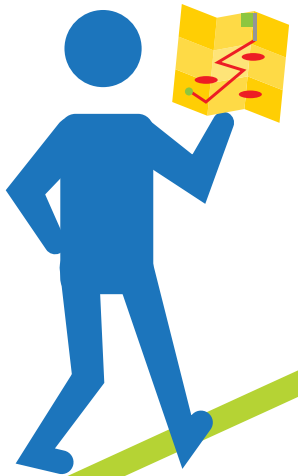
Barracuda MSP

The Smarter MSP's Guide to Ransomware



CONTENTS

Introduction

Ransomware has become a serious epidemic affecting businesses of all sizes, and protecting your customers is more essential than ever before as the number of ransomware attacks continues to rise. A report from Cybersecurity Ventures projects that on average **there will be a ransomware attack on a business every 14 seconds by the end of 2019 — up from a rate of one attack every 40 seconds in 2017**.[1]

As ransomware spreads, it continues to evolve and get more sophisticated — and more destructive. In fact, the Cybersecurity Ventures report predicts that **damages connected to ransomware attacks will cost $11.5 billion annually by 2019**, more than double the $5 billion in ransomware damages estimated for 2017.[1]

What does all this mean for managed service providers? As the IT professional tasked with protecting your customers from cyber threats, you need to keep ransomware and cybersecurity top-of-mind and educate your customers about this destructive type of malware and the damage it can do to their business.

To help you address the growing threat of ransomware, we've taken a closer look at how ransomware works and the most common variants that are active today. We've also gathered our best advice on how to protect your customers both proactively by taking precautions to help them avoid ransomware and reactively by helping them recover quickly and easily if they do fall victim to an attack.

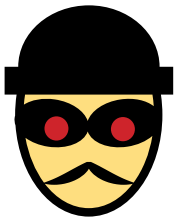
1. Ransomware Damage Report 2017 Edition, Cybersecurityventures.com, Retrieved February 2018.

What is Ransomware?

What is ransomware?

Ransomware is malicious software that encrypts files, locks the computer, and retains control until the user pays a certain amount of money. Ransomware can appear in two forms — either by locking your screen with a full-screen image or webpage to prevent you from accessing your PC, or by encrypting your files so they can't be opened. [2]

While each ransomware variant has its own twist, there a few key components that most ransomware types follow:



Email-borne infection – Although some variants have been known to attack via drive-by download advertising, malicious websites, or peer-to-peer network file sharing, ransomware typically attacks through spoofed emails, and the end user is tricked into opening an attachment. [3] Often arriving in zip files with enticingly common names, the zip file contains an .exe, which downloads onto the target computer, adding a key to the Windows Registry, allowing it to run.

Covert communication – Once downloaded, the malware establishes communication with a command-and-control server. For example, CryptoLocker, which started the modern ransomware craze, relies on a domain generation algorithm and hops between new servers routinely to avoid detection.

Advanced encryption – Once the server connection is established, CryptoLocker generates a pair of encryption keys — one public, one private — using the huge RSA-2048 bit encryption algorithm and military-grade 256-bit AES encryption. Most ransomware variants use a 256-AES (Advanced Encryption Standard) key or a 2048-RSA key, but some even go as far as 4096-RSA.

Bitcoin ransom – After encryption is complete, the cybercriminals usually demand Bitcoin or some form of payment for the key to unencrypt infected files. [4] Ransomware works quickly and quietly in the background before it unveils itself to users asking for ransom.

Tight deadline – A pop-up window usually tells the victim that important files have been encrypted and sets a time limit for payment before the private encryption key is destroyed and the files are lost forever.

Experts predict there will be a ransomware attack on a business **every 14 seconds** by the end of 2019 — up from one attack **every 40 seconds** in 2017. [1]

2. What is ransomware?, Microsoft, retrieved September 2016.

3. Cryptolocker 2.0 – new version, or copycat?, We Live Security, December 2013.

4. CryptoLocker Ransomware Information Guide and FAQ, Bleeping Computer, October 2013.

The Most Recent **Ransomware** Threats

Ransomware has grown tremendously since CryptoLocker first made a name for itself in 2013. With new variants of ransomware appearing on a daily basis, it can be tough to keep track of what the newest threat is. So we rounded up the top threats that could have a lasting impact on the ransomware landscape:

1. Locky

What defines Locky: Locky uses macros in a Word document to insert code into an IT environment that encrypts all of the organization's data. [6]

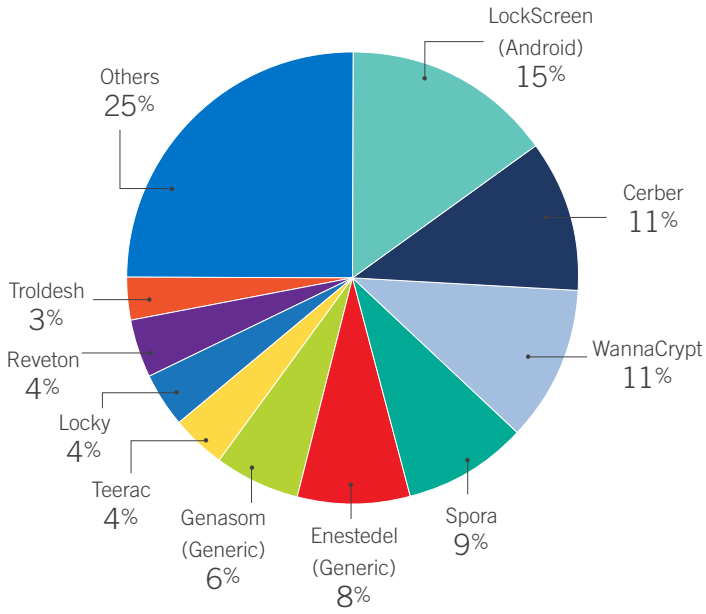
Most recent variant: Zepto infects computers with a ".zip" file email attachment that contains malicious JavaScript. The JavaScript runs quietly on the victim's machine, slowly locking files with the ".zepto" extension. The newest version, which appeared in September 2016, uses an embedded RSA key and abandons communication with C2 servers. [7]

2. Cerber

What defines Cerber: Cerber installs itself on the victims PC and is activated by enabling macros. After encrypting user's files and adding the ".CERBER" extension to them, it asks users to pay the ransom in Bitcoin, and if the ransom goes unpaid for more than a week, the ransom is doubled. [8]

Most recent variant: Cerber3 appeared in August 2016. The file extension added to encrypted files ends with ".Cerber3," and it renames the ransom note to #HELP DECRYPT #.txt. [9]

Top ransomware families [5]



5. Malware Protection Center, Microsoft, Image retrieved February 2018.

6. Here Comes Locky, A Brand New Ransomware Threat, Dark Reading, February 2016.

7. Locky now using Embedded RSA Key instead of contacting Command & Control Servers, Bleeping Computer, September 6, 2016.

8. Combatting the ransomware Blitzkrieg, ICIT, April 2016.

9. Cerber Ransomware Has a New Family Member – Cerber3 Has Been Spotted, Virus Guide, August 31, 2016.

3. WannaCrypt/WannaCry

What defines WannaCrypt/WannaCry: WannaCry ransomware exploits a Windows vulnerabiltiy called EternalBlue to spread quickly. Microsoft released a patch in March 2017, but WannaCry spread rapidly to dozens of countries, infecting tens of thousands of machines in May 2017 and making headlines around the globe.[10] The massive impact of the ransomware strain made it clear that many organizations weren't up to date with their security patches.

4. NotPetya

What defines NotPetya: Originally thought to be a strain of Petya — a type of ransomware that debuted in 2016 and encrypted portions of a machine's hard drive [11] — NotPetya wrecked havoc worldwide in June 2017. The new malware acts like ransomware, but flaws in the code make infected computers unrecoverable, suggesting that NotPetya was designed to cause destruction, not make money [12]

39% of corporate IT professionals estimate **recovering** from a successful **ransomware attack** would take up to **a few weeks** [13]

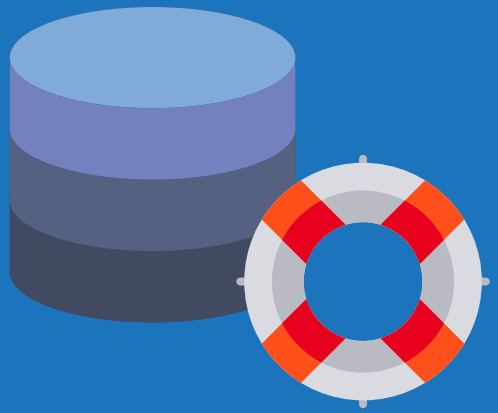
10. The Ransomware Meltdown Experts Warned About Is Here, Wired, May 12, 2017

11. Petya Ransomware Skips the Files and Encrypts Your Hard Drive Instead, BleepingComputer.com, March 25, 2016

12. The NotPetya Ransomware May Actually Be A Devastating Cyberweapon, Forbes, June 30, 2017

13. Ransomware 2017 Report, Cybersecurity Insiders, Access February 2018.

3 Steps to Recover from Ransomware



3 Steps to Recover from Ransomware

What do you need to do as an MSP if ransomware strikes one of your customers? You should take the following three steps immediately after an infection is discovered.

Step 1: Disconnect from the network and stop backing data up immediately

Instruct your customer on how to disconnect the infected machine from the network immediately after the infection is discovered. Not only do some ransomware variants encrypt shared files on the network, but you're also stopping the malicious software from overwriting clean backups with infected files. You should check and see if any other machines have been affected as well.

Step 2: Remove ransomware and clean computers of malicious software

If you have a good restore, remove all traces of the ransomware using antivirus software or an appropriate malware remover before proceeding. Don't test or try to recover data until the ransomware is completely gone. It's important to note that by removing the ransomware you are effectively forfeiting your ability to unlock files by paying the ransom. This shouldn't be a problem if you have backed up the customer's data to a separate offsite location and don't intend to pay the ransom. As an added precaution before you restore files, conduct a test run in Safe Mode on the network to see if there are any additional infected files.

Step 3: Restore from the most recent clean backup

Provided that the customer maintains consistent backups, locate a clean version of the files, and restore to your customer's latest backup set. Unfortunately, if the customer hasn't followed best practices for backup, they won't have an alternative. They'll either need to pay the ransom or accept that all of their data is gone.

Best Practices to **Protect** Your SMB Customers from **Ransomware**

Best practices to protect your SMB customers from ransomware

Tip #1: Educate users on security best practices

Education is still the best way to help SMBs avoid infection by ransomware — or any other form of malware. Make your customers aware of popular social engineering methods and tactics so they don't fall victim to phishing emails or spoofed messages. It's particularly helpful to share examples of these kinds of emails and the types of attachments that are often associated with social engineering attempts so that end users know to avoid them.

A few security best practices to share with your clients:

- Do not open emails from strange or unfamiliar email addresses
- Do not disable or deactivate antivirus or anti-malware software
- Do not download software from torrent sites — official or direct downloads are preferable
- If you receive an email from a familiar contact that includes an attachment or link, verify separately that the person or organization actually sent you this message

Tip #2: Consistently update operating systems, antivirus and anti-malware software

Most security vendors are constantly working on updates to catch and stop ransomware before it infects your customers' files. If you resell antivirus or anti-malware services to your customers, be sure they are running the most recent versions of these products and do regular updates. Contact your vendors to learn more about how they're defending against ransomware to see if there is any additional protection available to your customers.

Ransomware damages are expected to climb to

$11.5 Billion in 2019

It's also important to be sure your customers' operating systems are up to date with the latest security patches to avoid leaving any backdoors open. Often, backdoors are fixed in the latest patch or update, and hackers can prey on companies running out-of-date software, which gives them an easy "in" to the system.

Tip #3: Disable macros in Office documents

Many new ransomware strains trick users into running macros on Microsoft Office programs. Macros automate frequently used tasks and hold a potentially serious security risk. If malicious macros are introduced, it starts with one file and quickly spreads. Microsoft Office 2016 automatically disables macros, but if your customer is using an older version it can be disabled on a GPO (Group Policy Object). [14]

Tip #4: Prevent .exe from running in AppData or LocalAppData folders

Ransomware usually operates within the AppData or LocalAppData folders, so you may be able to prevent the initial malware download from executing by blocking .exe files from running in these folders.

Tip #5 Set up a cloud-generation firewall

Cybercriminals are releasing new malware variants into the wild at an increasingly fast pace. A cloud-generation firewall can combat numerous threats, and some can even detect zero-day threats before they infiltrate the system. Zero-day exploits are expected to increase from one per week to one per day by 2021, so the threat is growing. [15]

Firewalls help your SMB customers be proactive about defending against ransomware instead of just reacting to an attack. "Network security is akin to a home alarm system, whereas BDR is like a home owner's insurance policy that comes into play if something is stolen or damaged," says Brian Babineau, senior VP and general manager of Barracuda MSP. [16] Explaining it to your SMB customers that way will help them understand the importance of both approaches. Network security, like a cloud-generation firewall, goes hand-in-hand with a comprehensive BDR plan when protecting your customers from the latest ransomware threats.

14. Enable or disable macros in Office documents, Microsoft, Retrieved September, 2016.

15. Zero Day Report, Cybersecurity Venutres, Accessed February 2018

16. 3 Ways to Supercharge Your BDR Offering, Business Solutions Magazine, September 2016

Tip #6: Back up your data frequently and consistently

Offsite backup is a critical component to a ransomware recovery strategy and should be an integral part of your disaster recovery plan.

Why offsite? Because ransomware infections have been known to infect local drives and network shares that are mapped as a drive letter on the infected computer.[17] That means if you're using only a local backup solution, there's little chance of recovery without paying the ransom because your backups will most likely get encrypted as well.

1.Keep multiple versions of your protected files

Certain cloud backup offerings provide the advantage of sophisticated version histories, which is a critical component to successful restores after a ransomware infection. If you only back up a single version of your customers files, it's possible that your software has backed up an infected file. By saving as many revisions as possible, you have a better chance of restoring to a clean version of the data.

2. Keep multiple days' worth of files

Depending on how frequently you perform backups for a customer, it's possible to store multiple versions of a single file, all of which were backed up the same day. But it's important to also back up several days' — or even weeks' — worth of files to ensure maximum protection. By retaining clean backups over days, weeks, or months, IT solution providers give themselves additional safe restore points, raising the likelihood of a successful restore.

3. Frequently test your restores

SMBs' backups are only as good as the restore. Test your customers' restores on a frequent basis to make sure their data is being backed up properly.

More than **52%** of **small businesses** have experienced a **ransomware attack** in the past 12 months [18]

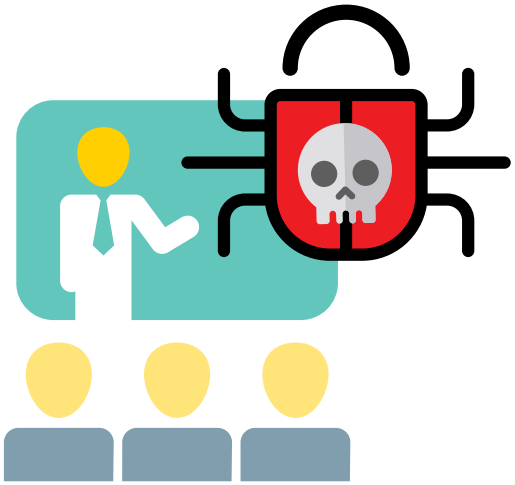
17. 2016 Vulnerability Review, Flexera Software, March 16, 2016.

18. 2017 State of Cybersecurity in Small & Medium-sized Businesses, Ponemon Institute, September 2017.

Conclusion

The FBI wants businesses to take ransomware seriously. "Because of the global reach of cybercrime, no single organization, agency, or country can defend against it," the organization explained in a recent statement about the growing threat of ransomware.[19]

As an MSP, it is impossible to stop the ransomware epidemic. However, taking the right proactive and reactive measures can help you mitigate the likelihood of an attack for your customers. No business vertical, large or small, is immune to ransomware attacks, and it is your job to manage your customers' network and set them up for success with best practices and tools to defend against it.



Watch our on-demand webinar:
Strategies for Stopping Email-Borne Threats

19. Cyber Crime, FBI, Retrieved September 2016.