School of Cybersecurity

Cybersecurity

CYSE 280_23588

Justin Landolina

UID: 01214163

Ransomware: What Is It and How to Defend Against It

Abstract

This paper aims to give readers a greater understanding of what ransomware is and how it works. We will look broadly at the two primary types of ransomware, locker and crypto, with a focus on crypto. I will layout a high-level view of how a ransomware attack takes place. Followed by an analysis of the types of encryption that ransomware might deploy. Next I will make an argument as to why people should be concerned, brief origins followed by major cases and impact. The paper will conclude with what one can do to protect themselves or their organizations from ransomware.

Key words: ransomware, malware, encryption, hacker

Introduction. Ransomware is a type of malware that infects a person's computer preventing access to the machine or files until a ransom is paid. Over the past decade ransomware attacks have been increasing rapidly. Hundreds of millions of dollars of ransom are being paid each year. Threat acters are unleashing ransomware attacks on public infrastructure. Therefore, it is more important now than ever before to understand the scope of the problem, and understand what ransomware is and how an attack might play out. Once all of this is understood users and organizations can lay a framework for defense.

Types of Ransomware. There are two primary types of ransomware, locker and crypto. Locker ransomware is a type of malware that blocks computer functions, locking users out of their device. Crypto ransomware encrypts users' personal files and threatens to delete them. In both instances victims are extorted for money to gain access back to their files or computer. This payment is usually made using cryptocurrency and it is estimated that ransomware extorts hundreds of millions of victims every year. For the scope of this paper, we will look more closely at crypto ransomware.

Ransomware Attack: Access. A ransomware attack begins first by threat actors gaining access to a computer network. They are able to do this through a variety of methods, some of which include deploying stolen passwords, phishing attacks, or brute force using intrusion software (Mehrotra, 2021). Ransomware attached to phishing emails is a common intrusion technique. There are cases where employees use the same password across multiple accounts. If

one of those accounts becomes compromised and the password is sold on the dark web threat actors can go from having access to a user's private/personal account to access to an entire corporate network. We will see this play out later on in one of the largest ransomware attacks to date.

Ransomware Attack: Intel. Once access is gained a hacker will either exploit this or sell their key to other bad acters (Mehrotra, 2021). There are groups across the globe that work developing ransomware. These groups will either carry out the attack themselves or sell the malware to other cybercriminals. With network access and ransomware obtained, the reconnaissance phase begins. The group who carries out the attack could be the hacker who gained access or a criminal syndicate that developed the ransomware or an entirely separate group (Mehrotra, 2021). The threat actor will sit on the network, for sometimes months, identifying the most important data. Once the attacker has gathered sufficient information they will execute the ransomware to encrypt the data.

Ransomware Attack: Aftermath. Once this occurs it is very hard for victims to gain access to their files without payment. However, there are a few resources available. The victim company could hire security services from companies like CrowdStrike who will help determine the source of the network compromise. Doing so won't necessarily restore access but it can prevent re-entry, and if backups are secure could result in restoration without payment (Mehrotra, 2021). If payment is required insurance will typically cover the expense and payout using cryptocurrency. Once completed the victims should receive a decryption key to regain access.

Encryption. What makes ransomware so powerful is in large part due to the strength of encryption. Advanced Encryption Standard (AES) is a type of encryption that uses symmetric keys, meaning the same key is used for encryption as well as decryption. AES is the encryption standard used by the United States government and with a key of 256-bits or higher it becomes near impossible to crack (Marinho, 2020). There is also asymmetric encryption that uses two different keys, a public and private key. The public key is used to encrypt while the private key is used to decrypt. A popular form of this encryption standard is Rivest, Shamir, Adleman or RSA (Marinho, 2020).

Encryption and Ransomware. The method of encryption used by ransomware can be broadly explained as a combination of the two encryption standards previously mentioned. It starts by generating a public encryption key and embedding it in the ransomware. Then, once the ransomware is activated it will encrypt victim's files using AES with a randomly generated symmetric key (Marinho, 2020). To prevent access to this now valuable symmetric key the program uses the embedded public key in the software to encrypt the random symmetric key. A threat actor might use RSA asymmetric encryption to accomplish this. The result is the threat actors private key becomes the only one that can decrypt the original symmetric key used to encrypt the victim's computer. Therefor the only one who can retrieve files. This layered encryption method is known as hybrid encryption (Marinho, 2020). The result is a small asymmetric ciphertext (key) as well as the symmetric ciphertext of the victim's data.

Origins. Ransomware has been around for a long time. The first documented attack was in 1989 (Dossett, 2021). The virus is referred to as the AIDS Trojan. In this case a threat actor distributed thousands of floppy disks containing a trojan virus at the World Health Organization AIDS conference in Stockholm titled "AIDS Information - Introductory Diskettes". This virus was designed to count the number of times a computer booted up and once that number hit 90 the virus hid all the directories and encrypted the filenames until a ransom of $189 was paid (Dossett, 2021). In this first instance the decryption process was able to be solved and security researchers released a free tool to help victims (Dossett, 2021).

Rise of Ransomware. The first attack in 1989 is not cause for much alarm, patches were released, and victims' files restored. However, over the years ransomware technology has become more sophisticated. Between 2014-2016 there was a marked increase in major ransomware attacks, partially due to the rise of the Internet of Things (IoT). IoT devices like Smart T. V's or refrigerators broadened the attack surface giving criminals new ways of infiltrating computer systems (Humayun et al., 2021). Some of these new types of Ransomware include Cryptowall (versions 1.0 to 4.0), TelsaCrypt, Linux.Encoder, Locky and mamba (Humayun et al., 2021). These programs used encryption methods like AES and/or RSA and could not be cracked so simply. In most cases users must pay or lose their files. Although payment does not guarantee one's files will be returned.

Notable Cases. Ransomware attacks from this time period start to show how powerful ransomware can be. One is the attack on the San Francisco public transportation system. Using the mamba malware hackers were able to target the whole hard disk of government computers (Mehrotra, 2021). The hard disk could then only be decrypted by a hacker after payment. Another example, more recently and more impactful, is the attack on the Colonial Pipeline, the largest fuel pipeline in the United States. In April of 2021 hackers were able to gain access to the network of the Colonial Pipeline though a compromised user account. The password for the account was discovered inside a group of leaked passwords on the dark web (Mehrotra, 2021). As mention before, in this case it appears that the employee used the same password on another account that was previously hacked. The resulting ransomware attack caused panic and fuel shortages across the East Cost of the U.S.

Financial Impact. It is important for users and organizations to understand the scope and impact of ransomware. Only once the threat is respected can one move to completely defend against it. The example of the Colonial Pipeline is one, if not the largest, ransomware attack on critical infrastructure (Lee, 2021). However, every year there are thousands of attacks that do not get publicity. Organizations quietly paying out large sums of money. 66 percent of organizations reported significant loss of revenue following a ransomware attack and in 2020 alone it is estimated that ransomware victims paid out $350 million (Lee, 2021). It is not just business or organizations being impacted. Individual users are at risk themselves or impacted at home by the attacks on larger enterprises.

Security: Backups. The first way users and organizations can protect against ransomware is to have robust data backups, and a recovery plan. It is not enough just to have these in place, enterprises must also perform regular tests to limit impact. It is important to note that if system backups are network-connected they can be affected by ransomware. Critical backups should be isolated from the network (Ransomware and Recent Variants | CISA, 2021). In the event of a ransomware attack, once the breech has been discovered and secured, critical data can be restored from backup.

Security: Software. A good security practice for organizations is application whitelisting. The idea behind whitelisting is that only approved programs are able to run. Applications that are deems acceptable are given privileges to operate, while all others are

blocked. This includes blocking malicious software (Ransomware and Recent Variants | CISA, 2021). Another software line of defense users and business will want to have is an anti-virus program. As a rule, any software or file downloaded from the internet should be scanned with the anti-virus before the program is executed (FAQ - Ransomware | Information Security Office, 2021). With these actions an unwanted program will not be able to run.

Security: Passwords. The most popular way organizations authenticate their users is through passwords, which are fraught with problems. It is common for employees to reuse passwords, choose weak ones, or store them in unsafe areas. As we saw before some of the most damaging ransomware attacks occurred because of compromised user passwords. A way to combat this is with a password policy. Setting parameters for what passwords are acceptable and how often they can be reused helps limit risk. While this does not solve the problem outright it can strengthen security. Adding two factor authentication is another way to bolster password security. Requiring employees to carry something with them for authentication makes it considerably harder for a hacker to access that account even if they know the user password.

Security: Updates. Organizations should keep computer operating systems and software up to date. A large number of software patches are designed to repair vulnerabilities. Vulnerable applications and operating systems are the target of most attacks (Ransomware and Recent Variants | CISA, 2021). It is important that anti-virus software is kept up to date. Anti-virus software relies on threat intelligence, a composition of known threats and how they can be identified. If this information is not current new threats will be able to slip past the anti-virus scan.

Security: Users. A major vulnerability in organization security is the user. Businesses spend a considerable amount of resources training users on best practices for internet usage, and for good reason. Social engineering is a popular method for hackers to infiltrate computer networks. Included in this category are phishing emails, one of the most common tools used to deliver ransomware (Ransomware and Recent Variants | CISA, 2021). Therefore, it is critical that users understand how to recognize phishing attempts. Additionally, users have to be trained to understand all forms of social engineering. This is an extremely difficult task as most organizations are comprised of employees ranging all levels of computer literacy.

Conclusion. Over the past decade there has been a marked increase in ransomware attacks. Today, ransomware is at an all time high, with some of the most damaging attacks happening in the past few months. While there are many forms of cyberattacks organizations should be aware of I believe ransomware needs to receive the most attention. Threat actors can see the success of recent ransomware attacks; prompting more to try it. With the tools to do so available for purchase on the dark web hackers with a wide range of skill levels are able to launch attacks. With the tools to attack readily available, and the success of these attacks at an all-time high, ransomware knowledge and defense should be at the forefront of organizationally cybersecurity.

Works Cited:

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

Dossett, J. (2021, November 15). *A timeline of the biggest ransomware attacks*. CNET. Retrieved November 19, 2021, from https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/

Frequently Asked Questions - Ransomware | Information Security Office. (2021). Security.Berkely. Retrieved November 19, 2021, from https://security.berkeley.edu/faq/ransomware/

Humayun, M., Jhanjhi, N., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Lee, N. (2021, June 10). *As the U.S. faces a flurry of ransomware attacks, experts warn the peak is likely still to come*. CNBC. Retrieved November 18, 2021, from https://www.cnbc.com/2021/06/10/heres-how-much-ransomware-attacks-are-costing-the-american-economy.html

Marinho, T. (2020, March 20). *Ransomware encryption techniques - Tarcísio Marinho*. Medium. Retrieved November 17, 2021, from https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9

Mehrotra, K. (2021, June 15). *Bloomberg - The Anatomy of a Ransomware Attack*. Bloomberg. Retrieved November 15, 2021, from

https://www.bloomberg.com/news/newsletters/2021-06-15/the-anatomy-of-a-ransomware-attack

Ransomware and Recent Variants | CISA. (2021). CISA. Retrieved November 19, 2021, from https://us-cert.cisa.gov/ncas/alerts/TA16-091A