Surviving Ransomware

A Look at the Past, Present, and Future

What is Ransomware?

Ransomware is a type of malicious software (malware) that is designed to encrypt a victim's files or lock their computer, rendering it unusable until a ransom is paid. The attacker then demands payment from the victim in exchange for providing the decryption key or unlocking the computer.

Ransomware is one of the most effective strategies for attacking businesses, critical infrastructures and individuals.

Types Of Ransomware

Crypto or Encrypting

- The Most common: It encrypts a victim's files and demands payment in exchange for the decryption key
- Encrypts all or some files.
- Ransom demanded in exchange for a decryption key.
- Newer variants also infect shared, networked, and cloud drives

Locker

- Locks a victim's computer or device
- Computer access is blocked until ransom is paid

Master Boot Record (MBR)

- Locks a victim's computer or device by targeting the MBR not allowing it to boot until a ransom is paid.

Scareware

- Displays a fake warning message that claims to be from a legitimate law enforcement agency, accusing the victim of illegal activity and demanding payment to avoid legal action

Double Extortion Ransomware

- Encrypts files and exports data to blackmail victims to pay ransom
- Attackers threaten to publish stolen data if demands not met
- Attackers still have access to stolen data even if ransom is paid

RaaS – Ransomware-as-a-Service

- More a business model it is offered as a pay-for-use service. Anyone can launch an attack
- RaaS creators host their ransomware on darknet sites
- Criminals can purchase as a subscription
- Fees depend on the ransomware's complexity and features
- A portion of the ransom is paid to the RaaS creator

Common Characteristics of Ransomware

1. Encryption: Ransomware typically uses strong encryption algorithms to encrypt the victim's files, making them inaccessible without the decryption key.
2. Ransom Demand: The attacker demands a ransom payment in exchange for the decryption key. The ransom demand can vary widely in amount and currency, and the attacker may use threats and intimidation tactics to pressure the victim to pay.
3. Time Limit: Ransomware often includes a time limit for payment, after which the ransom demand may increase, or the decryption key may be permanently deleted.
4. Contact Information: Ransomware typically includes contact information for the attacker, such as an email address or a Tor-based website, to facilitate communication and payment.
5. Social Engineering: Ransomware attacks often use social engineering techniques, such as phishing emails or fake software updates, to trick the victim into downloading and running the malware.
6. Multi-Stage: Some ransomware attacks involve multiple stages, with the initial infection used to establish a foothold in the victim's system, followed by further malware downloads and lateral movement to other parts of the network.
7. Anti-Detection: Ransomware often includes anti-detection techniques, such as code obfuscation or encryption, to evade detection by security software.

Just the Facts

The average ransomware payment in 2021 increased by 82% to $570k

The National Health Service (NHS) suffered a $100 million loss due to the WannaCry ransomware attack

10 million people were affected by ransomware scams targeting android users

Ransomware attacks have seen an increase of 62% globally in 2020 compared to 2019

The first half of 2022 saw nearly 236.7 million ransomware attacks worldwide

Statistics reveal that someone will fall victim to ransomware attack every 14 seconds. In 2031 it will be every 2.

A Few Variants of Note

Potentially Tens of Thousands Exist

1989 – The Beginning
AIDS Trojan -1989

2007
CryptoLocker -2007

2012
Reveton – 2012

2015
Shade/Troldesh – 2015

2016
Dharma - 2016
Cerber - 2016
Petya - 2016
Locky - 2016

2017
WannaCry - 2017
NotPetya - 2017
GlobeImposter – 2017

2018
SamSam – 2018
GandCrab - 2018
Ryuk – 2018

2019
Maze - 2019
REvil/Sodinokibi - 2019
Netwalker – 2019

2020
Egregor - 2020
Conti 2020

The top 10 ransomware strains by revenue in 2021 were:

- **NotPeyta - $1 Billion**
- **Conti – $175 million**
- **DarkSide – $80 million**
- **Phoenix Cryptolocker – $55 million**
- **REvil/Sodinokibi – $35 million**
- **Cuba – $17 million**
- **Clop – $16 million**
- **LockBit – $15 million**
- **Hive – $15 million**
- **BlackMatter -$14 million**
- **Ryuk – $13 million**

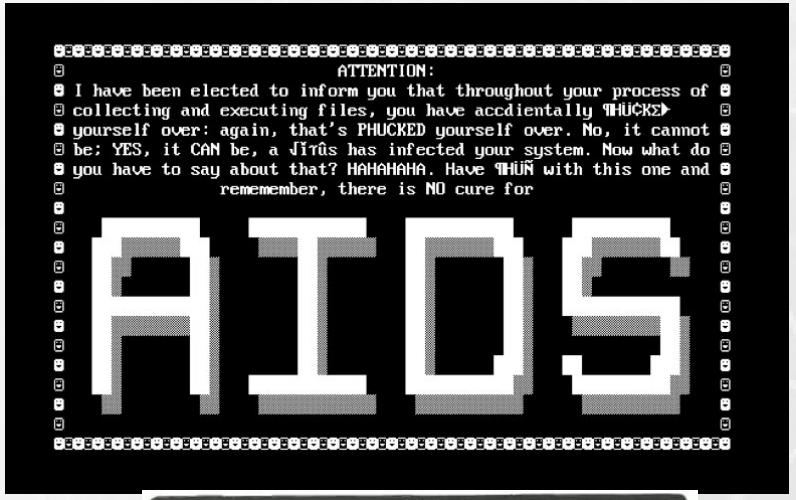
1st Ever Ransomware – AIDS Trojan or PC Cyborg

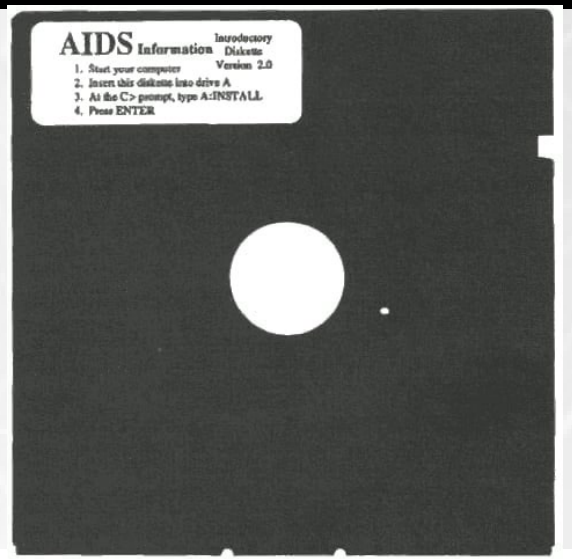
The AIDS Trojan, also known as the PC Cyborg virus, was the first ever ransomware virus documented.

- Created in 1989 by a biologist Joseph Popp who handed out 20,000 infected disks to attendees of the World Health Organization's AIDS conference.

How did it work:

- The program would count the number of times the computer was booted and once it reached 90 it would hide the directories and encrypt or lock the names of the files on the C drive.
- To regain access, the users would have to send $189 to PC Cyborg Corporation at a PO box in Panama. T
- It was pretty easy to overcome as it used simple symmetric cryptography and tools were soon available to decrypt the files.





CryptoLocker – Encrypting Variant

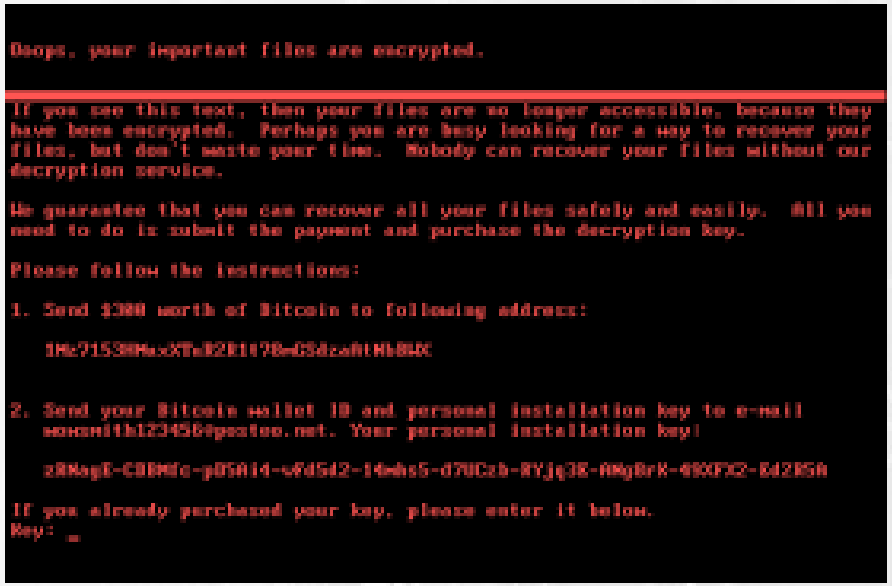
CryptoLocker was first spotted in 2007. The ransomware searched for important data on infected computers and encrypted it. An estimated 500,000 computers were affected. Law enforcement agencies and security companies eventually seized control of the worldwide network. Ultimately allowed for an online portal being set up where victims could obtain a key to unlock their data. This allowed their data to be released without the need to pay a ransom to the criminals.

How did it work:

- Botnet of hijacked Home Computers was used to deliver the Ransomware
- Delivered through infected email attachments.
- Once clicked it began searching data stores and infecting files
- Stored its keys on hacker server
- The victim was presented with a ransom note and given 72 hours

Petya to NotPetya – MBR Variant

Petya isn't a single instance of ransomware so much as a family of related malware. Petya first appeared in early 2016. When downloaded and opened, the attachment would unleash the malware onto the victim's computer. After a relatively unremarkable start, Petya exploded into the global cybersecurity conversation with a renewed attack in 2017. Dubbed "NotPetya," the new variant tore through organizations in Ukraine, including the National Bank of Ukraine, before spreading across Europe and the US. In total, the 2017 NotPetya attack caused over $10 billion in damages.



How did it work:

- Delivered through infected email attachments.
- Once clicked it encrypts the Master File Record (MFR)
- It forced a restart, then begins to encrypt the Master File TableThe victim was presented with a ransom note

Future: Ransomware of Tomorrow

1. AI-Powered Ransomware: With advancements in machine learning, ransomware attacks may be augmented with artificial intelligence capabilities. AI could be used to automate the discovery of vulnerabilities, plan attacks, and evade detection by security systems.
2. More Complex Encryption: Attackers may use more advanced encryption techniques that are even more difficult to break, making it harder for victims to recover their data.
3. More Collaboration Among Attackers: Criminal groups may increasingly work together to launch more sophisticated attacks, share information, and collaborate on more extensive campaigns.
4. Continued Use of Social Engineering: Ransomware attackers may continue to use social engineering tactics such as phishing attacks to trick individuals into downloading malware or giving up sensitive information.
5. Ransomware-as-a-Service: As ransomware attacks continue to become more profitable, the use of Ransomware-as-a-Service (RaaS) may increase. This would allow even non-technical criminals to launch ransomware attacks, making it harder to trace the origins of an attack.
6. Targeted Ransomware Attacks: Attackers may use more targeted attacks to maximize the potential payout. This could involve researching their victims in advance and customizing their attacks to specific vulnerabilities.

How to Protect Your Business

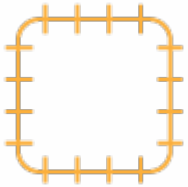
Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small. Apply these tips and practices to avoid attack.

Good Cyber Hygiene Habits Keep Your Network Healthy

Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

When in Doubt, Report It Out

Victims of ransomware should report to federal law enforcement via IC3 or a Secret Service Field Office and can request technical assistance or provide information to help others by contacting CISA.



Backing Up Is Your Best Bet

Maintain offline, encrypted backups of data and regularly test your backups.

Keep Calm and Patch On

Regularly patch and update software and Operating Systems.

inceptus

Restoring After a Ransomware Attack

Find the trigger file(s)

First things first: find and remove any trigger file(s) from all devices.

Determine attack style

Identifying the specific ransomware type will help determine next steps. There are two principal forms of ransomware: screen-locking and encryption-based.

Disconnect all devices

To limit the effects of ransomware, disconnect every vulnerable device from your network in order to block the attack from spreading.

Understand the ransomware

Depending on the type of ransomware attack, data recovery can be possible using web-based software. You might also be able to decode the encrypted files using a ransomware encryption removal tool. Seek guidance from malware experts.

Restore file systems

Ideally, you will want to restore as much “lost” data as possible. That’s done using backed-up data, but be careful. Ransomware can have dwell times as long as six months, so malware might have been included in your archival backups. Before restoring, run an anti-malware package on all systems.

Combatting Ransomware

Human Intervention in Preventing Ransomware Attacks

- DO NOT open emails in the spam folder or emails whose recipients you do not know.
- DO NOT open attachments in emails of unknown origin.
- DO NOT pay the ransom. The reason why the criminals keep utilizing this form of blackmailing attacks is that people keep paying. To try to get your data back, consult a professional in your area.
- Humans need to be trained -- they are the weakest link. Companies should employ at minimum a bi-annual training geared towards each user group (end-users, IT staff, managers, etc.) so that everyone is aware of the latest attacks.
- Patch your systems!
- Backup Daily!
- Do not use public Wi-Fi connections unless on a virtual private network or using encryption software.
- Install and enable “advanced” antivirus protection. Endpoint Detection and Response (EDR) at a minimum.