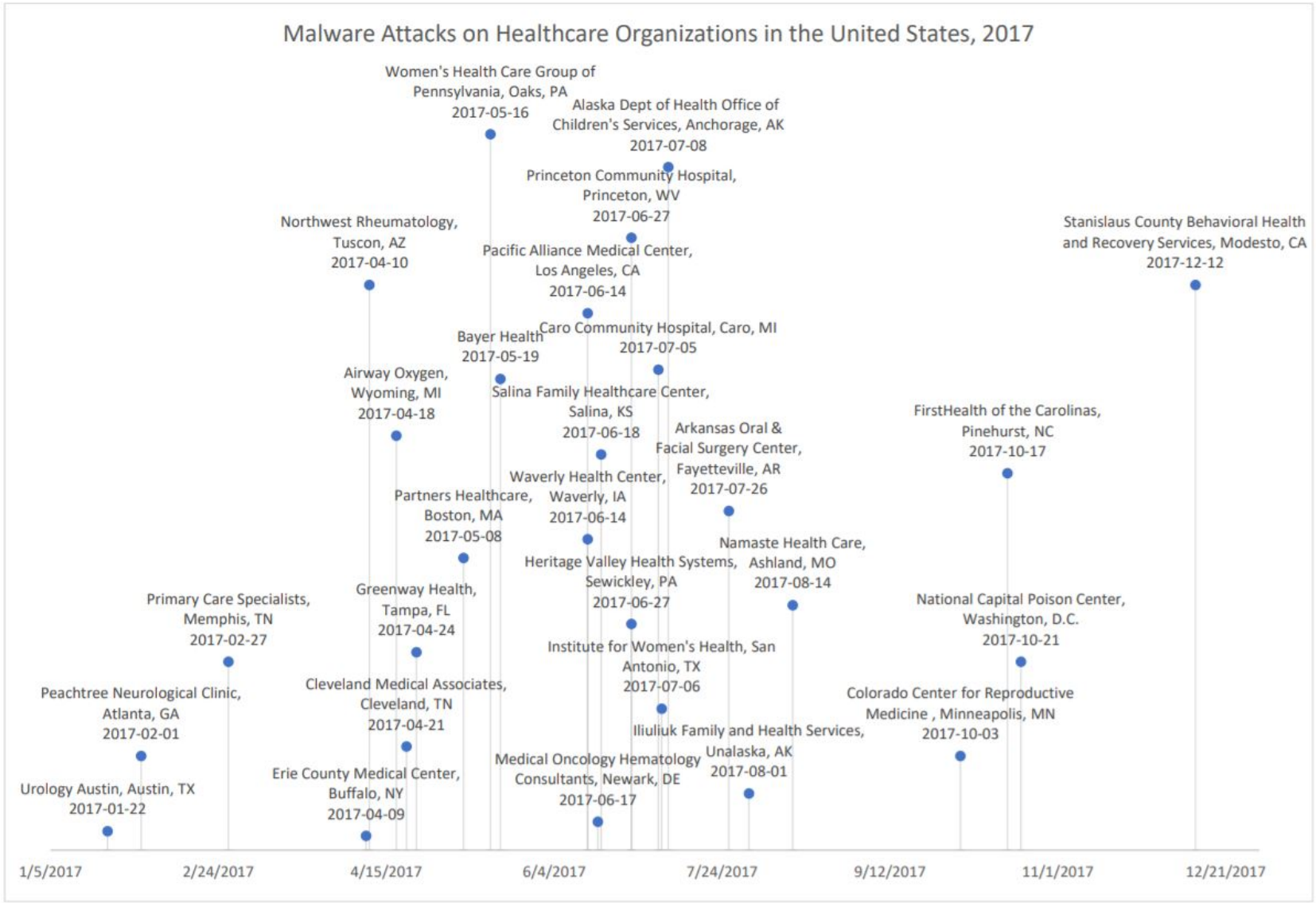


Figure 4. Timeline of Hospital Malware Attacks in the United States, 2017



the cases were labeled as 'ransomware' attacks (shown in Table 1). The articles reported that at least six organizations paid ransom (shown in Table 2). In one case (Kansas Heart Hospital), the hospital paid ransom and the hackers released only a portion of their files before demanding a second ransom. They did not pay the second ransom demand (20). The other cases either did not pay or did not disclose a payment to the press. Some of the articles reported outage times for the organizations, which ranged from 1 day to about 2 weeks (show in Table 3). The most frequent time offline that was reported was one week. The first ransomware attack against a hospital, Hollywood Presbyterian, paid $17,000 after a stand-off with hackers and almost two weeks offline. Another major impact identified was compromised patient or staff records. Sixteen of the attacks reported no records breached. Seventeen of the attacks reported less than 50,000 records impacted. The highest number of records reported 500,000 breached records, with three other attacks reporting more than 200,000 breached records (shown in Table 4).

One of the issues identified while completing this content analysis was the lack of consistency in reporting and defining this type of attack. Across all identified cases, there were different search terms required to identify certain cases. Table 5 shows the different terms that were required to find different cases. Ten of the cases only showed up in searches using the term "cyberattack", eight only showed up using the term "malware", and ten only showed up using the term "ransomware". The other 21 cases were identifiable using more than one of the listed search terms. This lack in consistent reference words make it difficult to fully identify all reported cases.

Logic diagram

Due to the complexity of healthcare organizations, there are a few steps hackers must go through to gain access. Figure 6 presents the steps as they would occur in an email phishing attack. The attack begins when a hacker sends mass emails to employees within an organization attempting to deceive at least one employee. The email would either contain a malicious link or attachment within that would allow the hacker to gain shell credentials to the organization. With the counterfeit credentials the hacker can impersonate the employee within the system, and depending upon the level of access they have, gain direct access to network applications or they can find another user credential with higher level access.

Once the hacker gains administrative level access, they can permeate across the organization's network to find the information they are looking for. In this scenario, Figure 6 shows the applications and confidential data the hacker would gain access to in this HCO. The software applications include timekeeping, imaging, medical scribing, catheter laboratory services, obstetrics and gynecology clinical services, the network email exchange and all organizational file shares. From this access, the hacker has access to protected health information, proprietary business data, payroll information, and other confidential data, such as social security numbers of patients and staff members.

Figure 5. Frequency of Malware Attacks in the United States, 2016-2017

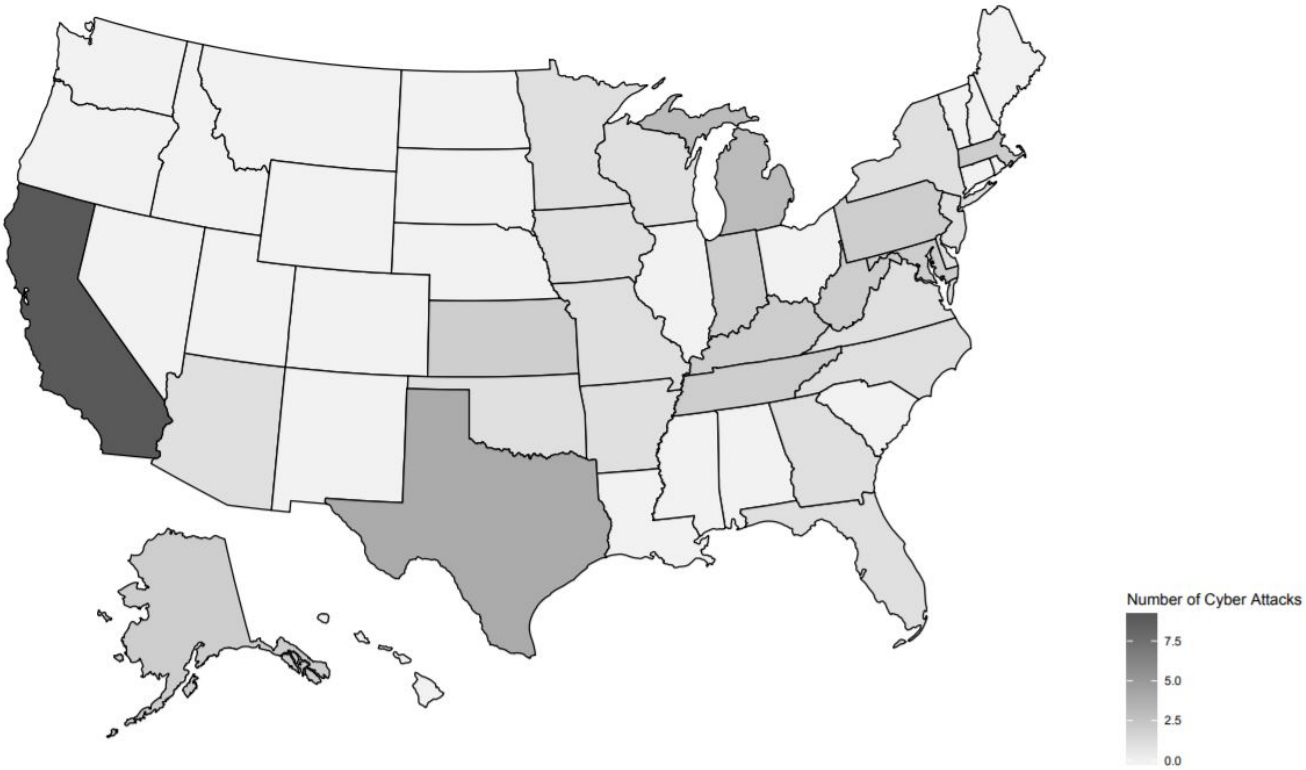


Table 1. Terminology Used to Describe Attack, U.S. Malware Attacks 2016-2017

Terminology	2016		2017		Total (N = 49)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Malware	5	22.73	3	11.11	8	16.33
Ransomware	17	77.27	24	88.89	41	83.67

Table 2. Ransom Payments, U.S. Malware Attacks 2016-2017

Payment Reported	2016		2017		Total (N = 49)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Yes	5	22.73	1	3.70	6	12.24
No	17	77.27	26	96.30	43	87.76

Table 3. Network/System Time Offline, U.S. Malware Attacks 2016-2017

Time Offline	2016		2017		Total (N = 14)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
1 day	0	0	2	33.33	2	14.29
>3days	0	0	1	16.67	1	7.14
>a week	3	37.5	0	0	3	21.43
1 week	1	12.5	2	33.33	3	21.43
2 weeks	1	12.5	0	0	1	7.14
> 2 weeks	0	0	1	16.67	1	7.14
3 weeks	1	12.5	0	0	1	7.14
5 days	2	25	0	0	2	14.29
Missing	14	.	21	.	35	-

Table 4. Number of Medical Records Impacted, U.S. Malware Attacks 2016-2017

Impact Range	2016		2017		Total (N = 41)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
0	7	43.75	9	36.00	16	39.02
Less than 10,000	4	25.00	5	20.00	9	21.95
10,000 to 50,000	5	31.25	3	12.00	8	19.51
50,000 to 100,000	0	0.00	2	8.00	2	4.88
100,000 to 200,000	0	0.00	2	8.00	2	4.88
200,000 and Above	0	0.00	4	16.00	4	9.76
Missing	6	-	2	-	8	-

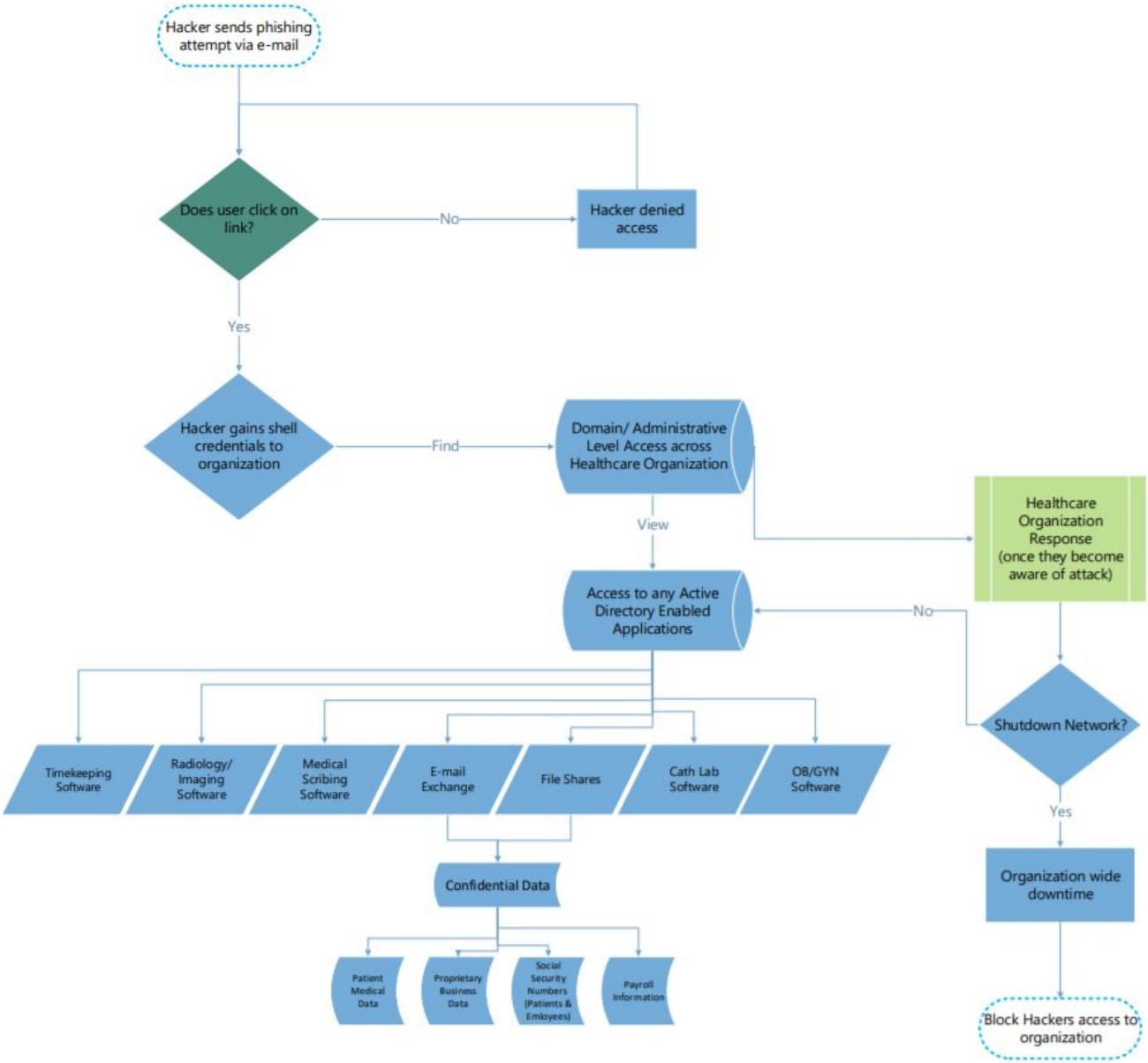
Table 5. Search Engine Terminology, U.S. Malware Attacks 2016-2017

Search Engine	2016		2017		Total (N = 49)	
	Frequency	Percentage	Frequency	Percentage	Frequency	Percentage
Cyber attack	2	9.09	8	29.63	10	20.41
Malware	5	22.73	3	11.11	8	16.33
Ransomware	6	27.27	4	14.81	10	20.41
Ransomware / More than one	9	40.91	12	44.44	21	42.86

If the hacker's goal is to deliver a malicious payload, such as ransomware, the hacker can choose where to drop it once they gain access to these organizational applications on the network. They can choose a location which would cause the biggest service disruption to increase likelihood the organization will pay the ransom demand.

Once a hacker gains access to the HCO's network, the HCO itself has limited options on how to stop access. The first step is that the HCO must realize they have someone with malicious intent inside their network. Often in the case of ransomware attacks, this does not happen until applications stop working or a ransom note appears on desktops across the organization. In cases like this, it is imperative the HCO shuts everything on the network down to stop the spread of the virus and to cut off the hacker's access to the network. This step would also cut off all users' access to the network and cause a complete organization-wide downtime. Once the network is shutdown, the HCO can conduct impact assessments to see how much damage has been done, if any, and can begin their recovery and business continuity processes. If the HCO decides not to shut down the network, the hacker has continued access to the network and the virus can continue to spread infecting more hard-drives.

Figure 6. Logic Diagram



Discussion

Over the last few years, we have seen an increase in this trend of cyber targeting healthcare organizations. This content analysis found 49 instances of malware attack on U.S. healthcare organizations during the years 2016 and 2017. These attacks occurred all over the country; with 27 states having a reported attack during this period. The attacks also impact all areas of healthcare delivery, including hospitals, primary care, outpatient clinics, medical suppliers, and electronic medical record providers.

With aspects of care delivery at risk, malware attacks are a threat to patient safety (6). The 49 attacks identified through this analysis had ranging levels of impact, but all were required to go offline for a period of time to stop the spread of the computer virus. Providing care without access to patient history can be hazardous. For example, without the system's automated checks and balances in place while prescribing medications, there is a chance that something in the patient chart gets overlooked. Medical devices are also at-risk during malware attacks, including therapeutic equipment (infusion pumps), life-support equipment (ventilators) and diagnostic equipment (PET scanners). Any of these devices can serve as backdoors in to healthcare networks if not secured. One report reviewed three case studies where medical devices were used by hackers to break in and move through a network (21).

Malware attacks can also affect patients and staff in ways other than through provision of healthcare services. Attacks can have direct impacts on the facility itself, which potentially has downstream impacts on patient care. At least one of the attacks from this

analysis saw impacts to their security systems. The hospital's security cameras went offline and they were forced to go in to lockdown until the cameras could be brought back online. Another system potentially at risk is the HVAC system. Without environmental temperature regulation, there is the possible need for evacuation of patients. Finally, as seen in other cyberattacks, the electrical grid and water treatment are also potential targets (22). Without power or clean water, hospitals could no longer provide care and would also be required to move patients. Evacuation of a hospital is an extreme undertaking regarding staffing and resource needs, as well as finding equivalent bed capacity to take patients. An extreme example of the impact of power loss and evacuation on patient care was seen during Hurricane Katrina at Memorial Hospital where physicians decided which patients to save and hastened the death of others (23).

This is the first known content analysis to develop a list of malware attacks across the healthcare industry. One limitation of this research is the reliance on public reports of attacks. Not all attacks are being reported and most of the reported attacks are large scale incidents. Based on FBI and HIMSS data, we know that this is a much bigger problem. The FBI urges HCOs to report attacks, but ultimately this is left up to the discretion of the facility. Attacks are only required to be reported when medical or financial information has been compromised. One reason for not reporting is that HCOs do not want to risk their reputation or income by being labeled a victim. This reporting loophole makes it much harder for the industry to get a clear picture of the attack trend (24). Another limitation is the lack of consistency in reports of each attack. This study tried to combat this inconsistency by using multiple search terms including 'malware', 'ransomware', and 'cyberattack'. With different terminology used in reports, there are potentially cases that are being reported but might not be captured by the content analysis. Even with this limitation, the dynamic understanding provided through this content analysis will illustrate the frequency and types of cyberattacks, which has not been previously researched. The sample of this analysis only includes successful attacks, but there are also many more institutions who are vulnerable to attack (5). There is a need for the healthcare industry to push for more public data regarding this hazard. If attacks were reported to a single database, this information could be accessed in one location and used to better educate healthcare administrators on the risk that cyberattacks pose to healthcare delivery and to business continuity. This information could also be used to better develop a more accurate hazard vulnerability assessment (HVA) for HCOs. A well-informed HVA is the basis for effective preparedness and response planning within emergency management.

In 2018, this trend against the healthcare industry continues to grow. As of September 2018, there have been reported malware attacks every month of the year affecting health systems, hospitals, third-party medical suppliers, hospice care, provider clinics, and medical device manufacturers. Healthcare Organizations have a few recommended actions they can take to protect their networks, including developing a security culture within the organization. It is recommended that HCOs teach safe-use habits to all staff and test on these rules. There are also IT solutions to protect against cyberattacks, such as the use of strong firewalls, antivirus software, intrusion detection and even limiting network access (21). Another avenue HCOs can explore in preparing for cyber threats is procuring cyber insurance. The costs of attacks are estimated to be in the trillions worldwide by 2020 (25). Cyber insurance is a way to protect the HCO enterprise. Insurance companies will do a full assessment of an organization's IT capabilities and offer differing levels of coverage for a price. Often, insurance does not cover loss of revenue from downtime during attacks (25). As this type of threat continues to evolve, so too will cyber insurance policies.

Cyber threats to our society are only expected to grow over time. A 2017 article from the American Public Health Association cited a cyber-firm report that estimates that over the next five years, cyberattacks would cost the United States Healthcare system $305 billion in revenue and these attacks would affect 1 in 13 patients (26). Due to the relatively low number of cases identified in this content analysis, a follow-up systematic review on this topic would be appropriate to compare reporting trends of these events. There is also a need for future research in this area to better define what happens within an HCO during an attack. Further review of attack cases could highlight lessons learned and potentially identify best practices. This research will help HCOs better understand this hazard in order to prepare for and plan for mitigation of this threat. The healthcare industry has a choice to make when it comes to emergency preparedness: are they going to prepare their organization to prevent threats and protect patient health, or are they going to rely on the recovery of cyber insurance?

References

1. Luna R, Rhine E, Myhra M, Sullivan R, Kruse, C.S. (2016). Cyber threats to health information systems: a systematic review. Technology and Health Care. 2016;24: 1-9. DOI: https://doi.org/10.3233/THC-151102
2. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017;25(1):1–10. DOI: https://doi.org/10.3233/THC-161263
3. Waddell K. The computer virus that haunted early AIDS researchers [Internet]. The Atlantic.

Atlantic Media Company; 2016 [cited 2018Nov2]. Available from: https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/

4. Narayana Samy G, Ahmad R, Ismail Z. Security threats categories in healthcare information systems. Health Informatics Journal. 2010;16(3):201–9. DOI: https://doi.org/10.1177/1460458210377468
5. HIMSS North America. 2018 HIMSS cybersecurity survey [Internet]. 2018 [cited 2018Nov4]. Available from: https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf
6. Ayala L. Cybersecurity for hospitals and healthcare facilities a guide to detection and prevention. Berkeley, CA: Apress; 2016. DOI: https://doi.org/10.1007/978-1-4842-2155-6
7. 93% of phishing emails contain ransomware [Internet]. Becker's Hospital Review. 2016 [cited 2018Nov2]. Available from: https://www.beckershospitalreview.com/healthcare-information-technology/93-of-phishing-emails-contain-ransomware.html
8. Siwicki B. Hackers hit 320% more healthcare providers in 2016 than in 2015, per HHS data [Internet]. Healthcare IT News. 2017 [cited 2018Nov2]. Available from: https://www.healthcareitnews.com/news/hackers-hit-320-more-healthcare-providers-2016-2015-hhs-data
9. Nakashima E. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes [Internet]. The Washington Post. WP Company; 2018 [cited 2018Nov2]. Available from: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.d3c66123570b
10. Chappell B, Neuman S. U.S. says North Korea 'directly responsible' for WannaCry ransomware attack [Internet]. NPR. NPR; 2017 [cited 2018Nov2]. Available from: https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack
11. Perlroth N, Sanger DE. Hackers hit dozens of countries exploiting stolen N.S.A. tool [Internet]. The New York Times. The New York Times; 2017 [cited 2018Nov2]. Available from: https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?_r=0
12. Larson S. Massive ransomware attack hits 99 countries [Internet]. CNNMoney. Cable News Network; [cited 2018Nov2]. Available from: http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html
13. Lee S. Researchers says April was the worst-ever month for ransomware attacks [Internet]. Newsweek. 2016 [cited 2018Nov2]. Available from: http://www.newsweek.com/ransomware-attacks-reached-record-high-april-and-not-slowing-down-report-455239
14. Radke BA, Waters MJ, Cleary JC. Ransomware rises among hospitals [Internet]. Lexology. 2016 [cited 2018Nov2]. Available from: http://www.lexology.com/library/detail.aspx?g=8f3d29a5-2f87-42b8-ada1-54a109e38b3f
15. Spitzer J. Atlanta's ransomware attack cost $2.7M [Internet]. Becker's Hospital Review. 2018 [cited 2018Nov2]. Available from: https://www.beckershospitalreview.com/cybersecurity/atlanta-s-ransomware-attack-cost-2-7m.html
16. Barrett B. Hack Brief: Hackers are holding an LA hospital's computers hostage [Internet]. Wired. Conde Nast; 2017 [cited 2018Nov2]. Available from: https://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/
17. Winton R. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating [Internet]. Los Angeles Times. Los Angeles Times; 2016 [cited 2018Nov2]. Available from: http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
18. Reed T. [Internet]. bizjournals.com. 2016 [cited 2018Nov2]. Available from: http://www.bizjournals.com/washington/news/2016/04/06/medstar-hackers-exploited-design-flaw-from-2007-to.html
19. Davis HL. ECMC spent nearly $10 million recovering from massive cyberattack [Internet]. The Buffalo News. The Buffalo News; 2017 [cited 2018Nov2]. Available from: https://buffalonews.com/2017/07/26/cost-ecmc-ransomware-incident-near-10-million/
20. Siwicki B. Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money [Internet]. Healthcare IT News. 2016 [cited 2018Nov2]. Available from: http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom
21. TrapX Labs. Anatomy of an attack: MEDJACK [Medical Device Hijack] [Internet]. TrapX Security. 2015 [cited 2018Nov4]. Available from: http://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf

22. Naylor B. Russia hacked U.S. power grid - So what will the Trump Administration do about it? [Internet]. NPR. NPR; 2018 [cited 2018Nov2]. Available from: https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it
23. During Katrina, 'Memorial' doctors chose who lived, who died [Internet]. NPR. NPR; 2013 [cited 2018Nov6]. Available from: https://www.npr.org/2013/09/10/220687231/during-katrina-memorial-doctors-chose-who-lived-who-died
24. Evans M. Why some of the worst cyberattacks in health care go unreported [Internet]. The Wall Street Journal. Dow Jones & Company; 2017 [cited 2018Nov2]. Available from: https://www.wsj.com/articles/why-some-of-the-worst-cyberattacks-in-health-care-go-unreported-1497814241
25. Siwicki B. What to know about risk, coverage before you buy cyber insurance [Internet]. Healthcare IT News. 2018 [cited 2018Nov2]. Available from: https://www.healthcareitnews.com/news/what-know-about-risk-coverage-you-buy-cyber-insurance
26. Krisberg K. Cybersecurity: Public health increasingly facing threats. The Nation's Health. 2017;107(8): 1195.

How to cite this article: Branch LE, Eller WS, Bias TK, McCawley MA, Myers DJ, Gerber BJ, Bassler JR. Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. *Global Biosecurity*, 2019; 1(1).

Published: February 2019

Global Biosecurity is a peer-reviewed open access journal published by University of New South Wales.