

# Best practices for escaping ransomware

How to detect and response to ransomware attacks

---

# About Your Speaker



# About José Amorós

---

- José F. Amorós, ManageEngine Certified Expert
  - [jamoros@informasipr.com](mailto:jamoros@informasipr.com)
- Informati Technology Solutions
  - Owner and Founder
  - Since 2013
  - ManageEngine, Official Partner of Business in Puerto Rico
  - [www.informasipr.com](http://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



Bombard networks with one type of malware around the clock.



Unleash different forms of malware to breach networks.



Break into the weakest network first.



Sneak in, grab data, and take off.



Encrypt files and extort victims to make money.

# 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.

# Ransomware example

Wana Decryptor 2.0

Oops, your files have been encrypted! English

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on 5/15/2017 20:34:43  
Time Left 02:23:53:13

Your files will be lost on 5/19/2017 20:34:43  
Time Left 06:23:53:13

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

Send \$300 worth of bitcoin to this address:  
115p7UMMngo1pMvvpHijcRdfJNXj6LrLn Copy

Check Payment Decrypt

---

# 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

---

**BAD BUNNY**



# Type of ransomware

---



Encryption 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

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.



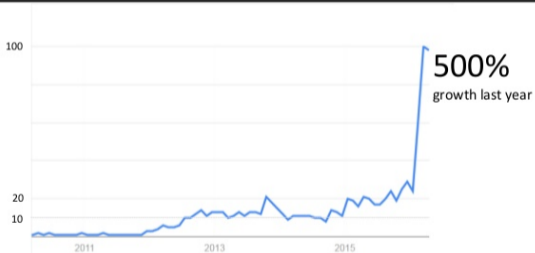
Master boot record ransomware

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 paid.

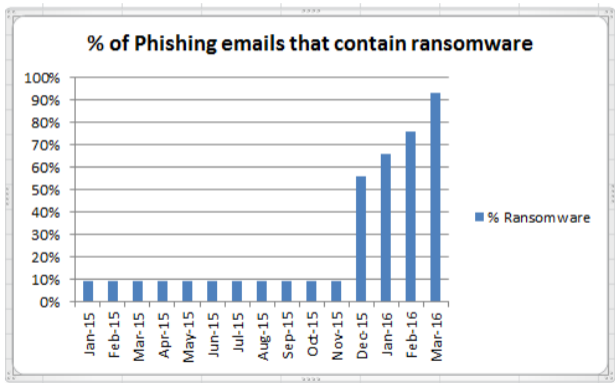


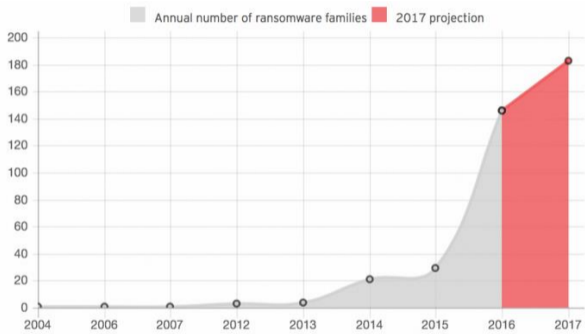
# Ransomware Statistics

Stats



Google Trends: "ransomware" search interest





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

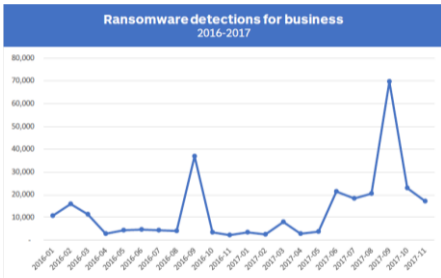


Figure 3. Ransomware detections among businesses 2016–2017

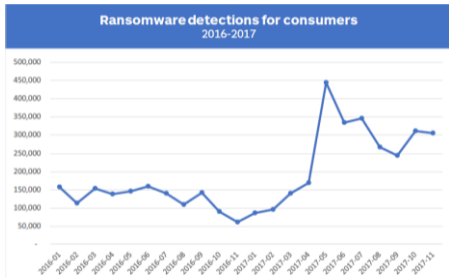


Figure 4. Ransomware detections among consumers 2016–2017

Source: Malwarebytes, 2017 State of Malware

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

Figure 1. Top 10 business threats of 2016 and 2017

| <b>Top 10 consumer detections</b> |           |               |
|-----------------------------------|-----------|---------------|
| 2016                              | vs.       | 2017          |
| Fraud Tool                        | <b>1</b>  | Adware        |
| Adware                            | <b>2</b>  | Fraud Tool    |
| Riskware Tool                     | <b>3</b>  | Riskware Tool |
| Backdoor                          | <b>4</b>  | Backdoor      |
| Hack Tool                         | <b>5</b>  | Hack Tool     |
| Hijacker                          | <b>6</b>  | Worm          |
| Crack Tool                        | <b>7</b>  | Hijacker      |
| Worm                              | <b>8</b>  | Crack Tool    |
| Banking Trojan                    | <b>9</b>  | Ransomware    |
| Rootkit                           | <b>10</b> | 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!

Ransomware Encrypted Files

ccc

cerber

crypt

cryptolocker

cryptowall

ecc

ezz

locky

micro

zepto

---

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 **ManageEngine**  
**Patch Manager Plus**
- Block Ports **ManageEngine**  
**Desktop Central**
- Update virus protection software
- Use software restriction policies
- Limited use of privileged accounts (administrator) **ManageEngine**  
**Password Manager Pro**
- Security auditing and alerting **ManageEngine**  
**Log360**

---

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](mailto:jamoros@informasipr.com)



INFORMASI  
TECHNOLOGY SOLUTIONS