AIRGAP

THE RANSOMWARE FUNDAMENTALS

Table of Contents

1 Part 1:
THE HISTORY OF RANSOMWARES

2 | How Ransomware Attacks Operate

3 | The First Ransomware Attack

3 | The Evolution of Ransomware

4 | The Biggest Ransomware Attacks and Most Prominent Variants

---

6 Part 2:
THE BASICS OF RANSOMWARE PROTECTION

7 | Stop Ransomware Attacks

7 | Ransomware Attack Prevention Tips

9 | Ransomware Prevention is Better than the Cure

---

10 Part 3:
THE TRADITIONAL METHODS TO IDENTIFY AND BLOCK RANSOMWARES

10 | Detecting a Ransomware Infection

Part 1

THE HISTORY OF RANSOMWARES

Ransomware has been a notable threat to enterprises, SMBs, and people alike since the mid-2000s. In 2017, the FBI's Internet Crime Complaint Center (IC3) sustained 1,783 ransomware complaints that cost victims over $2.3 million[1]. Those grievances, however, represent only the attacks reported to IC3. The actual amount of ransomware attacks and costs are much higher. There were an approximated 184 million ransomware attacks[2] last year alone. Ransomware was intended to target individuals.

In this three-part series on Ransomware, we will discuss the evolution of ransomware, how to recognize it, and how to (try to) curb it. We will be offering an in-depth analysis of these topics giving you an understanding of how ransomware has become a part of our lives and how we have to navigate the constantly threatening landscape.

Ransomware[3] is malicious software that obtains access to files or systems and blocks user access to those files or practices. Then, all files, or even complete devices, are held captive using encryption until the victim pays a ransom in exchange for a decryption key. The key permits the user to access the files or regularities encrypted by the program.

While ransomware has stayed around for decades, ransomware varieties have grown increasingly developed in their capabilities for spreading, evading detection, encrypting files, and forcing users into paying ransoms. New-age ransomware includes a combination of advanced distribution applications such as pre-built infrastructures used to easily and widely distribute new types and advanced development techniques such as applying crypters to ensure reverse-engineering is extremely difficult. Additionally, offline encryption methods are becoming popular in which ransomware takes advantage of legitimate

[1] *https://pdf.ic3.gov/2017_IC3Report.pdf*
[2] *https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide*
[3] *https://searchsecurity.techtarget.com/definition/ransomware*

system features such as Microsoft's CryptoAPI, eradicating the need for Command and Control (C2) communications.

With ransomware holding constant as one of the most significant threats facing businesses and people today, it is no shock that attacks are becoming frequently sophisticated, more challenging to prevent, and more damaging to their sufferers.

How Ransomware Attacks Operate

Let us now go over a more comprehensive way of how these malicious programs gain entry to a company's files and systems. The word "ransomware" describes the software's function, which is to extort users or companies for financial gain. However, the program has to obtain access to the files or system that it will hold ransom. This passage happens through infection or attack vectors.

Malware and virus software share connections to biological illnesses. Due to those similarities, considered entry points are often called "vectors," much like the world of epidemiology applies the term for carriers of harmful pathogens[4]. Like the biological world, there are numerous ways for systems to be corrupted and consequently ransomed. Technically, an attack or infection vector is how ransomware receives access.

A common method of deception employed to distribute ransomware is sending a compelling reason for companies to open malware camouflaged as an urgent email attachment. If an invoice comes to a business proprietor or the accounts payable department, it is expected to be opened. Like many related in this list, this tactic involves deception to gain access to files and systems.

Another means of subterfuge employed by ransomware assailants is to message victims on social media. One of the most obvious channels used in this approach is Facebook Messenger. Accounts that impersonate a user's current "friends" are created. Those accounts are utilized to send messages with file attachments. Once removed, ransomware could gain access to and lockdown networks connected to the infected device.

[4] *https://en.wikipedia.org/wiki/Vector_(epidemiology)*

Another popular, yet older, ransomware vector is the online "pop-ups." Pop-ups are made to ridicule currently-used software to feel more comfortable following indicates, ultimately designed to hurt the user.

The First Ransomware Attack

While ransomware has maintained distinction as one of the biggest threats since 2005, the first attacks transpired much earlier. According to Becker's Hospital Review, the first acknowledged ransomware attack occurred in 1989 and targeted the healthcare industry[5]. Twenty-eight years later, the healthcare area remains a top target for ransomware attacks.

The first known attack was launched in 1989 by Joseph Popp, Ph.D., an AIDS researcher, who attacked by disseminating 20,000 floppy disks to AIDS researchers spanning more than 90 nations[6], claiming that the disks contained a program that analyzed an individual's opportunity of acquiring AIDS through the utilization of a questionnaire. However, the disk also consisted a malware program that originally remained dormant in computers, only activating after a computer was powered 90 times. After the 90-start threshold was relinquished, the malware displayed a message demanding a payment of $189 and another $378 for a software lease. This ransomware attack became recognized as the AIDS Trojan[7], or the PC Cyborg.

The Evolution of Ransomware

Of course, this primary ransomware attack was rudimentary at best, and reports symbolize that it had flaws, but it did set the juncture for the evolution of ransomware into the involved attacks carried out today.

Early ransomware developers typically wrote their encryption code. Still, today's attackers are frequently reliant on "off-the-shelf libraries that are significantly harder to crack." They are leveraging more complicated delivery systems such as spear-phishing campaigns[8] rather than the traditional phishing email blasts, which are generally filtered out by email spam filters today.

Some of the most advanced cybercriminals are monetizing ransomware by allowing ransomware-as-

---

[5] *https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html*
[6] *https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html*
[7] *https://www.knowbe4.com/aids-trojan*
[8] *https://digitalguardian.com/blog/dont-get-hooked-how-recognize-and-avoid-phishing-attacks-infographic*

a-service programs[9], which has led to the rise in well-known distinction ransomware like CryptoLocker, CryptoWall, Locky, and TeslaCrypt.

After the first documented ransomware attack in 1989, this kind of cybercrime persisted uncommon until the mid-2000s, when attacks began utilizing more complicated and tougher-to-crack encryption algorithms such as RSA encryption. Popular during this time were Gpcode, Cryzip, Archiveus, TROJ.RANSOM.A, Krotten, and MayArchive[10]. In 2011, a ransomware worm appeared that imitated the Windows Product Activation notice, making it more challenging for users to tell the difference between genuine notifications and warnings.

By 2015, multiple variants affecting multiple platforms were wreaking havoc on users around the world. Kaspersky's SecureList states that from April 2014 to March 2015, the most prominent ransomware threats were CryptoWall, Cryakl, Scatter, Mor, CTB-Locker, TorrentLocker, Fury, Lortok, Aura, and Shade.

The Biggest Ransomware Attacks and Most Prominent Variants

Given ransomware and attack campaigns' progression, it's not surprising that the most significant ransomware attacks have occurred in recent years. Ransom demands are also on the rise. 51% of businesses were targeted by ransomware. There was a 40% surge in global ransomware, encompassing 199.7 million hits. By the end of 2020, ransomware costs have almost reached $20 billion for all businesses. The average ransomware payment demand was $233,817 in Q3 2020[11].

1. From April 2014 through early 2016, CryptoWall was among the most commonly employed ransomware varieties, with various ransomware forms targeting hundreds of thousands of people and businesses. By mid-2015, CryptoWall had extracted over $18 million from victims, prompting the FBI to release an advisory on the threat;
2. In 2015, a ransomware variety identified as TeslaCrypt or Alpha Crypt hit 163 victims, profiting $76,522 for the attackers behind it[12];
3. 2015 witnessed a group known as the Armada Collective carried out a string of attacks against

---

[9] *https://www.businessinsider.in/tech/there-are-now-programs-that-anyone-can-use-to-extort-money-from-you/articleshow/50211904.cms*
[10] *https://www.nomoreransom.org/ransomware-qa.html*
[11] *https://heimdalsecurity.com/blog/ransomware-payouts-of-2020/#:~:text=51%25%20of%20businesses%20were%20targeted,in%20Q3%202020%20(source)*
[12] *https://www.digitaltrends.com/computing/teslacrypt-ransomware-grows-as-victims-pay-up/*

Greek banks. “By targeting these three Greek financial institutions and encrypting important files, they hope to persuade the banks into paying the sum of €7m each. It goes without saying that, being able to pull three different types of attack over the course of five days, is quite worrying regarding bank security,” reported Digital Money Times[13].

4. In March 2016, Ottawa Hospital was hit by ransomware that impacted more than 9,800 machines[14] – but the hospital responded by wiping the drives. Thanks to diligent backup and recovery processes, the hospital could beat attackers at their own game and avoid ransom. That same month, Kentucky Methodist Hospital, Chino Valley Medical Center, and Desert Valley Hospital in California were hit by ransomware.
5. One of the first ransomware variants to target Apple OS X also emerged in 2016. KeRanger[15] mostly impacted users utilizing the Transmission application but affected about 6,500 computers within a day and a half[16].

2016 was a major year for ransomware attacks, with reports from early 2017 calculating that ransomware netted cybercriminals a total of $1 billion[17]. These events are catapulting ransomware into a new era, one in which cybercriminals can efficiently replicate smaller attacks and carry them out against much larger corporations to necessitate larger ransom sums.

---

[13] *http://digitalmoneytimes.com/armada-collective-targets-greek-banks-bitcoin-ransomware/*
[14] *https://www.welivesecurity.com/2016/03/14/ottawa-hospital-computers-infected-ransomware-virus/*
[15] *https://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/*
[16] *https://www.latimes.com/business/hiltzik/la-fi-mh-2016-is-the-year-of-ransomware-20160308-column.html*
[17] *https://www.csoonline.com/article/3154714/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html*

Part 2

THE BASICS OF RANSOMWARE PROTECTION

Ransomware is malicious software used by cybercriminals to encrypt important data from your computer and extract money from you in exchange to regain admittance to your data. Ransomware is a notorious malware that not simply attacks home computers but even systems of high-profile companies, including those from the education, IT, healthcare, and commercial service industries. In the second part of the three-part series on Ransomware, we will be reading few pointers on how would be possible to mitigate ransomware damage.

Over the last few years, ransomware has converted into a lucrative scheme for cybercriminals and proceeds to intensify as a persistent problem for individuals and businesses. Cybercriminals discarding their old schemes in favor of this malicious software, studying to prevent ransomware attacks from happening should be in preeminence.

No one is protected from ransomware. No matter who or where you are, and regardless of what industry your company refers to, as long as you have data saved in your system that you can't manage to lose, you are not safe from the outrageous skills and minds of cybercriminals...

According to Positive Technologies' third-quarter 2020 cyber threatscape report, ransomware attacks now account for over half of all malware attacks (51% in Q3 compared to 39% in Q2). Additionally, half of all attacks against health care institutions during the quarter involved ransomware, which tragically included the first fatality from a ransomware attack against a hospital in Germany[1].

[1] *https://www.sdxcentral.com/articles/news/mcafee-citrix-microsoft-back-ransomware-task-force/2020/12/*

Stop Ransomware Attacks

There are two types of Ransomware currently in distribution. The first one is called encrypting ransomware, which is the more popular. Encrypting ransomware is created to block system files and ask the victim for payment in exchange for the passkey required to unlock the encrypted data. The second one is identified as the locker ransomware. Though cybercriminals will demand money from you, locker ransomware does not encrypt any data at all but locks your operating system and prevents you from accessing your desktop or any file.

For example, household users are a significant target of ransomware creators due to their lack of knowledge about cybersecurity awareness. This makes them easier to manipulate into agreeing to any malicious link that can infect their computers. On the other hand, companies also are not off the hook from ransomware attacks. They are far more effective than household users and become an excellent victim in the ransomware creators' eyes. Indeed, everyone must be aware of blocking ransomware attacks effectively.

Just like other malicious software, though, ransomware gains away to a victim's system by utilizing a vulnerable software's security hole or by tricking a possible victim into downloading or installing it. I bet even now, and someone is clicking a malicious link that will download the ransomware into that user's computer and encrypt all his data after a few minutes.

With these startling facts about how dangerous ransomware attacks can be, you must implement yourself with adept understanding to prevent a ransomware attack. Don't wait till a threat strikes and make you the next ransomware victim. Make yourself well-informed about this malware and learn the methods to block ransomware.

Ransomware Attack Prevention Tips

1. Patch and update your software

To block ransomware attacks, make sure that all systems and software are updated. Computers operating with outdated software are more prone to an attack. Updated software can significantly decrease the possibility of ransomware resulting in any damage to your data. Most vendors usually

release security updates and patches at regular intervals. It would be best to enable automatic updates for your software to ensure that your software will always be up-to-date.

2. Don't click unfamiliar links and emails

Another way on how to block Ransomware attacks is to be vigilant about clicking unknown links and emails. Spam email campaigns are one of the most basic infection methods attackers employ. These emails contain malicious links or attachments that can download the ransomware to your computer. Take note to perpetually think twice before clicking so you can keep infected links and other ill-disposed sources away from your computer and important data.

3. Backup your files

Finally, make sure that you continually back up your files (especially the most important things). Regularly backing up your files is your most suited remedy when ransomware has affected your computer. This method might not keep ransomware attacks away from your computer, but it will make the damage significantly more limited as you don't need to deal with the attacker anymore to recover access to your encrypted content.

Being one of the most critical and widely spread malware on the planet, ransomware undeniably brought corruption on a global scale. With this malware threat, you must exert widespread precautions to prevent ransomware attacks from circumventing data loss and malware-related infection.

Never let any malicious file stay in your computer to prevent ransomware attacks from hitting you and obstruct trading with cybercriminals that can potentially cause you to lose a lot of money.

4. Don't download apps from unknown sources

When you need to download apps to your system or mobile device, stick with trusted sources. While there are genuine online marketplaces for PC and Mac, such as CNET's Download.com and Steam, third-party mobile app stores have earned a reputation for being rife with scams.

For example, to add an extra layer of security, go into your device's settings and disable its ability to

perform app installations from unknown sources. You should also be suspicious if an app asks for device administrator permission. Granting this permission enables the app's owner to access your device, which is a terrible idea remotely.

5. Be wary of pop-up installation requirements

Pop-ups are hardly your friends. Whenever you get a pop-up request to update or download and install software or a plug-in when you are online, close the pop-up without exerting any action. Vigilance is vital to blocking ransomware from infiltrating your devices and networks.

The next time you are on a site that casts up a notice that you need, for example, an Adobe Flash update to see the site's content, get the latest version directly from the source. This pertains to any software update pop-ups.

Ransomware Prevention is Better than the Cure

While getting free of ransomware and recovering your files is possible in some cases, it can be not simple. And note that we said "some cases", since only some strains have available, publicly available decryption keys. And since ransomware attacks are so lucrative, cybercriminals are constantly developing new strains.

Remember always to stay up to date, practice safe surfing, back up regularly, save to the cloud and external hardware. All of these practices will assist in keeping your devices and files safe and your mind at ease.

Part 3

THE TRADITIONAL METHODS TO IDENTIFY AND BLOCK RANSOMWARES

Ransomware remains to be a significant threat to organizations of all sizes[1]. Victims of an attack are refused access to their data. Numerous times, files are encrypted, and a ransom is necessitated to restore access. If hit, the best-case situation is to have clean backups to restore your systems and avoid giving the ransom. However, downtime is often more damaging than ransom costs. Recovery is costly, and there is a significant cost in system downtime, emergency acknowledgment, and reputation damage.

In this final part of our three-part Ransomware series, we are going to present a few traditional techniques to possibly identify an infection before encryption even starts.

Detecting a Ransomware Infection

The traditional and legacy systems for identifying Ransomware, were looking for basic symptoms of an attack:

1. Watch out for known file extensions

Even though the list of identified ransomware file extensions is growing rapidly, it was a valuable method for detecting suspicious activity. You could require to get file activity monitoring in place to have both a real-time and legacy record of all file and folder activity on your network file shares.

2. Watch out for enhanced file renames

File renames are not a common action when it appears to activity on network file shares. Over a typical day, you may end up with just a handful of renames, even if you have numbers of users on

[1] *https://www.k2e.com/articles/blackbaud-ransomware-attack/#:~:text=Ransomware%20remains%20a%20genuine%20threat,organization's%20reputation%20lasts%20for%20years.*

your network. When ransomware strikes, it could appear in a massive increase in file renames as your data gets encrypted.

You can apply this behavior to trigger an alert. However, if the number of renames goes above a definite threshold, you have a potential ransomware issue. The traditional systems normally did look for anything above four renames per second, or something like that.

3. Create a sacrificial network share

Ransomware usually looks for local files first, then moves onto network shares. Most variants are typically going through the network shares in alphabetical order: G: drive, then H: drive, to name a few.

Some traditional protection system was using an early drive letter like E:, something that occurs before your proper drive mappings. The network share should be put up on old, idle disks and contain thousands of little, random files. When doing small, random files, there's no simple way to get the list of files in the right order to bypass a lot of seeking around the disk. Depending on how it is executed, the cipher might need to be re-initialized for each file, which slows down the encryption process.

One could also set up an alert that triggers if a particular file was accessed somewhere within the network share. This would be an inevitable sign that something was going through your file shares.

4. Updating IDS systems with exploit kit detection methods

Many IDS, IPS, and firewall arrangements come with exploit detection features. Exploit kits are utilized to get ransomware onto a client through malspam or via discredited websites.

Two of the most prevalent exploit kits (EK) associated with ransomware are the Neutrino EK and the Angler EK[2]. Check if your network security monitoring systems are up-to-date and recognize if they have the capability to detect exploit kits.

[2] *https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit*

5. Use client based anti-ransomware agents

Many organizations have published anti-ransomware software applications. These are created to run in the background and block attempts by ransomware to encrypt data. They also monitor the Windows registry for text strings recognized to be associated with ransomware.

Researchers are also examining methods to "crash" computer systems when droppers are detected. Droppers are little applications that first infect target machines in improvement for downloading the main malware payloads. This will reasonably mean that the system is sent to IT, where the attack should be identified.

It would benefit if you also informed your network users to avoid installing agents themselves. There is additionally much of a risk that they will introduce the wrong agent or install more malware on their systems.

6. Getting your data decrypted

The infosec industry lately rallied around a common goal to combat ransomware under the No More Ransom initiative[3]. While this drive's public face is the portal nomoreransom.org, where almost 100 decryption tools are provided free to anyone who may have the disadvantage of being a ransomware victim, the action is a true collective of organizations and law enforcement agencies fighting ransomware and those behind such cowardly attacks.

You should attempt your best to avoid a ransomware attack. However, sometimes it is difficult to prevent this attack. You should regularly scan your system. If your antivirus identifies the ransomware, then you should immediately delete the file. This might assist you in avoiding the attack.

If hackers have already got admission into your data, then you should try to minimize the data. You should immediately isolate the machine from your network. This will help you in preserving your critical assets. It would help if you tried to restore your whole system. It is significant to download all the backups. System restore can also accommodate you in recovering many files and devices. However, you should still have access to your system.

[3] *https://www.nomoreransom.org/en/ransomware-qa.html*

If you have lost admittance to your system, then you should format your whole system. It would help if you tried to connect everything from your backups. If you have already backed up the data, then this is the most suitable option for you. You can effortlessly find the most reliable restore point. This will assist you in restoring the system without paying any ransom.

It is never a great idea to pay ransom to these hackers. They will only become more motivated. There is never a guarantee that they are going to decrypt your files. According to a Symantec report, more than 53% of businesses don't get their data back after paying the ransom. Thus, you should use your money in creating a good DR plan[4].

[4] *https://docs.broadcom.com/doc/istr-21-2016-en*

REFERENCES

https://www.immersivelabs.com/resources/blog/the-evolution-of-ransomware/#:~:text=Ransomware%20has%20been%20around%20since,informational%20software%20for%20the%20event.

https://www.skyboxsecurity.com/blog/the-evolution-of-ransomware-what-to-expect-in-2020-and-beyond/

https://www.researchgate.net/publication/330734778_Understanding_the_Evolution_of_Ransomware_Paradigm_Shifts_in_Attack_Structures

https://technocomusa.com/the-evolution-of-ransomware/

https://gbievents.com/blog/trust-attacks-and-the-evolution-of-ransomware

https://www.researchgate.net/publication/326083550_Evolution_of_ransomware

https://outpost24.com/blog/How-to-mitigate-Ransomware-attacks

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

https://www.infrascale.com/wp-content/uploads/pdf/Infrascale-Steps-to-Mitigate-Ransomware.pdf

https://rightcloud.asia/6-best-practices-to-prevent-and-mitigate-ransomware-attacks/

https://www.netwrix.com/encryption_ransomware_threat.html

https://www.zerto.com/wp-content/uploads/2019/09/ransomware-mitigating-the-threat-of-cyber-security- attacks.pdf

https://www.manageengine.com/log-management/detect-and-mitigate-coronavirus-ransomware-attack.html

https://deltarisk.com/blog/how-to-deal-with-ransomware-in-2018-mitigate-the-damage-and-dont-pay-the-ransom/

https://solutionsreview.com/endpoint-security/how-to-prevent-and-mitigate-enterprise-ransomware-attacks/

https://www.mcafee.com/blogs/enterprise/cloud-security/how-to-detect-ransomware-attacking-your-cloud-data-repositories/

REFERENCES

https://brightlineit.com/detect-prevent-ransomware-attacks/

https://www.rsa.com/content/dam/en/case-study/detecting-and-responding-to-a-ransomware-attack.pdf

https://link.springer.com/chapter/10.1007/978-981-15-0790-8_2

https://www.manageengine.com/data-security/how-to/how-to-detect-ransomware-attacks.html

https://www.crowdstrike.com/endpoint-security-products/ransomware/

https://www.nakivo.com/blog/methods-tools-ransomware-detection/

https://assets.extrahop.com/whitepapers/Ransomware_Detection_and_Prevention.pdf

https://www.avertium.com/how-to-leverage-your-siem-to-detect-and-respond-to-ransomware/