An Overview of Ransomware

Tristan N Woodard

Old Dominion University

CYSE 497: Tutorial Work in Cybersecurity

Dr. Saltuk Karahan

December 1st, 2023

An Overview of Ransomware

While the use of malicious software to target both individuals, businesses, and governments is not a new development, some may have been hearing it more and more in the news as of late. In particular, one specific type of malware has seen some close coverage: ransomware. The impact of ransomware has seemingly been felt even beyond an IT office or a help desk line. Apparently, such effects have been felt across the business world, throughout the manufacturing and infrastructure sectors, and even to the top of national governments and beyond. With the course set for increasing technological advancements and integration into perhaps every aspect of daily life, it could be beneficial to look into these claims and events, and investigate ransomware as a tactic, tool, and phenomenon. In the following, I will detail what ransomware is, how it works, its history, and how it can be better prevented, or protected from at multiple levels.

Ransomware usually refers to a form of malware that locks a computer, making it or an aspect of it, including the data contained on it, inaccessible to a user until some form of ransom is paid, where presumably access would be restored (Richardson & North, 2017). Due to the nature of the program and attack method, it is seen as a form of extortion (Morse & Ramsey, 2016). Extortion rackets like kidnapping and holding cargo for ransom have been a successful tactic for criminals for a significant period of time. Extortion over data, however, has only really been around since at least 2005 (Richardson & North, 2017). Since then, however, ransomware has seen significant focus placed on it as a notable method of extortion, and as a cybercrime. Ransomware itself comes in a number of different forms and types. Reasons for different methods of attack, levels of sophistication, methods of delivery, methods of activation, means of payment, and other features could be due to a variety of factors like the attacker's sophistication, intended result, and recency of the attack.

Overall, there are three broad categories that have been identified that are each associated with those various qualities (Beaman et al., 2021). The first type of crypto-based ransomware. This is a very common method, and as such, sometimes descriptions of ransomware are instead descriptions of crypto ransomware specifically. In this form, the data on the device is encrypted in some way, making it inaccessible to the intended user. The user is then directed to pay the ransom, in return, they are promised they will be given a private encryption key that would allow the user to decrypt the data (Richardson & North, 2017). Often, this method requires the attacker to be paid in cryptocurrency, with Bitcoin being particularly common.

Locker ransomware works similarly to crypto ransomware, but the inverse (Beaman et al., 2021). Instead of removing access to files and data but keeping computer function intact, locker ransomware will “lock” the computer, removing access to basic functions and control, but not actually changing or encrypting the data in any way. Instead, it attempts to simply block or restrict certain computer functions. Encryption may occur, but it will not usually be for user personal data, but instead for the purpose of controlling the central functions of the computer.

Scareware is the last broad type (Beaman et al., 2021). This would consist of a ransomware program that doesn’t significantly lock or encrypt data, or significantly lock the usage of the device as well. Instead, the intent is to appear as if it is doing either or both of those things, in order to intimidate the user into providing a payment, again, often through cryptocurrency means. Often, this method relies much more on social engineering techniques to cause fear or intimidation. It can also be combined with other forms of malware, where instead of ransoming data or access, the fear of the data or access being ransomed can prompt a user to install other forms of malware, or further compromise the system.

As stated previously, each type of ransomware has its own defining characteristics and qualities. For instance, payment through cryptocurrencies is heavily preferred by those employing crypto ransomware when compared to locker ransomware (Richardson & North, 2017). Locker ransomware, in the past, had already been using other methods to achieve payment before cryptocurrency was widely available or used. Not only that, but even today, due to the nature of locker ransomware, the device is left in an operable state. This makes purchasing and sending cryptocurrency more difficult. Thus, locker ransomware users will use alternative methods. This could include mailing pre-paid cards or redeeming local vouchers. In the past, users would even call a premium phone number that would earn the attacker money. Voucher based methods often laundered the money by using vouchers that could be used for online betting services. Eventually, this currency would be exchanged into a prepaid money card, which would be converted to cash through the use of a “money mule”, or a person whose sole job is to facilitate money exchange, knowingly or unknowingly.

Nevertheless, numerous ransomware programs will utilize and often rely on the functions of cryptocurrency. Some have even gone so far as to point out that ransomware really “took off” as soon as Bitcoin started to see wide use and viability around 2008 (Richardson & North, 2017). This was in part due to Bitcoin's and many other cryptocurrencies' greater capability to anonymize financial transactions and money transfers. In fact, in some cases, Bitcoin transactions are nearly impossible to trace. This is, in part, due to the numerous Bitcoin-based laundering services and Bitcoin anonymizers that are available for criminals to use. As of 2021, the U.S. Department of Treasury has said that the “vast majority of reported ransomware payments were made in Bitcoin.” (Oosthoek et al., 2023).

Actual payments for cryptocurrency based ransomware will usually follow a few steps. After the ransomware is deployed and the ransomware is displayed, the victim and perpetrators will usually discuss on anonymized channels the payment terms and price

(Oosthoek et al., 2023). From there, the victims who will pay the ransom will exchange their fiat currency for Bitcoin using a regular exchange platform. Then it is sent to a wallet of some kind, which, in some cases, is dynamically generated for specific transactions. From there, they will launder and anonymize the money. Operators could use the aforementioned voucher techniques, but could also exchange Bitcoin for physical goods and launder that way. It seems that there is not an exact set of specific standards and methods used by most operators to launder money, but often fraudulent exchanges and mixers are used.

Ransomware, as it exists today, largely functions through two major economic models (Oosthoek et al., 2023). These are commodity ransomware and Ransomware-as-a-Service (RaaS). Commodity ransomware was much more common as the primary business model during the early days of ransomware utilization. Commodity ransomware often utilizes and expands upon preexisting work. This led to the rise of different ransomware “families” of similar design, such as the WannaCry ransomware “family”. The operators often consisted of a small number of technically skilled creators of the ransomware technology and distribution, however, the overall operations were often seen as sloppy and less targeted. Sometimes they were poorly coded, and the methods for receiving payments were often non-functional or unable to properly scale. The modus operandi seemed to be the widespread, damaging, and disruptive spread of ransomware, with the goal of mass exploitation of those targeted. The vector for attack would often follow suit, being spread by mass phishing and executable campaigns, primarily through email. The sloppy nature of the code at times, the poorly scaling and often nonfunctional methods of payment, and the sometimes overly destructive and damaging code often rendered little to no financial success in actually retrieving ransoms for operators of the ransomware. Instead, this method was marked by widespread disruption and destruction of cyber ecosystems.

RaaS seemingly emerged as a business model in 2016 and has since dominated as the preferred method of ransomware operations (Oosthoek et al., 2023). Instead of individuals and disjointed teams modifying and furthering leaked software packages and exploits, therefore creating ransomware families based on things like Petya and Wannacry, RaaS took a different approach. Usually, a highly sophisticated development team would develop a sophisticated and highly efficient piece of ransomware. From there, they would receive payments by licensing that ransomware to others who wished to employ the software. Often, this team would even set up official portals on anonymized protocols using dark web services like Tor. In that way, victims could much more easily pay the ransom, making it much more economically viable as a business move for victims to pay said ransom when compared to commodity ransomware. The methods RaaS has allowed for, have paved the way for much more sophisticated methods of attack and exploitation. Often, as opposed to simple mass phishing attacks, spear phishing techniques designed to target specific individuals and enterprises are used. Also, more efficient price discrimination techniques can be used to meet the needs of each specific target, again, allowing for the option of paying the ransom to actually make economic sense for a target, thus becoming a viable business decision. This is amplified as double extortion schemes will also be employed by the operators. In these, the attackers will not only lock targets out of their data, but they will also threaten to publicly release sensitive data if the ransom is not paid. This further allows for larger and more lucrative targets to be attacked, who not only have the funds to pay for high-cost ransoms, but are more likely to be forced to do so.

Ransomware attacks themselves will occur in specific phases (Aldauiji et al., 2022). The infection phase is first. It involves the process of getting the malicious code onto the machine through some sort of attack vector. The majority of ransomware seems to be propagated primarily through email, using a link or attachment (Richardson & North, 2017).

Around 60% is propagated this way. One fourth of ransomware is propagated through a website or web application. The remaining percent is from a USB stick, a business application, social media, or is of unknown origin. Another known method used to infect targets with ransomware is the use of an exploit kit (Beaman et al., 2021).

The next phase that occurs is the installation phase (Aldauiji et al., 2022). In this phase, the malware will install itself onto the affected device. Importantly, it will attempt to do so without attracting any attention. From there, it takes control of the system, allowing for further exploitation. The following phase is the communication phase. This is where the ransomware, still undetected, will initialize and establish a connection back to the command and control server.

While the overall functional types of ransomware could be divided into crypto ransomware, locker ransomware, and scareware, ransomware can be further divided into categories based on the method of infection itself (Loman, 2019). The three categories based on that behavioral trait would then be cryptoworm types, RaaS types, and automated active adversary types. A cryptoworm is an individual piece of ransomware that has the ability to replicate itself and spread across a network. This allows for a network wide impact from potentially a single point of infection. RaaS, as previously mentioned, involves the leasing out of a specialized ransomware distributions from the developer team to those that purchase them. Because of this method, even those with limited technical skills could still utilize the ransomware effectively. This method allows for easy use with other common malware propagation techniques like spam emails, as well as drive-by downloads used in tandem with exploit kits. It could also be used alongside the final method, which is the automated active adversary type. This type involves an automated system scanning large numbers of systems for weak defenses and potential entry points. When potential entry points are found, attackers usually plan out and execute non-automated attacks to specifically target the vulnerable systems. Attackers will also use a number of methods to not only initially infect the target, but to bypass security measures, and enter the next phase of the process. One such technique that is used, is to fraudulently obtain signatures for the ransomware to falsely authenticate it like a regular program.

The very next phase is the execution phase (Aldauiji et al., 2022). This is the phase where the actual encrypting of files, data, or restrictions of access occur on the targeted device(s). As previously stated, locker ransomware will focus on removing access to the primary device functions themselves. Crypto ransomware will focus on encrypting the data within the device and holding that for ransom instead. Importantly for crypto ransomware, modern encryption techniques, if properly executed, are nearly impossible to decrypt without direct help from those that encrypted them (Beaman et al., 2021). Most often, AES or RSA systems are used. In addition, one of three encryption schemes could be used to encrypt the data. These are symmetric encryption, asymmetric encryption, or hybrid encryption. Purely symmetric encryption is almost never used. This is because, if used, it would require a key to be embedded within the ransomware itself, thus compromising the encryption. Asymmetric encryption can be used more often, but it has various limitations. Foremost among these is that asymmetric encryption is much slower. This could compromise the encryption as well. This could cause the installation and/or communication phases to have to be extended, which, in turn, prolongs the time in which the ransomware could be prevented or detected before full encryption could occur. On the other hand, the ransom could be activated before all files were fully encrypted. This could potentially prevent the ransom from being successful. This leaves the most effective and powerful approach for ransomware to be a hybrid encryption approach that utilizes both asymmetric and symmetric encryption methods.

A hybrid approach typically begins with a public and private key pair being generated on a command and control server operated by the attacker (Beaman et al., 2021). From there, the ransomware is propagated onto the target system, and the typical ransomware phases continue. The ransomware will then encrypt the files using a symmetric key system on the target system. From there, it will use the public key from the command and control server to encrypt the symmetric key it made to encrypt the files. The plaintext key is then deleted. From there, if the ransom is paid, and the promise to decrypt is followed through, the private key from the command and control server will be sent to the ransomware. It will then decrypt the symmetric key, which can then decrypt the files. Importantly, different encryption methods can be used together for this hybrid system, further ensuring a successful ransom. In addition, a new key pair is usually generated for every single separate infection to ensure multiple victims cannot bypass the ransom by sharing keys.

The encryption itself can be executed in a number of ways as well. For instance, each file could be encrypted individually, or multiple threads could encrypt more than one at the same time (Aldauiji et al., 2022). Files can also be encrypted alphabetically, or the files with the smallest file size could be prioritized first. The file encryption itself could also follow one of two processes, copy and overwrite. A copy method will encrypt a copy of the data and delete the original plaintext data. The overwrite method will work similarly, but will instead read the original file, and create an encrypted version that overwrites the original file. Using the overwrite method, it becomes seemingly impossible to recover the original files. The copy method makes it similarly difficult, but this method will require the ransomware to have an additional method to wipe data to ensure the original files are not able to be recovered.

The next phase is the extortion phase (Aldauiji et al., 2022). With the ransomware executed, and access taken away, the ransomware will then shift to explaining to the target user what has happened to their system. Often, a ransom note will be displayed, instructing the target to obey the attacker and pay the ransom. This often comes along with a number of social engineering techniques designed to further increase the likelihood that the target will pay the ransom.

The final phase is the emancipation phase (Aldauiji et al., 2022). The emancipation phase would begin after the ransom has been received, and the attacker has decided to follow through with returning access to the target's data to the target user. This will involve either the attacker sending keys or decryption methods, or directly having the program perform the function itself.

The traits and categories of ransomware have displayed themselves in different ways throughout the history of ransomware as a practice. Some notable historical examples of notable ransomware incidents and deployments include: the CyptoLocker ransomware attacks from 2013 to 2014, The WannaCry attacks in 2017, The 2017 NotPetya Attacks, and the 2021 Colonial Pipeline Attacks. (Harkins & Freed, 2018; Richardson & North, 2017; Reeder & Hall, 2021).

The CyptoLocker attacks occurred during 2013 and 2014 (Richardson & North, 2017). The program was developed by a notable hacker, and then initially distributed by a large Trojan Botnet. Eventually, it was also distributed by a mass phishing email campaign. The ransomware, as the name suggests, was of the locker ransomware type. It gave victims numerous ways to pay, including via bitcoin, but claimed to require victims to pay within three days. By December 2013, 250,000 systems were infected, by May 2014, 500,000 were infected. It was estimated that, in total, 1.3 to 3 percent of infected users ended up paying the ransom.

The WannaCry attacks occurred in 2017 (Harkins & Freed, 2018). They were built on a vulnerability known as EternalBlue. This vulnerability was leaked by a mysterious group called the "shadow brokers", and it was thought the vulnerability originated from the U.S. National Security Agency (NSA). The attacks had a global reach, impacting over 200,000 endpoints in over 150 different countries. The EternalBlue exploit, coupled with other exploits, allowed unpatched systems to be vulnerable to arbitrary code execution attacks from the ransomware. The EternalBlue exploit also allowed the ransomware to function as a worm, searching through, and self-propagating throughout a system. The vulnerabilities that allow it to function were patched by Microsoft in 2017, but numerous systems were still using unpatched systems. This was particularly true within the healthcare sector, leaving it particularly vulnerable.

The NotPetya attacks occurred in 2017 (Graboritz et al., 2020). They were widely attributed to a team tied to the Russian Government. This attack mimicked and behaved like ransomware, but is not considered to be by some. This is because the attack was seemingly purely destructive in nature. No actual ransom could seemingly be paid to regain access to files. It was targeted primarily at systems within Ukraine, but infections spread much farther beyond. It was estimated that over 10 billion dollars worth of damages were caused by the attack.

The Colonial Pipeline ransomware attacks occurred in 2021 (Reeder & Hall, 2021). They were different when compared to the previous attacks, as they focused on a more targeted model as opposed to a more primitive but widely targeted model. The attacks targeted key U.S. infrastructure, including the Colonial Pipeline. The attack heavily disrupted the U.S. economy for a time, as Colonial Pipeline had to shut down 5,500 miles of pipelines. Colonial Pipeline was forced to pay $4.3 million in ransom. Federal authorities did eventually secure $2.9 million of the ransom back, but the remaining amount was seemingly successfully obtained and kept by the attackers.

Two separate methods of operation are usually proposed within most sources that are focused on how to protect against ransomware. The first path would be geared towards what an individual, team, or organization can do and implement to protect from ransomware. The second path is more geared towards national-level policy suggestions and directives, and how the government itself can nationally implement a better safety environment.

The smaller-scale path usually contains many best practices, routines, and general suggestions. Firstly, one could protect against ransomware more effectively by knowing what to avoid and exclude. Many ransomware attacks are spread through phishing via email (Richardson & North, 2017). On an individual level, users should simply avoid suspicious emails, especially those containing links and attachments. On the organizational level, organizations and businesses should cultivate this type of behavior through training. Behind the scenes, it is recommended that organizations have a standardized ad-blocking program to help block malicious email components. Forwarding email through the Gmail service is also known to help, as it is often effective at filtering out many forms of ransomware. These are such incredibly important steps, as in 2016 alone, it was estimated that 93% of phishing emails contained ransomware of some kind, up from around 60% in 2015. In addition to the organization implementing and installing software to help, it is also vital that organizations keep all software patched and up-to-date. This is not only limited to operating systems, but to third-party software packages as well.

Another important recommendation is to both design and implement a solid scheme for backing up data (Richardson & North, 2017). Crypto ransomware, as discussed previously, often leaves the systems themselves operational, but the data encrypted (Beaman et al., 2021). This development leaves open the opportunity for up-to-date backups of data to simply replace the encrypted data, thus bypassing the need to pay a ransom (Richardson & North, 2017). There are a number of issues and concerns to consider when it comes to backups, however. Firstly, some ransomware will worm its way through a system, attempting to infect other devices, including those holding the backups (Anderson, 2016). A possible option to consider here, in addition to an online cloud-based backup service, is a network-attached storage, or NAS device. These devices are designed to not become infected or compromised when other devices on the network would. This means multiple backups, backups disconnected from the system, and/or cloud backups also need to be considered. In addition, some ransomware stays dormant for some time (Richardson & North, 2017). This could potentially cause the files to be encrypted before the ransomware is discovered, thus compromising the backup. All these considerations would require a cost-benefit analysis to balance multiple backup methods, standards, procedures, and frequency, along with software and hardware, in a way that would meet the goals of an organization.

While recommendations for best practices following the second, but broader, path to protecting against ransomware are scarcer, some quality suggestions have come forth. One such recommendation was published by the Army Cyber Institute in response to the aforementioned devastating Colonial Pipeline attacks (Reeder & Hall, 2021). At the heart of the recommendation was a call to action derived from what was seen as a lack of decisive action and leadership by the U.S. government as a whole. The address called for “clear, executable legislation and inspired leadership”, in addition to an embracement of further public-private partnerships. This would require a more serious regard for the cyber threats the nation faces as challenges that must be tackled without delay. To do this, it is also recommended to more closely integrate and streamline the agencies and players in the government already operating against cyber threats, to face the cyber threat as a unified coalition.

In conclusion, ransomware is a form of malware that removes access to important parts of a system, and thus allows the attacker to extort the victim for monetary gain (Richardson & North, 2017). Ransomware comes in three main forms, however, locker ransomware, which locks you out of the system entirely, has been replaced in prominence by crypto ransomware, which encrypts the data on the system itself, without impacting access to a device (Beaman et al., 2021). This development has come into being in part because the currency exchange method of choice for most ransomware is some form of cryptocurrency (Oosthoek et al., 2023). Ransomware has numerous ways it can operate and infect a device, with the most common being via email phishing, and it will typically follow through six phases in total (Aldauiji et al., 2022). These are the infecting a device during the infection stage, installing itself onto a device during the installation phase, establishing communication back to the attacker during the communication phase, executing the encryptions and removing of access during the execution phase, displaying the ransom note and negotiating for ransom in the extortion phase, and potentially decrypting data and restoring access after payments have been made in the emancipation phase. Ransomware historically has come in many forms, but has done considerable damage during notable attacks like the 2017 WannaCry attacks, and the 2021 Colonial Pipeline attacks (Reeder & Hall, 2021; Harkins & Freed, 2018). In order to properly protect from the highly sophisticated attacks, and to mitigate or bypass those aforementioned devastating damages, individuals, organizations, and nations as a whole should follow various recommended practices and procedures (Richardson & North, 2017). At the heart of each of these practices seems to be a call to prioritize and elevate cybersecurity to a much more revered and essential place.

References

Aldauiji, F., Batarfi, O., &amp; Bayousef, M. (2022). Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. *IEEE Access*, 10, 61695–61706. https://doi.org/10.1109/access.2022.3181278

Anderson, W. H. (2016). PROTECTING YOURSELF FROM RANSOMWARE AND CYBER-ATTACKS. *GPSolo*, *33*(5), 48–51. http://www.jstor.org/stable/44736964

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, 111, 102490. https://doi.org/10.1016/j.cose.2021.102490

Graboritz, B. D., Morford, J. W., & Truax, K. M. (2020). Why the Law of Armed Conflict (LOAC) Must Be Expanded to Cover Vital Civilian Data. *The Cyber Defense Review*, *5*(3), 121–132. https://www.jstor.org/stable/26954876

Harkins, M., & Freed, A. M. (2018). The Ransomware Assault on the Healthcare Sector. *Journal of Law & Cyber Warfare*, *6*(2), 148–164. http://www.jstor.org/stable/26441292

Loman, M (2019). How Ransomware Attacks, A Sophos Labs white paper. https://www.sophos.com/enus/medialibrary/PDFs/technical-papers/sophoslabsransomware-behavior-report.pdf.

Morse, E. A., & Ramsey, I. (2016). Navigating the Perils of Ransomware. *The Business Lawyer*, *72*(1), 287–294. https://www.jstor.org/stable/26419124

Oosthoek, K., Cable, J., &; Smaragdakis, G. (2023). A tale of two markets: Investigating the ransomware payments economy. *Communications of the ACM*, 66(8), 74–83. https://doi.org/10.1145/3582489

Reeder, J. R., & Hall, T. (2021). Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *The Cyber Defense Review*, *6*(3), 15–40. https://www.jstor.org/stable/48631153

Richardson, R., & North, M.M. (2017). Ransomware: Evolution, Mitigation and Prevention. International Management Review, 13, 10. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs