Spring 5-12-2023

Ransomware

Eleanor Mancini
La Salle University, mancinie2@lasalle.edu

Ransomware

Eleanor Mancini

Cybersecurity, La Salle University

CYB-880: Integrative Capstone

Dr. McCoey

April 30, 2023

Executive Summary

This paper explores ransomware and it's effect on organizations with the intent of uncovering the ideal way for an organization to handle an attack. It begins with a short introduction of ransomware and it's similarities and differences to traditional crimes, such as theft. Then the paper explains the two main categories of ransomware – crypto-ransomware and locker ransomware – and how most variants are derived from these categories. It includes a description of each category and the typical ways an organization would encounter it. The paper examines the emergence of ransomware-as-a-service (RaaS) and how it's divide-and-conquer nature allows cybercriminals to specialize in either malware development or network penetration. In addition, RaaS has enabled criminals with low-level programming skills to partake in and profit from ransomware. It discusses the most common RaaS business models and some of the most prolific and dangerous variants. The paper analyzes cryptocurrency's role in ransomware attacks and how it perpetuates the anonymity of the cybercriminals. It also investigates the evolution of ransomware from it's origin until 2020 and the different variants that have emerged. Then the paper shifts to focus on what can be done to combat ransomware. It looks at preventative measures, reactive measures, and mitigation. Finally, the paper concludes with the best way for an organization to handle a ransomware attack.

Introduction

A connection has developed between crime and technology, despite the transient history of the Internet (O'Kane, Sezer, and Carlin, 2018). While technology has and continues to evolve, many of the underlying concepts of traditional crime prevail (O'Kane, Sezer, and Carlin, 2018). Many traditional crimes, such as theft and blackmail, are old but the internet has provided a highly automated environment that aids in the criminal attacks (O'Kane, Sezer, and Carlin, 2018). The internet allows criminals to widen their focus from single large targets, such as a bank or corporations, to millions of online users (O'Kane, Sezer, and Carlin, 2018). Ransomware has the underlying concept of the traditional crime of kidnapping. It holds hostage someone or, in this case, something that the victim values greatly and demands a ransom if the victim wants the hostage back. Unlike the traditional crime of kidnapping, ransomware occurs in cyberspace and the hostage is typically company data.

Malware is defined by the Oxford dictionary as "software such as a virus specifically designed to damage or gain access to a computer system without the user knowing". Ransomware is malware that implements encryption to hold a victim's information, data, or system at ransom. In general, ransomware infiltrates and contaminates a computer system when a user opens a corrupted email or visits a corrupted website. After a successful infection, ransomware drops and runs a malicious binary algorithm on the contaminated system. This algorithm then locates and encrypts critical files. More specifically, ransomware employs asymmetric encryption which uses a set of keys to encrypt and decrypt a file. The pair of keys includes a public and private key that are engineered for the target victim by the attacker. The private key, which is the tool that enables decryption of the data, is kept on the attacker's server

and is the object that is offered in exchange for the ransom. Without access to the private key, it is implausible for the organization to decrypt the files that are being held for ransom (What Is Ransomware?, n.d.).

Crypto-Ransomware and Locker Ransomware

There are two main categories of ransomware that essentially all variants of ransomware can be traced back to: crypto-ransomware and locker ransomware. The first category – crypto-ransomware – is a type of malware that disrupts critical data with virtually impenetrable encryption and does not deliver the decryption key until the ransom is settled. Although victims are unable to access the disrupted files, they are still able to access the system and the browser. Crypto-ransomware is particularly dangerous because it is considered to be the form of ransomware that imposes the most damage due to the permanence of the disruption; many times it cannot be completely reversed (*Locker Ransomware Information Guide and FAQ*, 2016).

There are two customary ways an organization can be confronted with crypto-ransomware. First, crypto-ransomware can be encountered via emails or other forms of messaging that contain corrupted files or links. This is the most common way to encounter crypto-ransomware. The emails or other forms of messaging contain links that direct a victim to executable programs that contain the crypto-ransomware but are disguised as legitimate "documents". There are file formats that are commonly used to place crypto-ransomware in the messages and can therefore be an indicator of a potential attack. These formats include Microsoft word (.doc or .docx), or excel (.xsl or .xslx), or XML (.xml or .xslx) documents. It also includes a zipped folder containing a Javascript file (.js), and multiple file extensions. Javascript files will

attempt to download and install the crypto-ransomware itself from a remote website or server. Microsoft Word and Excel documents employ a macro. A macro is code that automates a function that is typically manual and contains embedded malicious code. Macros are disabled by default and therefore can only run if the user has already enabled macros in Word or Excel or are tricked into enabling it. If macros have already been enabled by the user when the file is opened, then the code will execute instantly. Otherwise, the user will be prompted to enable them via a pop-up notification. If the user enables the content, the embedded code will execute instantly. Second, crypto-ransomware can be encountered via downloads onto the device by threats such as trojan-downloaders or exploit kits. Exploit kits are toolkits that are positioned by attackers on websites. These kits probe the device of every website visitor for flaws and vulnerabilities that it can exploit. When one is found, the exploit kit can immediately place and execute the crypto-ransomware on the device ("What Is... Crypto-Ransomware: F-Secure", n.d.).

The second category – locker ransomware – blocks computer or mobile device access by locking the manual input devices. This type of ransomware is simple yet very effective. It is very similar to cutting an electrical cord. When electricity has nothing to run through, the end devices cannot be used unless the cord is repaired. Similarly, when locker ransomware has infected a system, no command can be communicated or executed through the keyboard or mouse because the devices are brought down to limited functionality. The victim can only use numerical keys only to type the ransom amount. When the payment process is completed, access to the data is restored. Locker ransomware is considered less advanced than crypto-ransomware because crypto-ransomware employs advanced level cryptography. This highlights a key difference between these two types of ransomware – a locker ransomware attack does not alter the files on a

system. It is important to note that there are countless ransomware variants. These two categories are simply the basis for most of the variants (Thakkar, 2017).

Ransomware-as-a-Service (RaaS)

Ransomware-as-a-service (RaaS) is a form of cybercrime that allows malware developers to profit from their creations without the need to implement the threat. Non-technical criminals buy and launch the developed malware (What Is Ransomware?, n.d.). The malware developers benefit from relatively risk-free work and the criminals end up doing the majority of the work (What Is Ransomware?, n.d.). RaaS has become an entry point for criminals with low-level programming skills to partake in and profit from ransomware (Mayangao, 2021). The customer typically contacts the ransomware developers via the darknet (Mayangao, 2021).

There are four common RaaS business models: monthly payment (subscription model), partner programs, one-time license fee, and profit sharing only (Feilner, 2023). RaaS companies make the process very easy. A customer simply has to log onto the darknet, choose a RaaS model, pay with Bitcoin, dispense the purchased malware, and wait for the ransom to be paid (Feilner, 2023). In addition to a design fee, the ransomware developers may take a 20-30% cut of the ransom as well (Mayangao, 2021).

RaaS benefits both the operator and the affiliate. The operator cultivates an operation that is of a larger scale and prioritizes maintaining the backend infrastructure. The affiliate, on the other hand, can focus their efforts on infiltrating networks and contaminating systems. It is a divide-and-conquer scheme. The ability to concentrate is a considerable benefit for the cybercriminals because very few are accomplished at both malware development and network penetration. RaaS is one of the primary reasons why ransomware attacks have been able to continually grow in recent years. Some of the most prolific and dangerous RaaS variants include:

Ryuk, Lockbit, REvil, and Maze (*Ransomware as-a-Service (RaaS)*, 2022).

REvil is one of the most prolific and widespread ransomware-as-a-service (RaaS) operations. REvil, also known as Sodinokibi, originally emerged in April 2019. In July 2021, REvil members capitalized on zero-day vulnerabilities in a systems management and monitoring tool developed by a company called Kaseya. The attack compromised over 30 managed service providers (MSPs) from all around the world and over 1,000 business networks managed by those MSPs. In addition, the attack gained extensive media attention and prompted U.S. President Joe Biden and Russian President Vladimir Putin to discuss ransomware. Yaroslav Vasinskyi, a Ukrainian national, was indicted for the Kaseya attack (*Ukrainian arrested and charged with ransomware attack on Kaseya,* n.d.). This example demonstrates some of the advantages of RaaS; namely, the extent of both the attack. Vasinskyi was able to focus his efforts purely on network penetration instead of having to divide his efforts between malware development and network penetration (Constantin, 2021).

Cryptocurrency's Role in Attacks

Transporting and concealing massive amounts of ill-gotten gains while avoiding detection has long plagued traditional criminals such as thieves and drug smugglers. Cybercriminals who launch ransomware attacks are no exception. The difference is that cybercriminals have found an almost perfect solution – cryptocurrencies such as Bitcoin. Use of anonymous cryptocurrency for monetary exchanges, makes it complicated and time-consuming to pursue the money trail and track down the responsible party (What Is Ransomware?, n.d.). Ironically, cryptocurrency exchanges in Bitcoin take place on what are called "public ledgers". This means anybody can observe the transaction but the parties involved are anonymous and disguised by a public address composed of a random string of numbers and letters. This "public

ledger" is an immutable, distributed ledger known as a blockchain (*Digital Currencies'…Third way,* n.d.). The trail of transactions on a blockchain remains available indefinitely so, in this sense, digital currencies like Bitcoin are pseudonymous, but not private (*Digital Currencies'…Third way,* n.d.).As a result, hackers can keep transporting the currency from one pseudo-anonymous account to another which can make it very difficult – though not impossible – to trace (Myre, 2021).

In addition, unlike bank accounts, no personally identifiable information is required to obtain a crypto wallet. The identity of the crypto wallet address holder remains concealed unless inferred through alternate means (*The Wild World of crypto ransomware payments,* n.d.). Bitcoin is the ideal cryptocurrency for many cybercriminals because it is the most widely used digital currency to date (*The Wild World of crypto ransomware payments,* n.d.). Cybercriminals prefer to remain anonymous, and acquiring a bitcoin wallet address requires no personally identifiable information (*The Wild World of crypto ransomware payments,* n.d.). This enables the cybercriminal to use bitcoin wallets to transfer payments in a timely fashion while keeping their identities hidden (*The Wild World of crypto ransomware payments,* n.d.). When utilizing digital currencies like Bitcoin, cybercriminals may use mixing services, also known as tumbling services, to sever the connection between the Bitcoin sender's address or wallet and the receiver's address or wallet (*Digital Currencies'…Third way,* n.d.). Once a user sends Bitcoin to a mixer, the mixer merges it with Bitcoins from alternate sources, or even newly mined ones, and returns Bitcoin with different addresses and transaction histories to a different wallet (*Digital Currencies'…Third way,* n.d.).

It is common for the cybercriminals in ransomware attacks to demand payment in cryptocurrency. For example, in the abovementioned Kaseya attack, $70 million in Bitcoin was demanded. However, Kaseya declined paying and instead chose to involve the FBI and the US Cybersecurity and Infrastructure Agency. In July of 2021, Kaseya obtained a universal decryptor key and distributed it to the organizations impacted by the attack. In April of 2021, German chemical distributor Brenntag discovered that 150GB of data was stolen in a cyberattack by Darkside. Similar to the Kaseya attack, the criminals demanded payment in Bitcoin. In contrast to the Kaseya attack, Brenntag chose to pay the ransom – although Brenntag was able to negotiate the payment from $7.5 million down to $4.4 million (Dossett, n.d.).

The History and Development of Ransomware (Origin – 2020)

Due to the criminal nature of ransomware, the general timeline of it's development was based on what is known about it with the possibility that some information is missing. The first ransomware virus emerged in 1989 and was known as AIDS trojan as well as PC Cyborg. It was developed by Joseph L. Popp, a Harvard-trained evolutionary biologist, to employ symmetric cryptography to encrypt file names. Tools were shortly thereafter available to decrypt them. The attack that employed AIDS Trojan was distributed by floppy disk – which is a storage medium that is now obsolete - at the World Health Organization's International Aids conference. In May of 2005, the first modern form of crypto-ransomware was released; it was known as Trojan.Gpcoder, as well as GP Code and GPCoder. Originally, it employed a custom symmetric encryption technique that was weak and therefore easily conquered. However, the malware developers continued to improve it after the original release. Trojan.Gpcoder infected systems via a spam email attachment disguised as a job application (Richardson & North, 2017).

In early 2006, ransomware continued to grow with the emergence of Trojan.Cryzip and Trojan.Archiveus. Trojan.Cryzip copied data files to password-protected archive files and deleted the originals . Trojan.Archiveus operated similarly with one notable difference – instead of asking for a ransom, it demanded victims to purchase medication from specific online pharmacies and submit the order ID in order to get the password that enabled decryption. The year 2007 brought the inception of locker ransomware. The earliest version originated in Russia and displayed a pornographic image on the infected system and then demanded a ransom via SMS text messaging or premium rate phone calls in exchange for it's removal. In 2008, a variant of Trojan.Gpcoder known as CPcode emerged. It used a 1024-bit RSA key. RSA is public-key cryptosystem that is used for secure data transmission. GPcode[MM2] planted a text-file that contained instructions in each subdirectory of the encrypted files. The ransom demand was $100 to $200 in e-gold or Liberty Reserve, both of which are cryptocurrencies. In 2011, emerging anonymous payment services contributed to the first large-scale outbreak of ransomware. In the first quarter of 2011, there were approximately 30,000 new ransomware variants. By the third quarter, there were 60,000 new variants. In 2012, ransomware toolkits were released, including Citadel and Lyposit. Lyposit was designed to produce and deliver ransomware under the ruse of being from law enforcement. It was advanced enough that the law enforcement agency being used saying it was the agency specific to the system's regional settings (Richardson & North, 2017).

The year 2013 was pivotal, as it was the dawn of CryptoLocker. CryptoLocker was developed by a hacker named Slavik and involved public and private keys to encrypt and later decrypt a victim's files. The original version of CryptoLocker was capable of encrypting 67

different file types and was released in August. Initially, CryptoLocker was distributed via a botnet. Later, it was distributed via an email that appeared to be from UPS or FedEx. In December, CryptoLocker 2.0 was released. CryptoLocker 2.0 is widely believed to have been developed by a different group of attackers, as it was written in a different language. In general, CryptoLocker gave victims three days to pay the ransom of two bitcoins; at that time, two bitcoins was approximately $100. While bitcoin was the most common form of payment, others included CashU, Ukash, Paysafecard, and MoneyPak. In some cases, if the three day deadline was not met, the victims could retrieve their files for a much steeper price. In 2013, it is estimated that three percent of cases resulted in the victim paying the ransom. From September 2013 to May 2014, about 500,000 different victims experienced a CryptoLocker attack. However, the percentage of victims who paid the ransom decreased to 1.3 percent. In June of 2013, the CryptoLocker distribution servers were taken down and the database of decryption keys was found and released as a service to all victims. In February of 2014, CryptoDefense was released and CryptoWall, an improved version, was released shortly after (Richardson & North, 2017).

In May of 2015, ransomware-as-service (RaaS) surfaced. This was due largely to a TOR website that enabled ransomware to be developed for free. The website handled payment and received a 20 percent cut of the ransom. In January of 2016, a JavaScript-only RaaS emerged. This is noteworthy because the use of JavaScript allows a multi-platform attack. In April of 2016. A ransomware known as Petya surfaced. Petya compromises the entire hard disk by overwriting the master boot record (MBR). In 2017, an improved variant of Petya, known as NotPetya emerged. According to the White House, NotPetya resulted in $10 billion in damage in the US. It is widely believed that NotPetya was developed in Russia and, as a result, the US

blames Russia for this variant of ransomware. Additionally, LeakerLocker and WannaCry both surfaced in 2017. LeakerLocker was a ransomware variant developed for Androids. In contrast to most types of ransomware, LeakerLocker did not encrypt any files; instead, LeakerLocker displayed data from the infected device and threatened to send the entirety of the phone's contents to every contact listed in the device unless the ransom was paid. WannaCry is one of the most notorious crypto ransomware variants. After materializing in May, it contaminated approximately 230,000 systems in 150 countries and resulted in about $4 billion in damages. An interesting note about WannaCry is that Microsoft had developed and distributed a patch for this variant before it emerged; however, many users had not updated their systems so the ransomware still had a significant impact. The WannaCry scenario highlights the importance of timely updates (Drake, 2022) (Richardson & North, 2017).

In January of 2018, GandCrab was released and rapidly became the most active variant of ransomware-as-a-service between 2018 and 2019. GandCrab's developers continued to improve the RaaS and periodically released more sophisticated versions until it merged with the strain known as Vidar. Vidar was RaaS variant that not only locked a victim's files but also stole them. GandCrab's developers announced that they would be retiring the RaaS on June 1, 2019 and shortly after the FBI released the relevant decryption keys. The most notable ransomware development in 2019-2020 besides GandCrab was the rise of leak sites. The purpose of leak sites was to pressure victims. Publishing stolen data meant that victims were vulnerable to additional financial loss if sensitive financial data, customer personally identifiable information (PII), or trade secrets were exposed. The history and evolution of ransomware provided only covers it's

origin until the year 2020. Ransomware continues to evolve and grow as time goes on (Drake, 2022).

Preventative Measures

There are a few different ways an organization can prepare for a ransomware attack. Firstly, the organization should be technically prepared; this involves the implementation of preventative measures and controls. Secondly, the organization should understand and protect common infection vectors. Thirdly, the organization should provide cybersecurity education to individuals within the company in an effort to promote safe surfing and using secure networks. A**n organization that is technically prepared and has protected common infection vectors does not need to pay the ransom in the event of a ransomware attack because the criminals have no leverage over the organization; all that needs to be done is to implement the backups.**

The first and best way to prevent or reduce the damage of ransomware is to be technically prepared (Leo, Isik, and Muhly, 2022). This involves having a viable and current backup (Leo, Isik, and Muhly, 2022). However, just having a backup is not enough. The organization also needs to validate and refine their ability to recover data with these backups in a crisis, with minimal obstacles (Leo, Isik, and Muhly, 2022). Research shows that this capability is underdeveloped in many organizations. According to Leo, Isik, and Muhly's article "The Ransomware Dilemma", fifty-eight percent of data backups fail during a restoration attempt. Another article – "5 Startling Statistics About Data Backup and Recovery" – points out that sixty percent of backups are incomplete and fifty percent fail during restoration attempts. Whatever the exact percentage may be, approximately half of all restoration attempts fail. Therefore, it is

essential that organizations routinely monitor their ability to recover so that they do not face an unpleasant shock during a crisis (Leo, Isik, and Muhly, 2022). Another important aspect of maintaining a viable and current backup is ensuring that the backup is stored offline, because many forms of ransomware will try to find and delete any backups it can access (Ransomware Guide | CISA, n.d.).

Being technically prepared involves more than simply maintaining a viable backup. Another preventative measure that organizations should take is to preserve routinely updated "gold images" of critical systems in case the critical systems ever need to be rebuilt. This involves maintaining image "templates" that can be quickly deployed to rebuild a system. These "templates" include a preconfigured operating system (OS) and the associated software applications. An example of software applications that may be associated with a critical system are a virtual machine or server. It is important to note that compatibility can be an obstacle when rebuilding from images, specifically when the hardware version is not the same as the primary system's version. Therefore, having the appropriate hardware is a necessary component to maintain regularly updated gold images. Applicable source code or executables should be at hand, in addition to system images. Source code is an integral component of a computer program that is created by a programmer. Source code is designed and formatted in a way that is readable and understandable to developers and users. The source code is comprised of functions, descriptions, definitions, calls, methods, and other operational statements. Executable code refers to the instructions that allow a computer to perform a certain task. It is object code, machine code, or other code readable by a computer when loaded into its memory. It is ideal to rebuild from system images, but this is not always feasible because some images are not able to be

installed on different hardware or platforms. In these cases, having independent access to necessary software will help (Ransomware Guide | CISA, n.d.).

Once an organization is technically prepared, the next best way to minimize their risk for a ransomware attack is to understand and protect common infection vectors. An infection vector is a route or method used by an attacker to illegally infiltrate a network or computer in an effort to take advantage of system vulnerabilities. This includes identifying and addressing internet-facing – which means directly accessible over the internet -- vulnerabilities and misconfigurations. One way of preventing internet misconfigurations is to verify that devices are properly set up and security features are enabled. This includes disabling ports and protocols that are not being employed for business aims. In general, organizations can protect infection vectors by conducting regular vulnerability scanning, especially those on devices that are accessible through the internet. This will restrict the attack surface. Another form of general protection involves routinely patching and updating software and operating systems with the newest released version (Ransomware Guide | CISA, n.d.).

In addition to general protection, organizations should be aware and protect specific infection vectors that are commonly targeted. A commonly attacked infection vector that organizations should prepare for is phishing attacks (Ransomware Guide | CISA, n.d.). Phishing is a social engineering tactic that tricks a user into installing malware (*What is phishing and how does it relate to ransomware?,* 2021). One of the most common techniques is tricking the user into clicking on an email (*What is phishing and how does it relate to ransomware?,* 2021). It is a simple but effective way of targeting victims and spreading ransomware (*What is phishing and how does it relate to ransomware?,* 2021). Organizations can protect this infection vector by

implementing a cybersecurity awareness and training program that covers how to identify and report suspicious activity or incidents (Ransomware Guide | CISA, n.d.). Another common attack vector are pop-ups and ads. Similar to phishing attacks, pop-ups and ads employ social engineering to trick users into clicking on them and downloading the malware (Arntz, n.d.). Similar to phishing, the best way to protect this infection vector is to implement a cybersecurity awareness and training program to educate individuals within the organization.

Remote desktop protocol (RDP) is another common attack vector because RDP ports lack adequate security and are therefore vulnerable (McNeal, 2023). Attackers can quickly infiltrate RDPs to harvest user credentials and then the attacker can easily elude endpoint protection and access data and even data backups (McNeal, 2023). To protect RDP, organizations should implement the principle of least privilege (Arntz, n.d.). This means that access to RDP should be limited only to users who need it and access should be limited to specific IP addresses to ensure this (Arntz, n.d.). In addition, strong passwords and multi-factor authentication should be implemented (Arntz, n.d.). To prevent password guessing attacks altogether, the organization could put RDP behind a VPN (Arntz, n.d.). However, this comes at the cost of maintaining a VPN and shifts the burden of access control from RDP to the VPN (Arntz, n.d.).

As previously mentioned, the main way to combat social engineering tactics that often lead to ransomware attacks is to implement a cybersecurity awareness and training program. There are many important elements to a thorough cybersecurity awareness and training program, including educating trainees about safe surfing and using secure networks and encouraging trainees to stay informed. The training program should emphasize using caution when you

clicking and warning trainees about the dangers of emails and messages for unknown individuals. It should also warn trainees about the danger of downloading applications that do not come from a trusted source because ransomware attackers often use social engineering tactics to try to get you to install dangerous files. The training program should warn (or require) trainees to avoid using public Wi-Fi networks, since many of them are not secure and cybercriminals can snoop on your internet usage. The training program should encourage trainees to stay informed by keeping current on the latest threats (What Is Ransomware?, n.d.).

Mitigation

Some organizations choose to accept that there is a really high probability that they will be attacked and, instead of focusing on preventing an attack, choose to focus on recovery after. It is important to note that organizations may still take preventative measures; they simply accept that these measures will probably not be enough to prevent an attack. The main form of mitigation is cyber insurance. Cyber insurance is insurance against the effects of cybercrimes such as malware, ransomware, and distributed denial-of-service (DDoS) attacks. Insurance companies began providing cyberthreat policies in the early 2000s and it has been growing ever since (Leo and Muhly, 2022). Nowadays, cyber insurance protection comes in three forms: third-party written coverage, first-party written coverage, and implicit silent cyber coverage (Bule, n.d.). Third-party written insurance covers the insured party for losses due to data breaches, malware infections, or other cyberattacks that are the fault of the insured party (Bule, n.d.). A metaphor for third-party written insurance is medical malpractice insurance, where health organizations are insured against harm they inflict on their patients (Bule, n.d.). First-party written insurance covers insured parties for losses incurred from cyberattacks that directly affect

their business (Bule, n.d.). First-party policies can vary greatly in the specificity of their terms depending on the needs of the organization (Bule, n.d.). Silent cyber insurance coverage refers to coverage of cyber-related losses from traditional property and casualty insurance (Bule, n.d.). For example, an organization's computer system is infected with malware and this sets off the sprinkler system, causing an individual to slip and fall (Bule, n.d.). Unless cyber perils are explicitly excluded, the medical bills of the injured individual would be covered by the organization's property and casualty insurance (Bule, n.d.).

There are a variety of types of cyber coverage available, including: data breach coverage, regulatory civil action coverage, cyber extortion coverage, virus liability, lost income coverage, loss of data coverage, and errors and omissions coverage. Data breach coverage insures against expenses from a data breach. Expenses covered typically include notification of the victims, setting up a call center, credit monitoring and restoration services for the victims, and crisis management services. Regulatory civil action coverage insures against fines after a violation of the Health Insurance Portability and Accountability Act (HIPPA) or similar regulations. It is important to note that some policies only cover the cost of defending against the action and some policies cover both the cost of defending and the fine. Cyber extortion coverage insures cases where a cybercriminal steals data from the policyholder and then attempts to sell it back. It also insures against cases where a cybercriminal positions a logic bomb in the policyholder's system and requests payment in exchange for disabling it. Policies typically cover the cost of a negotiator and the cost of the reward offered for information leading to the arrest of the perpetrator. Virus liability coverage insures against lawsuits by individuals or organizations whose systems allegedly got infected with a virus from the policyholder's system. Lost income

coverage insures the policyholder's lost revenue while a system is down. Insurers often require a minimum system shutdown time of 12 or 24 hours or require proof of actual losses. Loss of data coverage insures the cost of replacing the policyholder's data in the event that it is lost. Errors and omissions coverage insure against alleged failures by the policyholder's software (Bule, n.d.).

The cost of cyber insurance varies greatly. Depending on the organization, it can range from $500 per year to $50,000 or more per year. There are many factors that impact price, including: coverage limits, data access, security measures, industry, and claims history. Coverage limits impact price because the higher and more complex coverage an organization requires, the more expensive the policy will be. For example, if the organization uses multiple servers or stores an abundant amount of customer data, their insurance will be more expensive. Restricting access to sensitive data can decrease the cost of cyber insurance. For example, implementing access controls such as password-protection or face recognition software to access data. Security measures, such as anti-virus software and firewalls, can decrease insurance premiums. Industry impacts insurance price, insofar as the industry requires online operation. A software development business will have a higher premium than a brick and mortar business because it will face more cyberthreats. In addition, businesses in certain industries – like healthcare and accounting – that store massive amounts of sensitive data will also pay a higher premium. An organization with a history of multiple claims may have a higher premium. Compared to other types of insurance, the cost of cyber liability insurance tends to be greater because the fallout of a cyberattack can be catastrophic in terms of cost. Cyber liability coverage is an evolving area of insurance and there can be confusion around what cyber liability insurance

covers and what it does not cover. Ransomware attacks that are suspected to be state funded can free the insurer from liability to pay the claims because the attack can be classified as an act of war (Leo and Muhly, 2022). As a result, it is critical for an organization to carefully consider and read through a policy before committing to it (Bule, n.d.). With the right policy, cyber insurance can be an effective tool in mitigating the damage of a cyberattack (Bule, n.d.).

Reactive Measures

After an organization has been attacked, there are two main reactive measures that can be taken. The first is to gain an understanding of the attacker. Ransomware has grown and evolved but so has resistance and defenses. Ethical hackers - which are hackers who attempt to hack a system to discover vulnerabilities and understand attack methods - and researchers who crack ransomware variants often post resources online with decryption keys. Organizations who have been attacked with ransomware and are not prepared with up-to-date backups should check these online resources and check with federal law enforcement authorities to see if a decryption key is already at their disposal. In addition, organizations should analyze the threat intelligence reports provided by cybersecurity research organizations and vendors for any information about the cybercriminals attacking them. Unfortunately, there are many cybercriminals who are only interested in enlarging the volume of network penetrations and do not decrypt the data even once the ransom has been paid. As a result, knowledge of the attackers – and whether they are known to send the decryption key – can be essential when an organization is deciding on how to react to an attack. The first main takeaway is that an organization may be able to access the relevant decryption keys and restore their data without paying the ransom. The second main takeaway is

that threat intelligence about the cybercriminals can inform an organization on whether payment is likely to result in the desired outcome (Leo and Muhly, 2022).

The second reactive measure an organization can take without having a viable backup is to attempt to reduce the effects of the attack. The Cybersecurity and Infrastructure Security Agency (CISA) provides a ransomware response checklist that organizations can utilize in the aftermath of an attack (Leo and Muhly, 2022). According to the Cybersecurity and Infrastructure Security Agency (CISA) ransomware response checklist, the first step is to access which systems were attacked and promptly isolate them. If the impact of the attack was widespread and affected many systems, the CISA ransomware response checklist recommends taking the network offline at the switch level. Sometimes it is not feasible to take a network temporarily offline. In these cases, the organization should locate the network cable (i.e. Ethernet) and unplug contaminated devices from the network or disconnect the contaminated devices from Wi-Fi to contain the infection. It is important to note that this step will obsruct an organization from preserving ransomware infection artifacts and potential evidence stored in volatile memory. Therefore, this step should only be reserved as a last resort if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means. After the initial network penetration, the cybercriminals may monitor the organization's activity or communications to see if their attack has been detected. Therefore, the organization should proceed with caution during this step and isolate systems in a coordinated manner and use communication methods like phone calls to avoid notifying the attackers that the ransomware has been detected. Failing to proceed with caution could enable the cybercriminals to move

laterally to preserve their access or to spread the ransomware prior to the network being taken offline.

According to the CISA ransomware response checklist, the second step is to power down the infected devices to prevent a further spread of the infection. This step should only be taken if the organization is unable to disconnect the devices from the network. The third step on the checklist is to access impacted systems for restoration and recovery. This mainly involves identifying and prioritizing critical systems for restoration and determining the importance of the data on compromised systems. Prioritization of critical systems should be established based on a predefined critical asset list that includes information systems vital for health and safety, revenue generation, or other critical services; the list should also include the systems the organization depends on. It is equally necessary to identify systems and devices that have not been impacted so they can be deprioritized for restoration and recovery. This enables the organization to recover more efficiently (Ransomware Guide | CISA, n.d.).

According to the checklist, the fourth step is for the organization to consult with each other internally to develop and document an initial understanding of what has occurred. The fifth step is to provide internal and external teams and stakeholders with an understanding of what they can offer to assist the organization and inform them of any steps to follow to identify and contain the impacted systems. This step includes sharing pertinent information to receive timely assistance and keeping management and senior leaders informed via regular updates. The sixth step recommended by the guide is for the organization to take a system image and memory capture of a sample of affected devices (e.g. workstations and servers). Additionally, the organization is advised to collect any relevant logs as well as samples of any “precursor”

malware binaries and associated observables or indicators of compromise (e.g. suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). It is important to note that the organization should take care to preserve evidence that is highly volatile in nature – or limited in retention – to prevent loss or tampering (e.g. system memory, Windows Security logs, data in firewall buffers) (Ransomware Guide | CISA, n.d.).

The seventh step an organization should take to limit the impact of an attack is to consult with federal law enforcement for decryption keys. It is possible that researchers have already cracked the encryption algorithm for the variant. The eighth step is to research for the ransomware variant (from trusted sources such as the government) and follow any additional recommended steps to identify and contain impacted systems. Oftentimes, this includes disabling the execution of known ransomware binaries and deleting other associated registry values and files. The ninth step is to identify the systems and accounts involved in the initial breach; this can include email accounts. The tenth and final step is to use the information gained about the attack to contain any associated systems that may be used for further or continued unauthorized access. This may include: disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets (Ransomware Guide | CISA, n.d.).

Decision and Conclusion

When an organization undergoes a ransomware attack and is facing the decision of whether or not to pay the ransom, the decision ultimately comes down to a variety of factors. The first and most important factor is whether or not the organization has a viable backup or another prepared recovery plan. A viable backup means the organization has no reason to pay the ransom, as the cybercriminals have no leverage (Leo and Muhly, 2022). In other cases, an

organization has comprehensive cyber insurance and is covered under their policy or has some other recovery protocol prepared. In case that the organization does not have a viable backup, comprehensive cyber insurance, or another prepared recovery protocol, the decision of whether or not pay boils down to two main questions (Richardson & North, 2017).

First, is the data worth more than the ransom (Richardson & North, 2017)? The organization should consider their financial exposure and assess the potential repercussions the lost data would have on the organization (Richardson & North, 2017). This will offer insight into if paying the ransom is an economically feasible option (Leo and Muhly, 2022). With an assessment of whether it is economically feasible, the organization must then decide if it is reasonable; sometimes there is a better option (Leo and Muhly, 2022). Second, what is the organization's confidence level that paying the ransom will actually prompt the criminal to decrypt the data (Richardson & North, 2017)? This is why it is important for an organization to learn as much as possible about the attack and the attackers. The organization should research every potential resource for information before committing to a course of action.

Another factor the organization should consider are the legal implications of paying the ransom. When an organization does not have a viable backup, comprehensive cyber insurance, or another recovery plan, and paying the ransom is economically feasible, it can seem like the best course of action (Leo and Muhly, 2022). However, this path can face legal obstacles in cases where the organization operates under U.S. jurisdiction or the victimized individual is a U.S. citizen (Leo and Muhly, 2022). In September of 2021, the U.S. Department of Treasury issued a reminder that making or facilitating payments to cybercriminals on which is has imposed sanctions is illegal and can result in criminal prosecution (Leo and Muhly, 2022). Therefore,

specific knowledge of the jurisdictional framework and the cybercriminal the organization is dealing with is critical (Leo and Muhly, 2022). Nonetheless, ransomware criminals seem to have enough business sense to recognize that if word spreads that paying the ransom does not result in decryption, their business model will fail because victims will stop paying (Richardson & North, 2017). In addition to legal concerns, there is always the concern that paying the ransom will invigorate the criminals and prompt another attack in the future (Richardson & North, 2017).

Without a viable backup, comprehensive cyber insurance, or some other planned recovery protocol, paying the ransom may seem like the best option for an organization. However, experts provide four reasons not to pay the ransom. First, the organization sets themselves up as a desirable target (Richardson & North, 2017). Cybercriminals talk and spread the word about which victims paid and which did not (Richardson & North, 2017). Second the cybercriminal cannot always be trusted to decrypt an organization's data (Richardson & North, 2017). Third, the organization's next ransom will be greater (Richardson & North, 2017). The cybercriminals might demand a second ransom before decrypting the organization's data or even infect the organization for a second time (Richardson & North, 2017). Either way, the consequences will be greater the second time (Richardson & North, 2017). Fourth and finally, payment encourages the cybercriminal to continue developing and deploying ransomware (Richardson & North, 2017).

Every organization that experiences a ransomware attack must decide what is best. Understanding ransomware and the different options available is the first step. Considering the options and calculating the effects each option has on an organization is the second step.

Choosing whether or not to pay the ransom is the third and final step. Hopefully each organization chooses the best path for their specific circumstances.

Bibliography

Abrams, L. (2021, May 13). *Chemical distributor pays $4.4 million to Darkside ransomware*. BleepingComputer. Retrieved April 13, 2023, from https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-milli on-to-darkside-ransomware/

Armerding, T. (2017). To pay or not to pay: Too many victims say yes to ransomware: Paying a ransom to cyber criminals to unlock your files only encourages them to do it more, experts say. but many victims haven't left themselves any choice - which is what is fueling ransomware's explosive growth. *CSO (Online)*, Retrieved from https://www.proquest.com/trade-journals/pay-not-too-many-victims-say-yes-ransomware/ docview/1868604648/se-2

Arntz, P., & ABOUT THE AUTHOR Pieter Arntz . (n.d.). *How to protect RDP*. Malwarebytes. Retrieved April 11, 2023, from https://www.malwarebytes.com/blog/news/2022/03/protect-rdp-access-ransomware-a ttacks

"Article: What Is... Crypto-Ransomware: F-Secure." *F*, https://www.f-secure.com/v-descs/articles/crypto-ransomware.shtml.

Bule, G. (n.d.). *A beginners guide to Cyber Insurance*. ITSEC. Retrieved April 23, 2023, from https://itsec.group/blog-post-cyberinsurance.html

C. (2022, September 14). *Ransomware as-a-Service (RaaS)*. Check Point Software.

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ransomware-as-a-s ervice-raas/

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

Constantin, L. (2021, November 12). *Revil ransomware explained: A widespread extortion operation*. CSO Online. Retrieved April 13, 2023, from https://www.csoonline.com/article/3597298/revil-ransomware-explained-a-widesprea d-extortion-operation.html

Dossett, J. (n.d.). *A timeline of the biggest ransomware attacks*. CNET. Retrieved April 13, 2023, from https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware
-attacks/

Digital Currencies' role in facilitating ransomware attacks: A brief explainer – Third way. – Third Way. (n.d.). Retrieved April 4, 2023, from https://www.thirdway.org/memo/digital-currencies-role-in-facilitating-ransomware-at tacks-a-brief-explainer

Drake, V. (2022, September 14). *The history and evolution of ransomware attacks*. Flashpoint. Retrieved April 20, 2023, from https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/

Feilner, M. (2023, April 4). *"Ransomware as a service" as a business model: Why the business of extortion flourishes*. Greenbone. Retrieved April 13, 2023, from https://www.greenbone.net/en/blog/ransomware-as-a-service/

Leo, P., Isik, Ö., & Muhly, F. (2022). The ransomware dilemma. *MIT Sloan Management Review, 63*(4), 13-15. Retrieved from https://www.proquest.com/scholarly-journals/ransomware-dilemma/docview/2678515108/se-2

Lichtenwald, I., & CEO of Medsphere, S. C. (2021). *Ransomware in healthcare: The costly reality of withstanding hackers*. Atlanta: Newstex. Retrieved from https://www.proquest.com/blogs-podcasts-websites/ransomware-healthcare-costly-reality-withstanding/docview/2560825159/se-2

Locker Ransomware Information Guide and FAQ. (2016, March 21). BleepingComputer. https://www.bleepingcomputer.com/virus-removal/locker-ransomware-information

Mayangao, C. (2021, Oct 16). The madness of ransomware 'as a service'. *Mid-East.Info* Retrieved from https://www.proquest.com/wire-feeds/madness-ransomware-as-service/docview/2582432436/se-2

McNeal, A. (2023, March 13). *Top ransomware attack vectors & how to prevent them*. Graphus. Retrieved April 11, 2023, from https://www.graphus.ai/blog/top-ransomware-attack-vectors/

Mitigating malware and ransomware attacks. (n.d.). https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Myre, G. (2021, June 10). *How bitcoin has fueled ransomware attacks*. NPR. Retrieved April 4, 2023, from https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-att acks

ODonnell, L. (2021). *Cyber-insurance fuels ransomware payment surge*. Woburn: Newstex. Retrieved from https://www.proquest.com/blogs-podcasts-websites/cyber-insurance-fuels-ransomware-pa yment-surge/docview/2535475355/se-2

Ohio Supreme Court finds that ransomware attack did not result in direct physical loss to insured's software. Ohio Supreme Court Finds That Ransomware Attack Did Not Result In Direct Physical Loss to Insured's Software | Traub Lieberman. (2023, January 17). Retrieved April 19, 2023, from https://www.traublieberman.com/perspectives/ohio-supreme-court-finds-that-ransomware-attack-did-not-result-in-direct-physical-loss-to-insureds-software

O'Kane, P., Sezer, S. and Carlin, D. (2018), Evolution of ransomware. IET Netw., 7: 321-327. https://doi.org/10.1049/iet-net.2017.0207

Paying ransom doubles cost of recovering from ransomware attack: Reports. (2020, May 19). *Business World*, Retrieved from https://www.proquest.com/magazines/paying-ransom-doubles-cost-recovering-ransomwa re/docview/2404283613/se-2

Ransomware Guide | CISA. (n.d.). https://www.cisa.gov/stopransomware/ransomware-guide

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10-21,101. Retrieved from https://www.proquest.com/scholarly-journals/ransomware-evolution-mitigation-prevention/docview/1881414570/se-2

Spence, N., M.S., Bhardwaj, Niharika,M.B.B.S., M.S., Paul, David P, III,D.D.S., PhD., & Coustasse, Alberto, DrPH, MD,M.B.A., M.P.H. (2018). Ransomware in healthcare facilities: A harbinger of the future? *Perspectives in Health Information Management*, , 1-22. Retrieved from https://www.proquest.com/scholarly-journals/ransomware-healthcare-facilities-harbingerfuture/docview/2111721098/se-2

Tewfik, G., & Whitehead, V. (2021). Ransomware attacks on healthcare facilities present unique challenges for anesthesiology. *Journal of Clinical Anesthesia, 74* doi:https://doi.org/10.1016/j.jclinane.2021.110413

Thakkar, Dhanya. *Preventing Digital Extortion*, Packt Publishing, Limited, 2017. *ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/lasalle-ebooks/detail.action?docID=4867419.

The Wild World of crypto ransomware payments. FEI. (n.d.). Retrieved April 4, 2023, from https://www.financialexecutives.org/FEI-Daily/October-2021/The-Wild-World-of-Crypto-Ransomware-Payments.aspx

Ukrainian arrested and charged with ransomware attack on Kaseya. The United States Department of Justice. (2022, May 18). Retrieved April 13, 2023, from

https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

What is phishing and how does phishing relate to ransomware? Ransomware.org. (2021, November 2). Retrieved April 11, 2023, from https://ransomware.org/how-does-ransomware-work/active-defense-intrusion/phishing-att acks/

What Is Ransomware? (n.d.). Trellix. https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html

5 Startling Statistics About Data Backup and Recovery. (n.d.). Ontech Systems. Retrieved February 22, 2023, from https://ontech.com/data-backup-statistics/#:~:text=Did%20you%20know%3A%2060%25%20of