seccomglobal.
The Cyber Security Company

Ransomware ATTACK

Preparing For & Surviving an Attack

Seccom Global Pty Ltd
Level 30, Six Battery Road,
Singapore 049909
P: +65 6725 6238
www.seccomglobal.com

We have seen a significant increase in Ransomware attacks over the past 24 months – and there looks to be no slowing down!

These attacks can be devastating to businesses and while the best remedy is prevention, it pays to understand exactly how these attacks occur, and what action to take when they do!

How Does Ransomware Work?

Ransomware typically spreads via spam, phishing emails, or through social engineering activity. It can also be transmitted via websites or malicious downloads to infect an endpoint and penetrate the network – although this can be less common.

Attack methods are constantly evolving – but one thing they have in common is that once they are in place, the ransomware then locks all files it can access using strong encryption. A demand for a ransom is then issued to decrypt the data.

Encrypting ransomware or "Crypto ware" is the most common variety of ransomware we have seen to date.

However, some other types are:

- Non-encrypting ransomware - which simply restricts access to files and data instead of encrypting them.

- Ransomware that encrypts the Master Boot Record (MBR) of a drive or Microsoft's NTFS, which prevents computers from being booted up in a live OS environment.
- Leak ware or extortion ware – which steals compromising or damaging data that attackers threaten to release.

- Mobile device ransomware – infects mobile phones through malicious downloads or fake apps). ***Note: Ransomware for mobile phones is increasing and this promises to be a huge market for attackers in the very near future – it is also very often overlooked as part of the network security strategy for many businesses!***

- We have, in recent years, also seen the emergence of ransomware as a service (RaaS) – so cybercriminals can stage an attack without even having the skills required! It also reduces the cost of staging an attack, making it even easier (and more lucrative) to do so.

Brief Summary of the Steps in a Typical Ransomware Attack

An overview of the typical steps in a ransomware attack are:

1. Infection

After it has been delivered to the system (via an email attachment, phishing email, infected application or other method) the ransomware installs itself on the endpoint and any network devices it can access.

2. Control Contact

The ransomware activates and contacts the control server operated by the cybercriminals behind the attack to generate the keys to be used to encrypt your systems.

3. Encryption

The ransomware starts encrypting any accessible files on the network.

4. Extortion

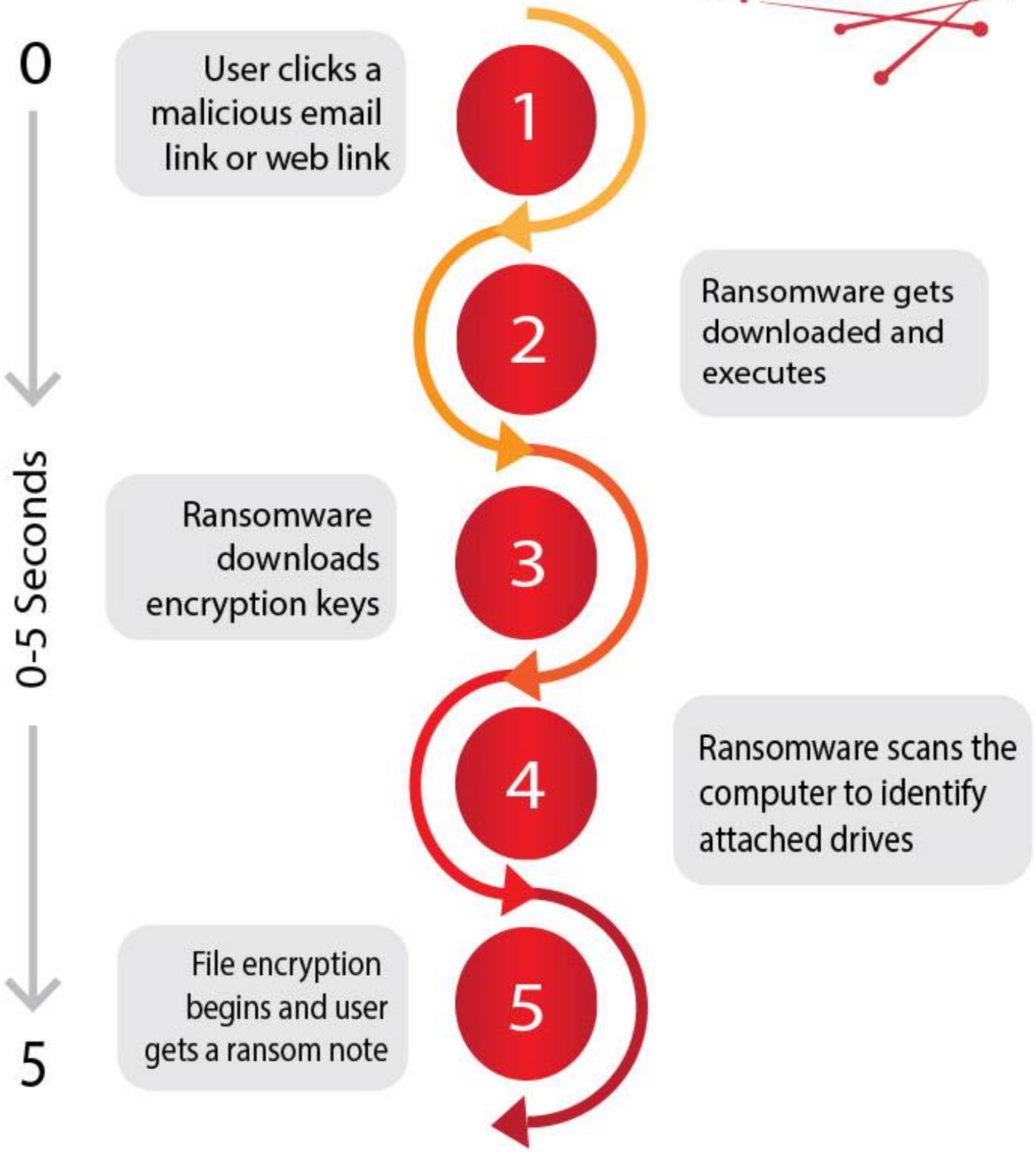
Encryption done, the ransomware displays a notification of the encryption and demands or instructions for a ransom payment, usually threatening destruction or leak of data if a payment is not made.

Businesses can then either pay the ransom or attempt recovery by removing infected files and systems from the network and restoring data from clean backups.

This is where having a strong backup and recovery strategy is crucial – as negotiating with cyber criminals can be unreliable. A recent study found that almost half of organisations who paid a ransom did not get their files decrypted.

Ransomware Infection To Encryption

seccomglobal.
The Cyber Security Company



Who Gets Attacked?

Ransomware is a decidedly opportunistic attack, and as such, no business is safe. Attacks are on the rise across the board in a variety of sectors and a variety of business sizes.

While Windows Endpoints are the most attacked, there are versions for Mac and Linux on the rise as well, so it pays to be vigilant.

Ransomware has unfortunately become so prevalent and arbitrary that for most businesses, it is a certainty that they will be a victim of ransomware at some point.

The best solution is to be prepared. Undertaking preparation and prevention measures will be the key to mitigating an attack effectively.

How to Respond to a Ransomware Attack

While prevention is the first line of defense, what should you do if an attack does occur?

---

1. Set Up a Quarantine

Prevent the infection from spreading by isolating all affected infrastructure.

The first thing to do when a computer is suspected of infection is to isolate it from other computers and storage devices, as well as the network and internet. Crypto worms actively seek out connections and other computers, so you want to prevent that happening. You must also stop the ransomware from communicating with its control centre.

Remember also that the ransomware may have entered your network through multiple routes or endpoints or may be inactive on some systems. The best way forward is to treat all endpoints as infected.

2. Identify the Ransomware

The ransomware will usually identify itself in the ransom request. If it does, there are several sites that can help you identify ransomware.

Identifying the ransomware helps you investigate how it functions, what types of files it encrypts, and any options there may be for removal.

3. Determine Your Options

You usually have three options at this point:

- Pay the Ransom
- Try to remove the malware
- Restore a clean version of your data in a fresh environment (recommended)

Your options, though, will ultimately be determined by whether you have backups you can restore from.

If you do, you should initiate restoration into a clean environment separate from any infected networks as detailed in Step 5.

If you do not have backups – your options may be limited. There are internet sites and software packages that claim to be able to remove ransomware – however, whether you can successfully and completely remove an infection is up for debate. Decryptors can be hit and miss and only work on more common ransomware, rather than newer versions.

Payment of the ransom is most definitely not a recommendation where possible, but this will depend on what options you must work with.

Ultimately, restoration into a fresh environment is the preferred method.

4. Restore and Refresh

- The surest way to be certain that ransomware has been removed is to do a complete wipe of all storage devices and reinstall everything from scratch. Formatting the hard disks in your system will ensure that no remnants of the malware remain.

- If you have a solid backup solution in place, you will have copies of your data from prior to the infection occurrence.

- It’s important to understand the date of infection as closely as you can. Select backups from prior to the date of the ransomware infection.

- If you have both local and off-site backups (3:2:1 rule) you should be able to use backup copies that you are sure were not connected to your network after the time of attack and hence protected from infection. Backup drives that were completely disconnected should be safe, as are files stored in the cloud.

Understanding How it Happened – Post Attack Assessment

- In order to mitigate the risk of further attack, it is important to understand how the attack occurred and what you can do to help prevent it from happening again – or at the least make recovery easier!
- This may include user education about malicious links, websites, or email attachments in addition to security measures on your network.
- It may also include an upgrade or changes to your current back strategy – or the introduction of one if none were in place!
- It's also crucial to know the entry points into your network to better understand how to mitigate risk – these entry points to your systems are known as "attack vectors".
- Attack vectors can be either human attack vectors or machine attack vectors.

Human Attack Vectors

Human Attack Vectors are essentially the ways in which human behaviour is exploited to help deploy malware.

Some common examples are:

1. Phishing

Phishing uses fake emails to trick people into clicking on a link or opening an attachment that carries a malware payload. The email might be sent to one person or many. Sometimes the emails are targeted to make them seem more credible, but often they are opportunistic, and relying on users being complacent or distracted.

Often, the attackers take the time to research the individual targets and businesses, so their email appears legitimate by making the subject credible or relevant to the user or the business. This more targeted technique is known as spear phishing.

2. SMSishing

SMSishing uses text messages to get recipients to navigate to a site or enter personal information on their device. These are becoming more and more common.

3. Vishing

In a similar manner to email and SMS, vishing uses voicemail to deceive the victim. The voicemail recipient is instructed to call a number that is often spoofed.

4. Social Media

Social media is a powerful tool to get a victim to open a downloaded image or file.

5. Instant Messaging

User accounts can be hacked through instant messaging and used to distribute malware to the victim's contact list. This technique is one of the methods previously used to distribute the Lucky ransomware.

Machine Attack Vectors

The other type of attack vector is machine to machine. Humans are involved only in the sense that they might facilitate the attack by visiting a website or using a computer, but the attack process is automated and doesn’t require any human actions to invade your computer or network.

- **1. Drive-by**

• Drive-by earned its name because all it takes for the victim to become infected is to open a webpage with malicious code in an image or active content.

- **2. System Vulnerabilities**

• This is where the vulnerabilities of specific systems are exploited to install ransomware. This mostly happens to systems that are not patched regularly with new security software updates.

- **3. Malvertising**

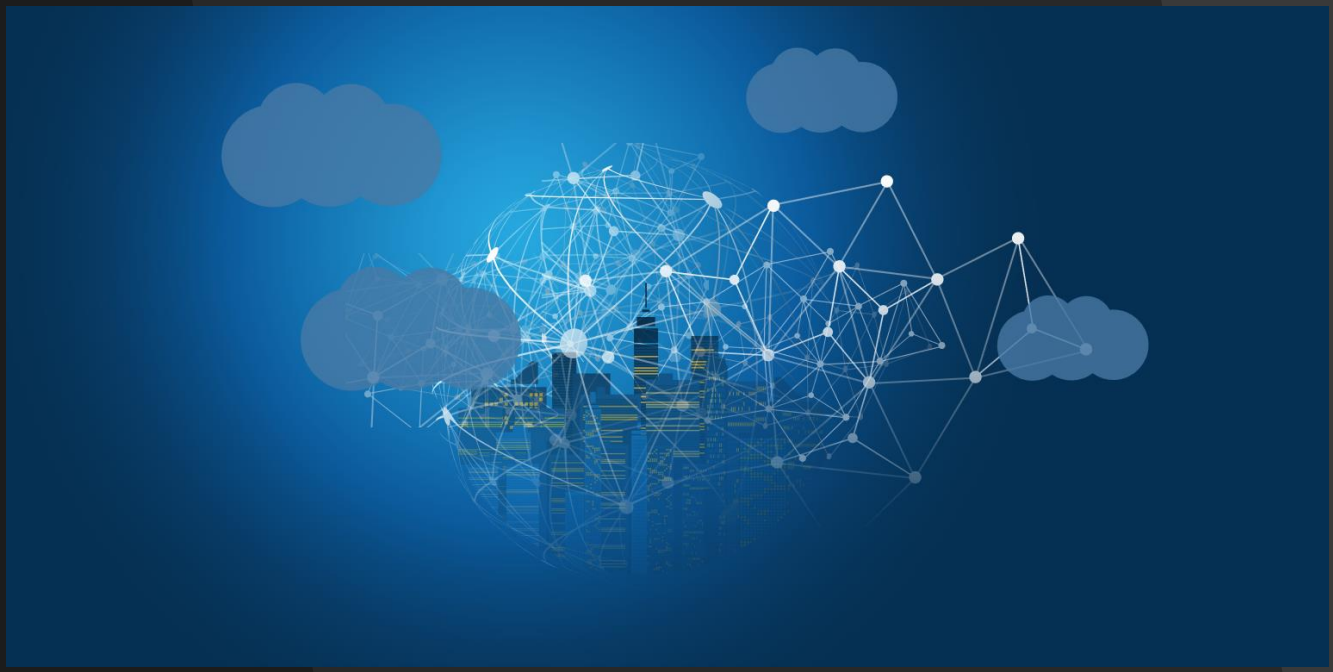
Malvertising is like drive-by but uses ads to deliver malware. These ads are often on search engines or popular social media sites – or commonly, on porn sites!

- **4. Network Dissemination**

This occurs when ransomware deploys and then scans for file shares and accessible computers. Once these are identified, it spreads itself across the network. It generally spreads continually until it is stopped at security controls – so the laxer the security is, the further it propagates.

- **5. Via Shared Services**

Cloud services such as file sharing or syncing services can be used to distribute ransomware. If the service is set to automatically sync when files are added or changed (which many file sharing services are) then malware can be spread quickly.



Measures to Mitigate Against Future Attacks

There are several measures you can take to effectively work to prevent a ransomware attack.

1. Use effective endpoint EDR software on your endpoints (including all servers) – preferably on that can block known payloads from launching.
2. Have an efficient and reliable backup solution in place – preferably employing the 3:2:1 rule (3 copies of your data, in 2 locations, 1 being offsite).
5. Ensure patching is kept up to date! Install the latest security updates issued by software vendors in a timely manner.
7. Educate your users to exercise caution and have a security mindset, such as using caution when opening email attachments and links. It is recommended that you have an ongoing education strategy in place to keep security front of mind.
8. Segment your networks to keep critical endpoints isolated and to prevent the spread of malware in case of attack. Turn off unneeded network shares.
9. Ensure strong access controls and permissions are in place. Give users the lowest system permissions they need to do their work.
10. Restrict write permissions on file servers as much as possible.
11. Install a good SIEM or Monitoring Solution to detect early and give visibility into threat activity.

As we have mentioned several times in this article – prevention is the best possible mitigation strategy for any cyber-attack.

It important that you have a robust backup and recovery solution in place, you employ network segmentation and ensure endpoints have a leading-edge security agent installed for detection and response. It is also crucial to have the visibility that a monitoring or SIEM solution can provide, and that you ensure patching of your systems is carried out regularly. Lastly, you simply MUST educate your users – they remain the most significant risk to your business!

seccomglobal.
The Cyber Security Company