INFORMASI
TECHNOLOGY SOLUTIONS

Best practices for escaping ransomware

How to detect and response to ransomware attacks

ManageEngine

About Your Speaker

About José Amorós

- José F. Amorós, ManageEngine Certified Expert
  - jamoros@informasipr.com
- Informasi Technology Solutions
  - Owner and Founder
  - Since 2013
  - ManageEngine, Official Partner of Business in Puerto Rico
  - www.informasipr.com
  - 787.957.5757

The rise of ransomware (Introduction)

- Cyber threats continue to grow more prevalent, more sophisticated and more destructive. As was described in your opening statements, one threat has been particularly troubling: **the rise of ransomware**.
- And because some ransomware variants can infect other computers, a single person opening an email or visiting an infected website can result in the network of an entire organization being held hostage.
- Defeating ransomware schemes, however, requires a strategy that encourages the public and private sectors to work together. Computer owners everywhere need to improve their “digital hygiene” by taking steps like installing the latest patches and ensuring that backups are up to date.
  - Richard Downing, Deputy Assistant Attorney General (Acting), U.S. Department of Justice / Computer Crime and Intellectual Property Section

Agenda

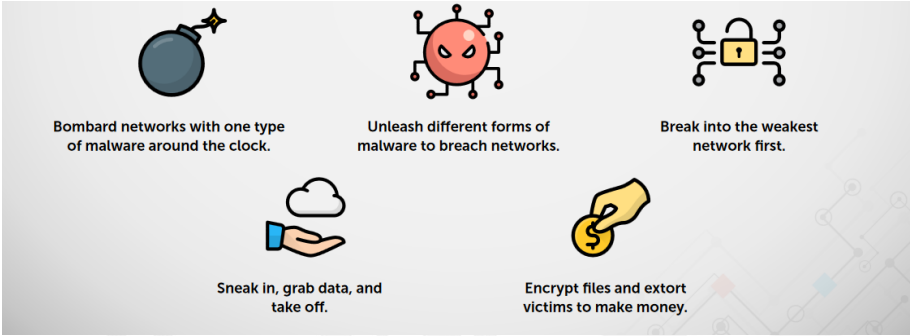
- Cyberattacks
- What is ransomware?
- Ransomware basics
- Type of ransomware
- Statistics
- What file extensions ransomware currently use
- What are basic steps to help protect against ransomware
- How you can setup monitoring to recognize ransomware
- How you can create actions after you know you are under attack from ransomware

Cyberattacks

- A cyberattack is an offensive act targeting computers, networks, or other devices in an attempt to either steal, encrypt, or destroy information on a system or network.
- A nation, state, individual, organization, or group may orchestrate an attack.
- There are different types of cyberattacks, including DDoS attacks, brute force attacks, phishing, Hacking, watering hole attacks, ransomware attacks, and more.

Cyberattacks

Cyberattacks five general strategies



Cyberattacks

- Of these strategies, number five has gained popularity recently.

- This strategy is used by ransomware attacks

What is ransomware?

- Ransomware is a type of malware that encrypts a system and then extorts money from the users or the entire organization.
- Basically, ransomware encrypts the victim's files, restricting the user from using their own files or documents.
- Or locks the computer to prevent normal usage.
- Demands payment as ransom to decrypt the files and provide access.

What is ransomware?

Prevents you from accessing your files and folders.

Completely locks you out of your system.

Demands ransom to restore your system to working order.

Ransoware example

ManageEngine

Ransomware basics

Ransomware basics

- Infection initially by Trojan – a type of malware that is often disguised as legitimate
- Infection can spread using OS weakness or unpatched security hole
- First known ransomware – 1989 “AIDS Trojan”
  - Created by a biologist Joseph Popp
  - Distributed 20,000 infected disks to attendees of the World Health Organization’s AIDS conference
  - Hide directories and encrypt files on C drive when PC booted 90 times after the diskette was inserted for first time
  - Asked for $189 USD
  - Was pretty easy to overcome as it used simple symmetric cryptography

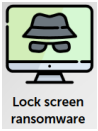
Ransomware basics

- Most significant ransomware attacks of 2017
  - WannaCry (2017)
    - Server Message Block (SMB) vulnerability CVE-2017-0144 (also called EternalBlue)
    - By far the largest ransomware attack to date, infecting over 400,000 devices in over 150 countries
  - Petya (2017)
    - CVE-2017-0145 (also known as EternalRomance)
    - Infecting users across Ukraine, the United States, the Netherlands, and more
  - Not Petya (2017)
    - Unlike Petya—which was designed for extortion—NotPetya focused on causing chaos and irreparable damage to data.
  - Bad Rabbit (2017)
    - Infecting users in Russia, Ukraine, Turkey, and Germany
    - Spread via a fake Adobe Flash Player installer

Ransomware basics

Type of ransomware

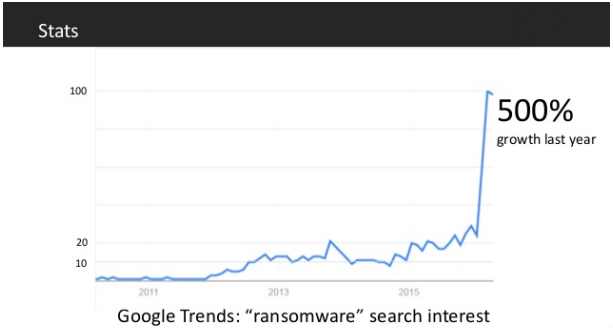
This ransomware encrypts your files and folders, preventing you from accessing your files by locking them with an AES-256 key. After encrypting your files and folders, encryption ransomware displays a pop-up message explaining that your files have been encrypted and you must pay a ransom to have those documents decrypted.

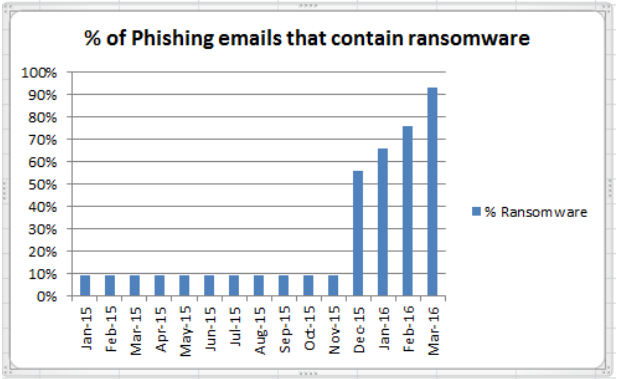


Lock screen ransomware locks your screen and demands a ransom. While this type of ransomware won't encrypt your files, it will block all your windows straightaway. Once your system is infected, you won't be able to access your windows until you pay the ransom or the hackers lift the attack.

MBR ransomware changes the MBR, interrupting the normal boot process by displaying a demand for ransom on the boot up screen. Users can't even boot their systems up until the ransom is payed.

Ransomware Statictics





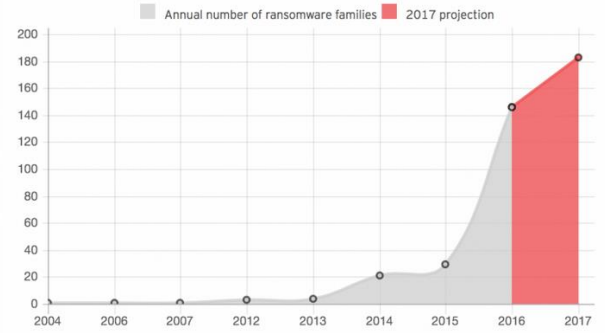


Fig. 3: Annual number of ransomware families, The Next Tier: 8 Security Predictions for 2017 (Trend Micro, 2016)

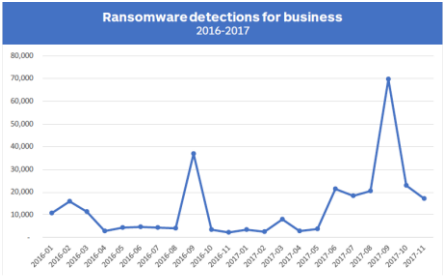


Figure 3. Ransomware detections among businesses 2016–2017

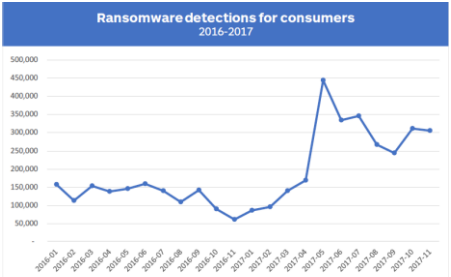


Figure 4. Ransomware detections among consumers 2016–2017

Source: Malwarebytes, 2017 State of Malware

Top 10 business detections		
2016	vs.	2017
Fraud Tool	1	Hijacker
Adware	2	Adware
Hijacker	3	Riskware Tool
Riskware Tool	4	Backdoor
Backdoor	5	Ransomware
Hack Tool	6	Spyware
Worm	7	Worm
Crack Tool	8	Hack Tool
Banking Trojan	9	Fraud Tool
Ransomware	10	Banking Trojan

Figure 1. Top 10 business threats of 2016 and 2017

Top 10 consumer detections		
2016	vs.	2017
Fraud Tool	1	Adware
Adware	2	Fraud Tool
Riskware Tool	3	Riskware Tool
Backdoor	4	Backdoor
Hack Tool	5	Hack Tool
Hijacker	6	Worm
Crack Tool	7	Hijacker
Worm	8	Crack Tool
Banking Trojan	9	Ransomware
Rootkit	10	Spyware

Figure 2. Top 10 consumer threats of 2016 and 2017

Source: Malwarebytes, 2017 State of Malware

Record ransomware volumes in 2017

- According to the Malwarebytes' 2017 State of Malware Report, ransomware attacks against consumers went up more than 93% while ransomware attacks against businesses increased 90%.
- Seeing ransomware among Malwarebytes' top threats of 2017 is no surprise if we remember that 2017 saw three major ransomware outbreaks —WannaCry, NotPetya, BadRabbit— that made tens of thousands of victims worldwide.
- A study for security software provider Malwarebytes found that while ransom demands are typically small, 22 percent of businesses were forced to cease operations immediately, leading to a crucial loss in revenue.

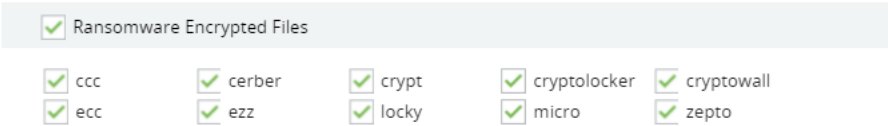
Remember

This is not **the first time** and will not be **the last time too**.

What file extensions ransomware currently use

What extensions ransomware currently uses for files

- Known extensions… at this time!



What are basic steps to help protect against ransomware

What are basic steps to help protect against ransomware

- Backup files
- Educate users
- Patch OS and third party Apps
- Filter emails for attachments
- Logically separate networks
- Use application whitelisting
- Implement limiting privilege access and secure passwords rule
- Block known bad IP addresses at firewalls
- Use software restriction policies
- Security auditing and alerting

How you can setup monitoring to recognize ransomware

How you can setup monitoring to recognize ransomware

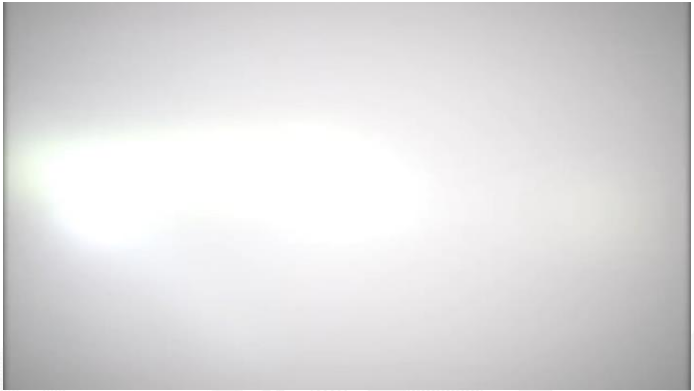
- Must monitor files being encrypted
  - Windows – Auditing using Group Policy
  - Event Viewer – Security log
  - FileAudit Plus – monitoring, reporting, alerting, actions
- Be sure to focus on key files and file types
  - Microsoft files (production), DB files, etc
- Monitor emails and email attachments
- Restrict applications to only known and needed applications (monitor for others to be started or installed)

How you can create actions after you know you are under attack from ransomware

How you can create actions after you know you are under attack from ransomware

- Use tools that can detect ransomware attacks
  - Shut down computer
  - Cut off network communications

Shut down infected devices to instantly halt the spread of ransomware



What should I do after I know I have been attacked?

- Clean up attacked computer
  - Microsoft Safety Scanner
  - Malwarebytes
  - Microsoft Windows Defender Offline
- Update patches
- Block Ports
- Update virus protection software
- Limited use of privilege accounts (administrator)
- Restore PC or reinstall

Why avoid if we can prevent?

- Update patches

- Block Ports
- Update virus protection software
- Use software restriction policies

- Limited use of privileged accounts (administrator)

- Security auditing and alerting

Only way to truly recover from ransomware?

Only way to truly recover from ransomware?

- Restore from backup!

ManageEngine
RecoveryManager Plus

- Active Directory
- Virtual Environment
- Windows Server

Its single, centralized reporting console and 3-in-1 backup and restoration capabilities make it a no-brainer choice for organizations that want all their organizational data backed up.

ManageEngine
OS Deployer

Restore PC or reinstall OS

ManageEngine

Thank you!

José Amorós

jamoros@informasipr.com

INFORMASI
TECHNOLOGY SOLUTIONS