RANSOMWARE

PROTECT YOURSELF. PROTECT YOUR EMPLOYEES. PROTECT YOUR COMPANY.

ALL IT TAKES IS ONE CLICK BY AN EMPLOYEE TO INFECT A WORK STATION, ALLOW HACKERS IN, AND CAUSE AN EXPENSIVE DATA BREACH ...

OR WORSE.

In recent years, cybercrime has changed drastically. While viruses and bugs are still popular, ransomware is now the most dangerous threat. Imagine a bank robber that discovers a way to get the bank to send all of their funds over the internet with no way to trace it back to the robber. This is how ransomware works. The criminals steal valuable information and data and stick them into a combination that only they know the combination to, then ransom off the combination. It is that simple. And it could ruin your company. It is time to be aware of the dangers out there and take the steps to protect yourself and your company. In this manual, we will discuss how to tell if you are infected with ransomware, what to do when you are infected, and how to protect yourself in the future. At the end, there is a checklist that will help your company in the event that you do become infected.

TABLE OF CONTENTS

About Alvaka

Alvaka Networks has enjoyed three decades working in partnership with our clients. Through our trusted partner position, we constantly strive to improve our practices and delivery methods. It is our unwavering commitment to constantly provide real value, and be there when our clients' need us.

"If you want to know how secure you are, just take a look around. Nothing's secure. Nothing's safe."

-Fred Durst

What is Ransomware?

Before we begin discussing the symptoms of Ransomware, let's first talk about what it is. There are many different versions of ransomware, but in basic terms it is a type of malware that prevents users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. The hackers use several different pathways to infect a machine such as websites, unpatched programs, free software downloads, phishing emails, and online advertising.

The scary part is that it only takes one infected machine to take down an entire company. The ransomware is smart enough to travel across all shared network drives to encrypt all files connected to the infected machine. It only takes one end user to bring an entire company to a halt. Want to know another scary fact? Ransomware can have sleeper versions of the malware. These versions are programed to hide within your machine until weeks after the infection, making it even harder to detect the machine that was originally infected or where the infection came from.

After the files have been encrypted, a message will display explaining how to pay a fee to decrypt the files. Ransoms can start as low as $100, but oftentimes they increase over time and can become thousands of dollars. With current trends, it is expected that future ransoms may demand millions of dollars. Generally, the ransom is paid in a form of e-currency such as Bitcoin. Once payment is verified, the encryption is unlocked and process of decrypting can begin.

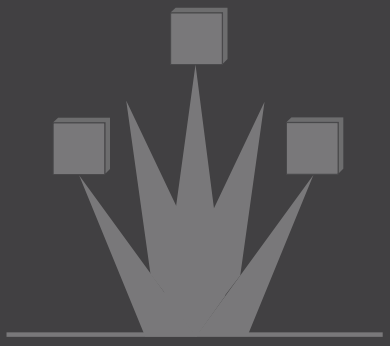
Know the Facts:

- Ransomware can infect more than just a PC. Versions have been created to infect iOS, Mac OS X, and Android.
- Ransomware commonly attempts to scare victims by displaying as a warning message from the government or law enforcement.
- An estimated 68,000 computers are infected with ransomware each month. That's 5,700 every day.
- In that same month, only 2.9% of victims paid the ransom. Yet the hackers still profited roughly $34,000 per day.
- An estimated $5 million is being paid to ransomware creators each year.
- There is no way to completely prevent Ransomware from attacking your company, but you can protect yourself by following the steps in this manual.

What are Bitcoins?

It is also important that you understand what Bitcoins are in case you ever have to use them. Bitcoins, commonly abbreviated as BTC, are a type of cryptocurrency. This simply means that they do not have a physical representation. They are completely untraceable and can be sent anywhere via the internet with total anonymity. Users can complete Bitcoin transactions directly without needing an intermediary.

Despite the fact that it is the ideal form of payment for hackers, using or owning Bitcoin is not against the law. Bitcoins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into the public ledger. This activity is called mining and the miners are rewarded with transaction fees and newly created bitcoins. Besides mining, bitcoins can be obtained in exchange for different currencies products, and services. Users can send and receive bitcoins for an optional transaction fee.



“Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business”

-Kevin Mitnick, Famous Hacker

How to Know you are Infected

Infection Pathways

Before we go over the symptoms of an infection, let’s first discuss the many ways that an infection can occur. In order for ransomware to make its way onto a machine, a user must download or run some sort of file. These files are usually hidden within several different pathways, so it is important that users know what not to click on.

Emails

Email is the most common pathway for ransom downloads. The ransomware is usually disguised as an attachment to the email, and if the user opens or installs the attachment it can lead directly to an infection. Another option is for the ransomware to be hidden in a button or a link in the body of the email. When clicked, this could take you to a dangerous website and lead to an infection. It is extremely important that end users verify the authenticity of any file before they open it. This can be done in several different ways:

- The most obvious question is: were you expecting the email? If it is something that you weren’t prepared to receive then you should probably be a little cautious.

- Check the sender. Is it someone that you do not know or have no connection to? If yes, then you probably shouldn’t open it.

- If there is an attachment, hover over it with your mouse without clicking. Look at the information that pops up. What is the size of the file? What kind of file is it? Do the same for any links or buttons in the body of the email. Hover over it without clicking to see the name of the website that you would be directed to if you clicked. Is it something strange that you have never seen before? If it sounds dangerous, then it probably is.

- One of the best solutions is to install a link integrity checker. These tools will help validate if a site is dangerous. This takes the discretion away from your users.

- If you aren’t 100% sure about either opening or deleting the email, contact Alvaka so that we can help you out.

Free Software

How often do you see free software downloads on the internet? It is very popular for hackers to hide ransomware within “cracked” versions of different software such as games, adult content, screensavers, online game cheats, and many more. When used in this way, the ransomware can sneak past firewalls and antivirus programs because the user is directly downloading it.

Website Downloads

Remember when we mentioned that emails can have links to dangerous websites? It is at these sites that drive-by-downloads can occur. When a user visits a site with a compromised or an old browser, a third party application can infect the machine. Once a hacker discovers a bug in a piece of software, it can easily be exploited to allow the execution of malicious code. This is why it is so important to download patches and updates for your software. When these "bugs" are discovered, the software vendor can quickly patch them and release an update. However, if you do not download the update, there is nothing protecting your machine from an infection.

Symptoms of an Infection

It is pretty easy to determine if you are infected with ransomware. When you try to open normal files, you will get an error message that claims the file is corrupted. Next, a message will be set to your desktop background with instructions on how to unlock your files. It is important to note that the program gives you a time limit before the ransom is increased or you can no longer unlock your files. Another symptom of an infection is when a ransomware window has been opened and you cannot close it. If you notice that you suddenly have files with names such as HOW TO DECRYPT FILES.TXT, then there is a high chance that your machine has been infected.

Ransomware screen from the infamous Cryptolocker

Ransomware | Fake law enforcement message from Great Britain

Ransomware encryption message

Ransomware | Fake FBI message

What to do when an Infection Occurs

In order to become infected by a strain of ransomware, a user will have to have at least downloaded and run some sort of file.

Disconnect
The first step is to disconnect the infected computer from any network it is on. Make sure that you turn off any Wi-Fi or Bluetooth on the machine. All storage devices like USBs and external hard drives need to be unplugged. Most importantly, do not erase ANY files.

Contact Alvaka
Contact Alvaka and let us know of the infection. It is crucial that this is done immediately after unplugging the machine. We need to be able to respond as quickly as possible to minimize the damage. The rest of the steps will be done with Alvaka's help.

Determine the Damage
Next, we need to determine how bad the damage is. How much of your infrastructure is encrypted? Ask yourself a couple of questions: Did the infected machine have access to shared drive or shared folders? Were there any external hard drives with valuable information attached to the machine? Was the infected machine connected to any cloud-based storage? The more access the infected machine had to your infrastructure, the higher the risk of damage.

Determine the Ransomware Variant
Next, we need to determine the strain of ransomware that infected the machine. All ransomware versions follow the same basic pattern, but there is always the off chance that your versions has had a decryption tool built by an antivirus company.

Determine your Action
Now it is time to determine what your next action will be. While Alvaka works on removing the actual malware from the infected computer, you will need to determine what you want to do about the encrypted files. You have a few options: restore from a backup, use a 3rd party decryptor, do nothing and lose your data, or pay the ransom. Once you choose the option you'd like to try, Alvaka will be with you each step of the way to help solve the problem.

Restore Your Files From a Backup

Restoring from a recent backup is the best solution to a ransomware infection. It is for this reason that it is so important that your company be making regular and redundant backups of vital data. If not, it is only a matter of time before an event like this will occur. If you are interested in starting a backup plan to protect your company in the future, Alvaka works with several companies that offer backup and storage solutions.

The first step is to determine the state that your backups are in. How recently did you last backup the vital documents? Where are these backups located? If they are on a physical backup media such as USB drives, we highly recommend that you manually verify the files from your backup. It is all too possible that these media have malfunction and your data is no longer recoverable. If your backups are stored in the cloud, depending on the size, they could take days to restore. For every minute that your business isn't functioning, you are taking a critical hit.

What if you don't have backups in place? There is still a slim chance that you may have inadvertently saved copies of your work that are recoverable. We just have to find them. Common places that you may find copies of your files are things like Gmail. If you have mailed an attachment to someone or uploaded a document to social media then it may be possible to recover it. What about shadow copies? Shadow copies are created when Windows creates a system restore point and takes snapshots of files. These snapshots can contain copies of files on your computer from that restore point.

Once you find and verify the files that you need, you can return your machines to the state they were in before the infection. Now, the ransomware can be removed from the infected computer. Alvaka will handle this by wiping and rebuilding the machine to ensure that there are no traces of any kind of malware left on the machine. Now that the ransomware infection has been resolved, it is crucial that you take the necessary steps to protect yourself and your company from a future attack. See the last section of this manual "Protecting Yourself in the Future" for more information.

Use a 3rd Party Decryptor

Because the number of ransomware attacks has grown in recent years, there is a chance that you could find a third party decryptor for the strain of ransomware infecting your machine. Please note that this is a slim possibility, but it is worth a shot. Because you should have already determined the version of ransomware, the next step is to locate a decryptor. You have to be extremely careful at this point and make sure that the decryptor is from a reliable antivirus source. Make sure you consult Alvaka to make sure that the decryptor is safe before using it. After finding a possible decryptor, there are two things that could happen: One – you're successful! Congratulations! Make sure you take the necessary precautions to prevent this from occurring again. Or two – failure. If the decryptor did not work, then it is time to look at some other options.

Do Nothing and Lose your Data

It may also be an option to take the hit and not attempt to recover the files that are encrypted. This is generally a solution when the impact would be small. If this is the path you choose to take, there are still a few steps to ensure everything goes smoothly. First, let Alvaka remove the ransomware from the infected machine. Next, backup your encrypted files. This may sound crazy, but there is always a chance that certain encryption keys could be uncovered by security experts. Even if this is several months after the attack, you might get lucky and be able to decrypt your files. Lastly, take the precautions necessary to prevent an attack from happening in the future.

Pay the Ransom

In some cases, paying the ransom may be the only solution. A lot of experts recommend that paying the hacker should be avoided at all costs, however in some cases there will be no other choice. It is important to remember that there is always a chance that your files will still be left encrypted even after payment. Hackers are not the most honest bunch, and they probably wouldn't lose much sleep at night knowing that they took your money and ran. If you still have no other choice, we will attempt to walk you through the complicated process of handling online payment.

Step 1: Locate the Payment Method Instructions

This step is usually pretty easy because most ransomware programs will display the payment methods in very clear instructions. Oftentimes there is a link to instructions on the ransomware screen. If you still do not see any instructions, looks for a file called something like INSTRUCTIONS TO DECRYPT.TXT.

Step 2: Obtaining Cryptocurrency

In most cases, you will use Bitcoin when making your payment. We briefly explained Bitcoin in the beginning of this manual. The first thing that you will need to do is set up an account with a Bitcoin exchange. Remember that you are most likely under a strict time limit, so you need to find an exchange where you can get Bitcoin fast. One option is http://www.localBitcoins.com which allows you to connect with a local seller and filter by payment types. Once you have created an account, you will be given a wallet address. You will need to give this address to the person you buy Bitcoin from. You will probably want to purchase slightly more Bitcoin than you need to account for any transaction fees.

Step 3: Install a TOR Browser

In most cases, you will need to use a TOR browser to make your payment. TOR is an anonymity network that was developed to anonymize and hide the originating and ending destination of internet traffic. Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored. However, hackers use the TOR network because they cannot be easily tracked by law enforcement. They can interact with their victims without fear of discovery. The name is an acronym derived from the original software project name The Onion Router.

To download the TOR browser, go to http://www.torproject.org and click the download button. Once you open the browser, it will look very similar to any other browser. The website address that you will need to navigate to is likely to be located in the decrypt instructions. The address will look something like: ksj4parff6k.onion/Ibda

Step 4: Pay the Ransom
By this step, you should now have Bitcoin in your wallet, a TOR browser installed on your machine, and a website address to navigate to. You will also need to make sure that you have the hackers Bitcoin wallet address that you will use when you transfer the Bitcoin. The wallet address looks like a long list of numbers and letters. A wallet address may look something like: 76jDh92vnS23quDney8S2apjh66bB4rt

After you make the Bitcoin transfer, you will usually receive a transaction hash which is another series of numbers and letters.

Step 5: Decrypt the Files
This is the step that you cross your fingers and pray that it works. After you've paid the hacker, you will probably have to wait a good deal of time before they give you access to the key that starts decrypting your files. Before you begin decryption, make sure that any external or network storage drives with encrypted files are connected to the machine so that they can be decrypted as well.

> **"U.S. computer networks and databases are under daily cyber attack by nation states, international crime organizations, subnational groups, and individual hackers"**
>
> -John O. Brennan, Director of CIA

Protecting Yourself in the Future

Whether you've been infected by ransomware or not, protection is vital to ensure security for yourself and your company. Make sure that your employees are educated about the dangers of ransomware. End users are the most common targets for hackers, and it is very important that your employees know how to protect themselves. Also make sure that you have software-based protection such as antivirus, antiphishing, antispam, firewalls, link reputation checking, and content filtering. These programs will help prevent the suspicious emails and websites from even making it to your end users. Lastly, make sure that you are running regular backups of your files. There are hundreds of on-site and cloud-based backup options, so there is no excuse not to have a backup in place.

Ransomware Infection and Prevention Checklist

Step 1: Disconnect Everything

- [ ] Unplug computer from network
- [ ] Disconnect any USB drives or external storage devices
- [ ] Turn off Wi-Fi and Bluetooth

Step 2: Contact your IT Provider

- [ ] Contact Alvaka immediately to let them know about the attack (949.428.5000)

Step 3: Determine the Damage

- [ ] What network drives was the computer connected to?
- [ ] Was there any external hard drives with valuable information attached?
- [ ] Was there cloud-based or network-based storage?

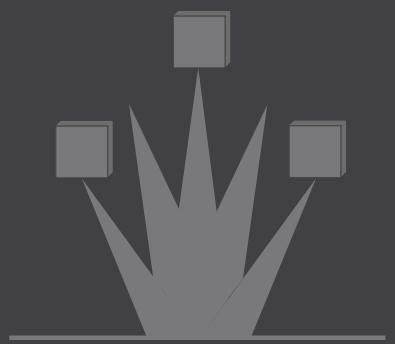
Step 4: Determine Ransomware Version

- [ ] What version of ransomware is it?

Step 5: What Action will you take?

Restore from Backup

- [ ] Locate your backup
- [ ] Remove the ransomware from your machine
- [ ] Restore from backups
- [ ] Determine where the infection came from and handle



Ransomware Infection and Prevention Checklist

Use a 3rd Party Decryptor

- [ ] Determine the version of the ransomware
- [ ] Find a decryptor
- [ ] (if successful) Attach any media that contains encrypted files
- [ ] Decrypt the files
- [ ] Determine where the infection came from and handle

Do Nothing and Lose Data

- [ ] Remove the ransomware (Alvaka)
- [ ] Backup your encrypted files for possible future decryption
- [ ] Determine where the infection came from and handle

Pay the Ransom

- [ ] Determine the payment amount and method
- [ ] Obtain the Payment
- [ ] Reconnect machine to the internet
- [ ] Install TOR browser
- [ ] Navigate to payment address and make payment
- [ ] Ensure all encrypted files are connected to machine
- [ ] Determine where the infection came from and handle

Step 6: Protecting Yourself in the Future

- [ ] Educate your Employees
- [ ] Implement Software-based protection
- [ ] Backup important data

PROTECT YOURSELF AND PROTECT YOUR COMPANY

CALL ALVAKA TODAY
949-428-5000