SIM2K

Adapting Technology to Your Business Needs

# Ransomware


## Don’t Fall Victim To Ransomware Attacks

### What to look for and how to mitigate exposure to this malware

A special report from SIM2K – Technology Consultants

Theft is theft. No matter how you disguise it, stealing is a time-tested flaw in our society. Whether it was Willie Sutton robbing banks "because that's where the money is" or a mugger stealing your wallet, the concept is the same. But in the realm of technology, theft has taken on a new twist. Rather than the robber having to go steal money *from* you, why not have you just go ahead and *send them* the money? And what could that robber do to get you to send money with no questions asked? Why not take all your important files and lock them up in a way you can't access your own data until you pay up? Thus the creation of Ransomware.

Ransomware is a growing problem for consumers and businesses alike. In a recent report from Symantec, the company's security researchers found all **targeted attacks** – including ransomware – **grew 91% year-over-year**. One estimate says businesses paid more than $27 million in the first months following the release of the Cryptolocker virus in September 2013, the first such Ransomware attack of significance. And the "bad guys" keep getting smarter. A variant, CryptoWall, was reported to rake in $325 million in just 18 months in the US alone. And the problem keeps getting worse as the new versions get even more sophisticated. Ransomware infections are already harassing small and medium businesses, according a survey by a security firm that found 60% of its partners have experienced one to five Ransomware attacks in the last year. **The FBI estimates cybercriminals raked in $1 billion last year in ransom payments.**

## What is Ransomware?


Ransomware infections work by targeting the victim's data and encrypting it. The virus is delivered in a variety of ways, either phishing e-mails, infected programs or poisoned on-line websites. These will be discussed in depth later on. When triggered, the virus launches **an attack that encrypts all the data it can find**. The software is smart enough to cross your network and encrypt any files located on both mapped and unmapped network drives. In other words, the action of one unsuspecting user can cripple the entire organization and bring all work to an immediate halt.

Once the files are encrypted, the hackers will then display some sort of screen (as shown to the left) announcing their attack, and providing details on what the company must do to unlock the files. The Ransomware threatens to delete the data unless a payment, usually in bitcoin, is made. **And, the data cannot be recovered without paying to obtain the "key" that decrypts all files**.

There is usually a time element involved for paying the ransom. As time expires, the monetary demand also increases. While the first demand may be in the $300 to $500 range, it can quickly escalate into tens of thousands of dollars as time passes.

The encryption in this attack typically uses the RSA 2048 protocol, the strongest level of encryption available. To demonstrate how powerful this encryption is, it would take the average desktop computer around 6.4 quadrillion years to crack an RSA 2048 key. This is why the hackers believe they have you in the "no-win" position, as paying the ransom is the only way to un-encrypt your data.

Paying the ransom means obtaining Bitcoins, an Internet currency, to pay off the hacker. This way the payment is untraceable. Once the hackers can verify the payment is made, they release the "decryptor" software that will defeat the RSA key and restore files to a readable state, a process that could take days, depending on the degree of encryption done to your connected machines and quantity of data. Of course, there is the possibility that the hacker might "take the money and run" and not release the decryptor, but most "ethical hackers" will do so as they wish the next victim to pay up, which they might not if the Ransomware variant has the reputation for not complying with the end game.

## It Happens Right In Your Backyard

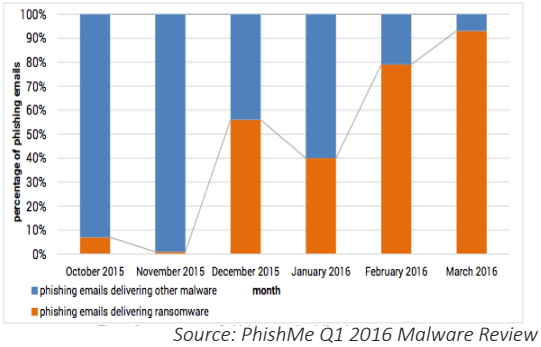
Madison County, Indiana, population of about 130,000, was the victim of a Ransomware attack in November of 2016. Government workers were forced to go back to using pen and paper without working computers, constituents were angry, and the County Commissioners unanimously voted to pay the ransom. County residents making special trips to the courthouse were turned away, or their information was jotted down on paper. County Auditor employees took vacation or burned personal time off, since "without the computer system there could be no work done," auditor Jane Lyons said. "We have to access all our information on the computers." The Ransomware attack affected 600 personal computers and some 75 servers.

After the attack occurred, Madison County IT Director Lisa Cannon was asked by reporters how could this happen "to an entire county's computer system?" In return, Cannon explained that the IT department took all the security measures they could have, but hackers found a way in. She was asked "Wouldn't taking all the security measures possible have included having off-line backups, or at least some backups?" Cannon told the media, "We're in the process of adding a backup system." Unfortunately, that was too little too late.

It is now estimated this attack ended up costing Madison County more than $200,000. The County Commissioners first paid the ransom and then approved contracts providing for off-site data storage, firewall protection and a backup court system. County officials say these contracts total $198,180. That's in addition to the $21,000 ransom paid to obtain encryption keys and get control of the county computers from the hackers. This figure also does not include the cost for the weeks spent restoring the county's government computer system and the lost productivity for all county offices while the computer network was down. **What would the cost be to your organization if this were to happen to you?**

## How Ransomware Infections Happen

To launch a Ransomware attack, the hacker must first gain access to a computer which then opens the door to your network. How does anyone become infected with Ransomware? Security experts have identified **seven ways companies are exposed to this malware:**



*Source: PhishMe Q1 2016 Malware Review*

**1) Phishing –** 93% of all phishing e-mails are now Ransomware. Phishing consists of a fraudulent e-mail that appears to be from an official source, such as a supervisor, a bank, or a partner organization. The e-mail includes an attachment which, when downloaded, infects the target computer. Once embedded in the computer, the malware typically spreads itself across the network. Network users need to be attentive to the signs that an e-mail is illegitimate. These can include things like poor spelling and grammar, broken or unusual images, unfamiliar names or headers, and so on. Users should not download any attachment from a source they are unfamiliar with, nor initiate installation of any programs from an untrusted source. A more defined phishing attack, dubbed "spearphishing" is even more insidious as it spoofs the name and e-mail address of a company official thus tricking the user into thinking that this is a legitimate e-mail. Here the user must be sure that the domain name is truly that of the company, as the hacker often will register a "close-to" domain name, with just a subtle mis-spelling, hoping that the user overlooks this difference. Also, the hacker may obtain company officials' names from the company website or a business directory service, so the user must be alert to any oddities in the e-mail. For example, does the company president use his full name or does he always refer to himself by a nickname (Jeff vs. Jeffrey) in company communications? And too, the user must consider the request in the e-mail in light of their regular duties for the company. Does that person expect to get an invoice sent to them, or receive some shipping notice from UPS or FedEx? If this falls outside of their day-to-day work, this should immediately raise a red flag. Remember, if the user doesn't trigger the virus, the infection doesn't occur, so proper training of employees on what to look for is critical here.

**2) Existing Botnet** – A botnet is a network of computers that has been covertly infiltrated by some form of malware. The owners and operators of the hardware that makes up the botnet typically don't realize that it has been compromised. Operating across dozens, hundreds, or even thousands of computers, software on the botnet orchestrates disruptive assaults on other networks. Botnets rob networks of their IT resources and gradually convert compromised computers into the botnet. A computer can be part of the botnet yet never show any outward signs to network users, so it operates behind the scenes. Here, when a user clicks on a link or triggers a program, the user's PC reaches out to the botnet to download the Ransomware payload rather than it being contained in the e-mail itself, further insulating the hacker from detection by making it appear someone else's computer was at fault.

**3) Drive-by Download** – A drive-by download occurs when compromised software or a website "pushes" a download to a target computer without the user's consent. This kind of attack has become less common over the years as more web browsers use proactive security to prevent unauthorized downloads and alert users. That said, it remains important to maintain up-to-date versions of web browser and other critical software. But the risk here is for an unpatched third party application to be present on the infected website that provides the entree for the Ransomware payload. Sometimes this "window of opportunity" is very brief, as the vendors update their programs as vulnerabilities are detected, but there is that possibility that you might encounter the website between patches and be infected.

**4) Bad "Free" Software** – Software should only be downloaded directly from the home page of known software vendors. Although some legitimate free software sites do exist, even these tend to include unwanted commercial "bloatware" that may serve up ads or change your browser settings without consent. Those changes, in turn, can make it more likely you'll be exposed to compromised websites. Free software on unknown sites is often a "trojan" disguising malware or other viruses. Employees should not be downloading any non-business software on their work computers ever, especially any "freeware" or "shareware" programs or apps. For example, one Ransomware attack exploited the on-line game Minecraft. The hacker offered a "mod" (game module) to players. When they installed it, the software also installed a sleeper version of Ransomware that activated weeks later (deflecting attention away from that download since time had passed from its installation.)

**5) Malvertising** – Malvertising is any form of advertising intended to spread malware through the Internet. This often happens when legitimate advertising is compromised by a virus. Illegitimate ads created by hackers can spread viruses directly using malicious scripts, causing "drive-by downloads." They might entice users to click the fake ad and potentially download Ransomware. Most malvertising can be prevented through common ad blocking software. For example, **a number of major news websites were hijacked by a malicious campaign that installed Ransomware on users' computers.** The attack hit websites including the **New York Times, the BBC, AOL and the NFL**. The malware was delivered through multiple ad networks, and used a number of vulnerabilities, including a recently-patched flaw in Microsoft's former Flash competitor Silverlight, which was discontinued in 2013. The vector of attack can often be warded off by installing adblockers for Internet browsers, but that won't always work.

**6) Social Engineering and Self-Propagation** – Social engineering can take place in two ways. Some Ransomware passes itself off as a "fine" from a government agency such as the FBI, which can confuse the end user and make them take actions that spread the infection. Once a computer is infected, the other form of social engineering takes place: The infected user's e-mail contacts and other data are used to spread the infection to other users. The new group of targets unthinkingly access the message, believing it to be from their colleague – a prime example of self-propagation. This was a common scam for e-mail offers and has now been extended into the Ransomware arena – it worked before, so they will try it again.

**7) Affiliate Schemes** – To the network administrator or end user, affiliate schemes manifest as one of the attack types above – but it's still important to know about them. Hackers are adapting the tactics of legitimate marketers, designing malware and then paying agents to infect computer systems. The "affiliates" do the hard work for a slice of the "commission," which can run to many thousands of dollars. While there are no known reports of inside actors infecting a business as a Ransomware attack affiliate, internal security best practices remain vital.

## Oh @$#$%^&! – We're Infected!

Should a user see a Ransomware screen (as shown on page 1) **IMMEDIATELY** disconnect the device from the network and shut it down. This includes any Wi-Fi networks in the building and Bluetooth connections. Disconnect any external USB devices, especially any being used for backup storage. This will help to stop the spread of the encryption if caught early enough. But, there will still be some damage done. Then **call an IT resource such as SIM2K ASAP**.

They will help you consider the scope of the infection – how far did it spread. Did the infected machine have access to:

- Shared or unshared drives or folders
- Network storage of any kind
- External hard drives
- USB devices with valuable files
- Cloud-based Storage (DropBox, One Drive, Google Drive and others)

They should also check whether or not your backup files were infected. As long as these were not infected, you have a path to be able to restore the files and avoid paying ransom.

They will determine which "flavor" of Ransomware you are facing, as every version is unique in the parameters – time allowed to pay, cost for the ransom, and way of encrypting (ie: does it just encrypt files or the entire hard drive so you can't access any data at all.) Once you know the strain of Ransomware it may be possible to locate a remediation tool that might decrypt files without you having to pay the ransom. If you're lucky. If not, you are then faced with decisions on how to proceed.

Once a network becomes infected, you will be faced with three options –

- Do nothing, admit you have lost all your data and start over;
- Pay up; or
- Wipe the infected computers, reinstall programs and restore data.

## Do I Pay?

So, should the ransom be paid? Security experts are generally opposed to making Ransomware payments, but some insert a caveat or two for consideration before rejecting a ransom offer. After all, it's easy to say you shouldn't pay the ransom, but you may have to do it to save your business if you cannot restore data, or if it can't be restored in a timely fashion without causing a major business disruption.

Paying the ransom has two negative impacts. First, this only rewards and encourages the cybercriminal to continue this exploit on other companies. The other reason is there is no guarantee the attacker will make good on the promise of releasing the decryption key after the ransom is paid – the attacker has every incentive to simply wipe the drive remotely in order to cover his tracks. The backers of Cryptolocker, a Ransomware strain that encrypts much of the data on the computers it infects, have a checkered record of providing the keys needed to decrypt files after a ransom is paid, but newer strains, like Cryptowall, are better about delivering what's necessary to recover files held for ransom.

If you decide to pay the ransom, you will have to delve into the dark side of the Internet. There should be instructions on the splash screen on how to pay, or there will be a text file on your drive with instructions. This will tell you 1) How much to pay; 2) Where to pay; and 3) How much time you have to pay (a countdown timer.)

You will probably be asked to pay the ransom in Bitcoin, an Internet currency. You will have to find a Bitcoin Exchange on-line and set up an account, called a "wallet address." Then you purchase the necessary Bitcoin ransom at the Exchange and have it deposited into your wallet. Since Bitcoin is a fluid currency, the dollar value of a Bitcoin will rise and fall constantly, so it may be wise to buy a bit more than necessary should the value change during the time of this

transaction. Once you have your wallet funded, the Ransomware instructions should provide the wallet address for the hacker – usually some string of gibberish like "19eXu88pqN30ejSmfed745crm4BO1" – which makes it untraceable to any individual. Transfer the requested ransom to that wallet. The hacker will be notified of the payment. You may or may not get a transaction confirmation.

Now, you wait for the hacker to send instructions to your strain of Ransomware to begin to decrypt your files. It is important to make sure that all devices that were connected to the network at the time of the infection are re-connected so that the decryption can reach all nooks and crannies of your network. Sometimes the hacker will provide a new executable file that you must install and activate. This will contain the key needed to decrypt your files. Then you sit and wait for the Ransomware to run its course – which could take hours or days depending on the strain used and the degree of infection in your network.

***Note:*** One option you may face paying the ransom is being asked to go to a TOR (The Onion Router) site. Things can get fairly complicated once you are navigating the so-called "dark web." This is another reason to engage an experienced IT resource like SIM2K to assist you through this critical period.

## Don't Pay – Restore

Of course, the best answer to the "should-I-pay-the-ransom" question is to avoid having to answer it at all. "The key is to remove power from the extortionists, and you do that by backing up your system regularly," said one malware research analyst. "This basic best practice is cheap and easy, thanks to removable hard drives," he added. "With backups, there's no need to pay the ransom to get your data back or interact with extortionists in any way, which can increase your risk." Experts recommend that businesses and users frequently back up their data and also test to those backups to make sure they work. **How long has it been since you verified your data is being successfully backed up, every day?** Having your data backed up on a regular schedule, then testing it to be sure that the data is in place and can be restored, is critical. Many companies believe they are backing up, but without the verification step, can receive an unpleasant surprise should they need to restore this data. Also, many Cloud-based backup solutions are not geared to download data, so restoring data from one of these services may take an extended time compared to local, on-site backup devices such as USB drives or a NAS (Network Attached Storage) device.

Also consider any alternate sources of files that can be downloaded and restored. Did you send or receive them via e-mail that can still be accessed? Did you use Dropbox or Google to share files that are still there? You may also have shadow files on your system – something that Microsoft creates when it sets a restore point for your software. Your IT specialist can help determine if any of these files do exist.

Then, you should consider completely wiping your infected computers to eradicate the Ransomware. Attempting to run an Anti-virus scan may or may not be effective, so for best results, remove all files from your drive and rebuild the machine. Some companies even go so far as to purchase all new hard drives for their servers and PCs so there will be no trace of the Ransomware left. This assumes you have copies of your operating system and other software, such as Microsoft Office, on hand to re-load on the machine(s). You will need your licensing information and product keys for this installation, so be sure to have those handy. This is another point at which the advice, counsel and assistance of your IT specialist will prove very valuable.

Once the infection is removed, you can begin the download of your backup files to the appropriate places in your network structure. Depending on the source of the backups, this may go quickly or could go for days. In some instances, if you are using an off-site backup source, it may be quicker to request a USB drive with your data transferred to it as opposed to relying on an Internet connection to download files. Check with your provider for details. Then check and verify that all your files are back in place, your software is installed and updated, and try to get back to normal business as quickly as possible. Confirm your backups are up-to-date and operational and hope that you don't get infected again.

## How can Ransomware Be Prevented?

There are some steps a business can take to try to ward off any Ransomware attacks, but these do not supersede the need to have good backups on hand. We strongly recommend a "defense in depth" strategy that includes:

- Active content filtering of web activity;
- E-mail filtering for viruses, malware and spam;
- Security on the perimeter of your network (typically software in concert with a firewall);
- Anti-virus software on individual workstations and servers;
- User training and education on the risks posed, methods used by hackers and appropriate behavior as a business user; and
- Allow users the minimal control and permission necessary to complete their tasks.

**How many of these does your network utilize?**

Your IT specialist resource can help identify and apply these steps. In addition, there are other tools that can be implemented to help prevent infections. Policy restrictions or software designed to mitigate zero day vulnerabilities can be deployed where cost and impact justify the effort. While good prevention may help avoid a successful attack, **no one has a foolproof method yet for preventing Ransomware.**

## Let SIM2K Help

Madison County was not unique. Similar stories can be found across the globe – companies hit with exorbitant ransom demands to un-encrypt data. A hospital in California paid $17,000. A university in Canada paid $20,000 (CN) to decrypt its e-mail. The Democratic party of Pennsylvania just announced it was hit with a Ransomware attack. A 2016 study by anti-virus company Malwarebytes revealed nearly 80% of organizations surveyed have been the victim of a cyberattack, and 47% have been the target of a Ransomware attack over the past 12 months. Of the enterprises targeted by Ransomware, 34% lost revenue and 20% had to cease operations immediately. Nearly 60% of all Ransomware attacks in the enterprise demanded over $1,000. Over 20% of attacks asked for more than $10,000, and 1% even asked for over $150,000. Of all the attacks, the survey indicated 40% of those infected went ahead and paid up, so the bad guys win frequently. USA Today stated a study of 618 small- to medium-sized companies paid an average of $2,500 per Ransomware attack in 2016. A study in the UK revealed 85% of companies targeted by Ransomware had their systems down for a week or more, causing thousands of dollars in financial damage as well as lost revenue during this downtime. A third of these companies had their data down for more than a month, and 15% reported their data was, in the end, unrecoverable. Therefore, the Ransomware question is not "if" but "when" will you be faced with a potential encryption of your business data.

While there is no 100% effective prevention for Ransomware, proper planning, education and following best practices will minimize the risk of being infected. Having good backups and a managed, organized response can help minimize the impact of any Ransomware infection should it occur. SIM2K can help you assess your vulnerability and provide a roadmap for improvements where needed to help boost your chances for avoiding infection and help you recover from an attack in that unfortunate circumstance. **Call us for more information or to set up a meeting** to discuss steps you can take to be prepared.

## Checklist

On the last page you will find a checklist of steps to take should you be faced with a Ransomware attack. This is just a rough outline of the steps you should follow. Please get SIM2K involved in this effort at the very first onset of a Ransomware attack.



SIM2K®
Technology Consultants

6330 E. 75th St., Suite 336
Indianapolis, Indiana 46250

317.251.7920
800.746.4356
www.sim2k.com
sales@sim2k.com

# *Ransomware Checklist*

**OH NO! You have triggered a Ransomware attack on your computer and your files are being encrypted as you sit and watch. Here are the steps SIM2K recommends to respond to this attack:**

**Step 1: Disconnect Everything**

- ☐ Unplug computer from network
- ☐ Turn off all wireless functionality – Wi-Fi and Bluetooth, etc.

**Step 2: Determine the Scope of the Infection.**

Check the following for signs of encryption:

- ☐ Mapped or shared drives
- ☐ Mapped or shared folders from other computers
- ☐ Network storage devices of any kind
- ☐ External Hard Drives
- ☐ USB storage devices of any kind
- ☐ Cloud-based storage (DropBox, Google Drive, Microsoft One Drive, etc.)

**Step 3: Determine Ransomware Strain**

- ☐ What type of Ransomware is present (ie: Cryptolocker, Crypto Wall, Teslacrypt, etc.)

**Step 4: Determine Response**

*Now that you know the scope of your encrypted files as well as the strain of Ransomware, you can make a more informed decision on the next action step(s) to take:*

***Response 1:*** Restore Your Files from Backups

- ☐ Locate Backups
- ☐ Ensure all the files you need are there
  - ☐ Verify integrity of backups
  - ☐ Check for Shadow Copies, if possible
  - ☐ Check for any previous versions of files that may be stored on a Cloud-based source
- ☐ Remove the ransomware from your infected system
- ☐ Restore your files from backups

***Response 2:*** Try to Decrypt

- ☐ Determine the strain and version of the ransomware
- ☐ Locate a decryptor. Remember, there may not be one for newer strains. If successful, then:
- ☐ Attach any storage media that contains encrypted files (hard drives, USB sticks, etc.)
- ☐ Decrypt files

***Response 3:*** Do Nothing (and lose files)

- ☐ Remove the ransomware
- ☐ Backup your encrypted files for possible future decryption

***Response 4:*** Negotiate and/or Pay the Ransom

- ☐ If possible, you may attempt to negotiate a lower ransom and/or longer payment period
- ☐ Determine acceptable payment method for this strain of Ransomware (Bitcoin, Cash Card, etc.)
- ☐ Obtain payment, likely Bitcoin (BTC)
- ☐ Locate an exchange you wish to purchase a Bitcoin through
- ☐ Set up account and wallet then purchase Bitcoin
- ☐ Re-connect your encrypted computer to the Internet
- ☐ Install the TOR browser if required by the strain of Ransomware
- ☐ Determine the Bitcoin payment address. This should be located in the ransomware screen or on the TOR site set up for this particular ransom case
- ☐ Pay the ransom by transferring your BTC to their wallet
- ☐ Ensure all devices that have encrypted files are connected to your computer/network
- ☐ File decryptions should begin within 24 hours, but often key will be released once Bitcoin receipt is noted

**Step 5: Protecting Yourself in the Future**

- ☐ Implement training for staff to recognize signs of possible ransomware payloads
- ☐ Ensure your firewall is functioning and is blocking non-essential ports
- ☐ Implement anti-spam/anti-virus programs if not already in place
- ☐ Implement restrictions on network to ensure unauthorized applications cannot run
- ☐ Implement a regular software patch program to reduce vulnerabilities
- ☐ Have a backup solution in place and working
- ☐ Test that files from your backup can be restored
- ☐ Set up a rotation for drives to be taken off-site or off-network so they cannot be infected

SIM2K
Technology Consultants

6330 E 75th St., Ste. 336
Indianapolis, IN 46250
www.sim2k.com • sales@sim2k.com
317.251.7920 • 800.746.4356