HIGH SCHOOL EDITION
Journal of Student Research
Volume 12 Issue 4 (2023)

Ransomware Attacks in the Healthcare Industry

Aditi Kesarwani

North Creek High School

ABSTRACT

This paper explores the growing problem of ransomware attacks in the healthcare industry. It dives deep into the meaning of ransomware attacks and the basics of the attack such as how hackers gain access to data through the ransomware. Furthermore, this paper specifically focuses on hospitals and patients that are directly affected by the impact of ransomware attacks. This writing also includes information about noteworthy attacks in the health sector that have caught the attention of people around the world and how they were addressed. An aspect of Bitcoin has been added as cyber criminals demand ransom money in this currency from their victims. Lastly, this paper mentions steps that can be taken by hospitals to reduce the risk of getting infected by ransomware or what to do during a ransomware attack, such as having preventative safety measures in place with the use of antivirus software and Artificial Intelligence security systems as well has having a response plan during an attack. Apart from the Information Technology team in hospitals practicing these preventative measures, businesses and individuals should put in the time to implement these precautionary steps to ensure that they aren't victims of ransomware attacks and that no one can gain access to any of their classified information. This paper was written by the researcher in a limited amount of time and the researcher was not able to conduct any of their own trials. Hence, all the information and data included has been previously collected from researchers around the world.

Introduction

As of 2021, there has been a 94% increase in the amount of ransomware attacks against hospitals (Alder, 2022). Hospitals are a vital part of the world's social system. They deal with patients, day and night, and numerous conditions every day, but under a cyber-attack, they can't use their resources to their full potential in treating patients. In 2017, the National Health Service (NHS) of the United Kingdom had identified a ransomware attack in more than 60 systems which then spread to over 200,000 systems in over 150 countries. Apart from the UK, Canada was also attacked with ransomware (Collier, 2017). Annual ransomware attacks in the US alone more than doubled from January 2016 to December 2021 from only 43 cases to 91 cases. During this period, 374 cases revealed personal healthcare information about over 42 million patients in the country. Apart from that, the ransomware attacks prevented the treatment of patients as well because they resulted in ambulance diversions, equipment inaccessibility, cancellations of appointments, etc. (Neprash et al., 2022).

When the Covid-19 pandemic hit in early 2020, many healthcare organizations laid off cyber security staff due to the declining economy (Weiner, 2021). This meant that the cyber security of hospitals was unprotected. Just in 2020, over 600 health care organizations were attacked, 10 million patient records were exposed, and the money spent to fight those attacks neared 21 billion dollars (Weiner, 2021). This made attackers realize that they had a good chance of receiving the money they demanded because hospitals had to deal with life-or-death situations, and it was in their best interest to pay the ransom. Another reason that ransomware attacks have increased on hospitals is because hospitals that are in a remote area needed to serve multiple districts and counties, so when they are attacked, they have no other choice than to pay the money and regain access to patient records and technology. "Teaching hospitals", such as biomedical research hospitals are a big target for ransomware attacks as well because of the amount of data they collect from studies (Weiner, 2021). By blocking access to the files and networks, doctors can't access important information needed to continue their research, hence they resort to paying the ransom. In short, healthcare organizations are a big target for cyber security attacks because they hold a lot of patient data, potentially affect many interconnected systems, and damage the reputations of affected organizations due to successful attacks (Aunger, 2022). Though the ransomware attack is considered an economic crime, it is more than an economic crime against a hospital because it directly puts patients' lives at risk (Riggi, 2020). Which is why it is vital to find

efficient solutions to this issue so that hospitals can provide the best care for their patients and not worry about a ransomware attack impacting their hospital. In this paper, there are different ransomware attacks that have been addressed such as the University of Vermont Ransomware Attack, the WannaCry attack, the CommonSpirit Ransomware Attack and others.

Ransomware Attack

A ransomware attack is a type of attack that blocks a user from accessing files, computer systems or networks. In order to regain access to these items, attackers demand a ransom. Opening an unsafe email, visiting an unsecure website, or downloading a malicious file can all lead to loading the ransomware onto a user's device and activating it. Users may not know they have been infected with ransomware until after the impacts come to light (Ransomware, 2022). Firstly, ransomware is a type of malicious software or malware for short. Malware is software developed by hackers to gain illegal access to information data, get access to computer networks or harm devices. Viruses, worms, spyware and Trojan horses are repeated examples of malware used to target people (What is malware? - Definition and examples, 2023).

Apart from loading ransomware onto a computing device by opening unsecure emails, downloading unsafe files or visiting unsecure websites, ransomware can be loaded onto networks through vulnerabilities in software. When a computer system's software has gaps in its security, these gaps are referred to as vulnerabilities. Hackers can then use these vulnerabilities to gain access to a system and upload any kind of malware or gain control of the system. The Common Vulnerability & Exposure Program, also known as the CVE Program, is a public system that records known vulnerabilities in packages (*Cve-website*, n.d.-a, *Cve-website*, n.d.-b). All the vulnerabilities ever reported are assigned a CVE id, have been configured into a list and are publicly available on a website known as the MITRE Corporation. Examples of CVEs that have been exploited by attackers in recent years to load ransomware are the CVE-2023-30024 in 2023, CVE-2022-23714 in 2022 and the CVE-2021-42258 in 2021. All these CVEs have given hackers a way to elevate their status from not being authorized to access certain content, to being able to access them and meddle with the integrity of the data as well as allowing cyber criminals to lock their victim's access to the data (CVE - CVE-2021-42258, n.d., CVE - CVE-2022-23714, n.d., CVE - CVE-2023-30024, n.d.).

How Hackers Prevent Access to Files

Hackers gain entry to the victim(s) systems through ransomware, and then use the encryption and decryption process to take control of their target's data. They first gain access to the victim's computer and files through the ransomware that has been loaded onto the computer. Next, they encrypt the data, by using asymmetric or public key encryption (What is ransomware, n.d.). This method includes a public and private key to encrypt and decrypt data. This type of encryption is normally used during message or data transfer from one device to another. The receiver's public key, which is known to everyone, is used to transform the information from plaintext to an encrypted message. Only the receiver can decrypt the information being sent to them from the encrypted message to the original plain text by using their private key. This is a secure form of cryptography because everyone knows the public key to send the messages, but only the receiver knows their private key to decrypt the messages, making it a lot harder for hackers to intercept communication and find the original plaintext (Brush, 2021). But in terms of a ransomware attack, the hacker uses public key encryption to create a unique public and private key for the victim. The attackers encrypt the data using the public key, locking access for the user and then demand a ransom. Once the ransom is paid, they may reveal the private key to decrypt the information and return access to the victims. There is a high chance that the cybercriminal won't return access to the encrypted data to the hospital after the ransom is paid. They may ask for more money, or simply refuse to give the decryption key. Federal organizations, such as the FBI (Federal Bureau of Investigation) encourage hospitals to report the attack to them as soon as possible to resolve the issue, but especially when the attacker doesn't cooperate (Ransomware, 2022).

Payment of Ransom

Should Ransom be Paid?

The FBI discourages paying the ransom that is demanded by the attackers and instead encourages filing a report with the FBI (Ransomware, 2022). In June of 2023, the US Department of Justice reported that the FBI stopped the Hive ransomware group which had targeted more than 1500 victims such as hospitals, financial companies and schools in over 80 countries. The organization used a RaaS (ransomware-as-a-service) model to carry out their attacks. This model is subscription based where developers create different ransomwares and then recruit people to use the malware against victims. The recruited people then earn a percentage of the ransom that is successfully paid. The FBI, over a series of months since gaining access to the Hive's network in July 2020, has provided victims with decryption keys to regain access to any information that the group had stolen. In June of 2023, the FBI gained control of all the Hive's systems, websites and sources of communication preventing them from carrying out future attacks. Additionally, they prevented the group from earning over 130 million dollars in ransom money from their targets (U.S. Department of Justice disrupts Hive ransomware variant, 2023).

Use of Bitcoin for Ransom

A popular way that attackers demand ransom from hospitals is in Bitcoin. Bitcoin is a cryptocurrency or digital currency that allows its users to maintain anonymity while completing transactions. Additionally, Bitcoin transactions are lower in cost sometimes and quick. Bitcoin accounts aren't tied to normal banks or the government, hence they aren't protected by other payment laws. Criminals prefer to use this type of payment because it tends to protect the identity of the user, hence it has been used increasingly to retrieve ransoms in ransomware attacks (Segendorf, 2014). In 2016, Hollywood Presbyterian Medical Center in Los Angeles, California, was under a ransomware attack. Employees of the hospitals didn't have access to various patient information such as X-rays, or patient records, and weren't able to restore information either (Paul et al., 2018). This caused them to give into the demands of the hacker and pay a ransom of 40 bitcoins which was about 17000 dollars at the time (Millard, 2017). Figure 1 explains all the steps previously discussed about how a ransomware attack progresses from the start of loading the virus onto the victim(s) computer, to the possible decryption of the victim(s) information at the end.

"In May 2022, the FBI filed a sealed seizure warrant for the fund's worth approximately half a million dollars. The seized funds include ransoms paid by health care providers in Kansas and Colorado" (Justice Department Seizes and Forfeits Approximately $500,000 From North Korean Ransomware Actors and Their Conspirators, 2022). The FBI was able to investigate the ransomware attacks conducted by a government sanctioned North Korean group. They were able to retrieve the ransom money paid by past victims and were able to identify the ransomware strain as "Maui." In May of 2021, the group had attacked a hospital in the District of Kansas, encrypting their servers so that they couldn't access those systems. This caused the hospital to pay the ransom of 100,000 dollars. Since this attack was reported to the FBI, they were able to trace the cryptocurrency accounts. In April of 2022, the FBI was alerted to a 120,000 dollars Bitcoin transaction to one of the flagged cryptocurrency accounts from a hospital in Colorado that was hacked. This allowed the FBI to seize the two accounts that received the ransom from the two hospitals and the process of returning the money to the hospitals began (Justice Department Seizes and Forfeits Approximately $500,000 From North Korean Ransomware Actors and Their Conspirators, 2022).

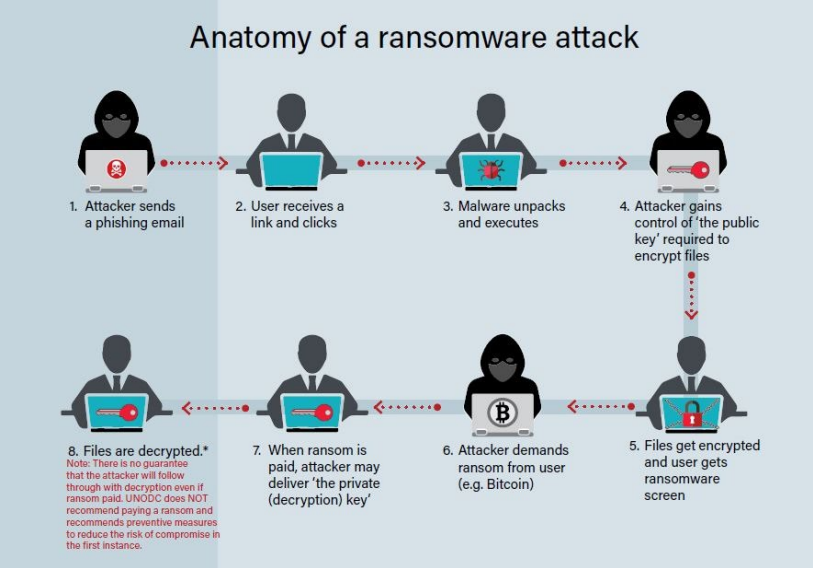

Figure 1: Anatomy of a ransomware attack (Ojha, n.d.)

Figure 1 summarizes the sequence of events that many hackers follow while conducting a ransomware attack. They first try to gain access to their victim's computer by sending them some kind of file that consists of malware, and once the malware is loaded onto the computer, they encrypt files and demand a ransom in order to decrypt the files.

Ransomware Attack on Hospitals

University of Vermont Medical Center Attack

On October 28, 2020, the University of Vermont (UVM) medical system was hit by a ransomware attack. Staff had reported unusual computer behavior to the IT (Information Technology) department. Upon investigating the issues, the IT team found an encrypted file with instructions to contact the hacker and learned that the hospital was affected by a ransomware attack. As a reaction to the attack the IT department shut down health record systems and employee emails to protect everyone's data and reported the attack to the FBI (The University of Vermont Health Network, 2020). Stacy Weiner from AAMC states that the hospital went almost a month without access to Electronic Health Records (EHRs), payrolls and other important information. They also didn't know when patient appointments were scheduled for and had to move cancer patients to different hospitals to continue their treatment since UVM didn't have access to the technology (Weiner, 2021). The UVM website states that perpetrators of the crime didn't gain access to any employee data, Personally Identifiable Information (PII), or Public Health Information (PHI) of patients. Due to good planning on the side of UVM, the IT department had most of the necessary information to restore their servers through back up records. Over the span of the next two months after the attack, the IT department examined around 5,000 infected computers to rid them of the malware. Additionally, they reconstructed their systems and placed back up data in their devices to resume usage of them. This process took more time than usual because usually, the ransomware doesn't impact the encrypted data infrastructure, but it did in the case of the UVM attack (The University of Vermont Health Network, 2020). It is unclear whether the attackers ever demanded a ransom, or if the hospital paid a ransom to the hackers, but the hospital endured a loss of 50 million dollars due to their inability to care for existing and new patients (Weiner, 2021).

Brno University Hospital Attack

In the midst of the Coronavirus pandemic, one of the earliest ransomware attacks was on the Brno University Hospital in the Czech Republic (Ransomware Attacks on Hospitals Have Changed, n.d.). It is the second largest hospital in the country and at the time was a major Covid-19 test center. When the attack was detected, authorities closed the entire network, prohibiting employees from accessing their computer. Patients were being directed to nearby hospitals for care and the maternity and children ward was closed (Kiguolis, 2020).

CommonSpirit Health Ransomware Attack

One of the largest ransomware attacks in 2022 against a healthcare organization was the attack on CommonSpirit Health on October 2, 2022 (Diaz, n.d.). When the hospital detected the ransomware, they immediately started an investigation. First, they took steps to secure their network by taking some systems offline. Then they determined what information was accessed from the third-party attackers and figured that the third-party had not stolen any data from the CommonSpirit Electronic Records, but the attackers had obtained copies of files on their systems. The hospital looked into individual information that was stolen such as name, date of birth, medical records and healthcare insurance information of patients and mapped it to individuals in February of 2023. They informed law enforcement of the attack and continued treating patients. Additionally, in April of 2023, the hospital started mailing individuals whose data was impacted by the attack notifying them about the incident (Notice of Data Security Incident, n.d.).

Preventing Ransomware Attacks in the Healthcare Industry

When hospitals are under a cyber-attack, they lose their ability to provide the best care they can to their patients. In order to minimize the number of times that hospitals are put in a situation like this, they should implement ways to reduce the risk of being attacked or know how to respond if they ever are under a cyber-attack.

Hospitals can prevent ransomware attacks by ensuring that their system firewalls are strong and can't be penetrated by attackers. They can also frequently update their antivirus software to fight any malware. Additional steps that hospitals can take, reported by the CISA in October 2020, is the 3-2-1 approach; saving 3 copies of important documents such as patient records in more than 2 formats and storing 1 copy offline so that malware can't affect it and patient treatments can continue (Targeting the Healthcare and Public Health Sector, 2020). They can also have a plan in place to refer to if they do ever come under attack. Firstly, hospitals should inform the police and higher authorities about the ransomware attack as soon as possible. The authorities will investigate the attack and put all their effort into containing the issue so that patient care can be resumed at its complete level. Next, hospitals should identify the devices and systems that have been affected by the malware, figure out the reason the attack took place and start working on fixing the problem. Another crucial decision that supervisors need to make during this time is whether to pay the ransom demanded by the hackers or not. As mentioned earlier, the FBI discourages payment of the ransom, but hospitals need to consider how well they can treat their patients. Hospitals should then implement a plan to relay information across hospital staff and different agencies aiding with the investigation. During the ongoing investigation, informing the public about the attack isn't the best idea because that may cause confusion or harm in ways that interfere with the investigation. Lastly, after the malware isn't an active threat to the hospital, the hospital should begin its recovery process. They should fix any vulnerabilities in their systems or any ways that malware can attack their systems again; they should also recover their data and monitor their systems to prevent future attacks (McKeon 2022).

Artificial Intelligence for Security Systems

Another great way to ensure data security is by configuring Artificial Intelligence in software security systems. International Business Machines, IBM for short, a technology company, created a product called QRadar SIEM. QRadar SIEM allows users a better view of their network along with "event log resources" which gives them access to device support modules

and environment activity monitoring analysts. This application also alerts its users about threats to the system, ordering alerts based on importance of attendance. This is a great tool for detecting ransomware attacks because it evaluates a threat, and then reacts to it using resources quickly to prevent the attack from causing too much damage. IBM also provides data regarding this product, it states, analysts were able to save over 14000 hours identifying false positives, were able to reduce the time spent checking on threats by 90 percent and there was a 60 percent decrease in users having a risk of experiencing a security breach (Security QRADaR SIEM, n.d.).

Another product on the market from IBM is the MaaS360. This product protects the user's data, content and devices allowing them to scale their workforce. Features of this product include allowing users to scale their workforce, detect any threats to their computer systems, access to AI advice on security insights, protection of data and access to data. Overall, this product allows its users to have an organized method for their devices but also have their data protected and have an application that detects any threats so that action can be taken (IBM Security MAAS360, n.d.).

WannaCry Ransomware Attack

In May of 2017, UK hospitals were hit with the WannaCry ransomware. Hospitals in the UK were severely impacted by this threat as staff weren't able to access patient records, leading to cancellation of appointments and unimportant surgeries being postponed. 16 hospitals were still affected by the cyber-attack on May 15th, but around 80% of the UK National Health Service trusts weren't hit by a second attack and had mostly recovered from the first one (Collier, 2017). Over time, as the attack spread around the world, and affected more hospital systems. The group behind the attacks demanded 300 US dollars' worth in Bitcoin from the victim(s) and doubled their demand after three days. Hospitals also received threats of not being able to gain access to data stolen ever again if the ransom wasn't paid within a week. The same group had targeted Lakeridge Health in Ontario, Canada. The security system of the hospital systems prevented the attack from causing damage and was able to prevent hackers from gaining access to any data (Collier, 2017).

Conclusion

Cyber-attacks are a massive problem around the globe right now. Ransomware, a type of cyber-attack, is also a huge problem around the world, a substantial amount of money is spent in fighting these kinds of attacks in order to keep user data safe. As technology advances, these attacks will only worsen, criminals from one side of the world will be able to gain information about a company on the other end of the world. They will then exploit this information by selling it and earning money. But when a hospital is impacted by a ransomware attack, its ability to help patients decreases tremendously. Instead of putting their whole effort into the care of patients, staff have to worry about patient data and their data being stolen too. In these scenarios, it is vital that hospitals alert the authorities to investigate the attack, but that hospitals also have a plan in place. Hospital staff need to work harder, because if a cyber-attack stops them from using equipment, that cannot affect how well they treat the patients. But, as technology advances, not only will these attacks worsen, but they can also be prevented more efficiently. Hospital staff's attention to online scams can be a first step to preventing ransomware attacks. Anti-virus programs and AI security systems can all be put together to build a robust cybersecurity system for the hospital. With these measures in place, not only will the hospital have a lower risk of enduring an attack, but if they were to get attacked by one, they can react immediately to contain the attack and provide the best treatment for their patients.

Acknowledgements

The researcher would like to acknowledge Dr. Sarada Prasad Gochhayat for teaching them different topics of cybersecurity. Dr. Gochhayat helped the writer understand different aspects of each topic and how it affects users in the real world. The researcher would also like to thank Jothsna Kethar for helping them understand how a research paper is written. Lastly, the writer would like to thank Professor. Virgel Torremocha for reviewing their paper and giving them feedback on it.

References

Alder, S. (2022). Healthcare ransomware attacks increased by 94% in 2021. *HIPAA Journal*. https://www.hipaajournal.com/healthcare-ransomware-attacks-increased-by-94-in-2021

Aunger, C. (2022, August 16). Ransomware 101 For Healthcare. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/08/16/ransomware-101-for-healthcare/?sh=66e0874e5b86

Brush, K., Rosencrance, L., & Cobb, M. (2021). asymmetric cryptography (public key cryptography). *Security*. https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography

Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal*, *189*(22), E786–E787. https://doi.org/10.1503/cmaj.1095434

CVE - CVE-2021-42258. (n.d.). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42258

CVE - CVE-2022-23714. (n.d.). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23714

CVE - CVE-2023-30024. (n.d.). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30024

cve-website. (n.d.-a). https://www.cve.org/About/Overview

cve-website. (n.d.-b). https://www.cve.org/ResourcesSupport/FAQs

Diaz, N. (n.d.). *289 healthcare organizations were impacted by ransomware attacks in 2022*. https://www.beckershospitalreview.com/cybersecurity/289-healthcare-organizations-were-impacted-by-ransomware-attacks-in-2022.html#:~:text=The%20largest%20ransomware%20attack%20on,protected%20health%20or%20personal%20information.

https://doi.org/10.1016/j.annemergmed.2017.07.008

IBM Security MAAS360. (n.d.). https://www.ibm.oreacom/products/maas360

Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators. (2022). https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors

Kiguolis, U. (2020). Hospital Brno in Czechia hit by a cyberattack during COVID-19 virus crisis. *www.2-spyware.com*. https://www.2-spyware.com/hospital-brno-in-czechia-hit-by-a-cyberattack-during-the-covid-19-virus-crisis#:~:text=A%20cyber%20attack%20on%20University%20Hospital%20Brno%20in,cyberattack%20in%20the%20middle%20of%20the%20coronavirus%20outbreak.

McKeon, J. (2022,). Responding To a Healthcare Ransomware Attack: A Step-By-Step Guide. *HealthITSecurity*. https://healthitsecurity.com/features/responding-to-a-healthcare-ransomware-attack-a-step-by-step-guide

Millard, W. B. (2017). Where Bits and Bytes Meet Flesh and Blood - Hospital Responses to Malware Attacks. Retrieved From: https://www.annemergmed.com/article/S0196-0644(17)30891-0/fulltext

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, *3*(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Notice of Data Security Incident. (n.d.). Commonspirit. https://www.commonspirit.org/notice-of-data-security-incident

Ojha, H. (n.d.). *Anatomy of a ransomware attack*. Unodc.org. https://www.unodc.org/roseap/en/2021/10/cybercrime-ransomware-attacks/story.html

Paul, D., Spence, N., Bhardwa, N., & Coustasse, A. (2018). Health Facilities: Another Target for Ransomware Attacks. Management Faculty Research. Retrieved from: https://mds.marshall.edu/cgi/viewcontent.cgi?article=1194&context=mgmt_faculty

Ransomware. (2022,). Federal Bureau of Investigation. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

Riggi, J. (2020). *Ransomware attacks on hospitals have changed | Cybersecurity | Center | AHA*. American Hospital Association. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

Security QRADAr SIEM | IBM. (n.d.). https://www.ibm.com/products/qradar-siem

Segendorf, B. (2014). What is Bitcoin? Sveriges Riksbank Economic Review. Retrieved from: www.riksbank.se/en/Press-and-published/Reports/Economic-Review

Targeting the Healthcare and Public Health Sector. (2020, October 28). JOINT CYBERSECURITY ADVISORY Ransomware Activity Retrieved From: https://www.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf

The role of AI and ML in ransomware protection. (2023, June 27). Acronis. https://www.acronis.com/en-us/blog/posts/role-of-ai-and-ml-in-ransomware-protection/

The University of Vermont Health Network. (2020). Statement from UVM Health Network on Cyberattack. *The University of Vermont Health Network*. https://www.uvmhealth.org/news/uvmhn/statement-uvm-health-network-cyberattack

U.S. Department of Justice disrupts Hive ransomware variant. (2023, January 26). https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

Weiner, S. (2022). The growing threat of ransomware attacks on hospitals. *AAMC*. https://www.aamc.org/news/growing-threat-ransomware-attacks-hospitals

What is malware? - Definition and examples. (2023, July 21). Cisco. https://www.cisco.com/site/us/en/products/security/what-is-malware.html

What is ransomware? | Trellix. (n.d.). Trellix. https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html#:~:text=Ransomware%20uses%20asymmetric%20encryption.,stored%20on%20the%20attacker's%20server.