OneNet
Delivering Your Software

Ransomware Planning, Protection and Removal Guide

OneNet
Delivering Your Software

Table of Contents

Are You Prepared for a Cyber Attack?

Businesses are being held to ransom. Cyber criminals are attacking with increasing frequency and effectiveness, and your business is on a target list.

With instances of malware attacks and cyber ransom demands increasing at a frightening pace, it's important to know the risks you face and how you're best to prepare for and deal with such an attack.

This guidance document is intended to provide business and IT leaders with an understanding of the urgent threat of Ransomware and provide practical steps that businesses can take to prepare for attacks, steps to prevent attacks occurring, but if attacked prescriptive steps to resolve.

Ransomware is getting more targeted, expensive

In an alert published on the 15th of September 2016, the U.S. Federal Bureau of Investigation (FBI) warned that recent ransomware variants have targeted and compromised vulnerable business servers (rather than individual users) to identify and target hosts, thereby multiplying the number of potential infected servers and devices on a network. Krebs on Security says "What we can expect is not only more targeted and destructive attacks, but also ransom demands that vary based on the attacker's estimation of the value of the data being held hostage and/or the ability of the victim to pay some approximation of what it might be worth."

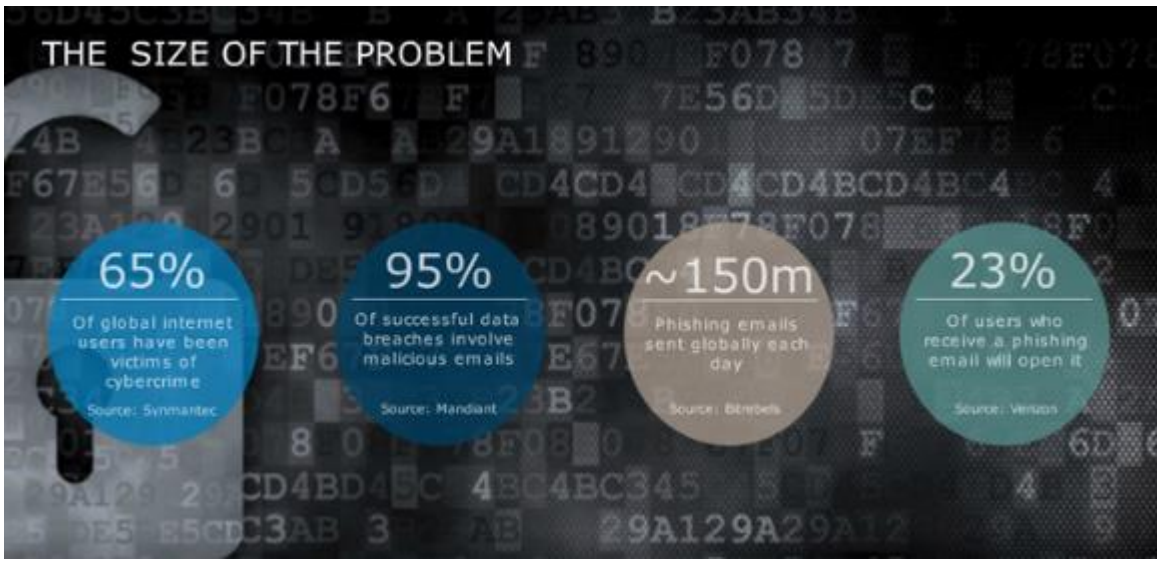
"Actors engaging in this targeting strategy are also charging ransoms based on the number of host (or servers) infected," the FBI warned. "Additionally, recent victims who have been infected with these types of ransomware variants have not been provided the decryption keys for all their files after paying the ransom, and some have been extorted for even more money after payment."

Everyone has a role to play

As stated in an Aug16 BlueNotes.anz.com post "Everyone has a role. Financial institutions, industry, government, law enforcement and consumers are all part of a cybersecurity ecosystem where everyone needs to work together, and everyone has a role to play in preventing and responding to cybercrime."

OneNet agrees that everyone is involved and as a practitioner in this domain, this guidance document has been written to highlight the valuable resources that are available to businesses to combat this significant threat.

In particular, this paper leverages ANZ BlueNotes Sep16 post "Eight ways to Protect your Business from the Cybercrime Wave" for a Business Audience (http://bit.ly/2bWulwi) and the KnowBe4 "Ransomware Hostage Manual" (https://www.knowbe4.com/resources) for a prescriptive response in the event an infection.



Russian Roulette

"An equally disturbing trend in ransomware is the incidence of new strains which include the ability to randomly delete an encrypted file from the victim's machine at some predefined interval – and to continue doing so unless and until the ransom demand is paid or there are no more files to destroy."

What is Ransomware?

Ransomware: A common form of malware restricting access to an infected computer system and demands a ransom to remove the restriction. Ransomware typically circulates as a virus within an email attachment disguised as a seemingly legitimate file.

Malware: Malicious software used to access or disrupt IT systems, gather sensitive information, or display unwanted advertising. It is often received through phishing or spam emails but can also be hidden in online ads and pop up messages.

Social engineering: Occurs when people are manipulated into doing things they shouldn't or divulging confidential information. It can be initiated in person, via email (Phishing), over the phone (Vishing), through an SMS message (Smishing) or via social media sites such as LinkedIn and Facebook. It is a more frequently used tool because it delivers a targeted and realistic attack enabled by publically available information and social media.

Phishing: Emails that appear to come from an official source when in reality are a scam attempting to extract sensitive information like usernames, passwords or credit card details. A victim could unwittingly enter account details into a fake bank website or click on a link which installs malware on their computer and network.

Spear phishing & email hijacking: More targeted versions of the above. Rather than a scattergun approach aimed at several individuals, spear phishing targets a specific person. An extension of the spear phishing attack vector is business email compromise or email hijacking. A common but effective example involves an email sent by a purported CEO of a company while they are travelling, urging the company's finance team to make an urgent and discreet payment.

What to do about it?

Although investment is necessary to manage cyber-risk exposures, there are still some simple steps organisations can take to improve their people, systems and processes.

Step 1: Protect your business

As highlighted by the ANZ post "for businesses, there are a number of key factors, both externally and internally focussed, which are important to cover to ensure you are adequately prepared."

Internal

- Understand your exposure. Know what information and assets the business holds. Ask yourself: what could be valuable to cybercriminals? What processes and people are in place to protect those assets?
- Educate yourself and your management on the risks of cybercrime. Implement in depth defences. Have a clear cyber policy which adopts a multilayer approach to defending your organisation.
- It's not enough to only invest in preventative measures, have a response process in place so your reaction is quick and organised.

External

- Leverage professionals. If you lack the internal capabilities, invest in external support.
- Look to best practice. There are a number of leading frameworks and examples of best practice which can steer your approach to investing and building the right capabilities.
- Share and seek intelligence. Work with industry partners and government departments to share intelligence.

The business impact of a Cyber-attack often extends well beyond the act and cost of recovery data. The Deloitte whitepaper – "Beneath the surface of a cyberattack" (http://bit.ly/2dBnY3X) provides a framework for evaluating the true cost of an attack and provides useful information for a Business Continuity Business Case. OneNet also recommends that businesses evaluate Cyber Risk insurance policies that are now available in the market.

Step 2: Understand the risk

Organisations are being attacked from all sides, with the most common approaches (vectors) of attack being malware, ransomware, phishing and social engineering (via phishing, spear-phishing and email hijacking). A successful cyber-attack is the result of many of these methods being used together.

The most common scenario involves an email attachment disguised as an innocuous file. If an email with an attachment or even a link to a software download is received and installed or opened without verifying its authenticity and the sender's intention, this can lead directly to a ransomware infection. Increasingly, infections happen through "drive-by downloads," where visiting a compromised website with an old browser or software plug-in or an unpatched third party application can infect a machine.

Another common way to infect a user's machine is to offer a free version of a piece of software. This can come in many flavours such as "cracked" versions of expensive games or software, free games, game "mods", adult content, screensavers or bogus software advertised as a way to cheat in online games or get around a website's paywall.

Cyber criminals also use Social Engineering by observing human behaviour, perhaps through phone calls to the company or on social media, to socially engineer a situation where the finance team bypasses the usual controls to make a payment.

Backups and restoration testing is critical preparation

In order to fully evaluate restoring from backups as a response to a ransomware attack, it is first necessary to determine the state of backups. If there is ready access to backup files, then an immediate restore process can be conducted, together with manual verification of the files from the backup. It is necessary to determine periodically whether the files are indeed backed up and recoverable.

Am I affected by a ransomware virus?

It is usually quite easy to tell – the symptoms include:

- You suddenly cannot open normal files and get errors such as the file is corrupted or has the wrong extension
- An alarming message has been set to your desktop background with instructions on how to pay to unlock your files
- The program warns you that there is a countdown until the ransom increases or you will not be able to decrypt your files
- A window has opened to a ransomware program and you cannot close it
- You see files in all directories with names such as HOW TO DECRYPT FILES.TXT or DECRYPT_INSTRUCTIONS.HTML

Step 3: Make a plan for resolving an attack

If attacked, it is imperative that action is taken immediately. At a high level these steps minimise exposure:

1. **Disconnect immediately:** disconnect from any network, turn off wireless capabilities and unplug any storage devices
2. **Determine the scope:** determine exactly how much of your file infrastructure is compromised or encrypted
3. **Determine the strain:** so you know exactly which ransomware you're dealing with
4. **Evaluate your response:** there are essentially four response options:
    1. Restore from a recent back up
    2. Decrypt your files using a third party decryptor
    3. Do nothing
    4. Negotiate/pay the ransom. [1]

1. Disconnect immediately

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

2. Determine the Scope

At this point, it is necessary to determine exactly how much file infrastructure is compromised or encrypted. Did the first infected machine have access to any of the following?

- Shared or unshared drives or folders
- Network storage of any kind
- External hard drives
- USB memory sticks with valuable files
- Cloud-based storage (DropBox, Google Drive, Microsoft OneDrive/Skydrive etc…)

Make a list of the above relevant items and check them for signs of encryption. In the case of cloud storage devices such as DropBox or Google Drive, it may be possible to revert to recent, unencrypted versions of the files. It will also be necessary to understand which files are backed up and which files need to be restored versus what may not be backed up. If it is necessary to pay the ransom the drives will need to be reconnected to allow the ransomware to decrypt them.

The scope of an infection may be determined by checking for a registry or file listing that has been created by the ransomware. This lists the files ransomware has encrypted so that when the ransom is paid, the ransomware software will know which files need decrypting. Often, this will be a file in the registry. Since every strain of ransomware is different, it is recommended that some Google research be done to determine the version

[1] Previous security reports have quoted FBI agents saying the agency condones paying such ransom demands. But in the 15th September 2016 release the FBI is unequivocal "The FBI does not support paying a ransom."

of ransomware that has hit. This means that any research is based on the relevant version of the ransomware.

3. Determine the Strain

It is very important to know exactly which version of ransomware is relevant. Each version of ransomware will follow a basic pattern of encrypting files, followed by a request for a ransom payment before a certain deadline. Knowing which version of ransomware is involved will help to inform the decisions to be made. For example, there is a new strain of ransomware recently discovered which encrypts the Master Boot Record and locks the user out of access to the whole hard disk.

Ransomware strains vary in that some are costlier in ransom payments than others. Some versions will have even more options to pay than just Bitcoin. Some strains have a decryption tool built by an IT security company that will allow decryption of files without having to pay anything. Other strains have emerged whereby cyber-criminals no longer rely on a "spray-and-pray" approach and target how important the locked data is. It may range from 0.5 BTC (BitCoin) to as much as 25 BTC, or USD$10,000. Of course, these terms are negotiated individually.

If the strain of ransomware is not known at the time of the attack, it will be necessary to consult with security experts or provide information on various system files in order to determine what kind of ransomware has been used. The www.bleepingcomputer.com website is a good place to start.

4. Evaluate Your Response

Once the scope of the encryption is known, together with the strain of ransomware installed, a more informed decision on the next action may be made. In essence, there are four options available, from best to worst:

1. Restore data from a recent backup
2. Decrypt your files using a third party decryptor
3. Do nothing and lose the data
4. Negotiate and/or pay the ransom requested

Detailed Response Steps

First Response: Restore Files from a Backup

In order to fully evaluate this option as a response to a ransomware attack, it is first necessary to determine the state of backups. If there is ready access to backup files, then an immediate restore process should be conducted, on a separate computer, together with manual verification of the files from the backup. This is especially critical if you are using physical backup media such as USB drives, DVDs or external hard drives to back up your data. By default, all data residing at OneNet is backed up daily, to disk, and replicated in two separate geographic locations.

It will necessary to determine periodically whether the files are indeed backed up and recoverable.

- How much data has been lost and how long will it take to restore it?
- Will the time lag seriously impact business functions in the time it will take to recover a backup?
- What other places may the files be recovered from?
- What files are you attempting to recover?

Once you know what key files you need, you can assess if they've been possibly used where a copy may be stored. Once you have verified the files you need, and are able to recover them from a backup, you can now take action on that infected computer and remove the ransomware.

Some businesses run multiple antivirus scans to ensure the malicious software is removed, but to be 100% sure that there are no traces left of any kind of malware, wipe and rebuild the machine. Once you are confident any traces of the ransomware have been removed, you can now restore your files.

Once you've resolved the ransomware infection, it's important to take precautions to prevent these types of attacks in the future. It is not enough just to have last week's backups or just to have antivirus. The weak link in any ransomware attack is the person sitting in the chair in front of the computer. By employing a combination of software based solutions like antivirus, antispam and backups, together with effective security awareness training for your users, you can plug holes with both a software firewall and a human firewall.

See the final section "Precautions to prevent future attacks" for more information.

Second Response: Try to Decrypt

The proliferation of certain strains of ransomware such as CryptoWall and Cryptolocker have resulted in some of the encryption keys being cracked or uncovered by mainstream antivirus companies. This response should not be considered in any way a concrete solution as it mainly works on older versions of ransomware, and hackers are constantly updating their software to counteract any uncovered workarounds.

Step 1: Determine the strain

While you probably already know which version you're dealing with by this point, it is important to know exactly the strain of ransomware you've been hit with. Often,

there will be version numbers, but take these with a grain of salt, as most ransomware seeds itself with completely random version numbers to help foil antivirus companies' attempts to determine if changes have been made. However, even noting the time of the infection and the general strain can help you determine if there is an applicable decryption method you can try.

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

This is the critical part. The KnowBe4 resource page has links to some of the mainstream unlockers, however you will probably need to do some "googling" to determine if the particular strain has an associated unlocker. Even then, you may find that it is unsuccessful at unlocking/decrypting your files. It can depend on the key that was used to encrypt your files and the version of the ransomware you've been hit with. Make SURE any decryptor/unlocker located is vetted from not only a reliable antivirus source, but also there should likely be more than a few references to the site/file you're downloading from other reputable antivirus or malware support forums. This is also a point during which you may want to consult security professionals or ask on popular security forums to see if the pros there know of any tools.

Step 3a: Success!

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

Step 3b: Failure

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

Third Response: Do Nothing

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

Step 1: Rid your computer of all ransomware

It is recommended that you run multiple anti-virus scans to ensure the software is removed. It's much safer to wipe and rebuild the machine though.

Step 2: Back up your encrypted files (optional)

Yes, that's right. You may want to back up your encrypted files. The reasoning here is that occasionally antivirus or computer security experts will uncover the encryption keys used in certain ransomware programs. This may be 6 months later, but it has happened. There was even a case where a rookie ransomware developer – in a flash of conscience – decided to decrypt all the files of the users who had been infected. So it may be a long shot, but you just might get lucky down the road with one of these types of discoveries.

Step 3: Prevent future attacks

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

We recommend having another look at the prevention steps below and institute the following:

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

Fourth Response: Negotiate and/or Pay the Ransom

If you have exhausted all other options, and you simply must have your files back; the only recourse may be to pay the ransom. This is a controversial opinion. Most IT security experts will recommend that users hit with ransomware absolutely avoid paying the ransom. After all, nothing encourages MORE ransomware attacks than a successful ransom being paid. The fact of the matter is though, in some cases there will be no choice. To many businesses, a few hundred (or even thousand) dollars is a drop in the bucket compared to the downtime and financial damage that would occur having lost access to critical files. There may simply be no other alternatives.

"Will these criminals actually decrypt my files if I pay?"

The answer here is a bit complex. The short answer is yes; they will almost always decrypt your files. There is a moral dilemma here, after all, the bad guys want money and they will provide fast and accurate customer service and tech support to facilitate the payment. If it is discovered that when users pay up and the hackers DON'T decrypt the files, they will lose all credibility and a quick search would reveal that it would be fruitless to pay, since the hackers won't do anything. So in an odd way, the only way they can encourage victims to pay, is by actually following through and decrypting your files when you pay them.

The process of dealing with all the aspects of paying a ransomware attacker and navigating the world of Bitcoin exchanges and transfers and complex, and these steps are detailed in Appendix 1 - Negotiate and/or Pay the Ransom.

Precautions to prevent future attacks

Once you've resolved the ransomware infection, it's important to take precautions to prevent these types of attacks in the future. It is not enough just to have last week's backups or just to have antivirus. The weak link in any ransomware attack is the person sitting in the chair in front of the computer. By employing a combination of software based solutions like antivirus, antispam and backups, together with effective security awareness training for your users, you can plug holes with both a software firewall and a human firewall.

Institute the following:

- Install and maintain high-quality antivirus software, as a layer you want to have in place, but do not rely on it – they always run behind.
- Configure weapons-grade backup/restore software and test the restore function regularly!
- 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.

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

- Avoid mapping your drives and hide your network shares. WNetOpenEnum() will not enumerate hidden shares. This is as simple as appending a $ to your share name.
- Work from the principle of least permission. Very few organizations need a share whereby the Everyone group has Full Control. Delegate write access only where it's needed, don't allow them to change ownership of files unless it is a must.
- Be vigilant and aggressive in blocking file extensions via email. If you're not blocking .js, .wsf, or scanning the contents of .zip files, you're not done. Consider screening ZIP files outright. Consider if you can abolish .doc and .rtf in favour of .docx which cannot contain macros.
- Install the old CryptoLocker Software Restriction Policies which will block some rootkit-based malware from working effectively.

For More Information

OneNet plans, protects and manages Ransomware and Cyber-Security threats for its clients every day. OneNet's YouTube channel (https://www.youtube.com/user/OneNetNZ) includes a short video clip on managing Security in the Cloud from our CTO at the Cloud Forum.

Don't hesitate to contact OneNet if you would like to benefit from OneNet's experience.

Visit OneNet.co.nz

Call 0800 66 36 38 or +64 9 376 7610

Email sales@OneNet.co.nz

Sources

Ransomware victims urged to report infections to federal law enforcement:
https://www.ic3.gov/media/2016/160915.aspx

Eight ways to protect your business from the cybercrime wave:
https://bluenotes.anz.com/posts/2016/08/eight-ways-to-protect-your-business-from-the-cybercrime-wave/

Ransomware Getting More Targeted, Expensive:
https://krebsonsecurity.com/2016/09/ransomware-getting-more-targeted-expensive/

Beneath the surface of a cyberattack:
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

RANSOMWARE Hostage Rescue Manual:
https://www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf
https://www.knowbe4.com/resources

http://www.bleepingcomputer.com/#ransomware

https://www.sans.org/security-resources/IAD_top_10_info_assurance_mitigations.pdf

Appendix 1 - Negotiate and/or Pay the Ransom

This section will walk you through the complex process of dealing with the aspects involved in paying a ransomware attacker and navigating the complex world of Bitcoin exchanges and transfers.

The most commonly asked question with regard to the ransom payment is, “Will these criminals actually decrypt my files if I pay?” The answer here is a bit complex. The short answer is yes; they will almost always decrypt your files. There is a moral dilemma here, after all, the bad guys want money and they will provide fast and accurate customer service and tech support to facilitate the payment. If it is discovered that when users pay up and the hackers DON’T decrypt the files, they will lose all credibility and a quick search would reveal that it would be fruitless to pay, since the hackers won’t do anything. So in an odd way, the only way they can encourage victims to pay, is by actually following through and decrypting your files when you pay them.

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

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

This document assumes that your ransom requires payment in the form of Bitcoin. The following are instructions and steps on obtaining Bitcoin and making the proper payments. If this is your first time dealing with Bitcoin, it can be very unfamiliar so we will attempt to alleviate that by providing specific resources for you to use.

Step 1: Locate the Payment Method Instructions

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

1. How much to pay
2. Where to pay
3. Amount of time left to pay the ransom (countdown timer)

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

Step 2: Obtaining Bitcoin

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

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

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

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

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

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

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

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

Step 4: Paying the Ransom

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

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

With many types of ransomware, you will have to visit a page on the TOR network that has been created specifically for paying your ransom. Enter the web address of the site into your TOR browser. You can usually follow the instructions on the site to locate the wallet ID you need to send your Bitcoin to. The wallet ID is usually a long string of numbers and letters and is usually provided by the ransomware payment instructions or somewhere on the screen explaining payment.

Once you've logged into your account at the Bitcoin exchange and transferred the Bitcoin to the hacker's wallet (this may take some time, 20-40 minutes) then you usually get a transaction confirmation hash, which is another long series of letters and numbers.

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

Step 5: Decrypting Your Files

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