RANSOMWARE

What it is, how it works, and how to protect against it

EXECUTIVE SUMMARY

Ransomware has become an unignorable presence in digital information technology. it's not a question of *if* an organization's IT will be the victim of a ransomware attack; it's a question of *when*. Everyone who relies on digital data, from personal computer users to the CIOs of large enterprises, should be aware of the potential for ransomware attacks and their consequences, which can amount to millions of dollars in payments with no guarantee that ransomed data will be recoverable, and should understand how best to guard against and recover from them.

This brief presents an overview of ransomware—its history, its evolutionary trajectory, and its mechanisms for infiltrating and attacking computers— and provides advice on protecting against and recovering from attacks. Based on extensive research and analysis by cybersecurity specialists, its goal is to raise IT practitioners' awareness of the danger ransomware poses, and suggest prevention and impact mitigation measures.

FROM HUMBLE BEGINNINGS...

In 1989, biologist Joseph Popp handed out 20,000 infected diskettes labeled "AIDS Information - Introductory Diskettes" to attendees at a World Health Organization AIDS conference.

Figure 1: The First Known Ransomware Attack

After several reboots, the "AIDS Trojan" program on the diskette would hide directories and encrypt or lock file names on the computer's system disk. To regain access, users were required to send $189 to PC Cyborg Corporation at a Panama PO box. The attack used relatively simple symmetric cryptography and tools were soon developed to decrypt files and recover from it. But the principle was established—digital data is valuable to its owners, and if it is lost to them, they will pay, and pay well, to recover it.

...TO A WORLDWIDE ECOSYSTEM

In the three decades since the PC Cyborg attack, ransomware has evolved into a sophisticated ecosystem that includes technologies for infiltrating computer systems and making stored data indecipherable, along with "attack for hire" contractors and difficult-to-trace cryptocurrency payment systems. Prime attack targets have shifted from individuals' files on personal computers to critical files and databases that enterprises rely on to conduct business. And ransom demands have mushroomed from PC Cyborg's $189 to tens of millions of dollars.[1]

RANSOMWARE THROUGH THE YEARS

Some primitive ransomware strains blocked logins to the attacked computer. Victims' computers could usually be recovered by rebooting into an operating system "safe mode." So-called "locky" ransomware did not affect data. Today, it has all but disappeared from the ecosystem.

The much more insidious and prevalent form of ransomware encrypts files that the attacker believes are valuable to the victim. In attacks on personal computers, documents, spreadsheets, images, calendars, and so forth are likely to be encrypted. In enterprise attacks, databases, large files, and object stores are the most likely encryption candidates. Today, virtually all ransomware attacks are of the crypto variety.

For about a decade after the PC Cyborg attack, ransomware attacks were relatively low-key, mostly targeting personal computers and demanding modest payments to restore files. In the early 2000s, however, there was a sharp uptick in ransomware activity. Emphasis shifted to enterprises and the data they require to operate, and attackers became more advanced technically, for example by:

- Searching the Internet to locate computers with known vulnerabilities
- Using advanced encryption techniques to make data increasingly difficult to recover without paying ransom
- Identifying and disabling or deleting backups and operating system repair tools before encrypting live data
- Including "scareware" in attacks, threatening consequences such as permanent obliteration or publication of sensitive or embarrassing data (the latter known as "doxing")
- Developing techniques for avoiding detection by antivirus software.

[1] A 2021 report by cybersecurity firm Coveware indicates that the average ransom paid by enterprise ransomware victims is currently over $200,000.

Business practices among the cybercriminal community also became more sophisticated. Along with ransom demands, attackers would:

- Promise confidentiality in exchange for prompt payment, ostensibly to avoid damage to victims' reputations
- Use anonymizing networks like Tor[2] to make interactions with victims' computers and ransom payment transactions difficult to detect and track
- Attempting to remain anonymous by demanding payment in cryptocurrencies such as bitcoin
- Use botnets to scour the Internet for systems with known vulnerabilities to identify possible attack targets. Today, cybercriminal teams even maintain botnets and rent their services to attackers[3]
- Use advanced encryption techniques to make "brute force" decryption virtually impossible (the first generally known use of RSA asymmetric encryption in ransomware occurred in 2006).

FOR EXAMPLE...

As security analysts and software developers discover and eliminate computer and network vulnerabilities, hackers evolve new, more complex ransomware strains. The evolutionary path of the well-known *Cryptolocker* strain is typical:

2013

Cryptolocker was spread by via the *Gameover Zeus* botnet,[4] which can emit millions of emails containing malicious attachments or links to infected websites.

2014

Operation Tovar,[5] a consortium of law enforcement, private sector, and academia, defeated Cryptolocker. During its short lifespan, it is believed to have attacked about 500,000 victims, of whom 1.3% paid an estimated total of $3M ransom. Victims who did not pay either recovered from backups or lost data permanently.

2 An overview of the Tor project is at https://2019.www.torproject.org/about/overview.html.en

3. https://en.wikipedia.org/wiki/Botnet

4. https://en.wikipedia.org/wiki/Gameover_ZeuS

5. https://en.wikipedia.org/wiki/Operation_Tovar

2014

Cryptolocker evolved into Cryptowall,[6] which used AES symmetric encryption to encrypt victims' files, and an asymmetric public key to encrypt the AES data encryption keys. It then sent its private key to the attacker's *command and control* (C&C) *server*, and erased itself to make discovery of the encrypted AES keys impossible.

2014

CryptoWall 2.0 was adapted to use the Tor anonymization network to make it difficult for authorities to track ransom payments, which it required to be made in bitcoin.

2015

CryptoWall 3.0 further strengthened encryption with 2048-bit RSA keys, and increased the number of file types it encrypted to over 300. In addition, it disabled virus detection and operating system repair tools, and used operating system utilities to silently delete shadow copies (online backups) of data to inhibit recovery.[7]

2015

CryptoWall 4.0 made tracking ransom payments even more difficult by replacing Tor with *Invisible Internet Project* (I2P) peer-to-peer anonymization. In addition, it encrypted filenames as well as contents, making attacks obvious to victims, and making identification of files for possible repair difficult if not impossible.

2016

CryptoWall 5.1 appeared. Researchers believe it differs significantly from earlier versions, and may be an entirely different strain, exploiting the name to gain credibility with victims.

The volume of CryptoWall attacks peaked between 2013 and 2016. Although largely supplanted by newer strains,[8] it is still occasionally found in attacks in 2021.[9]

RANSOMWARE TODAY

Today, ransomware has become a never-ending cyclic process:

- Attackers discover operating system, application, and network vulnerabilities and use them to infiltrate and install ransomware on victims' computers
- Software vendors develop patches that users apply to their computers and networks to block infiltration and malware execution
- IT users implement preventive and recovery measures, and the cycle repeats.

6. https://news.sophos.com/en-us/2015/12/17/the-current-state-of-ransomware-cryptowall/
7. https://www.sentinelone.com/blog/anatomy-of-cryptowall-3-0-a-look-inside-ransomwares-tactics/
8. https://www.bankinfosecurity.com/ransomware-landscape-notorious-revil-only-one-operator-a-17027
9. https://www.2-spyware.com/remove-cryptowall-virus.html

The ransomware ecosystem has developed to a point where cybercriminals offer botnet access and ransomware as a service (RaaS) in exchange for a share of the ransom. Today, it is technically possible for almost anyone to mount a ransomware attack on almost anyone.

During 2020 and 2021, the pace of ransomware attacks accelerated dramatically, both in terms of public visibility (Colonial Pipeline,[10] JBS Holdings,[11] Electronic Arts,[12] Revil,[13] etc.), and in terms of ransom demands. According to the previously cited Coveware report, the average ransom paid out (not demanded) increased 43% in the first quarter of 2020 to over $220,000.

And it appears that no one is exempt. A recent attack by the REvil organization (thought to be based in Russia) exploited a vulnerability in the Kaseya software,[14] widely used by both in-house IT teams and managed service providers for remote system management, to identify and attack thousands of small and medium-size businesses via a known vulnerability in a commonly-used database management application.

The IT community saw some new developments in ransomware in 2021:

- After a ransom demand was rebuffed by Electronic Arts Corporation, the attackers offered exfiltrated source code for sale to anyone for $28M.
- In the worldwide REvil attack, attackers demanded a single ransom payment of $70M, in exchange for which they promised to release a "universal decryptor." The logistics of assembling such a ransom were left up to the thousand or more victims. (The REvil group also offered victim-specific decryptors upon payment of per-victim ransoms that varied from a few thousand to hundreds of millions of dollars.)

Figure 2: A REvil Ransom Demand

Ransomware and other forms of malware have become so prevalent that governmental agencies and private sector organizations have begun to provide online catalogs of known vulnerabilities[15] to help IT operations assess the security of their operations.

10. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
11. https://en.wikipedia.org/wiki/JBS_S.A._cyberattack
12. https://therecord.media/hackers-leak-full-ea-data-after-failed-extortion-attempt/
13. https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack
14. https://www.zdnet.com/article/kaseya-ransomware-attack-faq-what-we-know-now/
15. For example, https://nvd.nist.gov/vuln

THE PATH OF A RANSOMWARE ATTACK

While there are many strains of ransomware, they all follow the general pattern shown in Figure 3 to mount and carry out attacks:

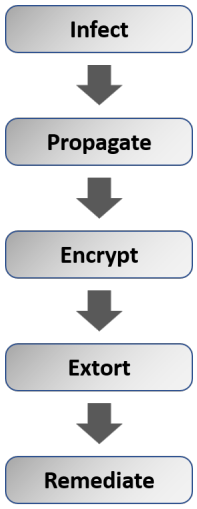

Figure 3: Attack Elements

Infect

An attacker first gains access to a victim's network either via "endpoints" (personal computers), using "phishing" emails containing malware or links to infected websites) or via "boundary" systems such as firewalls and VPNs with known vulnerabilities.

Propagate

In large enterprises, endpoints typically do not house data of significant value. The goals of an initial infection are to (a) raise the infecting software's privilege level so that it can perform actions not permitted to a normal user, (b) to discover computers that have access to valuable data and propagate ransomware to them, often using "exploit tools" readily available on the dark web.

Encrypt

The goal of a ransomware attack is to obscure valuable data in such a way that usability can be restored when ransom is paid. The usual vehicle is encryption.

Extort

Once they have made data unusable, attackers attempt to extort their victims, by demanding ransom, by exfiltrating data, by threatening to expose it publicly or to the victim's competitors, or by a combination of these.

Cryptocurrencies have been a boon to ransomware because they make it more difficult to identify payees than is the case with conventional transfers (but not impossible—about half the Colonial Pipeline ransom was recovered by the US Justice Department[16]).

Remediate

In principle, once the demanded ransom has been received, the attacker delivers the wherewithal to decrypt the user's data, typically one or more decryption keys, usually accompanied by decryption software and instructions for use.

This step is fraught with risk for the data owner:

- The data owner must perform the recovery. Having been paid, the attacker has no motivation to help, and may or may not provide technical support[17]

16. https://krebsonsecurity.com/2021/06/justice-dept-claws-back-2-3m-paid-by-colonial-pipeline-to-ransomware-gang/
17. One source reports that nearly half of victims surveyed did not recover data after paying ransom. (https://cloudian.com/lp/ransomware-victims-report-

- The attacker may have exfiltrated (copied) data before encrypting it, and may at some later time threaten to expose it publicly if additional payments are not made
- The attacker may strike again at a later time, either mounting a new attack or activating malware planted in the user's computers during the original one.

Thus, experts, including the US Federal Bureau of Investigation,[18] generally advise against paying ransom after a successful attack, although without other means of recovering data, payment, even if risky, may be a victim's only practical option. The subsections that follow describe different ways in which strains perform the basic tasks.

How Attackers Infiltrate

Ransomware attacks usually begin by infiltrating victims' endpoint computers or "boundary" systems. Typical endpoint infiltrations include:

Electronic mail

Infiltration often begins with email to users of a potential victim's network using social engineering techniques collectively called *phishing*. Phishing emails appear to come from legitimate sources, but in fact contain web links or attachments that attempt to install malware on the recipient's computer. Their general intent is to persuade recipients to open an attachment that contains malware or visit an apparently legitimate website that attempts to download malware or harvest user credentials for access to the intended victim's computers.[19]

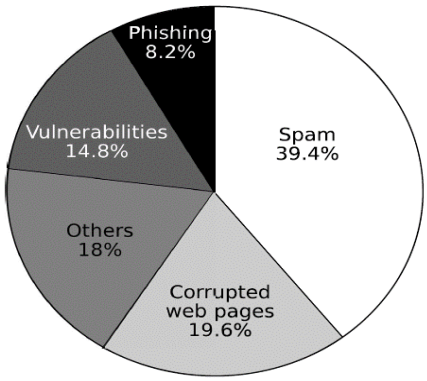

Figure 4: Sources of Infection

(https://ieeexplore.ieee.org/document/8861029)

Illicitly Obtained Credentials

Attackers may purchase stolen credentials of a potential victim's employees from the dark web, or publish offers to purchase credentials from disloyal employees or contractors.[20]

2021/?utm_medium=PR&utm_source=pressrelease&utm_campaign=dp-ransomware-veeam-0220&utm_content=2021RansomwareReport)

18. https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
19. https://www.varonis.com/blog/spot-phishing-scam/ describes a typical phishing infiltration.
20. Attempts to obtain user credentials illicitly may target users or administrators of endpoints, boundary systems, or mission-critical application servers.

Malicious Advertising

Attackers may purchase internet advertisements or infect legitimate ones to deliver malware through browser vulnerabilities or downloads. The advertisements typically attempt to run javascript within a browser to download malware without user awareness.

*The only effective protection against endpoint infiltrations is an informed and aware workforce. See "***Education***" (page 16) and "***Control the IT Environment***" (page 17).*

Boundary systems (firewalls, VPNs, etc.) are commonly infiltrated using:

Remote Desktop Protocol (RDP) Tools

Computer management tools with which IT administrators log in to computers via network connections. Attackers use RDP tools to gain access to computers connected to enterprise networks and use them as starting points for further infiltration. One security analysis firm estimates that in 2021, RDP is the most frequently used ransomware attack vector.[21]

Exploit Kits

Attackers sometimes take advantage of known security vulnerabilities in widely used operating systems, applications, and websites to deploy ransomware bundles called *exploit kits*. They may target either endpoints or servers that run an organization's critical applications. Exploit kits, also known as *advanced persistent threats* (APTs), often install themselves in operating systems in ways that are difficult to detect but that cause them to run whenever the infected computers are restarted. Some APTs escape detection by launching common operating system utilities and replacing their code with malware. APTs typically manipulate operating system startup files to ensure that they reactivate each time a computer is restarted.

Most APTs are designed to *move laterally* within victims' networks, patiently searching for and infecting additional vulnerable systems. In some instances, however, such as the Kaseya attack of July, 2021,[22] the attacker discovers a vulnerability in an electronically distributed software update and exploits it immediately to attack the vendor's customers.[23]

*"Good IT hygiene" is a metaphor often used to describe measures that minimize exposure to boundary attacks. These include rigorous security controls on networks, server and endpoint operating systems and applications. See "***Anti-Ransomware Best Practices***" (page 16).*

21. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
22. https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack
23. While not strictly ransomware, the 2021 SolarWinds malware attack (https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack) is a dramatic example of how attackers can exploit vulnerable software updates.

A sometimes-overlooked source of potential attacks is an organization's own employees or consultants with legitimate access to IT systems. Organizations that explicitly or implicitly trust their employees are susceptible to attacks that originate from within.

Attacks from Within

Employees or consultants with administrative access to IT resources may mount or abet ransomware attacks by altering firewall rules, installing malware on the organization's computers, or connecting unauthorized servers to data. Non-administrative users may expose their credentials to hackers, or deliberately respond to phishing attacks and visit infected websites.

*Organizations must balance the positive effects of a trust-based working environment and the integrity and security of their vital data. Carefully controlling individuals' access to IT assets can limit the damage that disloyal workers can cause. See "***Minimize Potential Attack Points***" (page 17).*

Whatever their source, malware infections may hide for weeks or months while they move laterally within the victim's network searching for vulnerable computers and data sets that appear to be attractive targets before mounting an attack.[24] From a recovery standpoint, data corruption begins at the point of attack, whereas malware removal may require restoring software to a state prior to infiltration, which may be much earlier than the time at which the attack occurred.

Some computer infections start with seemingly innocuous emails that appear to have been sent by legitimate sources. Attachments to the emails may contain executable files disguised as innocuous file types such as PDF by exploiting the common default behavior of not displaying file extensions. The executable installs a bot that communicates with a botnet to contact the attacker's C&C server and mount an attack.

Some newer ransomware strains send asymmetric encryption keys to a bot, which would use them to encrypt files deemed valuable by the attacker, both on the infiltrated computer's storage devices and on the storage devices of other systems to which it had gained access.[25] Decryption is impossible because the necessary decryption keys are never present on any of the victim's computers until the ransom had been paid.

24. https://www.varonis.com/blog/advanced-persistent-threat/
25. https://www.varonis.com/blog/cryptowall/

How Ransomware Encrypts Data

The original objective of ransomware was to make files indecipherable by legitimate users. Over time, attacks have become increasingly elaborate, and therefore more difficult to defeat:

Content Encryption

Early ransomware strains simply encrypted files that the attacker considered important under their original names. File owners could see that their files still existed, but the contents would be indecipherable by applications.

Renaming

To further obfuscate targeted files, later attacks would either rename files after encryption (a technique used by some ransomware strains[26] as an unmistakable signal that something bad has happened) or encrypt filenames as well as contents, making it impossible to associate encrypted files with the originals.

Exfiltrating

In addition to encrypting files on victims' computers, some ransomware strains exfiltrate (copy) them to the attacker's C&C servers. This is usually done to threaten the owner with sale or public exposure of sensitive data such as medical or financial records if ransom is not paid.

Encrypted files are obviously indecipherable, and encryption is CPU-intensive. Both unusable data and high CPU activity are detectable by monitoring tools, so ransomware usually attempts to keep encryption time as short as possible. Using less computationally intensive AES encryption for files and encrypting only key pieces of content, such as data encryption keys or "magic bytes" that applications use to identify files are two techniques that are sometimes used.[27]

26. 50 of the 52 strains studied by https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8861029 change file extensions.

27. Conversely, some strains attempt to avoid detection by encrypting all but files' magic bytes. https://resources.infosecinstitute.com/topic/a-brief-summary-of-encryption-method-used-in-widespread-ransomware/

How Attackers Manage Encryption Keys

The key to ransomware is literally the encryption keys. If an attack victim can locate encrypted files and discover (a) the key(s) used to encrypt them and (b) the attacker's encryption method, files can usually be recovered without paying ransom. Over time, evolving ransomware strains have used increasingly elaborate encryption techniques to avoid key discovery:

Symmetric Encryption

Many ransomware strains encrypt files using *symmetric* algorithms such as AES that use the same key to encrypt and decrypt. With sufficiently large keys (256 bit keys are typical), decryption without access to keys is virtually impossible.

Keys are sometimes stored on target computers using various techniques to hide them from forensic analysts. Upon payment of ransom, the attacker delivers a decryption tool that accesses the keys and decrypts the files. With this approach, target computers need not have Internet access, but if forensic analysts can locate the keys on a victim's computer, well-known decryption techniques can recover files without paying ransom.

Asymmetric Encryption

Asymmetric encryption, such as RSA,[28] uses pairs of keys, a *public* one for encryption and a companion *private* one for decryption. A source computer can distribute its public keys freely to correspondents who can use them to encrypt messages that only the source computer can decrypt by using its closely held private keys.

Some ransomware strains:

- generate an RSA public-private key pair on the target computer
- encrypt the victim's files using the public key
- send the private key to the attacker's C&C server
- delete the private key from the victim's computer, making it impossible to decrypt files.

Asymmetric encryption has two drawbacks:

- It is computationally intensive, so encryption can take 3-4 times as long as with AES,[29] making it easier for monitoring software to detect an attack in progress
- Both the target computer and the attacker's C&C server must be connected to the Internet during the attack so that the ransomware can send the private key to it.

28. https://simple.wikipedia.org/wiki/RSA_algorithm
29. One test comparing AES and RSA encryption speed can be found at: https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php

It may be possible to detect this type of ransomware by its computing or network activity before all targeted files have been encrypted and mitigate the damage.

Server-side Asymmetric Encryption

A variation of the asymmetric encryption technique generates the public-private key pair on the attacker's C&C server and embeds the only public key in the ransomware executable it sends to the victim's computers. Again, asymmetric encryption is slow, so detection iduring an attack may be possible, but the ransomware's private key needed for decryption is not on the victim's computer until the ransom has been paid and so cannot be discovered.

Hybrid Encryption

Several newer ransomware strains combine symmetric and asymmetric encryption to gain the speed of symmetric encryption while avoiding the need for communication between the attacker's C&C server and the victim's computer during the attack:

- C&C server and ransomware on the victim's computer generate separate RSA key pairs
- The C&C server embeds its public key in the ransomware executable it installs on the victim's computer
- When the ransomware runs, it generates symmetric keys which it uses to encrypt the victim's files. Some strains generate a separate key for each file to be encrypted
- The ransomware uses its own public key to encrypt the symmetric keys and encrypts its own private key using the C&C server's public key
- When the ransom is paid, a decryption tool on the victim's computer sends the ransomware's (encrypted) private key to the attacker's C&C server
- The C&C server decrypts the ransomware's private key and returns it to the decryption tool. The decryption tool uses it to decrypt the symmetric keys which it then uses to decrypt the victim's files.[30]

30. https://www.sentinelone.com/blog/anatomy-of-cryptowall-3-0-a-look-inside-ransomwares-tactics/

How Ransomware Locates its C&C Servers

Cybercriminals use C&C servers or clusters to control their ransomware attacks. Depending on the encryption and key management methods it uses, ransomware may need to contact a C&C server before or during an attack. This requires that attacked computers have Internet access, which can be problematic for attackers. Different ransomware strains use one of two techniques to locate their C&C servers:

Static Addresses

The simplest way for ransomware on a victim's computer to contact its C&C server is to have the server's DNS name or IP address (for C&C clusters, a list of names or addresses) embedded in the executable image. This method is simple but flawed—once a C&C servers' IP addresses are known, they can be added to firewall blacklists to prevent contact. Despite this flaw, about 60% of the ransomware strains that contact their C&C servers before or during encryption use this technique.[31]

Domain Generation Algorithms (DGAs)

With this technique, both C&C server and ransomware include an algorithm that generates DNS names dynamically. The C&C server generates and registers DNS names on a known schedule and unregisters them after known intervals. The ransomware generates the same names and issues DNS queries during the interval when they are scheduled to be registered. It is impractical for firewalls to block constantly changing C&C server IP addresses, but because propagating a DNS registration can take many hours, ransomware on victims' computers necessarily establishes a pattern of apparently random DNS queries, which can in principle be noticed by detection tools.

31. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8861029
About a third of strains examined in the referenced study do not contact C&C servers prior to encryption.

DETECTING RANSOMWARE

The best defense against ransomware is prevention. But with the rapid pace of software evolution, there are always possibilities of new vulnerabilities leading to infections that launch ransomware attacks. A significant amount of research has gone into detecting the presence of ransomware before and during attacks using information available to victims' computers and their networks.

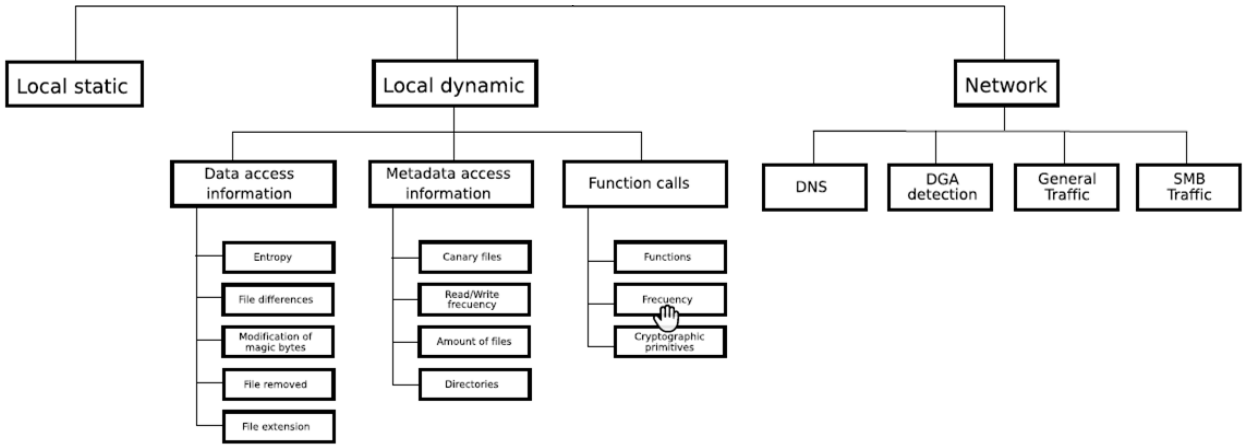

Figure 5: Ransomware Detection
(from https://ieeexplore.ieee.org/document/8861029)

Figure 5 shows how one researcher classifies Information that can be (and often is) used to detect malware. Because attacks are typically executed by an organization's servers or by network components rather than by storage systems, detection necessarily focuses on information captured from those two sources.

The information listed in Figure 5 falls into three broad categories:

Embedded in Executable Images (Local static)

Ransomware executables may contain common words or phrases such as "ransom" or "encrypt" that hint at their purpose. They may contain known DNS names or IP addresses for contacting C&C servers. As with all forms of malware, virus scanners can detect "signatures"—patterns in executable software that identify it as potential ransomware. These can be detected by anti-virus software that scans executables before they run and prevents execution if suspect content is discovered. However, strains can hinder or defeat this type of detection by obfuscating content likely to be suspect and transforming it into usable form at run time.

Program Behavior (Local dynamic)

Ransomware performs certain actions, such as searching directories, encrypting or renaming files, making DNS queries and network connections, and so forth. Perhaps surprisingly, many ransomware strains call operating system library functions to generate keys, encrypt data, and perform similar functions.

Monitoring software running on victim computers can detect these behaviors, but only after ransomware is running, and may already be encrypting files. Thus, behavior monitoring is more of a damage mitigation tactic rather than a complete prevention mechanism. Moreover, behavior monitoring is necessarily statistical—detectable actions performed by ransomware are also performed by legitimate software, so monitoring must detect unusual patterns of activity such as:

- High frequency of system calls such as file attribute retrieval, key generation and data encryption functions
- Accessing and/or modifying the names, extensions, or content of large numbers of apparently unrelated files, especially those in unrelated storage volumes or file systems
- Creating and/or deleting unusually large numbers of files
- Making improbable file modifications such as overwriting the so-called “magic bytes” that identify files to applications
- Writing unusually large amounts of “high entropy” (highly random) data (a fundamental outcome of encryption).

Network Activity Monitoring (Network)

Running ransomware can sometimes be detected by its network activity. Strains that communicate with C&C servers using static DNS names (the majority) can be identified by DNS queries. Strains that use DGA to locate their C&C servers can sometimes be detected by sequences of DNS queries with unusual domain names. Strains that exfiltrate data before or during encryption may be detectable due to large outflows of data to unknown IP addresses. The latter two actions are again statistical in nature, because they may also be performed by legitimate software.

DEFENDING AGAINST RANSOMWARE ATTACKS

Protecting critical data against ransomware attacks requires continuous review and improvement of both procedures and technology. A comprehensive defense strategy has four parts:

Prevention

The best defense against ransomware attacks is prevention. Because ransomware continuously evolves, total prevention for all time is impossible. But hardening the IT environment and implementing protective measures promptly as vulnerabilities become known increases the barriers to attack.

Limiting Impact

Once an attacker infiltrates an organization's network, the next priority is to discover data for which the owner is likely to pay a ransom. Firewalling, network segmentation, VPNs, and VLANs all make it more difficult for attackers to "snoop" in a potential victim's network.

Recovery

The victim's most urgent priorities after a successful attack are (a) determining the extent of damage and (b) restoring IT services to legitimate users with valid data. Offline backups of key datasets, snapshots, and tamper-proof logs can speed recovery and minimize data loss and corruption. Forensic analysis is a must, both for ensuring that data has been thoroughly purged of corruption before being put back into service, and for identifying vulnerabilities that can be eliminated to prevent future attacks of the same type. Retaining outside specialists with specific expertise in forensic analysis in advance can improve the speed and quality of recovery.

Education

Because phishing attacks on human computer users are a major infiltration vector, information security officers (CISOs) should ensure that all users of an enterprise's IT services aware of the nature and potential consequences of attacks, and should regularly reinforce that messaging. As endpoint threats are identified, they should be promptly, broadly, and visibly communicated throughout the enterprise.

ANTI-RANSOMWARE BEST PRACTICES

Without adequate before-the-event protection, paying ransom and trusting a cybercriminal to provide the promised decryption tools may be a victim's only alternative. Even when attacker-supplied decryption tools work, however, there is no guarantee of a permanent solution. Some attackers embed malware in victims' computers to facilitate future attacks. Others "double-dip"—exfiltrate a copy of data before encrypting it, and after it is ransomed, threaten to sell or publish it unless additional payments are made.

Prevention is therefore clearly the best defense. A comprehensive program to minimize chances of a successful ransomware attack and the impact of such attacks has four main components:

Control the IT Environment

An IT operation consists of equipment, software, applications, administrators, and users, all of which have roles to play in protecting against ransomware attacks. While not offering perfect protection against "zero-day" vulnerabilities (discovered by attackers before they become generally known), security-conscious IT practices can minimize exposure:

- Only utilize equipment and software with strong security features obtained from reputable vendors, and rigorously track changes to the IT infrastructure
- Firewall against untrusted connections such as rogue web sites and known attacker C&C servers wherever possible and tightly control and regularly review firewall rule sets
- Segment networks to limit application access to legitimate users performing authorized actions to block attackers' lateral propagation attempts
- Deploy malware detection software throughout the environment and update it promptly and consistently as new threats are discovered
- Utilize security analytics tools to monitor data stores, mailboxes, proxies, DNS, and VPNs to catch infiltration and ransomware attacks in progress[32]
- Employ artificial intelligence-based tools from reputable vendors to detect unusual access and usage patterns and act promptly to determine their legitimacy
- Regularly re-educate users about the techniques and dangers of spam, phishing, bogus web sites, and other forms of automated and human-based social engineering.

Minimize Potential Attack Points

The more types of IT equipment and software in use, the greater the potential vulnerabilities. The more applications and datasets a system or user can access, the greater the damage an infiltrator can do. To limit exposure to attacks:

- Minimize the equipment types, software versions, cloud providers, and so forth in use, and keep update and patch levels current and consistent across the environment
- Implement storage network zones, VPNs, and VLANs to confine access to key datasets to applications and users with legitimate needs
- Implement a "least privilege" model to control access to equipment, software, and data by (a) vetting account holders, (b) using multi-factor user authentication (MFA), (c) using role-based access control (RBAC), and (d) indelibly logging all administrative actions

32. https://www.varonis.com/blog/cryptowall/

- Ensure that remote access to key computers via RDP, SSH, and others is inside VPNs.

Erect Barriers to Attack

The harder it is to penetrate an IT operation, the less likely an attacker is to invest the effort. The harder it is to exploit stolen data, the less likely it is to be stolen. The harder it is to prevent recovery from ransomware, the less likely an attacker is to attempt extortion. In addition to controlling the IT environment, best practices can increase barriers for attackers:

- Encrypt all data transmitted within and outside data centers
- Detect and verify successful network connections, especially for bulk data transfer, before allowing them to transfer data
- Use techniques such as PPK and MFA to authenticate IT users and administrators
- Back up key data sets frequently, using immutable snapshots and/or moving backup copies to offline storage to balance between rapid recovery and preventing attackers' attempts to prevent recovery by deleting backups accessible by ransomware.[33]

Have a Recovery Strategy

Preventive measures notwithstanding, organizations should be prepared for the eventuality of a successful attack and be prepared to recover from it quickly and with minimal data loss. Recoverability requires both assets such as verifiable backups and logs and for identifying which assets to use and how to use them quickly and effectively. Because insurers or regulators may prohibit victims from reusing compromised equipment, recovery plans should include arrangements for obtaining and deploying replacement computers, storage, and network components.

WHEN AN ATTACK SUCCEEDS

While the top priority after a ransomware attack is minimizing damage (data loss) and restoring services and data, it is also important to understand why the attack succeeded so that future attacks of similar type can be prevented.

If an attack is recognized while it is still occurring, the most immediate need is damage minimization, usually by blocking network access, stopping applications or shutting down computers, disconnecting storage systems, and disabling access for suspect users and administrators. After immediate measures have been taken, the next tasks are (a) determining the extent of the damage, and (b) restoring IT service with valid data to legitimate users.

33. https://www.varonis.com/blog/cryptowall/

The extent to which data can be recovered without paying ransom depends in part on being able to determine when an attack occurred, typically by analyzing network and computer activity logs. If snapshots or backups of data, applications, and operating system images that pre-date an attack are available, they can replace corrupted data and software and limit the loss to legitimate updates that occurred during the attack. Legitimate updates can sometimes be recovered from uncorrupted application logs and re-applied to data restored from snapshots or backups, as long as malware and data affected by it can be identified and eliminated beforehand.

Whatever the extent to which recovery succeeds, successful attacks should be analyzed to determine how they were made and measures should be adopted to prevent recurrences.

PURE STORAGE AND RANSOMWARE

The most frequent points of infiltration for ransomware attacks are personal computer user interfaces. Ransomware propagates via software vulnerabilities in networks, applications, and operating systems. Nevertheless, storage systems that can be managed remotely can be penetrated if the same measures that secure access to other IT systems are not adopted.

Because FlashBlade, FlashArray, and Cloud Block Store encrypt all stored data and metadata, and administrative accounts have no access to stored data, attacking stored data directly would be very difficult. A more likely attack vector would be using administrator credentials obtained by phishing or penetrating a directory server to connect volumes, file systems, or object stores to servers controlled by the attacker. Such servers could access stored files or objects that *would* be susceptible to encryption by ransomware running in the server.

Attackers are adept at discovering and deleting backup copies and snapshots of data and logs that might assist in recovery. One defense against this is to move backups offline to “air-gapped” systems that are not visible to or accessible by an attacker using the organization’s network. After an attack, data can be recovered from offline backups while victimized computers are sequestered from the network.

This procedure works, but it is somewhat cumbersome to implement and moreover, the protected data is inherently out-of-date due to the time required to make and copy backups.

Snapshots of key volumes, file systems, and logs are another defensive tool that can be used to recover encrypted data faster and more current than offline backups. Attackers are aware of this and try to discover and delete snapshots of data or logs to render recovery and forensic analysis impossible. For example, while Pure Storage volume and file system snapshots are immutable, an attacker who gains access to an array administrator account could destroy and eradicate them before their scheduled expiration dates or could alter schedules to bypass scheduled snapshots prior to an attack.

Thus, attackers who gain administrative access to FlashArray or FlashBlade systems could eradicate snapshots that might otherwise be used to restore corrupted or encrypted data. To avoid this, customers can, in cooperation with Pure Storage Support, enable a *SafeMode* of operation which:

- Allows support engineers to extend the normal 24-hour interval between destroying a snapshot and automatic eradication of its image to as much as a month
- Prevents administrators from explicitly eradicating destroyed snapshots or making changes to snapshot schedules
- Requires verbal contact between Pure Storage Support and two or more designated customer representatives to manage snapshots, alter schedules, or disable SafeMode.

SafeMode effectively prevents attackers, including an organization's own employees, from eliminating recent snapshots that can be used to recover data corrupted by malware or rendered unreadable by ransomware attacks.

***In short**,*

protecting data against ransomware attacks is an on-going process that relies on technology, strictly enforced policies, and trustworthy employees and contractors.

With transparent always-on encryption, immutable snapshots, SafeMode, and rigorous administrative access controls, FlashArray and FlashBlade provide the most effective tools available to help protect critical data against destruction, loss of access, and misappropriation by ransomware, and to recover data when an attack does succeed.