What is Ransomware?

Ransomware can take different forms, but in its essence it denies access to a device or files until a ransom has been paid.

In this manual we discuss ransomware as PC or Mac-based malicious software that encrypts a user or company's files and forces them to pay a fee to the hacker in order to regain access to their own files. The hackers primarily use the following vectors to infect a machine: phishing emails, unpatched programs, compromised websites, poisoned online advertising and free software downloads.

Not only can ransomware encrypt the files on a workstation, the software is smart enough to travel across your network and encrypt any files located on both mapped and unmapped network drives. This can lead to a catastrophic situation whereby one infected user can bring a department or entire organization to a halt. Imagine a law firm or accounting firm having all their client files encrypted. It is happening more and more.

Once the files are encrypted, the hackers will display some sort of screen or webpage explaining how to pay to unlock the files. Also, ransomware typically has a one week deadline which, once passed, causes the ransom to increase. Most ransoms start in the $300-$500 area, and once the deadline has passed it will likely increase to over $1000.

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

Some Facts About Ransomware:

- Typical ransomware software uses RSA 2048 encryption to encrypt files. Just to give you an idea of how strong this is, an average desktop computer is estimated to take around 6.4 quadrillion years to crack an RSA 2048 key.

- One estimate indicates more than $27 million in ransom payments in just the first few months of the release of the Crypto Locker variant of ransomware in September 2013.

- CryptoLocker was followed up by the variant Crypto Wall, which made $325 million dollars in 18 months, half of that in the United States. By now there are thousands of ransomware victims, including a New Jersey School District, police departments in Maine, Massachusetts & Chicago.

- Cyber criminals are constantly updating ransomware themes. Some themes include an FBI variant, the Internal Revenue Service, and even a Breaking Bad television show themed ransomware. Mostly though, they use social engineering and send employees

emails with attachments that are supposedly invoices or other business documents they will likely open.

Bitcoins and Cryptocurrency

Bitcoins are a form of cryptocurrency, meaning they do not have a physical representation. Instead they are stored in anonymous digital wallets. They can be transferred anywhere in the world via the Internet. They can be paid from anywhere, to anywhere with total anonymity. The long and short of it is: apart from the benefits, they are the ideal form of payment for illicit activities.

It could be argued that cryptocurrency is one of the enabling factors of ransomware. After all, if the hackers couldn't accept payment safely, then the software would have no value. With the rise of Bitcoin has come a rise in ransomware.

Despite the above, using or owning Bitcoin is not an inherently criminal activity at all. Many respected companies accept Bitcoin and it is used the world over in non-criminal ways. However it is relatively new, so the lack of information associated with it can scare people, especially if their first encounter with Bitcoin is paying some cybercriminal to unlock their files.

Some quick facts about Bitcoins:

- Bitcoins are commonly abbreviated as BTC, and are untraceable.
- The price of Bitcoins is constantly fluctuating. At the time of this writing 1 BTC is roughly $400.
- You can buy partial Bitcoins. For example, you can buy 0.5 BTC (half of a Bitcoin). An individual
- Bitcoin can be split in up to many extremely small fractions.
- There will only ever be 21 Million Bitcoins in circulation once they are all available.

TOR (Anonymity Network)

TOR, which stands for "The Onion Router" is a network and browser developed to enhance and anonymize Internet traffic. It uses a special browser that is configured to use a worldwide volunteer network of relays. All traffic is encrypted and the network was designed from the ground up to anonymize and hide the originating and ending destination of the traffic.

Cybercriminals and other people who wish to anonymize their traffic can use this TOR network to communicate or host websites that cannot be easily tracked by law enforcement or government officials. In this way, it can be a tool for circumventing censorship, but also a tool for more nefarious use of anonymous traffic.

Since TOR is so well crafted for anonymizing activity, ransomware creators can use it to interact with their victims without much fear of retaliation or discovery.

A few facts about TOR:

- Instead of using .com or .net domains, onion web addresses end in .onion.
- You cannot browse TOR sites using a regular Internet browser.
- TOR was originally developed by the U.S. Naval Research Laboratory and Defense Advanced
- Research Projects Agency (DARPA).

Am I Infected?

Symptoms

It's fairly straightforward to find out if you are affected by a ransomware virus. The symptoms are as follows:

- You suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension.
- An alarming message has been set to your desktop background 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.
- A window has opened to a ransomware program and you cannot close it.
- You see files in all directories with names such as HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML.

I'm Infected, Now What?

Once you have determined you have been infected with ransomware, it is imperative to immediately take action:

1. Disconnect:

Immediately disconnect the infected computer from any network it is on. Turn off any wireless capabilities such as Wi-Fi or Bluetooth. Unplug any storage devices such as USB or external hard drives. Do not erase anything or "clean up" any files or antivirus. This is important for later steps. Simply unplug the computer from the network and any other storage devices. To find out which computer is "patient zero", check the properties of any encrypted file.

2. Determine the Scope:

At this point you need to determine exactly how much of your file infrastructure is compromised or encrypted.

Did the first infected machine have access to any of the following?

- Shared or unshared drives or folders
- Network storage of any kind
- External hard drives

- USB memory sticks with valuable files
- Cloud-based storage (DropBox, Google Drive, Microsoft OneDrive/Skydrive etc…)

Inventory the above and check them for signs of encryption. This is important for several reasons: First, in the case of cloud storage devices such as DropBox or Google Drive, you may be able to revert to recent, unencrypted versions of your files. Second, if you have a backup system in place you will need to know which files are backed up and which files need to be restored versus what may not be backed up. Lastly, if you end up being forced to pay the ransom, you will need to reconnect these drives to allow the ransomware to decrypt them!

Another way to determine the scope of the infection is to check for a registry or file listing that has been created by the ransomware, listing all the files it has encrypted. You see, the ransomware needs to know which files it encrypted. That way, if you pay the ransom, the software will know which files it needs to decrypt. Often this will be a file in your registry. Since every strain of ransomware is different, it is recommended to do a bit of googling to determine the version of ransomware you have been hit with and do your research based on the right version of the ransomware.

As a final option, there are tools available that have been specifically made to list out encrypted files on your system.

- See our Ransomware Knowledge base for links to decryption tools

3. Determine the Strain:

It is important to know exactly which ransomware you are dealing with. Each ransomware will follow a basic pattern of encrypting your files, then asking for payment before a certain deadline. However knowing which version you are going toe-to-toe with will provide you with more information with which to base your decision. (There is a new strain discovered which encrypts the Master Boot Record and locks the user out of access to the whole hard disk.)

Ransomware strains vary in that some are more costly (in ransom payments) than others, while some versions will have even more options to pay than just Bitcoin. There is the off-chance that your particular strain has had a decryption tool built by an IT security company that will allow you to decrypt your files without having to pay anything, but don't count on it. Finally, in the case that you are one of the very first people to be hit with this version, you may need to consult security experts or provide information on various system files in order to determine what kind of ransomware you're facing. The www.bleepingcomputer.com website is a good place to start.

A general note about ransomware infections: At the time of this writing (spring 2016), ransomware does not spread onto other computers on your network unless they have been directly shared with the infected machine. Meaning, if a machine is infected and has connections to drives or network folders, the ransomware will not "install" itself on other computers (like a worm) who also have access to those shared resources. However, the ransomware WILL try to encrypt any file it directly has access to, regardless of where it is stored. This means that

generally a ransomware infection will only affect a single machine and all shared resources it has access to, not an entire network of computers. But new strains have come up where cyber criminals are not counting on the "spray-and-pray" approach, but are doing this partly in-person, and the amount depends on how important the locked data is. It may range from 0.5 BTC to as much as 25 BTC (that is 10,000 dollars!). These terms are to be negotiated individually.

4. Evaluate Your Responses:

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.

To put it bluntly, you have 4 options, listed here from best to worst:

1. Restore from a recent backup
2. Decrypt your files using a 3rd party decryptor (this is a very slim chance)
3. Do nothing (lose your data)
4. Negotiate / Pay the ransom

It is important to be aware of the deadline you're facing, and whether or not paying the ransom is an option to be put forward at all. If that's out of the question, then you will be free to spend more time delving into the other responses given here. If you are desperate because your backup/restore failed, then a priority will need to be given to the response most likely to get results in a shorter time-frame.

Restoring from a recent backup is the ideal solution to any ransomware infection. In the past, backups were costly and required regular check-ups and maintenance. Now, with cloud storage like Google Drive and Dropbox, not to mention a plethora of set-it-and-forget-it backup software like Backblaze and Carbonite, combined with the ever-falling price of storage media these days, backups are not an optional part of operating a computer: they are an absolute necessity.

In a corporate environment, if your company is not making regular and redundant backups of vital files, it is only a matter of time before catastrophic failure. No hard drive lasts forever, and computers can break or be subject to all manner of data destroying events.

Step 1: Locate any possible backup sources

In order to fully evaluate this option as a response to a ransomware attack it is first necessary to determine the state of your backups. If you have ready access to your backup sources, then we recommend that you immediately (on a separate computer) begin a restore process and manual verification of the files from your backup. This is especially critical if you are using physical backup media such as USB drives, DVDs or external hard drives to back up your data. It can happen that these media deteriorate and you will need to know if your files are indeed backed up and recoverable. The other part of determining your backup state is the time factor. How much data have you lost access to and how long will it take you to restore it? Is that going to impact your business in the time it will take to recover a backup? You may have all your files stored in

the cloud, however downloading several terabytes of storage is no trivial matter. It could take days to restore your files.

The last part of this step could be the most crucial, yet can be the most complex: discovering the other places you might be able to recover files from. First, what files are you attempting to recover? Are they financial documents? Pictures and/or videos? Perhaps music project files or client information. Once you know what key files you need, you can assess if they've been possibly used where a copy may be stored.

Common places you may find a copy of a critical file are things like Gmail. Have you ever emailed anyone a copy of the file as an attachment? Have you shared the file on Google Drive? If you have Dropbox or Google Drive, the files may have been encrypted, but often these services will allow you to revert a file to a previous state. It's possible that while the current version of the file is encrypted, you can log into Dropbox and download an older, unencrypted one. Also be aware if any co-workers, friends or family may have a copy on their computer.

Step 2: Shadow Copies

We will preface this section with a warning. Cybercriminals are furiously innovating their ransomware strains. Recent versions now delete shadow copies of your files so this option may not work depending on the strain you have been hit with. Also, shadow copies may not always be the latest version of the file you're trying to recover but it's certainly worth a shot.

What are shadow copies? Shadow copies are a byproduct of something called Windows Snapshots. When Windows creates a system restore point, it will often create snapshots of files, and these snapshots can contain copies of files on your computer from that restore point. There is software available that can let you browse through your Windows snapshots for the files you may be looking for.

- See our Ransomware Knowledge base for links to these tools

Step 3: Resolution of the backup response

Once you have verified the files you need, and are able to recover them from a backup, you can now take action on that infected computer and remove the ransomware. Some people run multiple antivirus scans to ensure the malicious software is removed, but to be 100% sure that there are no traces left of any kind of malware, wipe and rebuild the machine.

Once you are confident any traces of the ransomware have been removed, you can now restore your files. It is important to take further precautions to prevent these types of attacks in the future.

Step 4: Prevention

Once you've resolved the ransomware infection, it's important to take precautions to prevent these types of attacks in the future. It is not enough just to have last week's backups or just to have antivirus. The weak link in any ransomware attack is the person sitting in the chair in front

of the computer. By employing a combination of software based solutions like antivirus, antispam and backups, together with effective security awareness training for your users, you can plug holes with both a software firewall and a human firewall. See the final section "Protecting yourself in the future" for more information on these types of utilities. Also, you can use our Ransomware Prevention Checklist to audit your network and determine where you can take further steps to prevent these types of attacks from causing damage.

Configuration Recommendations

Here are some technical controls you can put into place, suggested by Steve Ragan at CSO:

- Avoid mapping your drives and hide your network shares. WNetOpenEnum() will not enumerate hidden shares. This is as simple as appending a $ to your share name.

- Work from the principle of least permission. Very few organizations need a share whereby the everyone group has Full Control. Delegate write access only where it's needed, don't allow them to change ownership of files unless it's a must.

- Be vigilant and aggressive in blocking file extensions via email. If you're not blocking .js, .wsf, or scanning the contents of .zip files, you're not done. Consider screening ZIP files outright. Consider if you can abolish .doc and .rtf in favor of docx which cannot contain macros.

- Install the old CryptoLocker Software Restriction Policies which will block some rootkit-based malware from working effectively. You can create a similar rule for %LocalAppData%*.exe and %LocalAppData%**.exe as well. It was pointed out in the Reddit comments that if it's at all feasible, run on a whitelist approach instead of a blacklist. It's more time-intensive but much safer.

- Backups, having good, working version, cold-store, tested backups makes this whole thing a minor irritation rather than a catastrophe. Even Windows Server Backup on a Wal-Mart External USB drive is better than nothing. Crash plan does unlimited versioned backups with unlimited retention at a flat rate, and there's a Linux agent as well. Hell, Dropbox does versioned backups. Get something.

Second Response: Try to Decrypt

As the threat of ransomware attacks has grown, so have solutions and prevention measures. The proliferation of certain strains of ransomware such as CryptoWall and Cryptolocker have resulted in some of the encryption keys being cracked or uncovered by mainstream antivirus companies. As a warning, this response should not be considered in any way a concrete solution. It mainly works on older versions of ransomware, and hackers are constantly updating their software to counteract any uncovered workarounds. After all, the hackers read the same security blogs and forums that you and I do! It's worth a quick look, but is less and less a viable option.

Step 1: Determine the strain

While you probably already know which version you're dealing with by this point, it is important to know exactly the strain of ransomware you've been hit with. Often, there will be version numbers, but take these with a grain of salt, as most ransomware seeds itself with completely random version numbers to help foil antivirus companies' attempts to determine if changes have been made. However, even noting the time of the infection and the general strain can help you determine if there is an applicable decryption method you can try.

Step 2: Locate an appropriate decryptor/unlocker (if possible)

This is the critical part. Our resource page has links to some of the mainstream (at the time of this writing) unlockers, however you will probably need to do some googling to determine if your particular strain has an associated unlocker. Even then, you may find that it is unsuccessful at unlocking/decrypting your files. It can depend on the key that was used to encrypt your files and the version of the ransomware you've been hit with. Pay attention here, as hackers love to prey on desperate victims, and it can be easy to wish upon a star at this point and you may even be willing to try anything to get your files back. A little restraint goes a long way. Make SURE any decryptor/unlocker you have located is vetted from not only a reliable antivirus source, but also there should likely be more than a few references to the site/file you're downloading from other reputable antivirus or malware support forums. This is also a point during which you may want to consult security professionals or ask on popular security forums to see if the pros there know of any tools.

Step 3a: Success!

If you've managed to find a decryptor/unlocker that has worked for you, FANTASTIC! Make sure to acknowledge the creator/company that provided you with the tool to save your files! Take precautions to prevent these types of attacks in the future and follow our guide for prevention.

Step 3b: Failure

If, at this point you have not been able to locate or decrypt your files using a 3rd party application or site, then it's time to look into other methods of handling the infection. Either by restoring backups or (as a last resort) negotiating with the hackers to pay a ransom.

Third Response: Do Nothing

One obvious option is choosing to not recover the files that are encrypted. Take a hit and then restore your computer to a working state. This is often a valid solution in cases where work or personal life impact will be minimal, or where paying the ransom or restoring from a backup is not an option. In these cases, the main actions you will want to take are as follows:

Step 1: Rid your computer of all ransomware. It is recommended that you run multiple anti-virus scans to ensure the software is removed. It's much safer to wipe and rebuild the machine though.

Step 2: Back up your encrypted files (optional)

Yes, that's right. You may want to back up your encrypted files. The reasoning here is that occasionally antivirus or computer security experts will uncover the encryption keys used in certain ransomware programs.

This may be 6 months later, but it has happened. There was even a case where a rookie ransomware developer – in a flash of conscience – decided to decrypt all the files of the users who had been infected. So it may be a long shot, but you just might get lucky down the road with one of these types of discoveries.

Step 3: Prevent future attacks
This step is the MOST vital of the three steps here. If you're going to take a hit on your files, at least learn from any mistakes that were made. It's time to get some countermeasures in place and take some proactive steps to prevent this – and other issues like it – from being able to affect you again.

We recommend having another look at the Prevention step above, and institute the following:

1. Install and maintain high-quality antivirus software, as a layer you want to have in place, but do not rely on it – they always run behind.
2. Configure weapons-grade backup/restore software and test the restore function regularly!
3. Implement effective security awareness training combined with simulated phishing attacks to dramatically decrease the Phish-prone percentage of your employees. It is important to be able to recognize a threat before it causes downtime.

Fourth Response: Negotiate and/or Pay the Ransom
If you have exhausted all other options, and you simply MUST have your files back; your only recourse may be to pay the ransom. This is a controversial opinion. Most IT security experts will recommend that users hit with ransomware absolutely avoid paying the ransom. After all, nothing encourages MORE ransomware attacks than a successful ransom being paid. The fact of the matter is though, in some cases there will be no choice.

The Hollywood Presbyterian Hospital paid $17,000 to decrypt their files and get back into business. To many companies, a few hundred (or even thousand) dollars is a drop in the bucket compared to the downtime and financial damage that would follow losing access to critical files. There may simply be no other alternatives. As
a result, this section will walk you through the complex process of dealing with the aspects involved in paying a ransomware attacker and navigating the complex world of Bitcoin exchanges and transfers.

Now a word on the effectiveness of this method
The most commonly asked question with regard to the ransom payment is, "Will these criminals actually decrypt my files if I pay?" The answer here is a bit complex. The short answer is yes, they will almost always decrypt your files. There is a moral dilemma here, after all, the bad guys want money and they will provide fast and accurate customer service and tech support to facilitate the payment. If it is discovered that when users pay up and the hackers DON'T decrypt

the files, they will lose all credibility and a quick search would reveal that it would be fruitless to pay, since the hackers won't do anything. So in an odd way, the only way they can encourage victims to pay, is by actually following through and decrypting your files when you pay them.

However - yes, that's a big however - you are not dealing with a Fortune 500 company with a shareholder reputation to uphold or quarterly earnings to report. You are most likely dealing with an Eastern European group of hackers who may not lose much sleep if suddenly the network they set up to decrypt their victim's ransomware infections is taken down by an Internet Service Provider or law enforcement.

There are any number of reasons why the criminal creator of the ransomware you've been hit with may not respond upon payment. There is an inherent risk in dealing with these people, however, they have designed their systems with robustness and redundancy in mind from day one, because they know they will be shut down and want to continue their "business".

With all of that out of the way, it's time to get into the details of how to pay off a ransom. This document assumes that your ransom requires payment in the form of Bitcoin. We will walk you through the instructions and steps on obtaining Bitcoin and making the proper payments. If this is your first time dealing with Bitcoin, it can be very unfamiliar so we will attempt to alleviate that by providing specific resources for you to use.

Step 1: Locate the Payment Method Instructions

This step can be fairly easy since most ransomware will display the payment methods in large text or very clear instructions. Typically there will be a link to instructions right in the ransomware screen. In other cases you will have a file named something like DECRYPT_INSTRUCTIONS.TXT that you can follow. Regardless of the specific version of ransomware you've been hit with, the payment instructions will give you three pieces of information:

- How much to pay
- Where to pay
- Amount of time left to pay the ransom (countdown timer)

Once you have the above information, it's time to figure out how to pay the ransom.

Step 2: Obtaining Bitcoin

The first step is to set up an account with what is called a Bitcoin exchange and you will need to purchase some Bitcoin. On any other day, this would be fairly simple, however you may very well be under a strict timeline to pay the ransom and that complicates things a bit more. This means you'll need to find an exchange where you can get Bitcoin fast. You might even consider doing this now, before a ransomware infection and be prepared just in case you get hit.

• See our Ransomware Knowledge base for more about getting Bitcoin

Deciding which exchange to use can be tricky, because some require banking information, while others are more of a brokerage site between people wanting to buy and sell Bitcoin. In some cases you can even transact in person! In any case, you'll have to create an account. KnowBe4 has an account at http://www.CoinBase.com.

Once you've created an account, you'll likely have a wallet address. This is the address you'll need to provide to the person you're buying the Bitcoin from. The actual purchase of the Bitcoin can vary in forms of payment. There are some Bitcoin exchanges that ask you to link your bank account, but usually those exchanges will have longer wait times between transactions (up to 4 days for new accounts) so you may not have the time to wait for those transactions to clear. Using a Bitcoin broker site like http://www.LocalBitcoins.com will allow you
To connect up with a local seller and filter by payment types. This may be your best bet in terms of obtaining Bitcoin the fastest.

As a recommendation, you probably want to err on the side of purchasing slightly more Bitcoin than you need (Only by a few dollars) to account for any fluctuations in price and/or transaction fees.

Step 3: Installing a TOR Browser (May be optional)

If you are unfamiliar with what a TOR browser is, it is recommended you read the section in the beginning outlining what TOR is and how it works. Functionally for you, it will be just like browsing a regular website with some minor differences. To download the TOR browser, navigate to http://www.torproject.org and click the download button. Do not download a TOR browser from any other website.

Install the browser and open it. It will look very similar to any other browser. This will allow you to navigate to sites hosted on the TOR network. The ransomware creators often host their sites in very temporary locations in the TOR network and you may be forced to use the TOR browser to navigate to the site created specifically with your payment instructions. This is done so that the hackers can take down the site immediately after it is done being used and avoid any public tracking that would come with using normal hosting in your typical world-wide-web.

The website "address" given to you by the ransomware may look very odd, and it will usually be located in the Decrypt instructions or main screen.

Step 4: Paying the Ransom

Once you have a Bitcoin (or more) in your Bitcoin wallet, now it's time to transfer that Bitcoin to the wallet of the ransomware creator. Typically paying the ransom will require one or more of the following pieces of information:

- A web address to view your specific ransomware payment information (this may be a TOR address).
- The hacker's BTC wallet ID that you will use to transfer the BTC to.
- Depending on ransomware, the transaction ID or "hash" generated when you actually transfer the BTC to the hacker's wallet.

With many types of ransomware you will have to visit a page on the TOR network that has been created specifically for paying your ransom. Enter the web address of the site into your TOR browser. You can usually follow the instructions on the site to locate the wallet ID you need to send your Bitcoin to. The wallet ID is usually a long string of numbers and letters and is usually provided by the ransomware payment instructions or somewhere on the screen explaining payment.
Once you've logged into your account at the Bitcoin exchange and transferred the Bitcoin to the hacker's wallet (this may take some time, 20-40 minutes) then you usually get a transaction confirmation hash, which is another long series of letters and numbers.

In many cases, just sending the Bitcoin is all that is needed and the hackers will provide you with the decryption key for your files. Depending on the type of ransomware you've been hit with, you may need to provide the transaction hash ID to the hackers. The ransomware will usually have a field where you can type in or paste the transaction hash ID.

Step 5: Decrypting Your Files
Once you've paid the Bitcoin to the hackers, you will probably have to wait for a bit of time (up to several hours) before they have processed the transaction. Once the hackers have processed the transaction, they should give you access to the unique executable with the key that starts decrypting your files.

IMPORTANT: It is important to make sure that all original external drives, USB or even network storage devices that were connected at the time of infection are currently connected and active when you are at this stage. Otherwise the ransomware decryption may not include files that it cannot locate. This includes ensuring that any shared folders have the same path they did originally at the time of infection. Also ensuring any external hard drives or USB sticks also have the same path as at the time of encryption.