

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center



#RSAC

SESSION ID: SEM-M03

RANSOMWARE - HOW NOT TO BE A VICTIM, AND WHAT TO DO WHEN YOU BECOME ONE

Ben Rothke CISSP, PCI QSA

Principal Security Consultant

Nettitude

[@benrothke](#)

About me (since you asked)



- Ben Rothke, CISSP + other certs
- Principal Security Consultant - Nettitude
- Author - Computer Security: 20 Things Every Employee Should Know
- Member: Cybersecurity Canon
<https://www.paloaltonetworks.com/threat-research/cybercanon>
- The Security Meltdown
<https://www.csoonline.com/blog/the-security-meltdown/>

What you will learn today



- How to deal with ransomware and other types of cyberextortion
- Steps to ensure you don't become a victim
- What to do when you are a victim

What is ransomware?



HOME \ NEWS \ SECURITY

‘Ransomware’ among words added to Oxford English Dictionary in latest update

- A type of malicious software designed to block access to a computer system until a sum of money is paid.
- ‘although ransomware is usually aimed at individuals, it's only a matter of time before business is targeted as well’
- <https://en.oxforddictionaries.com/definition/ransomware>

It's real, expensive and getting worse



A Cyberattack Hobbles Atlanta, and Security Experts Shudder

By ALAN BLINDER and NICOLE PERLROTH MARCH 27, 2018



Observing, pondering, and writing about tech. Generally in that order. [FULL BIO](#) ✓
Opinions expressed by Forbes Contributors are their own.

Tax season can be pretty stressful, but malicious hackers don't care. As the filing deadline approaches, they'll ramp up their efforts to steal personal information and infect computers using tax-related scams. One nasty campaign that's been spotted recently tries to convince potential victims that they're late paying real estate taxes.

Why ransomware attacks

Ransomware attacks targeting businesses increased tenfold in the past two years

By Dan Patterson | February 12, 2018, 10:00 AM PST

Hackers held patient data system paid \$50,000

[Vic Ryckaert](#), vic.ryckaert@indystar.com Published 12:15 p.m. 1

A new ransomware-as-a-service scheme offers tools and tutorials for getting started with GandCrab, in return for a

MAR 30, 2018 @ 10:35 AM 2,304

Boeing Is The Latest WannaCry Ransomware Victim



Lee Mathews, CONTRIBUTOR
Observing, pondering, and writing about tech. Generally in that order. [FULL BIO](#) ✓
Opinions expressed by Forbes Contributors are their own.

The alarm bells were blaring this week at Boeing. In the early hours Wednesday morning, computers on the aerospace giant's network were being attacked by the WannaCry virus.



Ransomware attack on Hancock Health drives providers to pen and paper

The first reported hospital ransomware attack in 2018 was sophisticated – and not caused by an employee opening a malicious email.

by [Jessica Davis](#) | January 15, 2018 | 11:16 AM

Department in Dallas Lost Years of Evidence After a Cyberattack

They refused to pay the ransom of bitcoin worth \$4,000.

[AJ VICENS](#) FEB. 14, 2017 11:00 AM

Types of ransomware



Crypto ransomware

- Encrypts data and files
- Renders data useless until decryption key obtained
- Does not deny access to computing resources
- Targets weaknesses in user's security habits

Locker ransomware

- Denies access to computing resources
- Locks the endpoint - preventing victim from using it
- User can only interact with ransomware
- May be remediated using data recovery tools



Ransomware attack vectors



Email

- Usually sent as a Microsoft Office Document with a macro
- Sent as a JavaScript (.js), Windows Scripting File (.wsf) or PowerShell File.
- Targets weaknesses in user's security habits

Web

- Cerber and CryptXXX are delivered this way.
- Works in conjunction with exploit kits such as RiG, Sunset and Magnitude.
- Relies on unpatched browser plug-ins

Challenges in dealing with ransomware



- Most firms have not integrated ransomware into their incident response plans.
- Attackers out of legal jurisdiction
- Relatively new threat vector
- Victim often has no leverage if they don't have good backups

The best defense is good backups



- Ransomware exploits defects in a firms poor (or lack of) backup processes
- If you have good backups - don't pay the ransom, don't worry, and start your restoration plan
- If you don't have good backups, your options are sorely limited.



FBI Mantra: Follow the Money



Hard to follow the money - ransomware authors demand payment in anonymous crypto currencies

- Litecoin
- Bitcoin
- Peercoin
- Ethereum
- Namecoin
- Zcash
- ShadowCash
- Dash
- Monera



***Has ransomware exploded
because of bitcoin?***

Feature 23 FEBRUARY 2017

Bitcoin's anonymity is one of its greatest strengths, but it could also be the very thing that has led to the incredible rise of ransomware in recent years

Healthcare is a major ransomware target



- IDC 2018 - doubling of ransomware attacks on healthcare organizations.
- Impact on hospitals is well beyond simple financial losses.
 - Reports of ransomware that steal only patient data and sell it to third parties have also been documented.
 - The resulting susceptibility of hospitals to large-scale lawsuits both by individuals and governments is a threat that cannot be ignored.



Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

'Massive' Locky ransomware campaign targets hospitals

Ransomware – because It's so easy



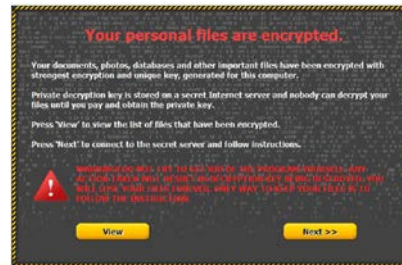
- Low-cost kits for generating ransomware are available for global distribution
- Ransomware variants have increased significantly since 2015.
- Cybercriminals are also using ransomware as a service (RaaS) as a distribution model, which will make it easier for less technically savvy cybercriminals to use ransomware to extort healthcare organizations
- Anti-virus software sees an encryption operation being performed (albeit by malware) and won't block it

How do you know if you have been infected?



You'll know it when you see it. Some signs include:

- Can't open your files
- When opening, error that file is corrupted or that it has the wrong extension
- Scary desktop message with instructions on how to pay to unlock your files
- Program warns you that there is a countdown until the ransom increases or you will not be able to decrypt your files
- Files in all directories with names like: HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML.



Effective backup processes



If you have good backups, you're blood pressure can go down a bit

- Enterprises that have effective backup/restoration processes in place
- that are tested regularly
- and off-site storage
- can likely easily recovery from a ransomware attack.

Backups must be fully isolated

- not a network share or shared drives
- completely segmented off the network

Information security and backups



- Enterprise information security is often not involved with backups
 - Generally handled by the DR/BC teams
 - But infosec will often be called in to help in the cleanup process
- CISO should develop visibility into backup processes
- Creating a comprehensive backup strategy is an involved process, especially for large enterprises with multiple types of data, files, and systems to protect.

Create a Bitcoin wallet



Attackers demand to be paid in Bitcoin(s)

- Setting up a wallet getting a Bitcoin can take time & blow a ransom deadline.
- Get a Bitcoin wallet now, and document its use
- Know where it is, who has access to it, and how to add funds.
- You may know need to install TOR
 - This is an easy step, but some enterprises block TOR



Ransomware sources



- Kaspersky Lab - more than 50% of ransomware attacks come from attachments in emails.
 - Using social engineering, a user is tricked into opening an email attachment, which launches the attack.
- Infected websites and online ads entice users to inadvertently download ransomware code.

To pay or not to pay...



- Survey of ransomware experts titled “Corporate IT Security Risks 2016” from B2B International shows that 19% of businesses did not recover access to their data even after paying the criminals.
 - Getting rarer as there’s honor amongst thieves.
- Paying could inadvertently encourage this criminal business model
 - But that’s not really your concern. You just want your data back
- If you don’t have any backups, then you may be forced to pay.



NO MORE RANSOM!



- Launched in July 2016 by a consortium of:
 - National High Tech Crime Unit of the Netherlands' police
 - Europol's European Cybercrime Centre
 - Kaspersky Lab
 - Intel Security
- Goal: help victims of ransomware retrieve their encrypted data without having to pay the criminals
 - <https://www.nomoreransom.org>

Steps to avoid being a ransomware victim



Backups and a tested DR/BC plan

- Off-site backup. Not connected to current network.
- Ensure backups are done for all critical data.
- If a restore is needed, ensure it's from a trusted non-infected backup.
- Update the DR plan regularly
- Ensure its comprehensive, thorough and tested.



Incident response




- Make sure your incident response team knows about ransomware
- ability to detect and conduct an initial analysis of the ransomware
- eradicate the ransomware
- recover from the ransomware attack by restoring data lost during the attack and returning to BAU
- conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident

Now that you are infected



RESOURCES

 **KnowBe4**
Ransomware Attack Response Checklist

STEP 1: Disconnect Everything

- ☐ a. Unplug computer from network
- ☐ b. Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC

STEP 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption

- ☐ a. Mapped or shared drives
- ☐ b. Mapped or shared folders from other computers
- ☐ c. Network storage devices of any kind
- ☐ d. External Hard Drives
- ☐ e. USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- ☐ f. Cloud-based storage: DropBox, Google Drive, OneDrive etc.

STEP 3: Determine Ransomware Strain

- ☐ a. What strain/type of ransomware? For example: CryptoWall, TeslaCrypt etc.

STEP 4: Determine Response

Now that you know the scope of your encrypted files as well as the strain of ransomware you are dealing with, you can make a more informed decision as to what your next action will be.

Response 1: Restore Your Files From Backup

- ☐ 1. Locate your backups
 - a. Ensure all files you need are there
 - b. Verify integrity of backups (i.e. media not reading or corrupted files)
 - c. Check for Shadow Copies if possible (may not be an option on newer ransomware)
 - d. Check for any previous versions of files that may be stored on cloud storage e.g. DropBox, Google Drive, OneDrive
- ☐ 2. Remove the ransomware from your infected system
- ☐ 3. Restore your files from backups
- ☐ 4. Determine infection vector & handle

RESOURCES

Response 2: Try to Decrypt

- ☐ 1. Determine strain and version of the ransomware if possible
- ☐ 2. Locate a decryptor, there may not be one for newer strains

If successful, continue steps...

- ☐ 3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)
- ☐ 4. Decrypt files
- ☐ 5. Determine the infection vector & handle

Response 3: Do Nothing (Lose Files)

- ☐ 1. Remove the ransomware
- ☐ 2. Backup your encrypted files for possible future decryption (optional)

Response 4: Negotiate and/or Pay the Ransom

- ☐ 1. If possible, you may attempt to negotiate a lower ransom and/or longer payment period
- ☐ 2. Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.
- ☐ 3. Obtain payment, likely Bitcoin:
 - a. Locate an exchange you wish to purchase a Bitcoin through (time is of the essence)
 - b. Set up account/wallet and purchase the Bitcoin
- ☐ 4. Re-connect your encrypted computer to the Internet
- ☐ 5. Install the TOR browser (optional)
- ☐ 6. Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been set up for this specific ransom case
- ☐ 7. Pay the ransom: Transfer the Bitcoin to the ransom wallet
- ☐ 8. Ensure all devices that have encrypted files are connected to your computer
- ☐ 9. File decryption should begin within 2.4 hours, but often within just a few hours
- ☐ 10. Determine infection vector and handle

STEP 5: Protecting Yourself in the Future

- ☐ a. Implement Ransomware Prevention Checklist to prevent future attacks

Use anti-virus software



Use antivirus software to protect your system from ransomware.

- Anti-virus vendors rely on static signatures (hashes) to identify malware, including ransomware.
- Ransomware writers automatically generate many copies daily and AV vendors often can't keep up.
- New approach: CryptoDrop monitors data, alert user when it notices data being transformed from useful formats to unrecognizable types.
 - Regardless of how a sample of ransomware tries to encrypt the file, it will stop the process.
 - And doesn't have to see your particular strain before it can stop it.

Practices to avoid becoming a malware victim



- Limit use of admin/root
 - If they operate as root, they're increasing chance that ransomware might manage to encrypt and corrupt data and DB.
- End-user awareness/education (train them on social engineering, email security, etc.)
 - But don't simply blame end-users and make them the guilty party
- SANS Institute:
 - most effective ways to combat ransomware attacks is a direct response
 - email security monitoring, sandboxing, employee awareness training/testing

More good practices to implement



- Pop-up blockers / ad blockers
- Strong endpoint security. All ransomware enters via a desktop, laptop, mobile, tablet, etc.
- Ensure your IR team is trained and processes in place to quickly handle an attack.
- Blacklist sites where possible
- Email server security
 - If relevant, use Microsoft *Software Restriction Policies*

An even more good practices to implement



- Segment Network
 - Prevent internal spreading via port 445 and RDP.
 - Block Port 445 at perimeter
- Disable Microsoft Office documents macros across the enterprise
- Automatically delete any incoming email attachments that are .js or .wsf files. Inspect any .zip, .rar, or .7z files.
- Disable unnecessary browser plug-ins
 - Especially Adobe Flash, Microsoft Silverlight, Java, and Adobe PDF

Patching and hardening



- It's 2018 and we have to remind firms to patch and harden
 - And therein lies the problem.
- Ensure *everything* is patched / all systems hardened
 - Anti-virus
 - Operating systems
 - Flash, Acrobat, Java, Desktops, laptops, mobile, smartphones.
- Out of support products
 - Now is a good time to eliminate non-supported products
 - Windows XP SP3, Windows 8, Windows Server 2003, etc.

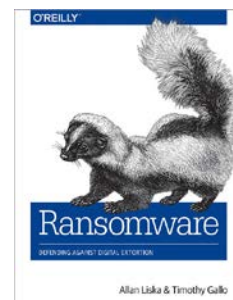


For more information.....



Ransomware: Defending Against Digital Extortion

- Allan Liska and Timothy Gallo
- FBI advice and position paper
 - <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf>
- Ransomware Hostage Rescue Manual
 - <https://info.knowbe4.com/ransomware-hostage-rescue-manual-0>
- Anti-virus vendor sites





- Ransomware is an attack which exploits weaknesses in information security and data backups
- An effective data backup and restoration process, combined with an equally effective incidence response program is a powerful double-edged strategy to successfully deal with the ransomware threats
- Questions / comments ?





Ben Rothke CISSP, PCI QSA
Nettitude
@benrothke