NEW 2020 EDITION

KnowBe4
Human error. Conquered.

RANSOMWARE
Hostage Rescue Manual

What You Need to Know to Prepare and Recover from a Ransomware Attack

"The adage is true that the security systems have to win every time, the attacker only has to win once."

— Dustin Dykes

Introduction

Pirate, Bandit, Raider, Thief... Hacker. As the times change so does the moniker, but the underlying concept is the same. You've got something valuable–maybe even only to you–and you're willing to pay money to protect it or get it back if stolen.

Early on, most hacking was done by "script kiddies" and mischievous teenagers more interested in pulling pranks or getting the recognition of their peers on a social media site. Today's hacking has gone pro. Most of it is criminal in nature, with bad guys looking for financial gain one way or another. And one of the most common ways is ransomware, which steals and encrypts your data and asks for payment to release. It is the Internet "Wild Wild West" right now in terms of cyber crime and it's every user's responsibility to be aware of the dangers and to take steps to protect yourself and your company's assets.

What is Ransomware?

Ransomware can take different forms, but in its most basic part, criminals utilize it to threaten to release sensitive data until a ransom has been paid.

In this manual, we want you to know what to expect BEFORE an attack happens. We discuss ransomware as PC, Mac, or mobile device-based malicious software that encrypts or steals a user or company's data and login credentials and forces them to pay a fee to the hacker in order to regain access to their data or prevent the unauthorized release of confidential data and credentials. The hackers primarily use the following vectors to infect a machine: phishing emails, unpatched programs, password guessing, compromised vendors, poisoned online advertising and free software downloads.

Not only can ransomware encrypt or steal data and credentials on a single computer, the software is smart enough to travel across your environment and encrypt or steal data and credentials from any other computer located on the same network. This can lead to a catastrophic situation whereby one infected computer can bring a department or entire organization to a halt. Imagine a law firm or accounting firm having all their client files encrypted or stolen. It is happening more and more.

Once the files are encrypted and/or stolen, the hackers will display some sort of screen or webpage explaining how to pay to unlock the data or prevent the unauthorized release of data and credentials. Also, ransomware often has a one-week deadline which, once passed, causes the ransom to increase. Ransoms can start in the $300-$500 area, however ransoms being paid in excess of hundreds of thousands of dollars are no longer uncommon.

Paying the ransom invariably involves paying a form of e-currency (cryptocurrency) like Bitcoin, abbreviated BTC. Once the hackers verify payment, they provide "decryptor" software and/or decryption keys, and the computer starts the arduous process of decrypting all of the data and not releasing the copied data and credentials.

In 2020, a Ransomware Infection is a Data Breach

Over the last year, ransomware has gone nuclear. There is a reason more than half of today's ransomware victims end up paying the ransom. Cyber-criminals have become thoughtful; taking time to maximize your organization's potential damage and their payoff. After achieving root access, the bad guys explore your network reading email, finding data troves and once they know you, they craft a plan to cause the most panic, pain, and operational disruption. Ransomware has gone nuclear and is now responsible for tens of thousands of cybersecurity incidents and billions of dollars in paid ransom.

Most of the ransomware gangs are now exfiltrating your most valuable data and threaten to expose it on publicly available websites as an additional extortion method. And some of these criminals make you pay twice, once for the decryption key, and then to delete the data they have stolen.

In 2020, the most popular ransomware programs including Ryuk, Dharma, Bitpaymer, SamSam, Sodinokibi, Phobos, GlobeImposter, Mrdec, and GandCrab. In the U.S. alone, a single cybersecurity insurance consortium said they are paying $1M a day in ransomware payouts to the ransomware gangs.

This figure doesn't include any other recovery and downtime costs, which often far exceed the cost of the ransom. By now, there are tens of thousands of ransomware victims, including school districts, police departments, and entire cities. It is important to understand that it is not just large organizations that are being impacted, it is also small and medium organizations.

Cyber criminals constantly use social engineering and update their ransomware themes. Some themes include the FBI variant, the Internal Revenue Service, and even sadly, now COVID-19 pandemic-themed ransomware. Mostly though, they and send employees emails with attachments that are supposedly invoices or other business documents they will likely open.

In addition to updating ransomware themes, cyber criminals are also developing creative new ways to spread the ransomware. These include offering Ransomware-as-a-Service (RaaS) strains such as "Dot" or "Philadelphia", where they offer your files back for free if you infect two other organizations. There are even marketing videos on YouTube for some ransomware strains.

In addition to updating ransomware themes, cyber criminals are also developing creative new ways to spread the ransomware. These include offering Ransomware-as-a-Service (RaaS) strains such as "Dot" or "Philadelphia", where they offer your files back for free if you infect two other organizations. There are even marketing videos on YouTube for some ransomware strains.

Bitcoin and Cryptocurrency
Bitcoin is currently the most popular form of cryptocurrency, but there are others including Ethereum, Litecoin, Ripple, Monero, and many more. Cryptocurrencies 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 near 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 cryptocurrencies has come a rise in ransomware.

Despite the above, using or owning cryptocurrencies is not an inherently criminal activity at all. Many respected companies accept cryptocurrencies 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 cryptocurrencies is paying some cybercriminal to unlock their files.

Some quick facts about Bitcoins:

- Bitcoin is commonly abbreviated as BTC, and is very difficult to trace.
- The price of Bitcoin is constantly fluctuating, sometimes by extreme amounts in a short time. In the beginning of 2016, 1 BTC was worth $400. In December 2017, it skyrocketed to just under $20,000, and as of May 2020 sits around $8,900 per bitcoin.
- 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.

Cryptomining
Cryptomining software is used to generate cryptocurrency by performing cryptographic calculations using a computer. Cryptominers can run CPU and GPU utilization to 100%, slowing down the computer and consuming a lot of electricity as they do their work.

Since the main goal of cybercriminals is to make money, it is no surprise that along with ransomware, we are seeing cryptomining malware being installed during an infection, so even if you can restore your data, they are making money using your electricity and resources for days, weeks, or even years after the infection.

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.

Cyber criminals 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).

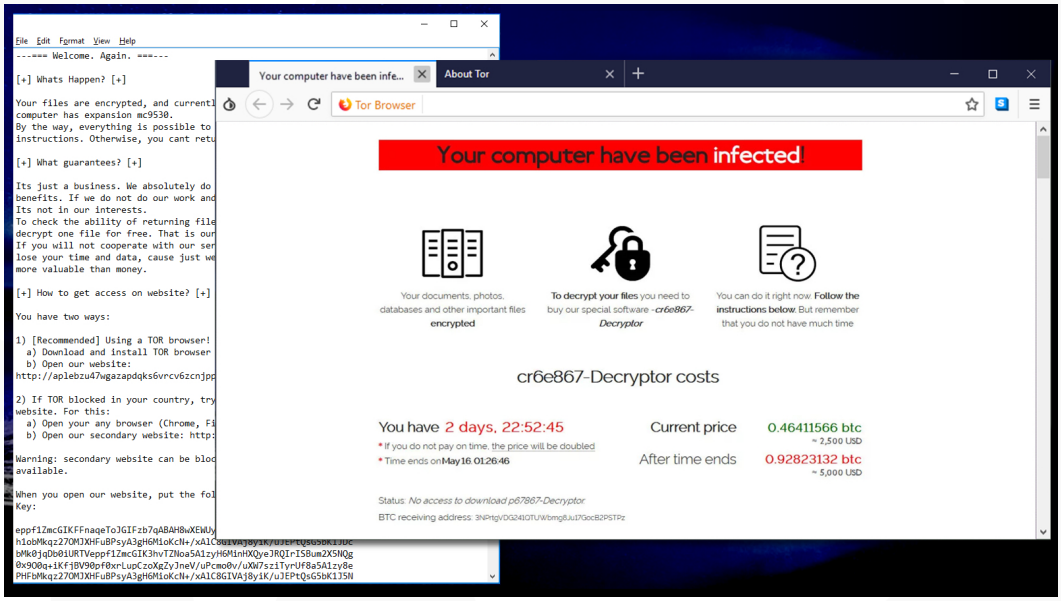
Am I Infected?

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 ransomware program or a related website 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.

Here is an example of a ransomware screen, the infamous Sodinokibi:



Here is an example of a ransomware webpage, threatening data exposure:

How do hackers obfuscate file extensions?

File Extensions are the last three parts of a filename after the period. A file may be called note.txt where the ".txt" section determines the type of file and what program opens it.

The reason this is important in ransomware, is often times your computer will be set to hide file extensions. Let's say someone sends you a file called "Payroll Accounts.xls". Often your email will show the file extension, but when you download the file, you may not see the extension anymore.

The "Payroll Accounts.xls" file is actually:

"Payroll Accounts.xls.exe"

This is a simplified example, since there are other ways to get around this.

A hacker may include a .zip file called "Family photos" that contains multiple files inside with altered extensions. Your email program only sees a .zip file, but in reality the .zip file contains a single file called "photo_album.jpg.exe".

The last thing to realize is that .exe files are not the only dangerous type of file out there. The following is a short list of potentially dangerous file types: .exe, .bat, .cmd, .com, .lnk, .pif, .scr, .vb, .vbe, .vbs, .wsh, .jar and .zip.

Infection Vectors

Email Vector

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 receives an email with an attachment or even a link to a software download, and they install or open that attachment without verifying its authenticity and the sender's intention, this can lead directly to a ransomware infection. This is the most common way ransomware is installed on a user's machine.

Drive-by-Download

Increasingly, infections happen through drive-by downloads, where visiting a compromised website with an old browser or 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 quickly caught and patched by the software vendor, but there is always a period of time where the software user is vulnerable.

Free Software Vector

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. After all, the user downloaded the file directly themselves! An example is a ransomware attack which exploited the popularity of the game Minecraft by offering a "mod" to players of Minecraft. When they installed it, the software also installed a sleeper version of ransomware that activated weeks later.

One method cyber criminals will use to install malicious software on a machine is to exploit one of these unpatched vulnerabilities. Examples of exploits can range from vulnerabilities in an unpatched version of Adobe Flash, a bug in Java or an old web browser all the way to an unpatched, outdated operating system.

Remote Desktop Protocol (RDP)

Internet-exposed Remote Desktop Protocol (RDP) sessions are another very common means of infecting networks. RDP sessions are used to remotely log in to Windows computers and allow the user to control that computer as if they were sitting in front of it. The technology typically uses port 3389 to communicate, and many organizations allow traffic from the internet through their firewall, so people can remotely access the computer. Hackers have become increasingly skilled at attacking these exposed computers and using them to spread malware within a network. RDP is exploited either due to an unpatched vulnerability or due to password guessing because the victims chose very weak passwords and/or did not enable account lockout protections.

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.

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*

Determine if your data or login credentials have been copied, and if so, how much and what. This can often be learned from the ransomware program's announcement itself, as it brags as to what data has been copied or the information regarding your stolen data that the hacker posts on websites or blogs. Check your logs and any data leak prevention (DLP) tools to see if it noted any stolen data. Look for large unauthorized archive (e.g., zip, arc, etc.) files that contain your data, that the hacker used for staging before they copied it. Look into any systems which might record large amounts of data being copied off the network. Look for malware, tools, and scripts that might have been used to look for and steal data. The main initial sign to look for to see if your data and credentials have been stolen is the ransomware gang telling you they have done it. If the ransomware gang tells you they have your data or credentials, believe them. They don't bluff that often.

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 or stealing your data and/or credentials, 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.

Ransomware strains vary in that some are costlier (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.

Most strains of ransomware are now able to spread onto other computers on your network even if they have not been directly shared with the infected machine. Meaning, if a machine is infected and has connections to drives or network folders, the ransomware can now "install" itself on other computers (like a worm) if it has access to those shared resources.

In the past, ransomware infections would generally only affect a single machine and all shared resources it has access to, not an entire network of computers, however that has changed, as evidenced by the WannaCry ransomware strain.

Today, ransomware typically gains access to a new organization and then "dials home" to update itself. Ransomware updates itself as many as 20 times a day to make sure it cannot be detected by most anti-malware scanners and to get new functionality and instructions. It notifies its owner of the new compromise and the ransomware gang visits the victim's environment at their leisure. The ransomware gang uses malware, tools, and scripts to look around the environment and they eavesdrop on emails to determine what digital assets they need to encrypt and steal to cause the most pain. They will research the organization to determine how much ransom to charge. They want to charge as much as they can without making the amount so erroneous that the victim will never pay. Common ransom payout requests are around 2% of annual net revenues. Then they set off their ransomware payload and start the extortion. Time from initial break-in to extortion notice can often be weeks and months.

4. Evaluate Your Responses:
Now that you know the scope of your encrypted and/or stolen data and credentials 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, if all you have is an encrypted data threat (and no stolen data or credentials), then 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

If your data and credentials have been stolen and the ransomware gang is threatening to release the information, your situation won't be saved by a good backup or decryptor. Instead, you need to figure out the ramifications of the stolen information being released if you don't pay the ransom. The information could include your own critical confidential data, and credentials for your employees and customers, possibly well beyond just work-related accounts. Your employee's personal passwords (e.g., banking, social media, etc.) may have been captured. Also, your customer's passwords to your services could have been captured. What does that information being publicly released mean for your employees and customers (if involved)? What is the goodwill damage if the stolen credentials were to be revealed publicly and everyone knows you didn't pay the ransom?

This manual will cover each of these options in detail to provide you with the best-case scenario as well as contingencies and other outlying issues surrounding each of the options listed above.

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, then a priority will need to be given to the response most likely to get results in a shorter time-frame.

First Response: Restore Your Files From a Backup

NOTE: This section assumes you only have an encrypted data problem and not a data or credential theft problem. As noted above, if your data or credentials are stolen, then the considerations go beyond just encrypted data recovery options.

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. Cyber criminals 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* at the end of this document to audit your network and determine where you can take further steps to prevent these types of attacks from causing damage.

Here are some technical controls you can put into place, suggested by Steve Ragan, a noted computer security writer:

- 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 Full control or Write/Modify access only where it's needed, don't allow ownership of or permissions of resources to be changed by regular end-users 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.

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 steps 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.

Hancock Health in Indiana paid $50,000 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 cryptocurrency 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 provide you with a way to 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.

Example TOR website addresses:
kprrj4jalkparf4p.onion/rqla 7yulv7filqlrycpqrkrl.onion

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.

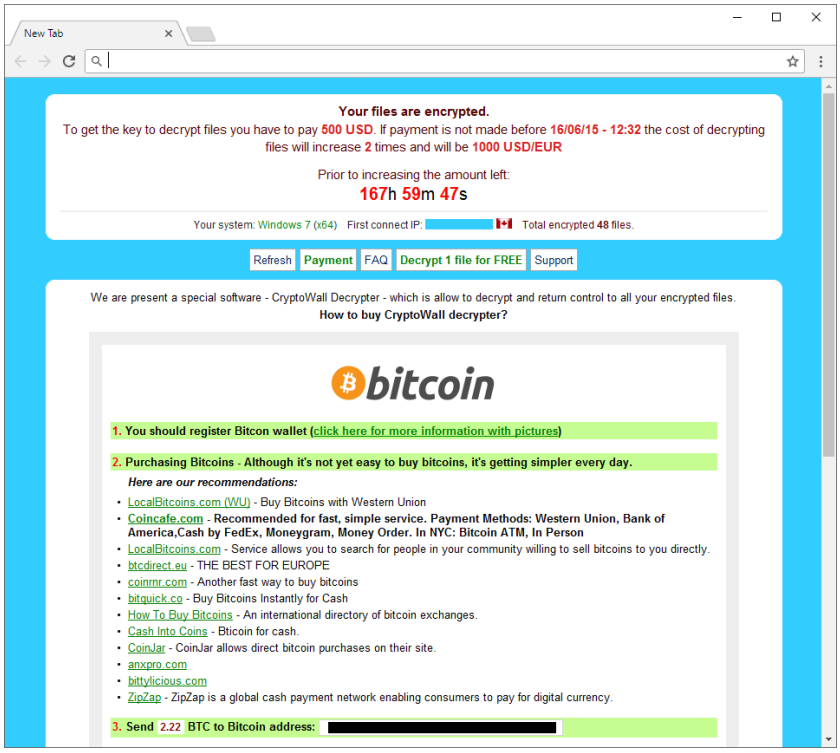
With many types of ransomware you will have to visit a page on the TOR network that has been created specifically for paying your ransom. Enter the web address of the site into your TOR browser. You can usually follow the instructions on the site to locate the wallet ID you need to send your Bitcoin 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.

Example of a Bitcoin wallet string:
19eXu88pqN30ejLxfei4S1alqbr23pP4bd

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.

To the right is an example of the CryptoWall ransomware payment screen.



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.

Protecting Yourself in the Future

Regardless of whether you've been hit with ransomware or not, protecting your network from these types of attacks is now an integral part of any network security framework for both individuals and companies.

Defense in Depth
Protecting yourself from intrusions and attacks requires securing your main layers of defense.

If you consider a computer network to consist of a series of layers that any malware or virus needs to penetrate, the outermost layer would consist of your users themselves. After all, it takes a user's interaction in order to initiate or allow a network intrusion. Only AFTER a user has clicked or visited a malicious link/site will your secondary and tertiary layers (firewalls and antivirus) come into play. Thus, the very first layer you will need to harden is that of the human operator. It is only in recent years that the importance of this layer of security has come to be recognized. In the past, software has been relied upon as a catch-all for these types of situations. Software just by itself is not enough anymore, users must be trained to prevent such attacks from happening in the first place.

Security Awareness Training
Yes, this is the part of the manual where we tell you that you need to implement effective security awareness training.

Despite evidence to the contrary, users do not come to work with the intention of clicking on phishing emails and infecting their computers! As many IT professionals can attest, a simple knowledge of what red flags to be aware of can make a huge difference in the ability of a user to discern malicious links/software from legitimate traffic. As the methods hackers and malware creators use to trick users are constantly changing, it is important to keep users up-to-date on not only the basics of IT and email security, but also the ever changing attack types and threat vectors. After all, everyone knows that there is no Nigerian prince out there and it's just a scammer right?

But what if "Becky" from the "accounting firm" accidentally sends you a payroll spreadsheet? Not everyone is going to question the ambiguous origin of a well-crafted phishing email, especially with a juicy attachment like Q4 Payroll.zip. HR may receive 20 resumes a day, but only one of those needs to be malicious to cause an incident.

Increasingly, hackers and attacks utilize "social engineering" to entice or trick a user into installing or opening a security hole. KnowBe4 Security Awareness Training covers not only software based threat vectors and red-flags, but physical security training as well. User security training is a vital piece of securing your network.

Simulated Attacks
While training can have a big impact on hardening the first layer of security, it is the one-two punch of training combined with simulated phishing attacks that can create a constant state of users being on their toes with security top of mind, which will make it extremely hard for any phishing attempt or email-based attack to succeed.

Today, with KnowBe4's simulated phishing campaigns, you can send fully randomized and completely customizable simulated phishing attempts to any number of users in your environment. It is important that your users are constantly on the lookout for these attacks. After all, if they know that the organization is phishing them, they will pay extra attention to what is coming through their inbox. Users can no longer rely on "the antivirus" or "IT" to handle any slip-ups—they are being actively tested! Also, any lapses or errant clicks can be used as opportunities for further training on what types of red-flags to be aware of. The consequence of clicking on a simulated phishing email is far less destructive than the alternative.

Another benefit of simulated phishing attacks is immediate inoculation against current threats. For example, you can use simulated phishing attacks to get an accurate idea of how your users will respond to malware and phishing emails that are actually being used by ransomware developers to infect systems. This way, you can immediately detect vulnerabilities and educate users on current threats so they know what to watch out for. KnowBe4 keeps an updated list of ransomware and current event email templates that you can use to check for any phish-prone users in your environment.

Software-Based Protection: Antivirus, Antispam/Phishing & Firewalls
One simply cannot operate a computer these days without a software based protection in-place. It is vital even for stand-alone computers to utilize this software. In fact, it is almost assured that you or your organization are already utilizing one or more of these solutions. While this document could go on for chapters about the whys and wherefores of various security software, the focus of this manual is on ransomware. As a result, we are going to point out some particular software solutions to this issue that can be implemented.

First, Microsoft has a feature called AppLocker that can be used in a secure environment to ONLY allow certain software (as defined in the policy) to run. There are certain directories that ransomware infections will typically start in, and by isolating these directories with a software restriction policy, you can cut down on the susceptibility of infections.

Another option for reducing the chance of ransomware infections (on top of your existing antivirus solution) is to use a specialized software for scanning for these types of infections.

In addition, Microsoft has developed a "Controlled Folder Access" feature which prevents files in specified folders from being modified by unauthorized applications.

- *For more information on these topics, visit our Ransomware Knowledge base*

Backups
The last piece of the puzzle in any ransomware protection must include a regular backup of your files as well as a regularly TESTED restore procedure. With so many options available for both on-site backup solutions and cloud-based backup solutions, there is no reason any user or company should not have a very regular backup of files. To help prevent your backups from being compromised, you should always have an off-site or redundant backup in place. If your backups are easily accessible by a computer infected with ransomware, don't be surprised if your backups are encrypted as well! Having off-site and recent backups are standard "best practices" for backup procedures against ransomware.

An often overlooked part of any backup procedure is testing that your restoration of files actually works! There is nothing worse than discovering an old hard-drive or DVD that you burned with backups is now unresponsive or malfunctioning. Always ensure you have adequate and fast enough access to your backup sources and a function restoration method in place. "I have DropBox" is not an adequate backup solution. While DropBox does have versioning, they are not a backup service and recovering older versions of your files from common cloud based storage such as DropBox, Google Drive and OneDrive can be a very tedious or time-consuming task as they are not set up or designed to be a backup service.

Readers should note that since ransomware is now routinely copying data and stealing credentials that a backup alone will not save you. Prevention against getting exploited by ransomware is essential. A backup alone will not save you. You must use a defense-in-depth protection strategy to prevent ransomware from being executed in your environment in the first place. That should be your primary goal. And then also have a great, tested backup that you are able to restore in case you need it as well.

KnowBe4

Ransomware Attack Response Checklist

STEP 1: Disconnect Everything

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

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

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

STEP 3: Determine if data or credentials have been stolen

- [ ] a. Check logs and DLP software for signs of data leaks.
- [ ] b. Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files.
- [ ] c. Look for malware, tools, and scripts which could have been used to look for and copy data.
- [ ] d. Of course, one of the most accurate signs of ransomware data theft is a notice from the involved ransomware gang announcing that your data and/or credentials have been stolen.

STEP 4: Determine Ransomware Strain

- [ ] a. What strain/type of ransomware? For example: Ryuk, Dharma, SamSam, etc.

STEP 5: Determine Response

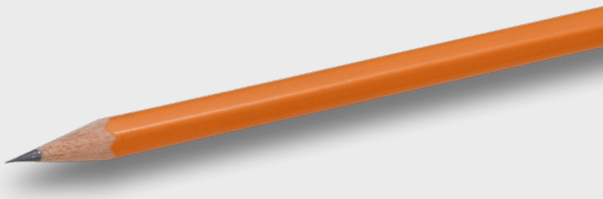
Now that you know the scope of the damage as well as the strain of ransomware you are dealing with, you can make a more informed decision as to what your next action will be.

Response 1: If Data or Credentials are Stolen

- [ ] 1. Determine if ransom should be paid to prevent data or credentials from being released by hackers.
- [ ] 2. If ransom is to be paid, you can skip steps #1 and #3 of Response 2 from recovery.

Response 2: If Ransom Is Not Paid and You Need to Restore Your Files From Backup

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



Response 3: Try to Decrypt

- [ ] 1. Determine strain and version of the ransomware if possible
- [ ] 2. Locate a decryptor, there may not be one for newer strains. If successful, continue steps...
- [ ] 3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)
- [ ] 4. Decrypt files
- [ ] 5. Determine the infection vector & handle

Response 4: Do Nothing (Lose Files)

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

Response 5: Negotiate and/or Pay the Ransom

- [ ] 1. If possible, you may attempt to negotiate a lower ransom and/or longer payment period.
- [ ] 2. Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.
- [ ] 3. Obtain payment, likely Bitcoin:
    - a. Locate an exchange you wish to purchase a Bitcoin through (time is of the essence).
    - b. Set up account/wallet and purchase the Bitcoin.
- [ ] 4. Re-connect your encrypted computer to the internet.
- [ ] 5. Install the TOR browser (optional).
- [ ] 6. Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been set up for this specific ransom case.
- [ ] 7. Pay the ransom: Transfer the Bitcoin to the ransom wallet.
- [ ] 8. Ensure all devices that have encrypted files are connected to your computer.
- [ ] 9. File decryption should begin within 24 hours, but often within just a few hours.
- [ ] 10. Determine infection vector and handle.

STEP 6: Protecting Yourself in the Future

- [ ] a. Implement Ransomware Prevention Checklist to prevent future attacks.

KnowBe4 Ransomware Prevention Checklist

First Line of Defense: Software

- [ ] 1. Ensure you have and are using a firewall.
- [ ] 2. Implement antispam and/or antiphishing. This can be done with software or through dedicated hardware such as SonicWALL or Barracuda devices.
- [ ] 3. Ensure everyone in your organization is using the very latest generation endpoint protection, and/or combined with endpoint protection measures like whitelisting and/or real-time executable blocking.
- [ ] 4. Implement a highly disciplined patch procedure that updates any and all applications and operating system components that have vulnerabilities.
- [ ] 5. Make sure that everyone who works remotely logs in through a VPN.

Second Line of Defense: Backups

- [ ] 1. Implement a backup solution: Software-based, hardware-based, or both.
- [ ] 2. Ensure all possible data you need to access or save is backed up, including mobile/USB storage.
- [ ] 3. Ensure your data is safe, redundant and easily accessible once backed up.
- [ ] 4. Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups for at least 3 or 4 months in the past. Bad guys lurk in your networks for months and compromise your backups.

Third Line of Defense: Data and Credential Theft Prevention

- [ ] 1. Implement Data Leak Prevention (DLP) tools.
- [ ] 2. Use least-permissive permissions to protect files, folders, and databases.
- [ ] 3. Enable system logs to track data movements.
- [ ] 4. Use network traffic analysis to note any unusual data movements across computers and networks.
- [ ] 5. Encrypt data at rest to prevent easy unauthorized copying.

Fourth and Last Line of Defense: Users

- [ ] 1. Implement new-school security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.
- [ ] 2. Your email filters miss between 5% and 10% of malicious emails, so conduct frequent simulated phishing attacks to inoculate your users against current threats, best practice is at least once a month.

Additional Resources

Ransomware Simulator
Find out how vulnerable your network is against ransomware attacks.

Free Phishing Security Test
Find out what percentage of your users are Phish-prone.

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click!

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do.

Free Domain Spoof Test
Find out if hackers can spoof an email adress of your own domain.

CEO Fraud Prevention Manual
CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

To learn more about our additional resources, please visit www.KnowBe4.com/resources

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make better security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

V022021