Enterprise Ransomware Survival Guide

The Ultimate Playbook to Keep Your Data Safe

Infrascale™

TABLE OF CONTENTS

INTRODUCTION

Ransomware attacks are increasing, and so is the price to get your data back and systems running. The FBI recently reported, that hacking victims have paid "more than $209 million in ransom payments" in the first three months of this year, compared with $25 million in all of 2015." And while no one is immune the recent high profile attacks have established a pattern that hospitals, police stations, and schools are targets. **Why?**

ALL THREE PUBLIC INSTITUTIONS HAVE THESE TWO THINGS IN COMMON:

1. They all lack sophisticated cyber security infrastructure (i.e. anti virus, backup, disaster recovery).
2. They are open 24/7 and have irreplaceable data.

This combination makes these institutions vulnerable and easy targets. And without taking the proper preventative measures they are stuck with the FBI's recommendation "to just pay up". So, what can be done? This ebook will provide you with a new set of best practices, from prevention to recovery, so you can keep your data safe from ransomware.

"Ransomware extortionists will wreak havoc on corporate IT infrastructures in 2016 like never before."

Institute for Critical Infrastructure Technology

ICIT

RANSOMWARE TRENDS

2,900 new malware modifications were detected in Q1 2016.

72% of ransomware victims were unable to access their data for 2 days.

$209,000,000 has been paid in ransomware in the first 3 months of 2016.

34% of SMBs fell prey to phishing emails in 2015.

(Source: Kaspersky Lab Q1 Threat Evolution Report, May 2016)

(Source: Intermedia 2016 Crypto-Ransomware Report).

(Source: ThreatTrack Security, March 2015).

(Source: Verizon 2015 Data Breach Investigations Report).

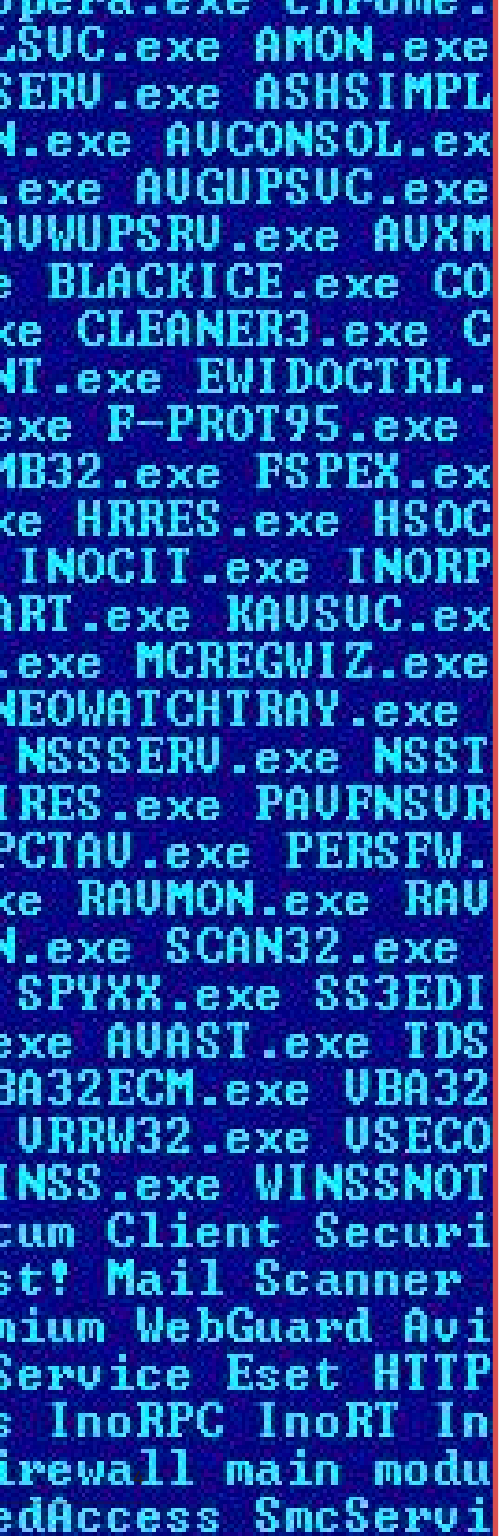
WHAT IS RANSOMWARE?

Ransomware can take different forms, but it is a type of malware that denies access to a device or files until a ransom has been paid. Ransomware encrypts your employee's or corporate files and forces you to pay a fee to the hacker in order to regain access to their files.

Ransomware encrypts the files on a workstation, and can travel across your network and encrypt files located on both mapped and unmapped network drives. It's how one infected user can bring a department or entire organization to a halt.

Once the files are encrypted, the hackers will display a screen or webpage explaining how to pay to unlock the files. Historically, ransoms started in the $300-$500 range, but fast forward to 2016 and companies are being hit with ransoms in the thousands of dollars.

Paying the ransom invariably involves paying a form of e-currency (cryptocurrency) like Bitcoin. Once the hackers verify payment, they provide "decryptor" software, and the computer starts the arduous process of decrypting all of the files.



STRAINS OF RANSOMWARE

With over 2900 new malware modifications reported in the first quarter of 2016, it's hard to keep up with all of the latest threats. Here are a few examples of some of the basic types of ransomware in circulation.

LOCKY

Locky renames all of your important files so that they have the extension .locky and encrypts them so only the cyber criminals have the decryption key. You can buy the decryption key from them via the dark web for $400 in bitcoin.

CRYPTOLOCKER

CryptoLocker targets computers running Microsoft Windows and restricts access to infected computers. Like other ransomware strains, victims need to provide a payment to the attackers in order to decrypt and recover their files. CryptoLocker appears to have been spreading through fake emails designed to mimic the look of legitimate businesses and through phony FedEx and UPS tracking notices.

CERBER

When infected, a victim's data files will be encrypted using AES encryption and will be told they need to pay a ransom of 1.24 bitcoins (or $500) to get their files back. It can play a text-to- speech or synthesized recording, show a web page, or a plain text document. Unfortunately, there is no known way to decrypt a victim's encrypted files for free.

RANSOM32

Ransom32 is a variety of "ransomware-as- a-service" that effectively puts the power to create ransomware into the hands of just about anyone - regardless of their technical know-how. What makes Ransom32 really dangerous is that it is coded entirely using JavaScript, which means it can be used to target computers running Windows, Mac OS X and Linux.

JS/FAKEBSOD

FakeBsod uses a malicious piece of JavaScript code to lock your web browser and show a fake warning message when you visit a compromised or malicious webpage. The warning message tells you to "contact Microsoft technicians"about an "Error 333 Registry Failure of operating system – Host: Blue screen Error 0x0000000CE". If you call the phone number in the message you will be asked to pay money to "fix" the issue.

HOW DO COMPANIES GET INFECTED?

Hackers primarily use the following vectors to infect a machine: phishing emails, unpatched programs, compromised websites, poisoned online advertising and free software downloads. An attack typically starts when a user opens a malicious email attachment that installs a virus on to their desktop that begins encrypting all of their files.

PHISHING ATTACKS

By far the most common scenario involves an email attachment disguised as an innocuous file. Many times hackers will send a file with multiple extensions to try to hide the true type of file you are receiving. If a user opens the email attachment or clicks on a link to a software download, without verifying its authenticity, the ransomware infection begins.

DRIVE-BY-DOWNLOAD

Increasingly, infections happen through drive-by downloads, where visiting a compromised website with an old browser, software plug-in, or an unpatched third party application can infect a machine. The compromised website runs an exploit kit (EK) which checks for known vulnerabilities. Often, a hacker will discover a bug in a piece of software that can be exploited to allow the execution of malicious code. Once discovered, these are usually caught and patched by the software vendor, but there is always a period of time where the software user is vulnerable. Examples of exploits can range from vulnerabilities in an unpatched version of Adobe Flash, a bug in Java or an old web browser, and an unpatched operating system.

FREE SOFTWARE

Another common way to infect a user's machine is to offer a free version of a piece of software. This can come in many flavors such as "cracked" versions of expensive games or software, free games, game "mods", adult content, screensavers or bogus software advertised as a way to cheat in online games or get around a website's paywall. By preying on the user in this way, the hackers can bypass any firewall or email filter. For example, one ransomware attack exploited the popularity of the game Minecraft by offering a "mod" to players of Minecraft. When users installed it, the software also installed a sleeper version of ransomware that activated weeks later.

AM I INFECTED?

Educate your employees to notify you if they experience any of the following symptoms:

- ☑ They suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension.
- ☑ A window has opened to a ransomware program and you cannot close it. This is usually accompanied with an alarming message with instructions on how to pay to unlock your files.
- ☑ The program warns you that there is a countdown until the ransom increases or you will not be able to decrypt your files.
- ☑ You see files in all directories with names such as HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML.

Here is an example of a CryptoLocker screen:

RANSOMWARE EVOLVING PAST NUISANCE COSTS (AND CONSUMERS)

Initially, attempts to extort money were largely confined to consumers; but that's changing fast.

Cyber criminals are increasingly targeting vulnerable organizations, from hospitals and schools to police stations, where the ransom amounts can be significantly greater than those targeting consumers. And hackers are raising the stakes by crippling systems (i.e email, CRM), which means that companies are paying higher ransoms and absorbing larger downtime costs.

The recent attack at Hollywood Presbyterian hospital signaled a shift from the "high volume, low-dollar crimes" business model to larger scale attacks that yield bigger paydays. From an IT perspective, this highlights a need for more sophisticated backup and restore, and disaster recovery capabilities.

5 STEP GUIDE TO CONTAIN RANSOMWARE INFECTIONS

Ransomware is hard to detect while it's encrypting user files and the average user may not recognize the danger until the ransom demand finally appears.

This means that you may not learn about the infection until after the damage has begun and the malware is already inside the network. At this point, your priority has to be to contain the virus and prevent it from spreading within the network. We recommend you do the following.

1. REMOVE INFECTED MACHINE FROM THE NETWORK. Always assume that the malware could make use of an internet connection (i.e. sending information back to the criminals, or spreading itself to other users). In the worst-case scenario, you should turn off network access for the entire office until you can get the outbreak under control.

2. RESET YOUR BIOS TIME. According to David Balaban with Privacy PC, IT admins don't need to be afraid of the ransomware's countdown timer that imposes a deadline at which point the ransom doubles. Just set your BIOS time back. This will reduce your stress and give you more time to recover your key files and eliminate the malware.

3. ROLL BACK FROM PREVIOUS BACKUP. Having a recent backup (and access to unlimited version history) will make it easy for you to restore your operations as quickly and painlessly as possible, saving time and money for both you and your customer. As the downtime stakes have increased with each ransomware attack, having a backup solution in place and regularly testing backups to make sure they're running properly is a critical part of protecting your company from ransomware.

   Determining which backup to restore after a ransomware infection is imperative, but you must first ensure that your most current backup does not also contain the infection.

   > PRO TIP: A better way to identify your recovery point – the point at which your files were uninfected – is to leverage a disaster recovery as a service (DRaaS) solution. The ability to quickly 'spin up' a DR image on your local appliance gives you the ability to confirm that the image you're restoring does not contain the infection. Plus, by spinning up the image in a self-contained VM, you can inspect the DR image without exposing it to the local network.

4. STAY CURRENT WITH THE LATEST THREATS. IT admins can stay up to date on the latest ransomware threats by following sites such as Bleeping Computer or the Microsoft Malware Protection Center. These technical support sites provide powerful self-education tools to learn about the latest security threats.

5. ALERT AUTHORITIES. Ransomware is a serious form of extortion. Notify the FBI and don't be tempted to pay the ransom. Paying them would be a mistake because they might continue to extort you and may not release your information.

RANSOMWARE BEST PRACTICES

As ransomware attacks increase, it's only a matter of time before your customer calls seeking your help. And while there is no silver bullet, here are the top best practices you can employ to prevent and mitigate the impact of ransomware.

IMPORTANCE OF ENTERPRISE CLOUD BACKUP

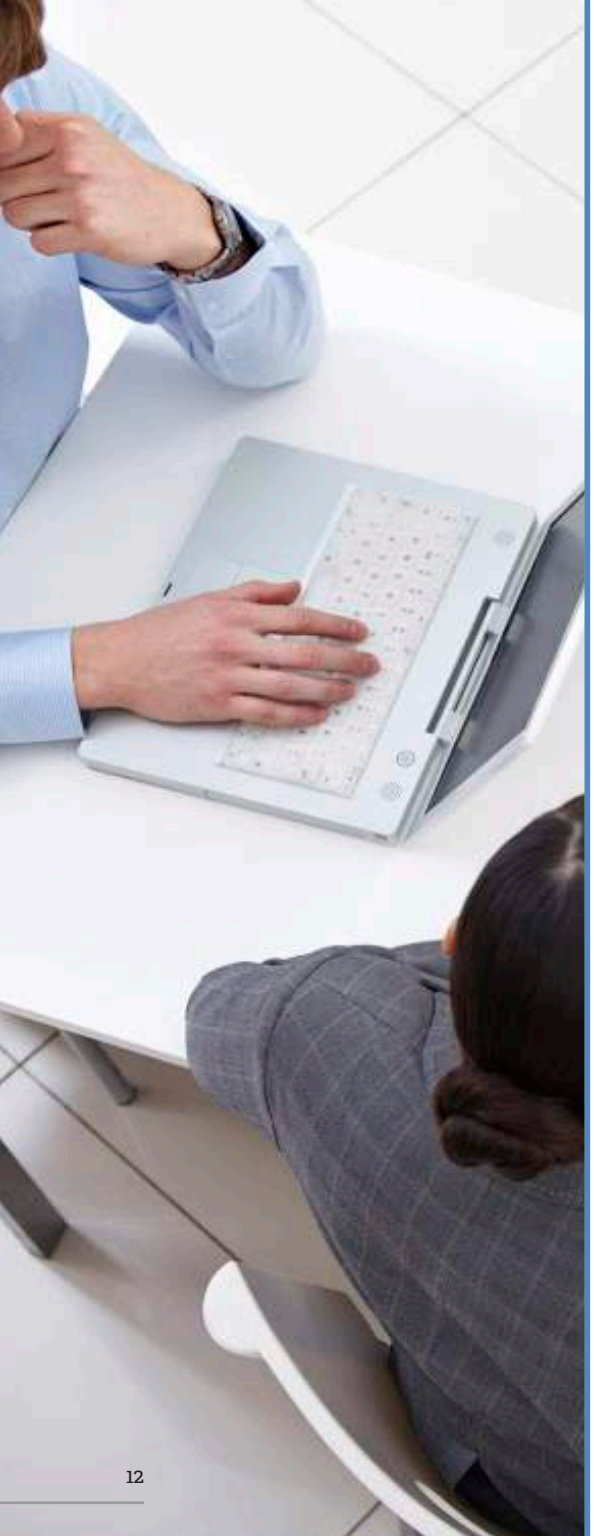
You may think all backup solutions are the same. But when it comes to thwarting ransomware, the limits of consumer-grade backup severely reduce the impact you can make. **Why?**

MIND THE GAP: LIMITED VERSION HISTORY

Many consumer-grade backup services only preserve a limited version history, so many IT admins find them useless in safeguarding employees from ransomware. If your current backup solution only retains a limited version history, you'll be stuck with recent backups that include the newly encrypted files that contain the malware. And you won't be able to restore critical files from a historic clean backup.

ENTERPRISE SUPERHERO POWER: UNLIMITED VERSION HISTORY & DRAAS

A proper enterprise-grade cloud backup solution maintains a complete version history of your data, not just a portion of it. This will enable you to restore to any earlier revision just prior to the ransomware infection which could have happened weeks before the ransom message appears. Some cloud backup vendors offer cloud-backed disaster recovery as a service to provide you with the fastest and reliable way to identify a recovery point.



EDUCATING YOUR CLIENTS

Even if you have all the right technical safeguards (such as antivirus software, spam filters and firewalls) in place at your company, employees can still fall victim to ransomware. All it takes is one person to accidentally click on a suspicious link or open the wrong attachment, and a whole system could be infected. According to Gary Pica with TruMethods: “To help combat this, you need to teach your employees about what ransomware is, how it can hurt their business and the warning signs they should watch out for.”

This should include training your clients to:

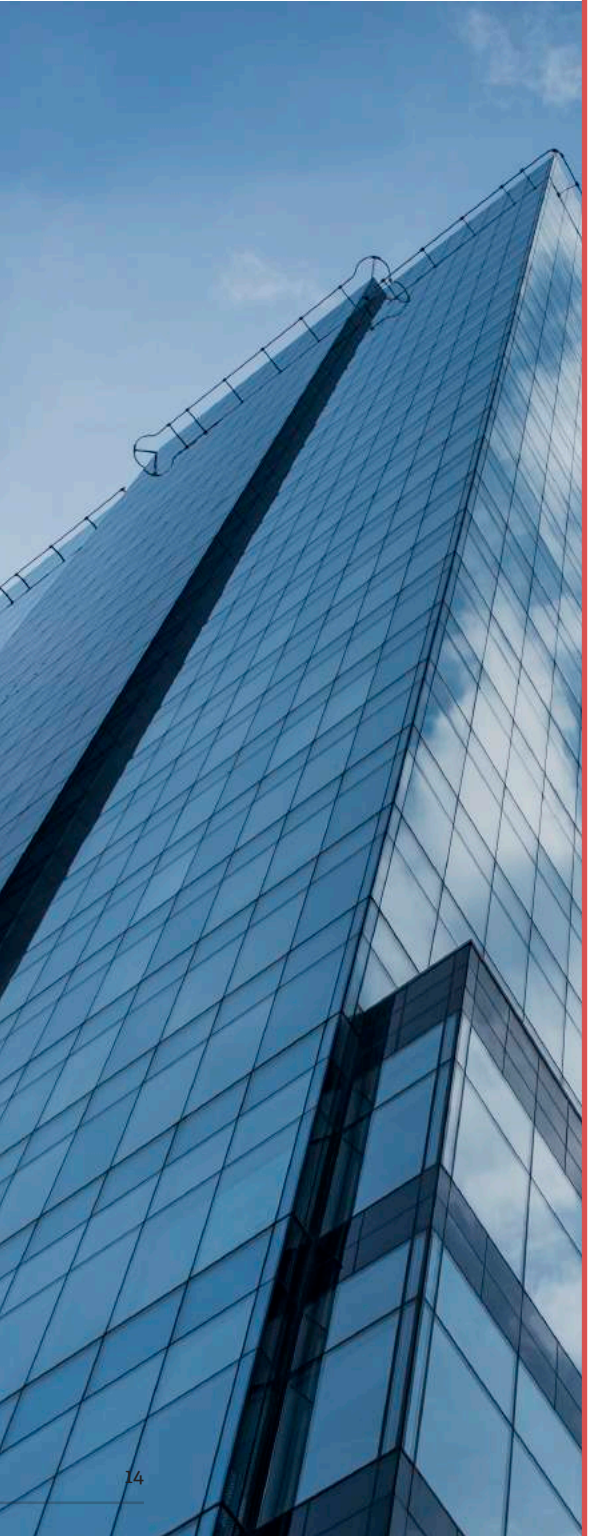
1. USE REPUTABLE ANTIVIRUS SOFTWARE AND A FIREWALL. Maintaining a strong firewall and keeping your security software up to date are critical. Anti-malware programs are built to deal with malware after it gets onto a machine and include pro-active monitoring of your system to identify potentially risky programs or behaviors, even if there is not yet a known definition.

2. EXERCISE CAUTION. Don’t click on links inside emails, and avoid suspicious websites. According to security experts, one of the principal infection vectors of ransomware is through Javascript attachments sent in spam email. If your PC comes under attack, use another computer to research details about the type of attack. But be aware that hackers are devious enough to create fake sites, perhaps touting their own fake antivirus software or their de-encryption program. Partners and system administrators must be proactive in filtering incoming messages and use security programs to prevent users from mistakenly opening malware.

3. BACK UP OFTEN. If you back up files to either an external hard drive or to an online backup service, you diminish the threat. Even if your mail security, AV and anti-malware fail, your backups will be your final option to avoid paying costly ransoms to protect your data. Security guru and expert Bruce Schneier stresses the importance of 'good backups' as the most important piece of any IT framework because your backup is your last resort.

4. ENABLE POPUP BLOCKER. Popups are a prime tactic used by hackers, so installing a pop-up blocker reduces the risk of clicking on an infected popup.

5. DISCONNECT FROM THE INTERNET. If you receive a ransomware note, disconnect from the Internet so your customer's personal data isn't transmitted back to the criminals and shut down the computer.



CONCLUSION

The rapid revolution of ransomware is raising the stakes for every business and prompting considerable changes to current best practices in order to protect data. A solid data backup and disaster recovery plan is proving to be an IT admin's best friend in this fight. If you can replace the encrypted data, then these cybercriminals have no leverage. You can always count on attackers being able to get in the front door, but with the right recovery capabilities you can stop the threat before damage is done.