“In 2015, security experts were predicting ransomware would be huge for cybercriminals in 2016. The majority had no idea it would be this huge.”

Greg Edwards
CEO, WatchPoint

Ransomware Rapid Response Kit

WatchPoint
COMPREHENSIVE CYBER SECURITY

CONTENTS

INTRODUCTION

Throughout history, people have gone to great lengths to steal money from others. For most of history, the act of stealing something from another was followed by serious consequences. Bank robbers, jewelry thieves, and pick-pocketers have gone to great lengths to steal money for a living, only to experience a life high in risk and low in reward. It's rare that a criminal pulls off a heist that nets enough money to retire on. Bonnie and Clyde knocked off a lot of banks when security was just a bank vault door. Eventually, the law caught them in a hail of bullets, and they didn't rob banks anymore. Modern cybercriminals have found a way to invert the traditional high risk, low reward model by using the latest technology and social engineering. The police, FBI, CIA, and even the US government are powerless in stopping today's cybercriminals who reside overseas and are out of US jurisdiction. Russia, China, North Korea, Iran, and India are safe havens for cybercriminals, and their respective governments do nothing to stop the attacks on foreign computer systems. Because of this, the cybercriminals have taken malware and monetized it to generate millions of dollars in an extremely short period of time. Cryptographic ransomware and banking Trojans are the weapons of choice for today's cybercriminals. Their payloads are launched in email and precision-guided to your employee's mailboxes where 45% of the time they are opened and launch the attack on your internal network. Within just a few minutes your valuable files are encrypted, and a ransom is delivered to your desktop.

This is where WatchPoint comes in. Before Greg Edwards founded WatchPoint, he started Axis Backup, a backup and disaster recovery company for the insurance industry. He saw firsthand the rapid increase in the damage cybercriminals were doing with debilitating malware, resulting in high financial loss to vulnerable companies. Between 2012 and 2015, one in five of Axis Backup's clients was hit by cybercrime. Greg realized effective cybersecurity could save businesses from costly downtime and compromised systems. In 2015, Axis Backup was acquired by J2 Global, freeing Greg to create WatchPoint and focus exclusively on cybersecurity.

"Cyber crime costs projected to reach $2 trillion by 2019 up from $400 billion in 2015."

-Forbes Magazine

"Ransomware On Pace To Be A $1 Billion Business In 2016."

- *FBI*

"In 2015, security experts were predicting ransomware would be huge for cybercriminals in 2016. The majority had no idea it would be this huge."

- Greg Edwards, CEO, WatchPoint.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that denies access to a device or files until a ransom is paid, at which point the cybercriminals will provide a decryption key to allow the user to regain access to their system or files. The main attack vectors used to infect a computer include phishing emails, compromised websites, online advertisements and free downloads.

Ransomware typically starts at a user workstation and spreads to your critical network servers by infecting network shares. Because ransomware can encrypt thousands of files per second, it can easily destroy important files for entire departments. For small businesses with relatively few servers and few shared folders, ransomware can quickly devastate an organization's data to a point where systems crash and productivity comes to a halt.

Debilitating your network was once the end goal of hackers. Today cybercrime syndicates from across the globe and most notably Russia and China have discovered how ransomware allows them to monetize their attacks. Cybercriminals of the 21st century make millions in short order by sending bogus emails to American businesses, spoofing fax reports, invoices, utility bills, and malicious URLs that entice the employees into opening and launching an attack against their own organization. Ransoms typically start at $250 but can quickly increase to $1000 or more if you attempt to restart your computer or wait too long to pay.

There are some options that you have when you are hit with ransomware that we will discuss later, including restoring data from backup, paying the ransom and purchasing a decryption key, or doing nothing. All of these options come with consequences that typically manifest in lost employee productivity, inability to service customers during downtime, and a mark against the business' reputation.

In the first three months of 2016, businesses and individuals paid $213 million in ransomware payoffs, according to the FBI. The total paid is expected to eclipse $1,000,000,000 in 2016. That's billion with a B. Cyber criminals are targeting businesses of all sizes and even individual's personal computers.

Now isn't the time to panic. Now is the time to boost your defenses and set the traps to stop cybercriminals in their tracks.

WHAT IS BITCOIN?

Bitcoin is an innovative payment network and a new kind of money.

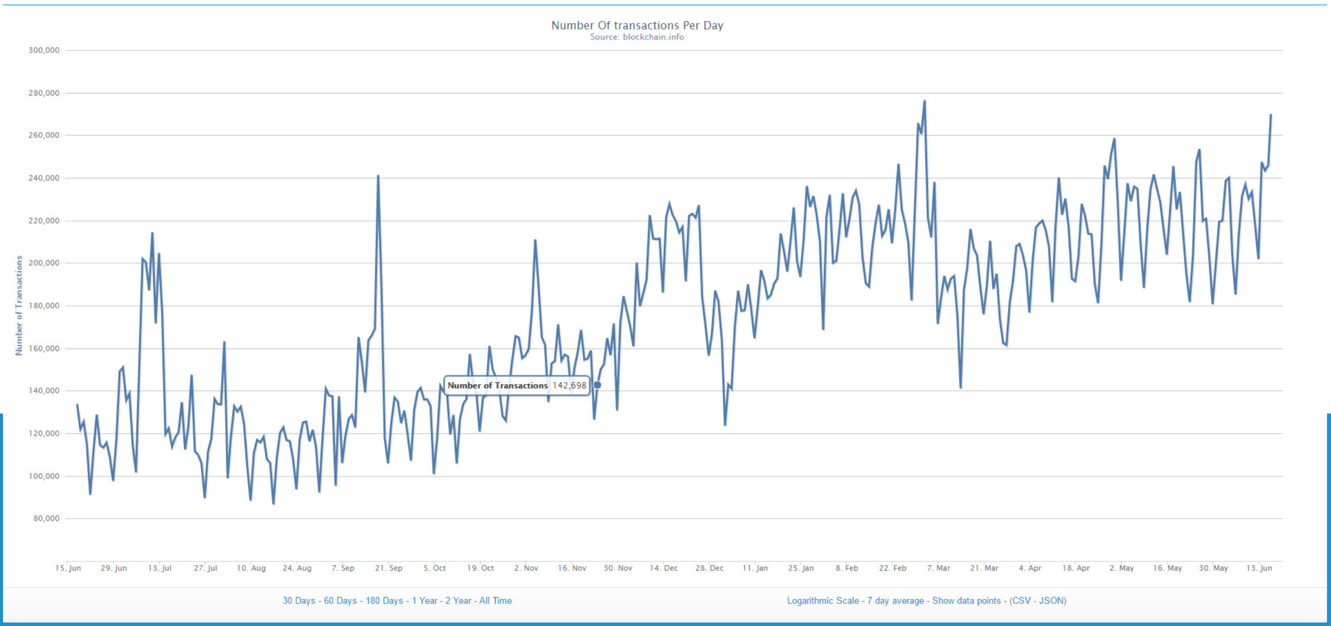
“Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.” - Bitcoin.org

Bitcoins are a form of cryptocurrency. It’s a digital currency that has no physical representation. Encryption techniques are used to regulate the generation of bitcoin units and verify the transfer of funds, operating independently of a central bank. These decentralized cryptocurrencies provide an avenue to personal wealth that is beyond regulation and confiscation.

Bitcoins are stored in anonymous digital wallets which can be transferred anywhere across the globe through the World Wide Web. Anyone can send payments to anywhere in the world with complete anonymity. The anonymous nature of cryptocurrency makes it an ideal payment system for cybercriminals. However it is a legitimate payment system used by legitimate businesses and individuals all over the world for non-criminal means. Ransomware has given Bitcoin cryptocurrency a bit of a bad reputation because many people are only finding out about Bitcoins as they are hit with ransomware.

Bitcoin fast facts:

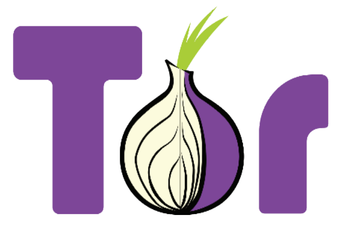
- • Bitcoins are abbreviated to BTC and are untraceable.
- • The price of a Bitcoin fluctuates like a commodity. Currently, one BTC is worth approximately $739.
- • Only 21 Million Bitcoins will be allowed in circulation.



Growth in Bitcoin transactions from June 2015 to June 2016 – blockchain.info

TOR – ANONYMITY ONLINE

The Onion Router



TOR stands for:

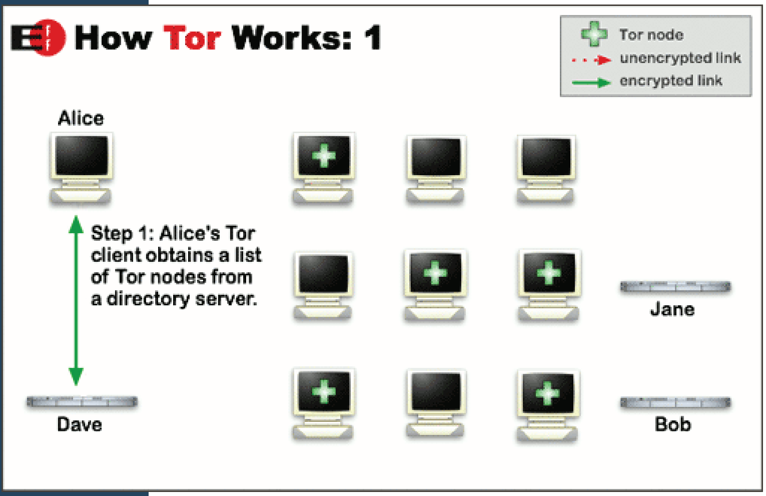
“The Onion Router” which was derived from an acronym for the original software project name.

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor is free software and an open network that helps defend against traffic analysis - a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships and state security.

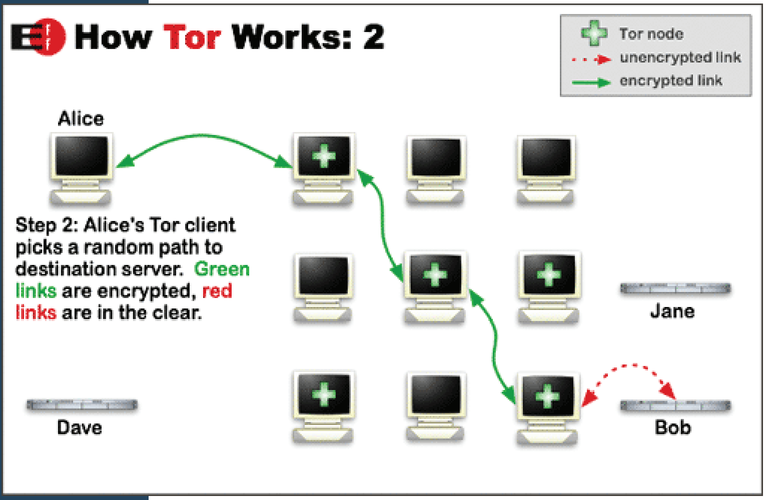
Initially released in September 2002, Tor has been nicknamed the anonymous internet due to the ability to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis.

Tor uses a special Tor browser that is configured to relay traffic through the worldwide volunteer networks. The traffic is encrypted, and the network was designed to anonymize and hide the original and end destination of the data transfer.

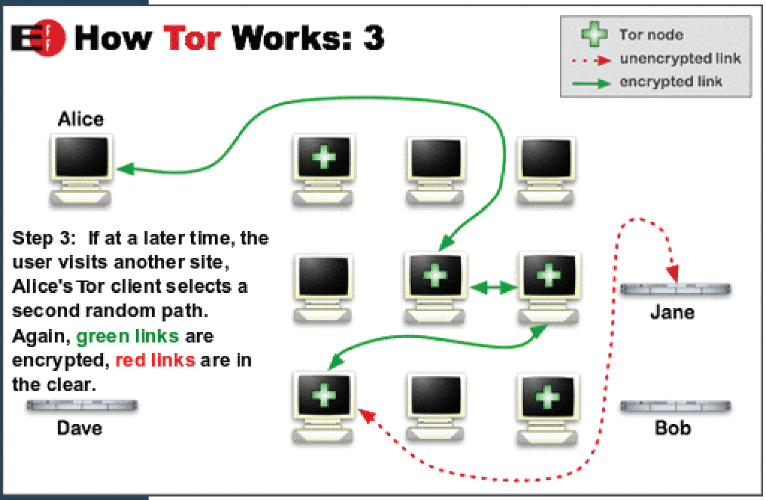
Many organizations including businesses, the media, law enforcement and political activists use the Tor network to ensure their communications are confidential and protected. Cybercriminals have also gravitated to the Tor network to anonymize their traffic, to communicate with others and host websites that cannot easily be tracked by law enforcement or government entities. Cybercriminals use the Tor network extensively to collect ransomware payments from their victims without fear of their identities or location being discovered. Cybercriminals use the network to host command and control servers, ransomware payment systems, and exfiltration of stolen data from victims. Tor has the ability to run hidden services on the Tor network, which is also utilized for cybercrime.


How Tor Works: 1

Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.


How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.


How Tor Works: 3

Step 3: If at a later time, the user visits another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

HAVE I BEEN INFECTED WITH RANSOMWARE?

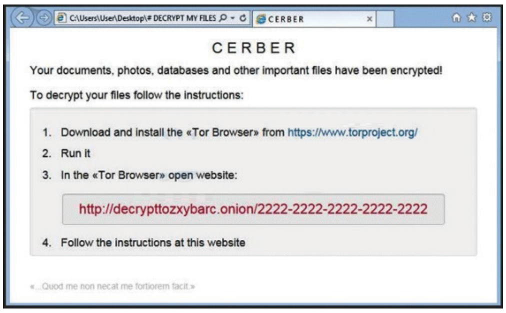
SYMPTOMS OF RANSOMWARE INFECTION

The symptoms of a ransomware infection are pretty straightforward. The cybercriminals want you to pay the ransom to decrypt your files, so they make it pretty obvious that your system has been compromised.

The following symptoms are clear indicators of a ransomware infection:

- All of a sudden you have issues opening files and receive errors that the file is corrupt or has the wrong file extension.
- Files with names like "Help_decrypt.pdf or HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS. HTML start to appear on your desktop and other directories.
- A new image has replaced your desktop that gives instructions to pay a ransom to decrypt your files.
- Your web browser pops up unexpectedly with a ransom demand to decrypt your files.
- A program opens to warn you that a countdown has been initiated and failure to pay within the time limit will increase the ransom demand.
- A program opens with the ransomware demand that cannot be closed.
- Your PC unexpectedly begins to play an audio message demanding a ransom payment to decrypt your files.
- Critical management systems crash, kicking users out.

Cerber



CERBER

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files follow the instructions:

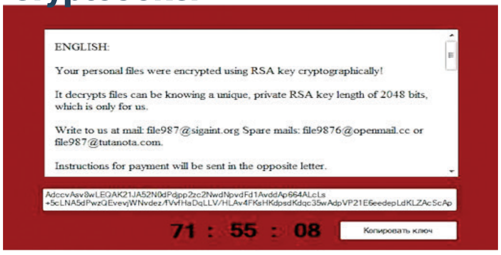
1. Download and install the «Tor Browser» from https://www.torproject.org/
2. Run it
3. In the «Tor Browser» open website:

   http://decrypttozxybarc.onion/2222-2222-2222-2222-2222

4. Follow the instructions at this website

«...Quod me non necat me fortiorem facit.»

CryptoJoker



ENGLISH:

Your personal files were encrypted using RSA key cryptographically!

It decrypts files can be knowing a unique, private RSA key length of 2048 bits, which is only for us.

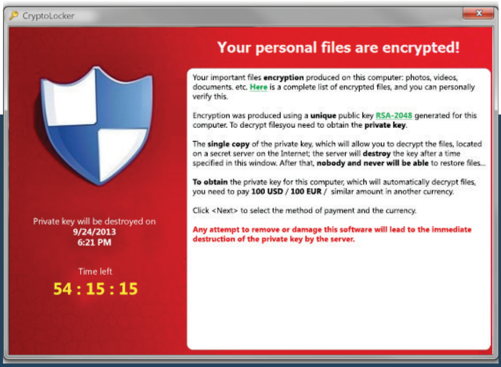
Write to us at mail: file987@sigaint.org Spare mails: file9876@openmail.cc or file987@tutanota.com.

Instructions for payment will be sent in the opposite letter.

```
AdccvAsv8wLEQAK21JA52N0dPdjpp2zc2NwdNpvdFd1AvddAp664ALcLs
+5cLNA5dPwzQEvevjWNvdez/1VvfHaDqLLV/HLAv4FKsHKdpsdKdqc35wAdpVP21E6eedepLdKLZAcScAp
```

71 : 55 : 08

CryptoLocker



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

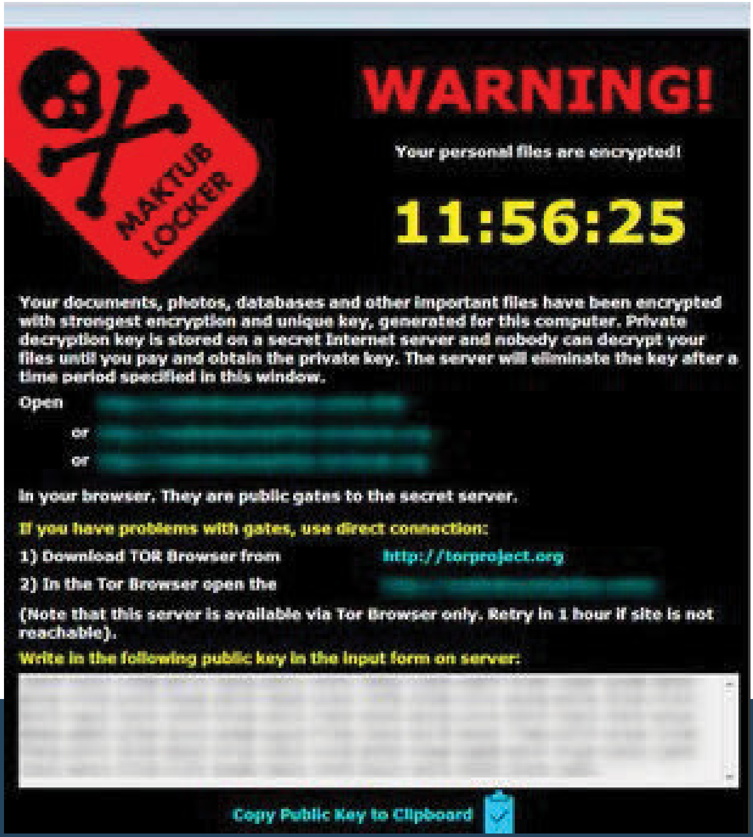
Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Maktub Locker



WARNING!

Your personal files are encrypted!

11:56:25

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open [redacted]
or [redacted]
or [redacted]

in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1) Download TOR Browser from http://torproject.org
2) In the Tor Browser open the [redacted]

(Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable).

Write in the following public key in the input form on server:

[redacted]

SCREENSHOTS OF COMMON RANSOMWARE

RANSOMWARE INFECTION VECTORS

EMAIL

Email is the most common infection vector used by cybercriminals. A single individual can send hundreds to thousands of emails spoofing fax reports, invoices, utility bills, or malicious URLs. The only objective is to entice the recipients into opening and launching an attack against their own organization. The emails launch an obfuscated payload that immediately begins to encrypt the user's files and network shares and then presents the ransom to the victim explaining how to decrypt files by making a Bitcoin payment on the Tor network. It's important that employees are educated and tested regularly on the threat of phishing emails. They must be able to identify and deal with these threats.

FREE SOFTWARE

Everybody loves free software. With many vendors switching to a subscription model to make more money; individuals have started searching for free alternatives. Why pay a subscription to use Adobe Photoshop when a free alternative like GIMP works just fine? Cybercriminals know people like free stuff and they have learned to use that against us. Ransomware can be injected into "cracked" versions of games and software, free game downloads, gaming or software mods, adult content or fake software that tricks users into downloading the malware. The free downloads extract ransomware onto your system, and it can be programmed to activate and run weeks later.

DRIVE-BY-DOWNLOAD

A drive-by-download refers to the unintentional download of a virus or malware onto your computer or mobile device. You do not have to click on anything or accept any download prompts. Just visiting the site can lead to infection. Drive-by-downloads work by exploiting old outdated browsers, software plug-ins or unpatched third party applications to infect your machine. These compromised websites run an exploit kit (EK) to check for known vulnerabilities. If a cybercriminal finds a bug that can be exploited to allow the execution of malicious code, they will launch an attack and compromise your system. These zero-day threats are usually caught and patched by the software vendor, but there is a period of time where it will not be detected by antivirus software until a virus definition has been created and installed.

EDUCATE YOUR END USERS TO WATCH FOR SIGNS OF RANSOMWARE!

DO:

- ► Hover over links to identify spoofed links; make sure that an embedded link is taking you to the exact website it presents.
- ► Inspect emails for obvious red flags: misspelled words, incorrect URL domains, unprofessional and suspicious visuals and unrecognized senders.
- ► Visit the website of the company that allegedly sent the email to make sure the deal being advertised is also on the retailer's homepage.

DO NOT:

- ► Do not click on any links in any email sent from unknown or suspicious senders.
- ► Do not forward the suspicious email as you may just help spread the threat to others.
- ► Do not download content that your browser or antivirus identifies as malicious.
- ► Do not give away personal information like your credit card number, home address, or social security number to a site or e-mail address you think may be suspicious.

YOU’RE INFECTED!

Once you realize you have been infected by ransomware, it is already too late. Your files have been encrypted. Employees have been booted from the applications they were working in and are looking to management and IT to tell them what happened and how quickly they can get back to work. The unfortunate answer is “…it will be a while…” This is the moment your IT technician nervously puts one finger in their shirt collar and lets out an audible “Gulp” as the sweat beads down their forehead. Yes, your day just went from terrific to terrible in seconds.

1. ISOLATE THE INFECTED STATION ASAP!

You have to find the infected machine first! It is critical that you immediately disconnect the infected workstation from the network. Unplug the network cable, disconnect Wi-Fi and Bluetooth, and unplug all external storage devices such as USB or external hard drives. Remove the workstation and secure it in a locked location if necessary. It is important that you get the workstation off the network, but this isn’t the time to reimage the machine or attempt a “clean up” using antivirus software.

Steps to Isolate the Infected Station

1.1. Look at the files in an infected folder

1.2. Locate a file named ”instructions” or ”decrypt instructions” – TXT or HTML

1.3. The owner of that file is your culprit. Right-click the file and view the properties. Click the Details tab to see who the owner is

1.4. Now disconnect and shutdown, but don’t wipe that station

2. DETERMINE THE SCOPE OF THE INFECTION

There are a lot of things to consider when trying to determine the scope of the infection. To find out how much of your network infrastructure was infected, you need to examine a number of storage areas including the following:

- All folders on the infected workstation
- Shared folders
- Network attached storage
- Cloud storage (Box, Dropbox, OneDrive, iCloud, Google Drive, etc…)
- USB drives
- External Hard Drives

It may be possible to revert your files in cloud storage to previous unencrypted versions so check out this option before reverting to backups. Take an inventory of what files and directories were infected so you are prepared when it is time to restore. If you are forced to pay the ransom, you will need to have cloud storage drives connected in order to decrypt those files. One way to find encrypted files is to search for the ransom notes. Since every file encrypted contains at least two corresponding ransom notes, you can search for the title of the ransom note to easily find them. Search at the root of the drive and sort the results by file path to see how far into your directory structure you need to restore.

Another place you can check is the registry. Some ransomware variants place a file listing in the registry to document all the files encrypted. These ransomware variants use this file listing to determine what files need to be decrypted once the ransom has been paid.

3. WHAT RANSOMWARE VARIANT DO I HAVE?

There are a number of different variants of ransomware, with some being much more sophisticated than others. All versions of ransomware to date share some common traits. To start with, all variants of ransomware encrypt files, but not all versions use the same level of encryption. Most ransomware today demands a bitcoin payment within a certain deadline, however, a new variant of crypto-ransomware called TrueCrypter accepts Amazon gift cards as payment. The payment amount demanded can vary wildly by strain. There is ransomware that uses audio to speak its ransom demand to victims, and even better, there is a version called CryptoJoker that allows you to negotiate the ransom with the attacker. Keep in mind there are versions of ransomware that can be decrypted with free tools developed by IT security experts, so you certainly want to check into this before paying a ransom. WatchPoint has documented many of these ransomware strains in our blog. If you are facing a new strain of ransomware, you may need to consult with security experts and provide certain system files to determine what strain of ransomware you are infected with.

4. RESPOND: RESTORE, DECRYPT, IGNORE, PAY UP

After you have isolated the infected workstation, determined the scope of the attack and the ransomware variant, you are ready to craft your response. Unfortunately, the options are few, and all are painful.

Following is your short list of options to carefully consider:

1. Restore files from backup.

2. Decrypt your files using a third party decryptor.

3. Ignore the ransom and do nothing.

4. Negotiate and pay the ransom.

The FBI has recommended that you pay the ransom and in some situations that may be your only option. It's important that you make a decision quickly as to how you will react in this situation since you are facing a time limit. Restores can be time-consuming, and restore failures should be taken into consideration to determine if the restore is a viable option.

In the next section, we will examine these four options in detail including any additional issues and dependencies related to them.

RANSOMWARE REMEDIATION OPTIONS

Backups are an important part of any organization's disaster recovery plan, and regular backups including offsite backups are not optional. Restoring data over the internet from cloud-based storage can be very time consuming so it is still ideal to have an onsite backup system using hard discs, or at a minimum, a very fast internet connection ready in case you need to restore a lot of data very quickly from cloud storage. In the best case scenario, you will be back in business in a few hours, in the worst case, hundreds of gigabytes of data restored over the internet could take several days.

1. RESTORING FROM BACKUP

Since you already determined the scope of the ransomware infection, you are now ready to proceed with the restore process.

Server Restore:

Most of an organization's critical data resides on the server which had data in shared folders encrypted. Since the server may host management systems necessary for business operations, it's always best to start with the server restore first. Your server may contain shadow copies that can be used to restore data. A shadow copy is a Windows snapshot that contains copies of your data from that Windows restore point. Unfortunately, most of the current versions of ransomware delete the Windows shadow copies, making restoring from shadow copy impossible.

Configure your backup software to restore files only to the infected shares to save valuable time and restore from the latest incremental backup. Once the files on the server have been restored, you can search the shared directories and delete the ransom notes.

Cloud Storage Restore:

If your offline backup media doesn't include copies of documents in cloud-based storage like Dropbox, Box and Google Drive, you will need to login to those cloud storage accounts and restore your files. If the latest version of the file has been encrypted, you may have the option to restore from a previous version.

Infected Workstation:

Many people will attempt to run multiple virus scans on the infected workstation to quarantine and delete the ransomware until the machine is reported to be cleaned. At WatchPoint, we highly recommend you wipe and reimage the infected workstation instead of attempting to save it. Ransomware makes changes to the registry and even after being cleaned by antivirus will leave remnants behind that can have negative effects on the workstation.

If you cannot wait for the computer to be reimaged, run the restore to a spare workstation and deploy that in place of the infected workstation. Once the workstation has been reimaged, you can restore data to it.

2. IS A DECRYPTOR AVAILABLE?

Be very careful when attempting to find a decryptor to make sure you don't end up downloading additional malware from a nefarious website. Make sure you are searching reputable websites and make use of security forums to see if anyone else has reported finding a decryptor for your version of ransomware. The decryptor you download may or may not decrypt any or all of your files. If it works is dependent upon the decryptor using the correct key for the version of the ransomware variant that has infected your workstation.

3. REFUSE TO PAY

If the workstation isn't business critical and didn't contain a lot of valuable data, it might be a better choice to refuse to pay the ransom. For some, the decision not to pay is pretty straight forward. Their moral principles will not allow paying a ransom to cybercriminals. When Bob Howard, owner of Hard Times Café in Rockville, Md. was hit with ransomware and facing a demand of $10,000, Bob chose to close down shop for a week while his technicians worked to restore the damage.

"I just said there's no way I'm paying these guys because that is not me. My biggest concern is that no one could guarantee if I did pay them the site would be secure for transactions."

If you refuse to pay you will still need to follow the process of reimaging your machine before placing it back onto your network. WatchPoint highly recommends that you create a backup of the encrypted files. It's possible the decryption key could be released at a future date and at that time you could use a decryptor to remove the file encryption.

4. NEGOTIATE AND PAY THE RANSOM

In certain situations, it may be necessary to pay the ransom if you find you have no other options to restore or decrypt your files, and it is absolutely necessary that you get your files back. The cybercrminals attempt to make paying the ransom very easy by offering simple step-by-step instructions on how to purchase bitcoins, gain access to the Tor network and send them the ransom payment.

Paying the ransom comes with some risk. Sometimes the ransom links don't work because law enforcement or the ISP shut them down and there are times when you will pay a ransom and still won't be able to decrypt your files. What is most interesting is that the FBI recommends paying the ransom while most industry technicians will say not to. The reason for not paying the ransom is that it will discourage cybercriminals from continuing their campaigns if victims stop paying the ransom. We should be realistic here and understand the criticality of the data under attack and understand that in some cases you do have to negotiate and pay the ransom demand. Lastly, the genie is out of the bottle and realistically there is no way ransom attacks are going to stop without intervention by IT experts since cybercriminals have monetized ransomware and learned how to make huge sums of money in short order.

In the next section of this document, we will walk through the steps of retrieving the ransom note and following the instructions to pay the ransom to decrypt files and get you back in business.

STEPS TO RETRIEVE & PAY THE RANSOM NOTE

STEP 1. LOCATE THE RANSOM NOTE

This should be pretty easy. The cybercriminals have designed their ransomware variants to make paying the ransom as simple as possible. In most cases, once the ransomware has finished encrypting files it will launch a web browser with the ransomware demand. You will also see documents on your desktop and other personal and shared folders with a name similar to Help_Decrypt.pdf or DECRYPT_INSTRUCTIONS.TXT that contain the ransom instructions. Once you have collected the following information from the ransom, you can proceed with the payment.

- The dollar amount of the ransom demand
- Links to the payment website
- Time remaining to pay the ransom

STEP 2. PURCHASE BITCOINS

Purchasing Bitcoins when you are facing a ransom demand with a time limit can be tricky. Many Bitcoin exchanges require you to connect your bank account to complete transactions, and those exchanges can have longer wait times between transactions (up to 4 days for new accounts) which make paying the ransom before the deadline expires next to impossible. There are exchanges that allow you to buy and sell Bitcoin instantly by connecting to any U.S. based bank account. Coinbase.com is a popular Bitcoin exchange and is highly reputable. It is even possible to purchase Bitcoins through local sellers using cash. LocalBitcoins.com is a great website that can help you find local sellers quickly and you can filter by payment types. This may be the fastest way to get your Bitcoins. You can review the Bitcoin wiki here to see all the possible payment options.

After you have created an account, you will have a Bitcoin wallet address. This is the address you will use to send payment to the cybercriminal. It is recommended that you purchase more Bitcoin than is demanded in the ransom to cover the fluctuation in the price of Bitcoins and cover any transactions fees.

STEP 3. INSTALL THE TOR BROWSER

Downloading and installing the Tor browser is no different than installing Chrome or Firefox and functionally you will notice very little difference in the browsers. Navigate to www.torproject.org and click the large purple "Download Tor" button and run the installation. Do not download Tor from any other website or you risk infecting your workstation with additional malware.

Once the browser installation completes, open the Tor browser. You can now view and navigate sites hosted on the Tor network. Cybercriminals host their ransomware in temporary locations on the Tor network which allows them to shut down the site immediately after payment in an attempt to thwart public tracking attempts.

You will notice that the web address given for the payment looks rather strange. This is normal and nothing to be concerned about. Tor uses unique web addresses. Here is an example of a Tor address.

http://32rfckwuorlf4dlv.onion/ – Onion URL Repository

http://kpvz7kpmcmne52qf.onion - Uncensored Hidden Wiki

STEP 4. PAY THE RANSOM

Now that you have purchased Bitcoin(s) and have money in your wallet, you are ready to transfer the payment to the cybercriminals Bitcoin wallet. You will need the following key pieces of information to complete the ransom payment.

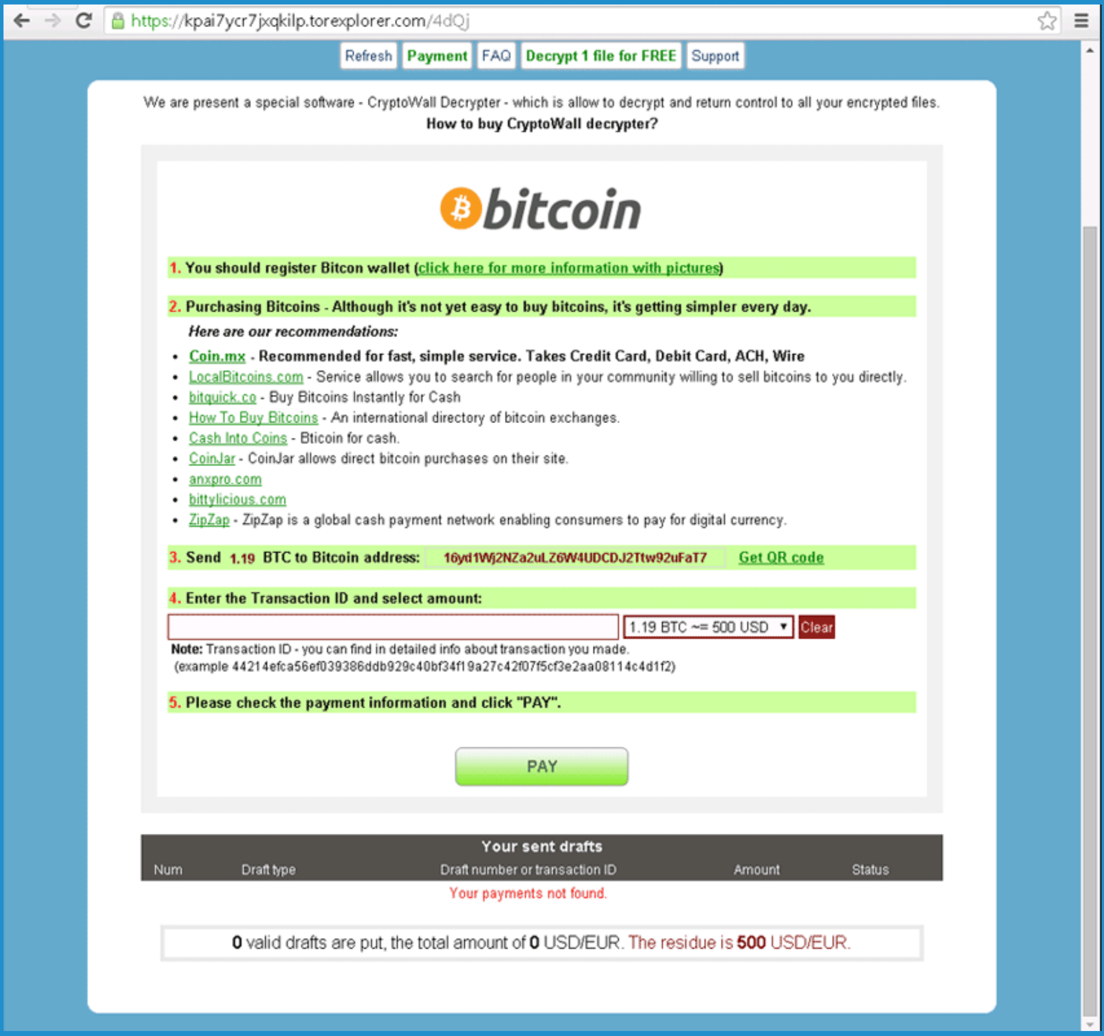
- The Tor web address to view the specific payment information.
- The cybercriminals Bitcoin wallet ID for payment.
- A transaction ID or "hash" generated when the Bitcoin payment has been transferred.

You will need to launch the Tor browser and navigate to the web address created for your ransom payment. Enter the address given into the Tor browser. On the website, you will find the wallet ID that you need to send your Bitcoin payment to. The website will be included in the ransomware payment instructions.

Here is an example of a Bitcoin wallet string: 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Once you have made the Bitcoin payment through your Bitcoin exchange and the funds have been transferred to the cybercriminal's Bitcoin wallet, you will get a transaction confirmation hash which looks a lot like the Bitcoin wallet string. If the ransomware includes a field for the transaction ID, you will need to input the ID along with the Bitcoin amount.

Example of Bitcoin payment screen of the CryptoWall ransomware



We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- **Coin.mx - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bticoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.19 BTC to Bitcoin address: 16yd1Wj2NZa2uLZ6W4UDCDJ2Ttw92uFaT7

4. Enter the Transaction ID and select amount:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

5. Please check the payment information and click "PAY".

Your sent drafts				
Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

0 valid drafts are put, the total amount of **0** USD/EUR. The residue is **500** USD/EUR.

As you can see from the Bitcoin payment screen, the cybercriminals go out of their way to provide all of the information you need to complete the ransomware transaction, including everything we have already covered.

Section 1. Provides information on registering for a Bitcoin wallet.

Section 2. Provides information on purchasing Bitcoins and offers recommendations for Bitcoin exchanges.

Section 3. Provides the Bitcoin ransom demand and the Bitcoin wallet address for payment.

Section 4. Field to enter the Transaction ID and select the Bitcoin payment amount.

Section 5. Asks you to review the information entered and press “Pay“.

STEP 5. DECRYPT YOUR FILES

It may take several hours for the cybercriminals to process your Bitcoin transaction and during this time you will simply have to wait. Once that transaction has completed, the cybercriminals will give you access to the decryptor software along with the decryption key.

NOTE: It is important to remember that you need to make sure that all of your external drives and network drives are connected at the time that you run the decryptor, or you may not be able to recover all of the encrypted files. Make sure you have access to all the shared folders, that you have the correct mapped drives with the original drive letters and use the exact same UNC paths for all the folders being decrypted.

PREVENT FUTURE RANSOMWARE ATTACKS

Hit by ransomware once…shame on them. Hit by ransomware twice…shame on you.

WatchPoint has received many desperate calls from businesses looking for a solution to constant ransomware attacks. In fact, we have noticed a pattern where several businesses have been hit with ransomware, paid the ransom and then been attacked with ransomware again weeks or months later. Several businesses have reported paying a ransom four to five times in one month! That is incredible and unacceptable. Whether you have been hit with ransomware or not, it is time to put in place the proper network protection to stop these attacks.

MULTILAYERED APPROACH TO NETWORK DEFENSE

Your information network consists of many layers of people, network devices and ports/services that need to be protected from both internal and external attacks. Carefully consider each layer when constructing your defenses.

End Users: The weakest link in any ransomware attack is always the end user. A firewall cannot protect your network from your employees opening attachments in email; it cannot stop them from downloading free software laced with malware, and it cannot stop users from visiting disreputable websites and keep them from getting infected by drive-by downloads. Hardening your network starts with employee education.

- **Security Awareness Training:** It is important that your employees understand what attack vectors to look for in every email they receive to identify and avoid opening emails that contain malware. An organization should host quarterly training and include examples of real phishing emails and demonstrate a ransomware attack.
- **Simulated Attacks:** Once your employees are educated on what phishing attacks are and how to identify phishing emails; you need to test them with simulated phishing campaigns. These campaigns will help you improve your employee training and will keep your employees up-to-date and alert to the latest attack vectors.

Internal Network: You may have a large number of devices like routers, switches, firewalls, wireless access points, printers, and IP telephones that transmit data and need to be secured from packet sniffing or a cybercriminal using nmap to enumerate your network.

Hosts: Hosts should include antivirus and a software based firewall installed and up-to-date on virus definitions. You might also consider a host-based intrusion detection system and advanced endpoint protection like Carbon Black. It's very important that your host operating systems and applications are updated on security patches to rid them of vulnerabilities that could be exploited in an attack.

Application: Software developers need to make sure their applications are secure and free of flaws that can be exploited. 84% of all attacks occur at the application layer because cybercriminals know exploiting flaws in software applications that you use daily such as Adobe Acrobat, Adobe Reader, Microsoft Office, and Quickbooks are the easiest methods of access to your data network.

Data: Proprietary data and Personally Identifiable Information (PII) are key components of your business that must be kept safe from cybercriminals. Your business is liable for breaches of PII. A cyber liability policy should be considered to protect yourself in the event of a breach, but failure to secure your network can result in a refusal by your insurance company to pay the cyberliability claim.

ANTIVIRUS AND BACKUPS MORE IMPORTANT THAN EVER

At WatchPoint we rail on antivirus quite a bit. Antivirus is a terribly antiquated method of dealing with ransomware. Antivirus is a signature based solution that requires constant updates to stay on top of the latest malware threats. Only after a new virus or ransomware threat is found and studied can antivirus vendors create a definition to detect the new threat. Antivirus is still a must to protect your devices from the millions upon millions of different malware threats but time and time again it fails to detect and prevent ransomware due to the number of strains, the different variants within these strains and the speed at which new ransomware strains are released by competing cybercriminals.

As you have probably learned by now, data backups are critical! Data needs to be backed up at frequent intervals, and those backups should be tested regularly. There are a number of backup options available, but whatever option is chosen you should include both onsite and offsite backups. Offsite backups are very important in resuming business operations in the event of a disaster at your current business location. Onsite backups on physical hard drives are typically the fastest method to restore your data as opposed to using a cloud-based service where data must be downloaded over your internet connection.

CRYPTOSTOPPER.IO ™

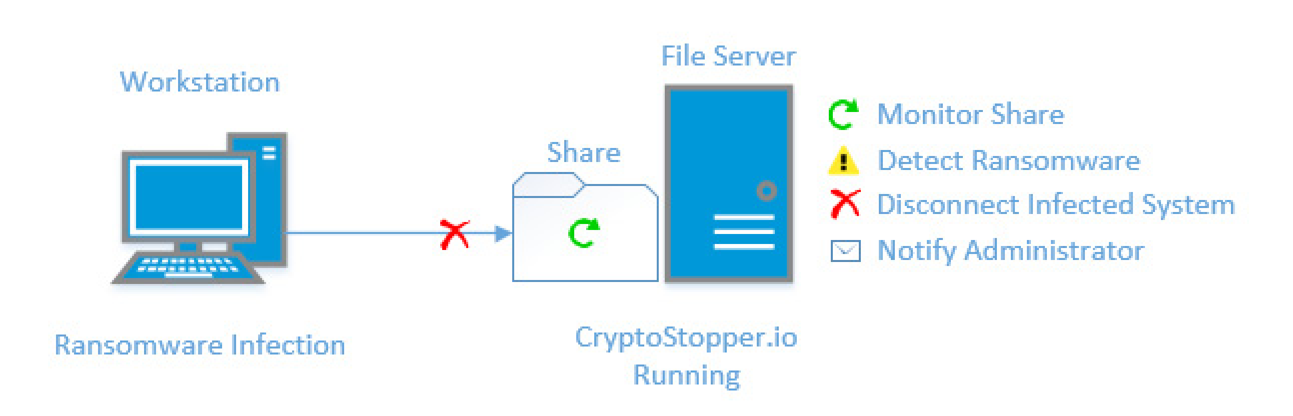
Stopping Ransomware Attacks in Seconds

Stopping ransomware from entering your network is next to impossible. CryptoStopper will contain the damage and save your network from complete compromise and downtime.

CryptoStopper is the answer to the ransomware problem plaguing the world today. CryptoStopper was developed to identify ransomware by watching the data on your network. By monitoring watcher files for read/write operations, Cryptostopper can detect the presence of ransomware the moment it happens.

CryptoStopper provides information about the infection such as the infected user account, the infected computer account, and most importantly, it disconnects the infected workstation from the rest of the network.

Cryptostopper is a true ransomware killer. We do not use whitelists which need to be updated, and constant false positives are a thing of the past. When ransomware attacks, Cryptostopper recognizes the behavior and stops it in seconds, immediately sending out alert messages and saving the day from the ransomware attack.



- Know the moment a ransomware attack hits.
- Identify which user launched the ransomware payload.
- Identify which workstation is infected.
- Disconnect the infected workstation; stopping the ransomware attack.

RANSOMWARE RESPONSE CHECKLIST

Step 1. Disconnect the Infected Workstation

- ☐ Disconnect the computer from the network by removing the network cable
- ☐ Turn off wireless including Wi-Fi, Bluetooth, NFC

Step 2. Determine the Scope of the Infection – Where to Look for Encrypted Files

- ☐ All folders on the infected workstation
- ☐ Mapped Drives
- ☐ Shared folders
- ☐ Network attached storage
- ☐ Cloud storage (Box, Dropbox, OneDrive, iCloud, Google Drive, etc…)
- ☐ USB drives
- ☐ External Hard Drives

Step 3. Determine the Ransomware Strain

- ☐ Determine strain/variant of ransomware. Is it CryptoLocker or CryptoJoker, etc.?

Step 4. Determine Your Response

Option 1. Restore Your Files from Backup

- ☐ Locate Your Backups
  a. Check cloud storage for previous versions of files
  b. Locate and connect all backup media
  c. Verify the integrity of the backup media (i.e. read errors or corrupted files on media)
  d. Examine Shadow Copies (mostly likely deleted or corrupted by the ransomware)
- ☐ Remove the ransomware from the infected workstation
- ☐ Restore the files from backups
- ☐ Determine infection vector and act to prevent further exploitation

Option 2. Determine if a Decryptor is Available

- ☐ Determine strain and version of the ransomware
- ☐ Locate a decryptor online
- ☐ Locate and connect all backup media
- ☐ Decrypt your files
- ☐ Determine infection vector and act to prevent further exploitation

RANSOMWARE RESPONSE CHECKLIST (CONT'D)

Option 3. Refuse to Pay

- □ Remove the ransomware infection
- □ Backup the encrypted files and wait for a future decryptor release
- □ Determine infection vector and act to prevent further exploitation

Option 4. Negotiate and Pay the Ransom

- □ Negotiate a lower ransom. CryptoJoker was designed with negotiation in mind and other companies have had success negotiating a lower ransom.
- □ Determine the acceptable payment method for the ransomware strain
- □ Obtain currency for payment (Typically Bitcoin)
  - a. Find and create an account with a Bitcoin exchange
  - b. Setup Bitcoin account
  - c. Create Bitcoin wallet
  - d. Purchase Bitcoins
- □ Re-connect your infected workstation to the internet
- □ Locate and connect all backup media
- □ Install the Tor browser
- □ Determine the Bitcoin payment address
- □ Pay the ransom
- □ Determine infection vector and act to prevent further exploitation

Step 5. Prevent Future Ransomware Attacks

- □ Implement the Ransomware Prevention Checklist
- □ Continue Employee Education
- □ Deploy CryptoStopper to monitor your network shares for ransomware attack

RANSOMWARE PREVENTION CHECKLIST

Employee Education

- □ Conduct security awareness training with all employees in your organization. Examine and discuss actual phishing emails
- □ Present a live ransomware infection
- □ Present tips for safe software downloads

Inspect the Applications

- □ Setup and use a high-quality firewall from a trusted manufacturer
- □ Implement antispam/antiphishing software
- □ Keep antivirus definitions up to date
- □ Implement advanced endpoint protection
- □ Use software restriction policies on your network to prevent unauthorized applications
- □ Implement a patch management policy to keep all applications free of vulnerabilities
- □ Close unused network ports
- □ Deploy CryptoStopper to monitor for ransomware attacks and stop it within seconds

Backups are Critical

- □ Implement a backup solution
- □ Ensure all critical data is backed up, including that contained on removable storage
- □ Store backups in a safe, secure environment and keep redundant copies offsite
- □ Test the backups regularly and make sure you can easily and quickly restore files

ABOUT WATCHPOINT

At WatchPoint, our goal is to make cyber security uncomplicated and more successful. That means faster time-to-detection and fewer false positives. The field of cyber security has lost its way. In the pursuit of creating advanced next generation systems, companies have overcomplicated their own solutions and have excluded tried and true methods. Cyber security should offer more than just defense, it should give you the upper hand.

WatchPoint gives businesses an advantage over their attackers. By using proven methods, which emphasize the essentials, we allow businesses to withstand an attack, even after it's reached the internal network. Our system of traps and decoys lowers the time-to-discovery, and safeguards the most critical aspect to a business, its data.

WatchPointData.com
Phone#: (319) 383-0165
Support@WatchPointData.com