KnowBe4
Human error. Conquered.

Ransomware Hostage Rescue Manual

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

NEW EDITION

Table of Contents

INTRODUCTION

Ransomware is one of the most damaging types of cyber attacks of all time, and the one feared the most by business owners and cybersecurity defenders. This worry is not without reason. In an instant, an organization's critical IT infrastructure can be brought down for weeks to months, completely stopping all business. Some data and systems may be lost forever. Complete recovery may take over a year. Intellectual property and confidential data may be stolen, publicly posted, or used adversely in future attacks. Customer impacts may last long past the technical recovery process.

While 2023 started out looking fairly typical, global ransomware attacks saw a resurgence later in the year. According to the Corvus insurance Q3 report, there was an 11% quarter-over-quarter increase in Q3 and a 95% increase year-over-year on leaks sites, with many attacks increasing against law firms and municipalities.

Researchers estimate that 2023 will be the first year to have over 4,000 victims posted on leak sites, a dramatic increase over the 2,670 in 2022. Groups such as Clop, AlphV and LockBit were some of the key players behind these attacks in 2023, but there are a lot of new players in the games as well, some with ties to previous groups.

The financial impact continues to be huge across the board, however the theft and public dumping of sensitive data, from intellectual property to employee and financial records, is a gift that keeps on giving. While the cost of a ransomware attack and downtime due to unavailable systems can be significant, organizations can typically recover and return to business eventually, however publicly dumped information, especially PII, can never be made private again, creating ongoing issues for those impacted.

Most ransomware victims suffer catastrophic business interruption for days to weeks due to critical systems being encrypted and may not get back to full capacity for many months. This can severely impact operations. A clear example of this was the attack against Clorox, the bleach and cleaning product manufacturer, which suffered a ransomware attack in October of 2023 and has reported a 20% sales decrease, equaling about $356 million, for Q1 of 2024. The same group that hit Clorox, also hit Caesars Entertainment, who paid a $15 million ransom to avoid data being publicly dumped, and the group was also responsible for taking down MGM Resorts for 10 days, causing an estimated $100 million in damages. Clearly this was a good year for the Scattered Spider and AlphV ransomware groups behind these attacks, who, unsurprisingly, seem to favor social engineering attacks as the way to accomplish their goals.

Even in cases where encryption was not employed to impact operations, the Clop group proved that the simple threat to make sensitive information public is enough to make a comfortable living after earning between $75 and $100 million just from the MOVEit vulnerability it exploited in early to mid-2023.

Regional impacts:

Ransomware is a global problem with no region being free from attacks. International groups such as the International Counter Ransomware Initiative (CRI) are being formed between governments and coordinated takedowns of groups have occurred, however there is still a lot of room for improvement.

Germany:

Germany is a part of the CRI which is aiming to help fight against the BSI information security office's estimated loss of 203 billion euros due to cyber attacks in 2023. According to the BSI, small and medium businesses and local government and municipal websites are being targeted, however it's clear that larger enterprises such as Rheinmetall AG are not avoiding attacks.

UK:

A recent parliamentary committee has made the bold statement that Britain is at high risk of a catastrophic ransomware attack, largely due to poor planning and lack of investment. The joint committee chair went on to say that, "The UK has the dubious distinction of being one of the world's most cyber-attacked nations…." In 2023 Manchester Police, Royal Mail and the British Library have all been victims of ransomware along with countless other private organizations.

Other European attacks:

Europe is not safe from the threat of ransomware, with some significant events happening across the region. In late 2022 the Barcelona Health Center in Spain was impacted, causing the cancellation of surgeries and thousands of patient checkups. Shortly after Antwerp, Belgium was taken offline by ransomware and had 16 years' worth of data, including that from the police unit, being made public by the attackers. 2023 started out with the ION Group attack which had customers across Europe and the US having to switch to manual processing of derivative trades, causing delays and other issues.

APAC:

The APAC Region is not off the hook either, with significant attacks happening to Denso (Japan), MSI (Taiwan), TSMC (Taiwan), Development Bank of Southern Africa, Port of Nagoya (Japan), Auckland Transport Authority (New Zealand) and Sony (Japan) being some of the headliners from ransomware attacks in 2023.

In summary, at the very least, ransomware causes perilous business interruption, critical data loss, and a long, expensive recovery and is not geographically limited. There's a reason why ransomware has been a top cybersecurity fear for over a decade.

But you can take steps to significantly reduce the risk of a successful ransomware attack and decrease recovery time and costs if you create and follow your own ransomware incident response plan. That's what this document is all about.

WHAT IS RANSOMWARE?

Ransomware can take different forms, causing many different types of threats and damage. In its most common form, criminals use it to threaten to prevent access to critical data and systems and/ or to release sensitive data unless a ransom has been paid. Here are some of the common impacts of ransomware:

- Encrypts data and systems, causing downtime and recovery costs
- Steals confidential data, exfiltrates it outside the organization, and threatens to release it
- Steals organization, employee and customer login credentials
- Denial of service attacks against sites and services
- Resource hijacking (e.g., installs crypto-miners, etc.)
- Uses compromised victims' systems and earned trust to compromise customers and business partners
- Publicly shames victim, causing reputational damage

The general media has coined the term "double extortion" to describe the threats and damage that ransomware groups promise and/or accomplish along with the traditional encryption of data. All-in-all, the damage that the average ransomware attack causes to a victim organization is often quite extensive.

> *Today, over 80% of all ransomware attacks involve "double extortion," data and credential exfiltration.*

The ransomware attackers primarily use the following vectors to infect a machine: phishing emails, unpatched programs, password guessing/theft, compromised vendors, poisoned online advertising, and compromised software downloads, however these bad actors are increasingly using vishing, or voice phishing, to do their work over the phone.

If the ransomware attack is successful, once the files are encrypted and/or stolen, the attackers 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. Ransomware often has a less than one-week deadline, which if passed, may cause the payment demand to automatically increase or may cause the encryption may be left in place permanently and the stolen data released publicly or to other cybercriminals.

Bitcoin and Cryptocurrency

Paying the ransom invariably involves paying with some form of cryptocurrency, such as Bitcoin (abbreviated BTC). Bitcoin is currently the most popular form of cryptocurrency and the most popular type required to pay ransomware extortions. But there are other popular cryptocurrencies including Ethereum, Litecoin, Ripple, Tether, XPR, Dogecoin, and many more.

Enhanced privacy cryptocurrencies, like Zcash and Monero, are gaining popularity with some ransomware groups because they make it harder for law enforcement to trace and block the extorted money.

Some ransomware groups use other types of payments, such as gift cards or money-wiring services, but Bitcoin and cryptocurrencies remain the number one payment method by a large margin because of their increased privacy over cash and traditional forms of payment. Cryptocurrencies can be transferred anywhere in the world via the Internet. Anyone looking in the right places can see the associated "digital wallets" involved in any cryptocurrency transaction, but it takes an observer skilled in cryptocurrency tracking with access to a very large database of transactions to track particular cryptocurrency transactions to the involved real-world people or groups. Associating wallets and transactions to real world identities can be done in most cases, but it takes time, money, and commitment. In recent years ransomware gangs have sometimes used laundering services called crypto "mixers" or "tumblers,", services that break up cryptocurrency into small amounts and mix it with other funds, to further makeing tracking much more difficult. This makes cryptocurrency the ideal payment method for ransomware groups.

TOR (Anonymity Network)

Ransomware groups will often require that all communications between the victim and themselves happen across TOR ("The Onion Router"). TOR is a virtual network and related browser developed to attempt to anonymize Internet traffic. It uses a special browser (the TOR browser) that is configured to use an ever-changing worldwide volunteer network of network traffic relays. All traffic is encrypted at the origination point and then sent across an anonymized set of randomly selected "TOR nodes," until it reaches its intended destination. The TOR network was designed from the ground up to anonymize and hide the originating and ending destination of the traffic from other observers.

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 (and cryptocurrencies) are so well crafted for anonymizing activity, ransomware groups 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) 3
- Although the TOR network and browser do a good job at hiding participants' real locations and activities, those locations and activities can sometimes be discovered using other methods, often not related to the TOR network or browser

Typical Ransomware Process

Today, a ransomware program typically gains initial access to a new organization and then "dials home" to its involved "command and control" servers. Ransomware often updates itself to make sure it cannot be detected by most anti-malware scanners and to get new functionality and instructions. It notifies its controlling operator of the new compromise. The ransomware hacker or gang can then let the ransomware program do what it was automatically programmed to do, give it new instructions, or visit and explore the victim's environment at their leisure.

The ransomware attackers or gangs often use additional malware, tools, remote management programs, and scripts to look around the victim's environment and they eavesdrop on emails to determine what digital assets they need to encrypt and steal to cause the most pain. They will usually research the victim organization's financial status to determine how much ransom to charge. They want to charge as much as they can without making the amount so onerous that the victim will never pay. Common ransom payout requests are around 2% of annual net revenues. They will exfiltrate credentials and data and then launch their encryption programs, encrypting files or folders, and start the extortion. The time from initial break-in to encryption and the extortion notice can be measured in minutes to months. Some ransomware programs immediately encrypt the single host they are on. Most ransomware programs allow their hacker controllers to come in and access the victim to get the largest potential payout and then encrypt multiple computers.

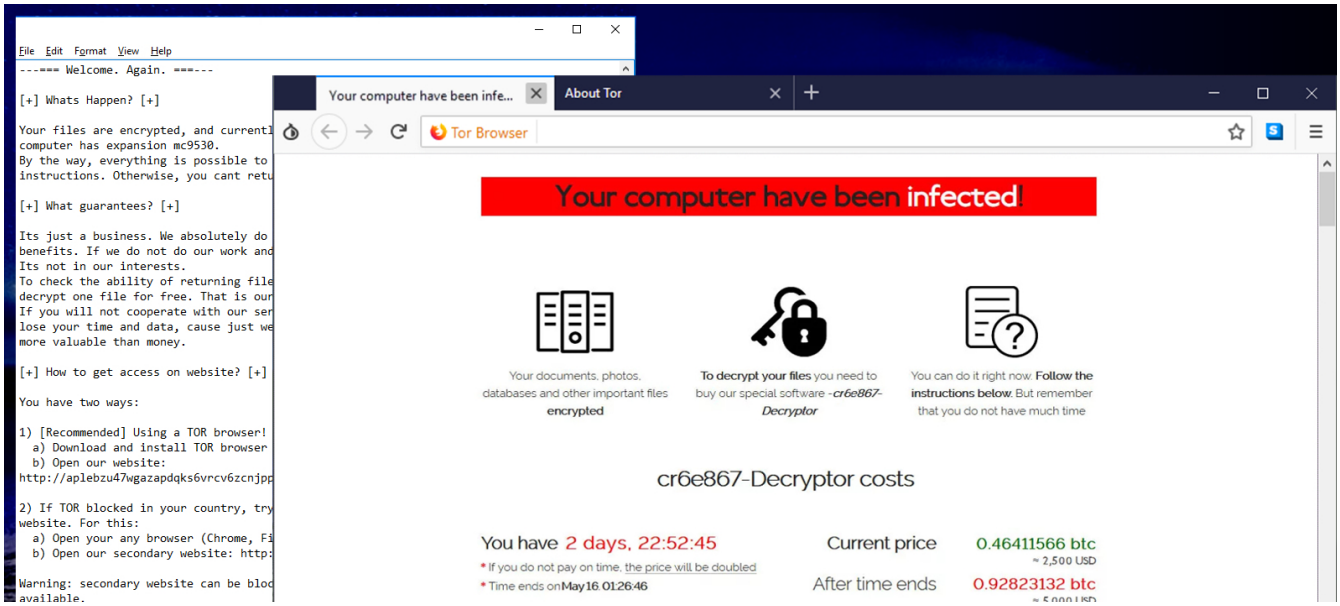
If the victim decides to pay the ransom, once the hackers verify payment, the bad actor usually provides the victim with "decryptor" software and/or one or more decryption keys. The victim can then start the arduous process of decrypting all of the encrypted data. If data exfiltration is involved, the hacker then promises not to release the copied data and credentials.

AM I INFECTED?

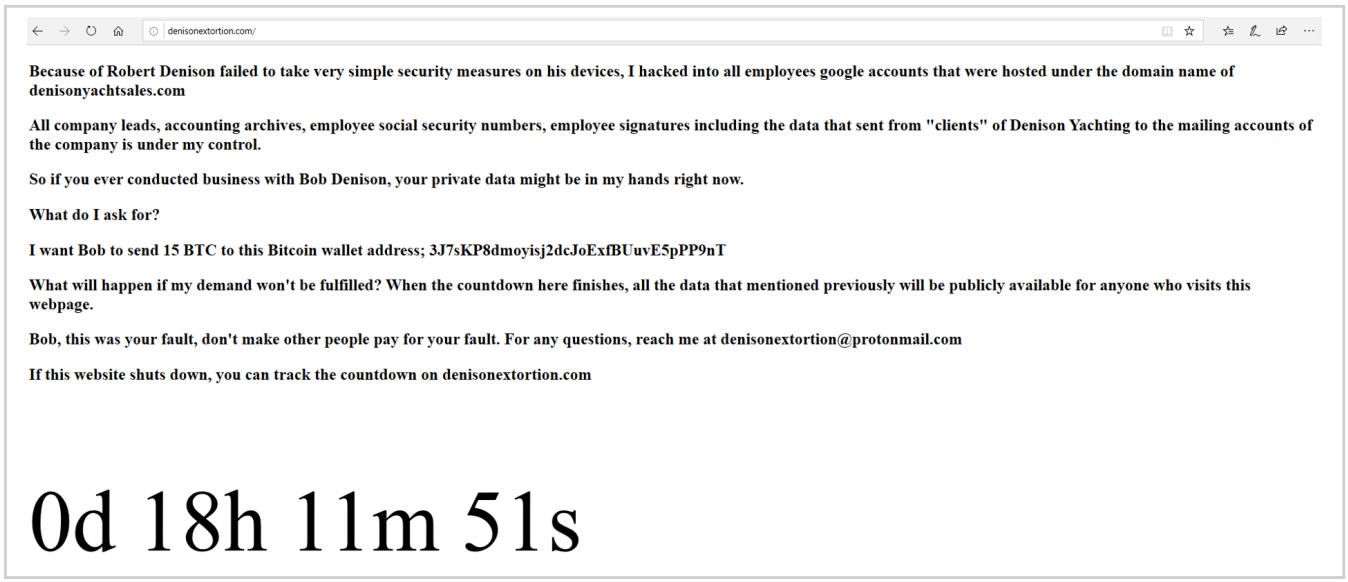
It's usually straightforward to find out if you are exploited by a ransomware program. The most common signs and symptoms are:

- One or multiple unexplained sudden "crashes" on otherwise unrelated systems on the same network
- A ransomware "notice" is visibly displayed
- You suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension
- 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 warning message window has been opened by the 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 from the Sodinokibi ransomware program:



Here is an example of a ransomware notice on an exploited customer's website, threatening data exposure:



HOW MOST RANSOMWARE VICTIMS WERE EXPLOITED

Since the beginning of computers, only two root cause methods have accounted for the vast majority of malicious breaches on most devices and most organizations:

- Social engineering
- Unpatched software

This also holds true for ransomware attacks. There are various other malware and hacking methods that became very popular for a few years (such as boot viruses, USB key infections, etc.), but social engineering and unpatched software have been either the number one or number two most popular exploit methods for most years over three decades.

Every organization, unless they have experience and expectations to show otherwise, could benefit from more focus on putting down social engineering and phishing, and better patching their environment. Doing so would best decrease the overall cybersecurity risk most efficiently.

As stated in KnowBe4's *The Root Causes of Ransomware* whitepaper, social engineering and unpatched software remain the top attack vectors exploited by ransomware groups to gain access to victim devices and networks. But some other attack vectors are also prevalent in ransomware attacks, in particular, as shown in the summary table of other collected ransomware mitigation vendor surveys (as displayed in KnowBe4's The Root Causes of Ransomware whitepaper):

Report Name	Social Engineering	RDP	Unpatched Software	Password Guessing	Credential Theft	Remote Server Attack	Third Party	USB	Other
Coveware Report	30%	45%	18%	-	-	-	-	-	5%
Statista	54%	20%	-	-	10%	-	-	-	-
Forbes Magazine Article	1st	3rd	2nd	-	-	-	-	-	-
Datto's Report	54%	20%	-	21%	10%	-	-	-	-
Hiscox Cyber Readiness	65%	-	28%	19%	39%	-	34%	-	-
Sophos Report	45%	9%	-	-	-	21%	9%	7%	9%
Averages	50%	24%	23%	20%	20%	21%	22%	7%	7%

Although numerous attack vectors are categorized differently by the various vendors, it is clear that a third additional common attack vector is commonly used by ransomware groups: password attacks. Either the ransomware group logs into the victim's devices using a previously stolen valid login name and password or they successfully guess at a login credential.

This initial login access is then leveraged into additional exploitations, which eventually allow more of the network to be compromised.

With ransomware attacks, in particular, it is clear that three attack vectors allow the vast majority of ransomware attacks:

- Social engineering
- Unpatched software
- Password attacks

Here are some further descriptions of some related attacks

Social Engineering by Email
The most common social engineering scenario involves an unexpected email arriving with an email attachment disguised as an innocuous file. If a user installs or opens that attachment without verifying its authenticity, this can lead to a ransomware infection.

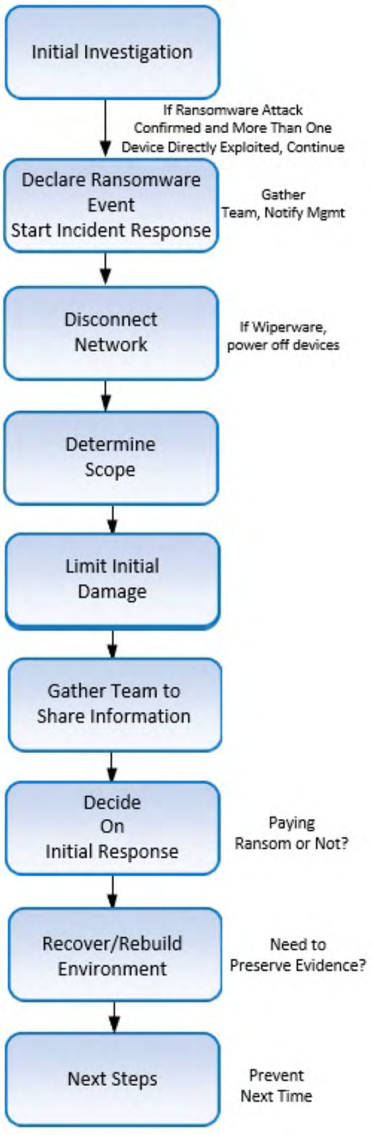
Silent Drive-by-Download
Aa user with a vulnerable, unpatched software program on their computer visits a rogue or compromised website, which attempts to exploit an unpatched vulnerability. If successful, usually the victim is not aware their computer has been compromised (i.e., the "silent" part).

Unpatched Servers or Services
Hackers will seek out vulnerable, unpatched software programs on the victim's machine or network that can then be exploited to allow the execution of malicious code. A dedicated effort to discover and patch vulnerable software can prevent these exploits.

Free Software Vector
A free version of a piece of software can come in many flavors, such as "cracked" versions of expensive games or software, free games, game "mods" or adult content.By preying on the user in this way, the hackers can bypass any firewall or email filter.

Remote Desktop Protocol (RDP)
Microsoft Windows Remote Desktop Protocol (RDP) are often used to remotely log into Microsoft Windows computers and allow the admin/ user to control that computer as if they were sitting in front of it. Hackers have become increasingly skilled at attacking these exposed computers running RDP and using them to spread malware within a network.

RDP is usually exploited either due to an unpatched vulnerability or password guessing because the victims chose very weak passwords and/or did not enable account lockout protections.



I AM EXPLOITED WITH RANSOMWARE, NOW WHAT?

Once you have determined you have been exploited by ransomware, it is imperative to immediately take action.

Each step will be covered in more detail below:

1 | Initial Investigation

All potential ransomware attacks begin with one person or more people reporting a suspicious cyber event. Someone may even report a ransomware message or files which seem to be encrypted, either of which strongly points to a likely ransomware event. The initial investigation is to confirm the existence of real ransomware.

For example, some ransomware messages may be from hoax messages that really do not encrypt files. Or some random encrypted files were found, but they appear to have happened in the past during an older event. Other times, an initial responder may strongly suspect ransomware, but not be 100% confident in their initial diagnosis.

When ransomware is suspected, there are two main data points to confirm one way or another. First, does the reported suspected event(s) involve real (and not hoax) ransomware? Second, are more than two devices involved? If only one device is involved and no other devices are yet suspected or proven exploited by ransomware, it may be too early to declare an "official" ransomware event which requires a full, "all-hands-on-deck" ransomware event response.

Many organizations discover the ransomware program during its initial exploitation, before it has had a chance to spread or even encrypt a single file. It is still very important to discover if the ransomware event has spread to more than one machine and prevent its spread to other devices if possible. However, if only one computer is confirmed to be exploited, it may not yet be time for an incident response by the entire ransomware response team. When in doubt, treat the single finding as if multiple computers may be compromised and continue to follow the ransomware response plan.

If you confirm even a second device is involved, you must consider the possibility that ransomware has spread across all network-connected devices within the same organization until proven otherwise and proceed with a full ransomware response.

NOTE: while classified as ransomware due to similarities in tactics and the demand for a ransom in exchange for not making information public, many of the steps related to decryption of data and data recovery may not apply. It is still critical to determine the scope of intrusion and other steps, such as negotiating with the attackers and closing any back doors they may have left. Keep this in mind if dealing with a theft and extortion only group.

2 | Declare an Official Ransomware Event

If two or more devices have been exploited by ransomware, it is time to declare an official ransomware event. This means the full, "all-hands-on-deck," incident response approach is needed. Senior management should be notified, along with currently known details. Legal should be notified and get actively involved as soon as possible. All involved ransomware incident response team members should be notified and told to start to check for additional signs

of ransomware compromise and spread. Everyone should document what they check, what they check for and what was determined. Every asset on the network(s) should be considered exploited and monitored by the involved ransomware group until the asset is determined to be unimpacted or declared officially clean or recovered. Any existing passwords should be considered compromised. One compromised device on a network means the entire network is considered untrusted until it is cleaned and recovered.

Any existing used or stored passwords should be considered compromised.

Everyone should start to use previously agreed upon, alternate, communication methods, which exclude the involved compromised networks and assets. Usually, this means using cell phones and/or external messaging applications (e.g., Slack, WhatsApp, etc.) for ransomware response team communications. You do not want any asset that could possibly be compromised being used by the ransomware incident response team for communications. The ransomware incident response team, along with management, and legal, should use the alternative communication method going forward until further notice.

Legal should make all external communications to any other third parties outside the impacted victim organization, because such communications are more likely to be considered "privileged communications" and harder to learn by other parties in the event of a legal lawsuit or investigation. Assume any previous communications on the compromised network and assets could have been eavesdropped on and known by the attacker.

You should already have a previously agreed upon alternate communication method to use for ransomware response and recovery.

3 | Disconnect Network

If only one device is currently known to be exploited by ransomware, immediately disconnect it from the network (e.g., all wired and wireless connections, if they exist). If multiple devices are exploited by ransomware, disable network abilities across all possibly impacted devices. This includes any Internet access, and any ingress or egress network points. Consider disconnecting all network access for all devices even if only a single exploited device is currently known if you want to decrease the risk of ransomware spread and active control.

Some organizations may want to disconnect the network by disabling network features on each potentially impacted device—either manually or using an automated method. In most cases, disconnecting the network can be more easily done by disabling the shared network equipment (e.g., routers, switches, VLANs, Wi-Fi routers, etc.) that the devices share. You can disable the network on each device separately, but it will usually take longer and require individual physical access to re-enable network access when networking is again allowed. Unplug any storage devices such as USB or external hard drives.

If you have to disable networking on a device connected to the network, disable it on shared network device(s) instead, if you can.

Do not power down devices. Do not erase anything or "clean up" any files or antivirus (at this time). This is important for later steps and may cause issues with recovery or evidence preservation if done too early.

There are two important exceptions to this rule. First, if you see a computer in the early stages of file encryption (i.e., you have caught it early before it has encrypted most files) or if you suspect "wiperware," you can immediately power down (not a graceful "shutdown") the impacted device(s). Wiperware is malware which simply erases, corrupts or encrypts disk information or files without any intention of allowing any easy recovery, even if a ransom payment was requested and paid. There are examples of malware that pretend to be ransomware, but are instead wiperware.

Unfortunately, it can be impossible and difficult to know the difference between ransomware and wiperware early on, especially when wiperware is pretending to be ransomware in order to spread more and do more damage before defenders start damage mitigation. Luckily, instances of wiperware pretending to be ransomware are extremely rare in occurrence, so in light of any evidence to the contrary, most defenders should assume malware claiming to be or acting like ransomware is actually ransomware. But always keep in the back of your head the risk of wiperware.

4 | Determine the Scope

At this point you need to determine exactly how much of your infrastructure is compromised, what is encrypted/corrupted, and if any data and/or credentials have been exfiltrated. When looking for exploitation, investigators should look for and report any unusual or unexplained new processes, services or daemons. When confirming the scope of the encryption, be sure to include the following during investigations: Shared or unshared drives or folders

- Network storage of any kind
- Cloud-based storage (DropBox, Google Drive, Microsoft OneDrive, AWS, etc.)
- External hard drives
- USB memory sticks with valuable files

Inventory the above and check them for signs of encryption. This is important for several reasons: First, you want to determine the scope and spread of the ransomware program. What did it encrypt? Second, in the case of cloud storage solutions such as DropBox, Microsoft OneDrive, or Google Drive, you may be able to easily revert to recent, unencrypted versions of your files. Third, 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 at all. 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. All 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, and the hacker knows which key(s) to send. Often this tracking list will be registry entries or a tracking file(s). Since every strain of ransomware is different, it is recommended to do a bit of Internet research to determine the version of ransomware you have been hit with and do your investigations 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 (if possible). This can often be learned from the ransomware program's announcement itself, as it

boasts 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.

Note: With that said, if a ransomware group is claiming they have exfiltrated data and/or credentials, ask for "proof of life," which means proof that the hackers actually have your files or credentials. Most will readily offer samples. In some rare cases, the files they've stolen may not have been that important. Getting a good idea of what has and hasn't been stolen is important to future recovery decisions.

Do a full forensic analysis of every involved device, or at least a very good sampling of involved devices (if many devices are involved). You want to determine what malicious activities and processes are involved. Ransomware groups often install many more malicious programs and scripts beyond the initial ransomware exploitation. Only by doing serious, detailed, forensic analysis can you begin to get a decent understanding of the full extent of what has happened. Let someone trained in forensic analysis do this part of the investigation. You want to disturb the involved devices as little as possible. This means using dedicated forensic analysis tools for making copies of storage devices and memory from impacted devices; and then having the knowledge to determine what is or is not malicious.

Try To Determine the Strain/Version of Ransomware

It is important to know exactly which ransomware program 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 dealing with will provide you with more information on 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. Some strains of ransomware are known to be buggy, and paying the ransom usually does not result in reliable decryption. Other ransomware gangs are known to be otherwise reputable and competent to deal with. Knowing the ransomware program and version can only help the recovery process.

There is a small chance that your particular strain has had a decryption tool or publicly released decryption keys that will allow you to decrypt your files without having to pay the ransom, but don't count on it. Finally, in the case that you are one of the very first people to be hit with a new version of ransomware, the information you provide can help the experts helping to recover your environment and help future victims of the same ransomware strain.

The result of this step is to determine what is impacted and how. What has been exploited and how badly? Are only particular types of devices involved (e.g., only Microsoft Windows), is the ransomware event only occurring in a single location or multiple, and what is not impacted? Many times, what is not impacted is as important as what is impacted in determining the scope of damage and how to respond. Can you determine if any data or credentials have been exfiltrated? Can you determine the initial cause of root exploitation?

Are the data backups still safe and reliable? Many ransomware victims refuse to initially negotiate with the ransomware group mistakenly believing their backups will "save" them. In many cases,

the ransomware attackers were able to erase or corrupt what the victims thought were safe and reliable backups. It can be embarrassing to the recovery team at all levels to be told one thing only to have to reverse your understanding at a later date. Do not make this mistake. Have someone who is in charge of backups test and confirm that all involved backups are safe and reliable, before reporting the status of data backups to the incident response group. Assume backups are compromised and unreliable until proven otherwise. If backups are safe and reliable, what is the estimate of how long it will take to reliably restore all impacted devices and services from those backups? Many victimized organizations have realized that it would take hundreds to over a thousand years to restore impacted data and services, even if they had safe and reliable backups.

Remember with most ransomware performing data and credential exfiltration, oftentimes, a data backup will not be enough to remove all risk.

You want to gather as much information as possible in this stage.

5 | Limit Initial Damage

If there is any way to limit initial damage, investigators should do so (keeping in mind any requirements of needed evidence preservation). Disabling the network and unplugging any directly connected storage devices is one way of doing so. Powering off any devices still actively encrypting more files may be another, although most victims refrain from powering off actively encrypting devices unless it is needed to save the unencrypted/uncorrupted data.

Change Any Compromised Passwords
Another way to limit damage is to change all possibly compromised passwords on any services to which the attacker has current access. Many services run on Internet-based systems that cannot be disabled. For example, any public, cloud-based service. Any victim should assume that all stored and used passwords from the time of the ransomware program's initial exploitation up until this current point have been compromised. Compromised credentials can include any login credentials used on the involved devices and network, including organizational passwords, employee passwords, and any customer passwords, if a customer portal was accessible from the compromised environment. An inventory of all possible compromised passwords should be made and then a fast group effort coordinated to change them all as soon as possible. Normally, this takes coordination and planning with a future "password reset day" established. Every second the passwords are not changed increases risk of future damage.

For any passwords used on the directly compromised devices and network(s) that are currently disabled and protected from further damage by the disconnected network, any password resets can wait until all involved devices and services are recovered. All potentially impacted passwords should be changed before allowing access by the involved hacker group to the service(s) involved (i.e., turning back on the network access).

6 | Gather Team to Share Information

Now is the time to gather the team, using the previously agreed upon alternative communications method or using a known safe physical meeting space to discuss what was learned about the scope of impact from the ransomware event. What was and was not impacted? What has been encrypted? Was data and credentials exfiltrated? How did the ransomware program first make it into the environment?

NOTE: Some victim organizations made the mistake of using meeting areas with compromised video or telephone systems, which then allowed the attackers to listen in on their recovery plans.

This is often the time that any externally invited parties may be involved with the larger group. Senior management, legal and any marketing/PR resources (if any) should advise attendees on what information can be shared outside the group. Staff should be reminded not to share any unallowed information and to stay within the predefined incident response plan. It is not unusual for internal personnel to reach out to external parties without prior authorization in the belief that this additional, unapproved, communications will be tolerated and even celebrated. Ask any participants if they have communicated to anyone outside the group about the involved event, and if so (it is fairly common, even if participants have been told not to), what did they say to whom?

The goal of this step is to ensure that everything that can be learned so far has been shared, that everyone has the same understanding of impact and scope, and that everyone recognizes what the next steps are likely to be. Each team member should be encouraged to speak out and disagree with any others if they think incorrect or incomplete information is being presented. It is not uncommon for different people in the incident response team to have different understandings or a sole team member ending up having better information than the larger group.

This is also the time for senior management and/or legal to decide on whether to notify other external parties, such as industry regulatory groups, law enforcement and in the United States, the Cybersecurity Infrastructure Security Agency or CISA. CISA is the United States' highest national agency for coordinating cybersecurity defense and recovery. Many nations have similar cybersecurity bodies. In the United States, CISA recommends all ransomware victims contact CISA, the FBI, or Secret Service (if the scope applies) for disclosure and help with the ransomware event. Doing so can result in useful information, advice and additional legal protections. This is likely also the point where your insurance company should be contacted, if you have an insurance company that covers cybersecurity incidents such as this. The decision to reach out to any external party should be made by senior management and the legal team and done so solely by the legal team.

7 | Decide on Initial Response

Once the initial information and scope of the attack are known, you have two basic options which will drive the rest of the ransomware response. This is true whether an encryption event has occurred or if data was still stolen and being leveraged against the organization:

- Pay the ransom
- Do not pay the ransom

Always let senior management and legal make the decision of whether to pay the ransom. If your organization decides not to pay the ransom, you can proceed immediately to the recovery portion of the response.

If you decide to pay the ransom, know that there should be no shame or guilt. Ransomware gangs make it difficult as possible not to pay the ransom. It is estimated that about 40% of ransomware victims pay the ransom, and that figure is falling over time as more victims better prepare for ransomware attacks. Many victim organizations pay because it is the quickest and least costly way to get back to normal business operations or to prevent exfiltrated data and credentials from being further exploited. Many victims find out their backups are not as safe, secure, or as effective as they first believed.

If an insurance company is involved in the event and allowed to make the decision, they most often agree to pay the ransom in a bid to reduce overall downtime and cost.

If you have decided to pay the ransom, you will likely need to decide on who will be the ransom negotiator (an internal or external person), how much the organization is willing to pay (if not the whole requested amount) and determine on how to access the cryptocurrency likely needed for the payment (more on this below).

If you (or the insurance company) decide to pay the ransom, you do not want to pay the whole amount of the extortion request. It is common for ransomware groups to ask for higher than expected inflated amounts initially that will later be negotiated down to smaller amounts. It is not unusual for ransomware groups to take half of what was originally asked for. It is also not uncommon for ransomware groups to ask for more money if they think they have been disrespected in any way.

Either way, never pay the ransom (whatever the final agreed upon amount is) without first getting proof from the attacker that their decryption program or keys will decrypt the data in a way that is useful to the organization. Sometimes, the ransomware group is lying about the decryption process or their process simply does not work as well as they claimed simply because ransomware is not a very tested type of program.

Can It Be Illegal To Pay the Ransom?

Yes. If the victim decides that paying the ransom is the best way to proceed, then they first need to make sure that doing so is not illegal, especially in the U.S. In the U.S., on October 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) released a memo specifically addressing the threat of potential legal issues for people and organizations who pay ransomware ransoms and their helpers. And, yes, there are past and active ransomware groups that are illegal to pay (at least from companies required to follow U.S. laws).

Ransomware developers/spreaders on the OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) include: Evgeniy Mikhailovich Bogachev, the developer of Cryptolocker, an early ransomware program, two Iranians for providing material support to a malicious cyber activity and identified two digital currency addresses used to funnel SamSam ransomware proceeds, the North Korean Lazarus Group, behind the WannaCry ransomware, and two ransomware subgroups, Bluenoroff and Andariel. Paying ransom to someone on the OFAC list can result in civil fines and penalties even if the victim did not know the ransomware group was on the OFAC do not pay list.

To minimize your legal risk, if paying the ransom, always consult a lawyer familiar with the involved legal issues first. You can consult with a service that can follow the money and let you know if the ransomware group you are dealing with is on the OFAC's block list. These cryptocurrency tracking companies include Chainalysis and Elliptic. There are even services which can help you make the official determination of whether it is legal to pay the ransom. It never hurts to get CISA, the FBI, or the relevant jurisdictional law enforcement involved to assist. But even then, let your lawyer make the final recommendation.

8 | Recovery: Repair or Rebuild?

Whether or not you pay the ransom, you will have to decide whether you will REPAIR or REBUILD the impacted systems and information. Even if there was not a mass encryption event, it is important to consider rebuilding or repairing systems that may have been compromised.

REPAIR Only

Many victims, with monetary, resource or time constraints considered, can only do the bare minimum to get involved devices and services back up and running as soon as possible. They do their best to remove all malware and malicious modifications, change all involved passwords, restore impacted systems to a working state (often by decrypting encrypted files) and then get back up and operating as fast as possible.

This usually allows the quickest and cheapest type of recovery, but it increases the risk that something malicious was missed that could allow the attackers (or other future attackers) back in more easily.

REBUILD Everything

The safest (and usually most expensive) option is usually a complete rebuilding (and/or replacement) of every device and service in the network, rebuilding all things from the ground up, using brand new login credentials and ensuring that any old vulnerabilities are no longer present. Oftentimes, ransomware victims will use the downtime opportunity to rebuild infrastructures without the encumbrance of any past weaknesses or errors that may have been present. Many victims add new software programs, updated versions of existing programs, new computer security defense programs, and MFA (if it was not used before). Some victims' rebuilt infrastructure looks completely different to the old, exploited infrastructure.

Preserving Evidence

Many victims, because of legal considerations, must preserve all possible evidence of the ransomware attack. To do so, all actions, repair or rebuild, are done on other devices (at least initially). The victim may even do complete backups of current impacted systems, restore them to other similar devices, and then do the repair or recovery from the new devices (leaving the older devices unimpacted for the time being). Other victims will make forensic copies (memory

and storage areas) and then start doing recovery on the existing impacted devices. Let senior management and legal decide on whether repair or rebuild is right for you and if evidence preservation is a concern.

With either overall guiding choice, repair or rebuild, you will likely have a ton of work to do to recover your environment and ensure that you can safely work going forward. If you do not already have one, do a business impact analysis (BIA) and decide what services should be restored in what order to maximize recovery and decrease overall damage. With both options, it is likely that you will have one or more external third parties helping with the recovery process.

Rebuilding Supporting Infrastructure

In most cases, after identifying which applications and services need to be restored first, all the underlying supporting infrastructure (e.g., IP Address Management, DHCP, DNS, Active Directory, security services and tools) must be restored to a known clean state first. Most applications rely on a known clean supporting infrastructure as the baseline of what is needed before restoring specific applications. Some applications may be located on external clouds or other unimpacted infrastructures and easy to put back online. Others may require days to weeks of work on the supporting infrastructure before the application can be put back in place.

There is also the hybrid option where the victim starts out repairing some systems only to learn that some systems and services cannot be repaired and must be rebuilt; and vice-versa. Just remember that repairing is usually quicker and cheaper, but higher risk for future attacks; and rebuilding is the opposite. Choose the right option for your organization.

Back Up Your Encrypted Files (Optional)

In most cases, you will want to back up encrypted files. If you pay the ransom and the ransomware group sends you a program or decryption key(s), you do not want your first restoration test to be on the only copy of the encrypted files. This is because the first restoration often does not work and sometimes even corrupts the files, preventing further decryption when the problem is figured out. No serious ransomware recovery person recovers the impacted files directly. They back up the encrypted files every time and recover the secondary copy of the encrypted files.

Even if you are deciding not to pay the ransom you may want to back up your encrypted files.

Yes, that's right. The reasoning is that occasionally the involved encryption keys may be discovered or released at a future date. There have been many cases where the ransomware developer—in a flash of conscience or fear—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.

Negotiate and/or Pay the Ransom

The most commonly asked question with regard to the ransom payment is, "Will these criminals actually help decrypt my files if I pay?" The answer here is a bit complex. The short answer is yes, most of the time they will almost always provide you with a way to decrypt your files (although it depends on the ransomware group). There is a moral dilemma here, after all, the hackers 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 reliably, the hackers will lose all credibility and a quick search by other future victims would reveal that it would be fruitless to pay. 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.

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.

Locate the Payment Method 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.

Obtaining Bitcoin

The first step is to set up an account with what is called a Bitcoin exchange, which will allow you to purchase bitcoin. This would be simple on any other day, however you may very well be under a strict timeline to pay the ransom, which 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. KnowBe4 has an account at www.CoinBase.com.

- See our Ransomware Knowledge base for more about getting Bitcoin

NOTE: If the cryptocurrency involved is not Bitcoin, replace the word Bitcoin with whatever cryptocurrency you are dealing with.

Once you've created an account, you will 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 four 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 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.

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.

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/rqla7yulv7filqlrycpqrkrl.onion

Paying the Ransom

Once you have Bitcoin in your Bitcoin wallet and proof the decryption process works, it's time to transfer the requested Bitcoin amount 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 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.

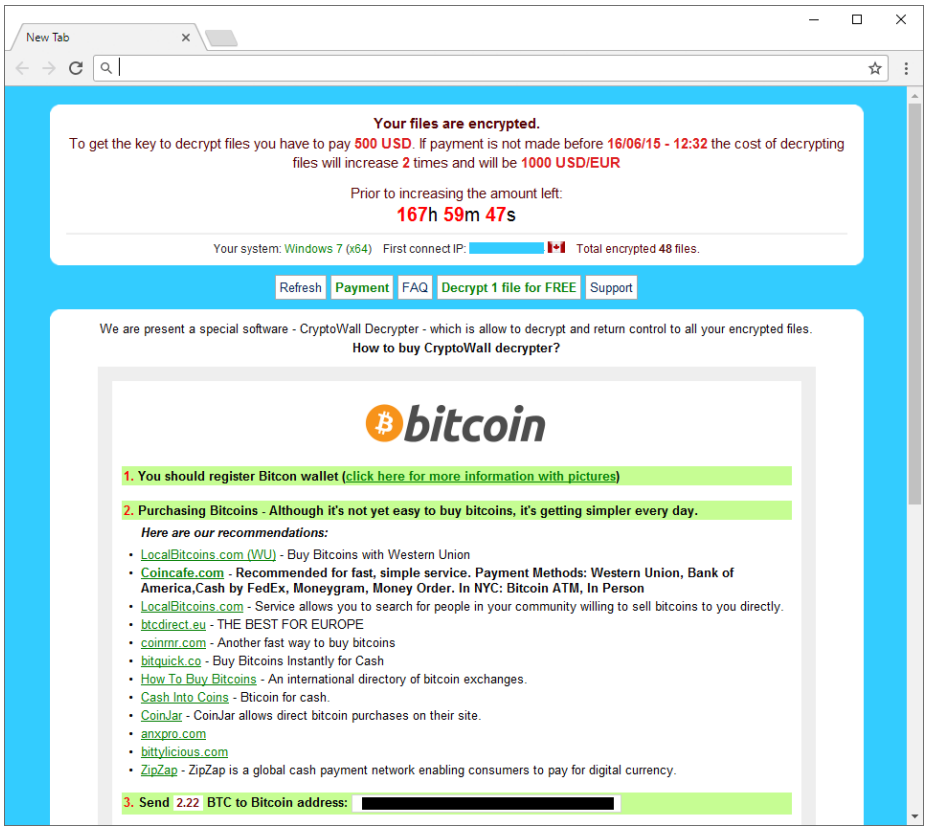
Example of a Bitcoin wallet string:
19eXu88pqN30ejLxfei4S1alqbr23pP4bd

Note: Don't visit any ransomware web site until absolutely necessary. Oftentimes the first visit starts the countdown timer. By avoiding setting off the timer, a victim can have more time to deal with the ransomware event.

Once you have 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.

An example of the CryptoWall ransomware payment screen.



Decrypting Your Files

Once you've paid the Bitcoin to the hackers, you will probably have to wait (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 file with the key or keys that can be used to start 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.

Most ransomware victims, even when paying the ransom and getting the decryption keys or program, end up with files that do not recover back to their pre-encrypted state. Even if they do get completely decrypted, oftentimes they cannot be used in their original form because the other decrypted files were encrypted at different times and are not in a synchronized state. Expect any recovery process to be full of successes and failures. It is the rare victim that gets back every file and their systems work as they did prior to the ransomware encryption without lots of additional work. Still, most victims that do decrypt their files have less work to do than victims without a backup who did not

pay the ransom. Of course, victims with great backups often have the best recoveries (if they can restore the files in a timely manner).

9 | Next Steps: Prevention of Future Cybercriminal Events

Regardless of whether you have 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. This step is vital. If you are going to take a hit on your files, at least learn from any mistakes that were made. It is 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 the following steps as the bare minimum:

- 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.
- Install and maintain high-quality antivirus or endpoint detection and response software, as a layer you want to have in place, but do not rely on it—they always run behind.
- Patch all critical patches within two weeks of the vendor releasing the patch.
- Use strong, (phishing-resistant), multi-factor authentication (MFA) where you can and strong, unique passwords which are not shared across any two websites or services.
- Configure high-quality backup/restore software and test the restore function regularly!

Defense in Depth

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 is 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 use “social engineering” to entice or trick a user into installing or opening a security hole. KnowBe4 security awareness training and simulated phishing 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 Phishing Attacks

While training can have a big impact on hardening the first layer of security, it is the two-pronged approach 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 mistakes—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 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.

To summarize, if you do an incredible job at just four things, you will be at a far less likely risk for any cybercriminal exploit, including ransomware attacks. These four mitigations are:

- Mitigate social engineering, including using security awareness training and simulated phishing attacks
- Patch your software
- Use (phishing-resistant) MFA where you can
- Use strong and unique passwords where you cannot use MFA

There are many other mitigations that should be deployed by every computer and network defender. But it is the inability of most defenders to more strongly focus on these critical four mitigations well enough that allows most hackers, malware and ransomware to successfully exploit their devices and environments.

Hopefully this document has provided you with a summarized series of steps to include in your ransomware response plan. We hope you and your organization are never successfully exploited by ransomware, but if you are, this manual can tell you how to proceed, recover, and prevent in the future.

KnowBe4

Ransomware Attack Response Checklist

STEP 1: Initial Investigation

- [ ] a. Determine if it is a real ransomware attack
- [ ] b. Determine if more than one device is exploited

If so, continue:

STEP 2: Declare Ransomware Event and Start Incident Response

- [ ] a. Declare ransomware event
- [ ] b. Begin using predefined, alternate communications
- [ ] c. Notify team members, senior management and legal

STEP 3: Disconnect Network

- [ ] a. Disable networking (from network devices, if possible)
- [ ] b. Power off devices if wiperware is suspected

STEP 4: Determine the Scope of the Exploitation

Check the Following for Signs:

- [ ] a. Mapped or shared drives
- [ ] b. Cloud-based storage: DropBox, Google Drive, OneDrive, etc.
- [ ] 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. Mapped or shared folders from other computers

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 that 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

Determine Ransomware Strain

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

STEP 5: Limit Initial Damage

- [ ] a. Initial investigators should try to stop/reduce any damage they discover, if possible

STEP 6: Gather Team to Share Information

- [ ] a. The goal is to make sure the team correctly understands all information, including scope and extent of damage

STEP 7: Determine Response

- [ ] a. Pay the ransom or not?
- [ ] b. Repair or rebuild?
- [ ] c. Invite in additional external parties?
- [ ] d. Notify regulator bodies, law enforcement, CISA, FBI, etc.?

STEP 8: Recover Environment

- [ ] a. Repair only or rebuild
- [ ] b. Need to preserve evidence?
- [ ] c. Use business impact analysis to determine what devices and systems to recover and the associated timing
- [ ] d. Restore critical infrastructure first

Step 9: Next Steps

Prevent the Next Cyber Attack:

- [ ] a. Mitigate social engineering
- [ ] b. Patch software
- [ ] c. Use multifactor authentication (MFA) where you can
- [ ] d. Use strong, unique passwords
- [ ] e. Use antivirus or endpoint detection and response software
- [ ] f. Use anti-spam/anti-phishing software
- [ ] g. Use data leak prevention (DLP) software
- [ ] h. Have a good back up and regularly test

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 three or four months in the past. Bad actors lurk in your networks for months and can 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 cybercriminals 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.

About KnowBe4

KnowBe4 is the provider of 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 ongoing 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 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 smarter 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

01E01K01