EMIS
connecting healthcare

CYBERFORT

Facing down the ransomware threat

By Pankaj Mistry, CISO – EMIS Group
(CITP, CISM, CRISC, CISA, Associate-IFS)

Contents

Introduction

For any organisation - big or small, public or private - being held to ransom from Ransomware attack is a 'nightmare situation'. Why? Because it has a crippling effect on the target organisation, and impacts on the services it may provide, as well as the subject of the data that was encrypted by the attackers.

Ransomware is:
"A type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return."
[FBI]

FBI - source https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware]

Background

Ransomware is one of the ever-growing categories of cybercrime that now affects organisations of all kinds across the world. While organisations from both the private and state sector are on high alert due to the security impact of the Ukraine conflict, ransomware is a very distinct form of cyberattack. It evolved out of the initial wave of cybercrime that included phishing, ID theft, and distributed denial of service (DDoS) attacks.

It's a simple concept: criminals deploy malware to a target network to hold its information to ransom. The malware may cause a device to become locked or unusable, or allow criminals to steal, delete, or encrypt data.

It may also involve taking control of your devices to attack other organisations, obtaining credentials that allow access to your organisation's systems or services, and even mining cryptocurrency. The criminals will then demand a ransom in return for restoring access to the affected data.

So, "ransomware" in fact covers a whole range of criminal activity. From locker ransomware, a type of malware that blocks basic computer functions, to crypto ransomware, that aims to encrypt a company's important data, (such as documents, pictures and videos), ransomware relies on companies allowing vulnerabilities in their systems.

Ransomware is a weapon capable of mass destruction and disruption. Unfortunately, the Wannacry days are being resigned to history too soon!

I've put this article together for one purpose only and that is to educate ourselves to become wiser and more prepared about this threat.

As a CISO, it is my responsibility to raise awareness about this subject at senior levels and in the Boardroom. Hopefully this saves you time, as I've tried to pull many aspects of this subject together to help in your own thought process.

https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled

EMIS connecting healthcare

CYBERFORT

What is ransomware?

Simply put, ransomware is advanced 'malicious software.' Lacking regulation in the form of effective international law enforcement, cybercrime has evolved into a rich, industrialized, and highly efficient free market economy. Within this broad market, ransomware is – and is expected to remain – a growing and profitable segment.

While technical innovations have always been a driving force behind the continued growth of cybercrime, business models and operational innovations are also meaningful contributors.

The blossoming "ransomware-as-a-service" market is made possible by increased functional specialisation, and cooperation between different cybercrime providers.

Because ransomware-as-a-service lowers the entry barriers for prospective cybercrime entrepreneurs, it has the very real potential to increase the supply of ransomware operators.

This means that, for legitimate organisations, there will be an increase in threats - because more criminals are going to have-a-go!

What is more alarming is that these developments raise the financial risk due to ransomware — most notably the pattern of cooperation between ransomware gangs (and even the formation of cartels) and the widespread adoption of double- and triple-extortion tactics.

These strategies have the dual effect of increasing the likelihood that a victim will pay (at least one) ransom, and of causing the average ransom amount paid to soar. Unfortunately, raising the financial rewards of cybercrime attracts still more players to the marketplace, and better funds the ransomware operators - fuelling a vicious cycle.

Protecting against determined and well-funded attackers is not going to be easy!

Ransomware Brands

Some well-known Ransomware brands are listed below:

Maze Ransomware

Maze is a strain of ransomware that has been impacting organisations since 2019. Although one main group created Maze, multiple attackers have used Maze for extortion purposes.

In addition to encrypting data, most operators of Maze also copy the data they encrypt, and threaten to leak it unless the ransom is paid. A Maze ransomware infection combines the negative effects of ransomware with those of a data breach, making it particularly concerning for businesses.

Netwalker

Netwalker ransomware is a Windows-specific ransomware that encrypts and exfiltrates all the data it beaches. After a successful attack, victims are presented with a ransom note demanding a bitcoin payment in exchange for a full decryption of the compromised data.

The secret behind Netwalker's ransom pay-out success lies in their double-extortion tactic - a strategy also used by ransomware gang Maze. A sample of the breached sensitive data is instantly published on the dark web as proof of the breach. Victims are presented with this evidence and given an ultimatum to pay the ransom price to avoid publishing more data on the criminal-infested network. The cybercriminals group behind the Netwalker ransomware is known as Circus Spider.

REvil/Sodinokibi

Discovered in April 2019, REvil/Sodinokibi ransomware (AKA Sodin) is a highly evasive and upgraded ransomware that encrypts files and deletes the ransom request message after infection. Sodinokibi shortly became the 4th most distributed ransomware in the world, targeting mostly American and European companies.

The message informs the victim that a bitcoin ransom must be paid. If the ransom is not paid on time, the demand will double. REvil is a perfect example of Ransomware-as-a-Service. It is a cybercrime that involves two groups teaming up for the hack: the code authors who develop the ransomware, and the affiliates who spread it and collect the ransom. This aspect makes Sodinokibi ransomware dangerous for companies of all sizes.

Ryuk

Ryuk (pronounced ree-yook) is a family of ransomware that first appeared in mid-to-late 2018. In December 2018, the New York Times reported that Tribune Publishing had been infected by Ryuk, disrupting printing in San Diego and Florida.

Ryuk tops the list of the most dangerous ransomware attacks. In the CrowdStrike 2020 Global Threat Report, Ryuk accounts for three of the top 10 largest ransom demands of the year: USD $5.3 million, $9.9 million, and $12.5 million. Ryuk has successfully attacked industries and companies around the globe. Hackers call the practice of targeting large companies "big game hunting" (BGH). A Russian cybercriminal group known as WIZARD SPIDER is believed to operate Ryuk ransomware. UNC1878, an Eastern European threat actor, has been behind some healthcare-specific attacks. The deployment of this ransomware is not direct; hackers download other malware onto a computer first. When Ryuk infects a system, it first shuts down 180 services and 40 processes. These services and processes could prevent Ryuk from doing its work, or they are needed to facilitate the attack. At that point, the encryption can occur. Ryuk encrypts files such as photos, videos, databases, and documents – all the data you care about – using AES-256 encryption. The symmetric encryption keys are then encrypted using asymmetric RSA-4096. The hackers leave ransom notes in the system as RyukReadMe.txt and UNIQUE_ID_DO_NOT_REMOVE.txt

SunCrypt Ransomware

SunCrypt is a RaaS (Ransomware as a Service) group that was first seen in October 2019, and was one of the first groups to apply triple extortion tactics to their attacks. Unlike other RaaS groups, SunCrypt runs a small and closed affiliate program. The first version of this ransomware was written in GO, but after C and C++ versions were released in mid-2020, the group became much more active. SunCrypt mostly affects the Services, Technology, and Retail industries. Recently, we have seen the introduction of triple extortion. This is where the first two extortions of file encryption and publication to the world are not enough. If the victim still fails to comply, the ransomware operator will DDOS the victim - making it even more difficult for them to get back up and running.

Lockbit

LockBit functions as ransomware-as-a-service (RaaS). Willing parties put a deposit down for the use of custom for-hire attacks, and profit under an affiliate framework. Ransom payments are divided between the LockBit developer team, and the attacking affiliates, who receive up to ¾ of the ransom funds. Considered by many authorities to be part of the "LockerGoga & MegaCortex" malware family, this means that it shares behaviours with these established forms of targeted ransomware.

Attacks are:

- Self-spreading within an organisation, and don't require manual direction
- Targeted - not scattergunned like spam malware
- Using similar tools to spread, like Windows Powershell and Server Message Block (SMB)
- Able to self-propagate - so it spreads on its own. In its programming, LockBit is directed by pre-designed automated processes. This makes it unique from many other ransomware attacks that are driven by manually living in the network – sometimes for weeks – to complete recon and surveillance.

Wannacry

WannaCry ransomware is a crypto ransomware worm that attacks Windows PCs. It can spread from PC to PC across networks (hence the "worm" component) and then encrypt critical files on a computer (the "crypto" part). The perpetrators demand ransom payments to unlock these files. The name is taken from strings of code detected in some of the first samples of the virus. WannaCry spreads using corporate networks to jump to other Windows systems. Unlike phishing attacks, computer users don't have to click on a link, or open an infected file. WannaCry looks for other vulnerable systems to enter (possibly using stolen credentials), then copies and executes the program – again, and again, and again. So, a single vulnerable computer on an enterprise network can put an entire organisation at risk.

LV

Researchers have discovered that the LV ransomware that has been in use since late 2020 is a modified version of the REvil ransomware binary that is being distributed by a separate threat group. The LV operators have their own payment and leak sites, and seem to have the capacity to set up a ransomware-as-a-service (RaaS) operation. GOLD NORTHFIELD threat actors increased their maturity in the ransomware ecosystem. Without spending resources on ransomware development, the group can operate more efficiently than its competitors and still offers a best-in-class ransomware offering. This means a more profitable business model. Like other current ransomware groups, they maintain leak sites where they publish details about current victims, and threaten to post stolen private data if victims don't pay.

BlackCat

BlackCat engages in "triple extortion" by threatening to launch distributed denial-of-service (DDoS) attacks, if victims do not give in to their demands. This added threat makes it more appealing to potential affiliates – and BlackCat promises a higher percentage of the payout to those who use it. BlackCat is a particularly sophisticated ransomware strain because it is both human-operated and command-line driven, making it difficult for traditional detection tools to alert accurately on its presence within a system. BlackCat is known to use a variety of encryption methods, and has proven adept at getting into networks, and moving in them. To accomplish this, BlackCat almost certainly targets Active Directory (AD). Compromising AD is the default attack vector for modern ransomware attacks. Attackers have total control to move laterally within the organisation, gain administrative privileges, disable security tools, and identify new information to steal, encrypt, or delete to prevent recovery.

Common Attack Tactics

Three of the most common tactics that attackers use to initiate a ransomware attack are:

1

Phishing schemes, vulnerability exploits, and purchasing credentials on the dark web

These have become the most common ways for attackers to gain initial access to your infrastructure. Once they have access, they're free to create a backdoor into your organisation, observe existing security tools and behaviours, then identify your most critical assets to encrypt.

2

Risky apps and software vulnerabilities

The software supply chain has also become a way for attackers to cast a wide net and gain access to a broader number of assets that could potentially be encrypted in the execution of a ransomware attack.

3

Remote Desktop Protocol (RDP) vulnerabilities

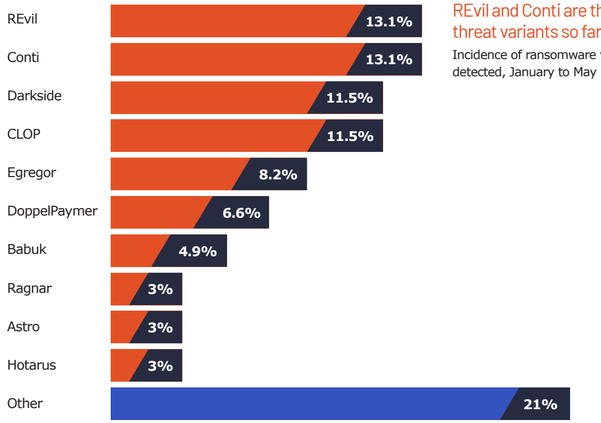
Securing remote access is the most critical way to mitigate the risk of ransomware, and makes it easier to link to the wider security strategy.

EMIS connecting healthcare

CYBERFORT

Behind the Attacks

Recent analysis of the distribution of the malware used in ransomware attacks so far this year, conducted by security provider BlackFog, reveals the top ten ransomware gangs in 2021. Although the identities of group members are mostly unknown, understanding their intentions and ways of operation can help organisations anticipate attacks.



REvil and Conti are the most common threat variants so far this year

Incidence of ransomware variants as a % of threats detected, January to May 2021

Source: BlackFog Global Ransomware Report - May 2021

How Ransomware Works

Unlike legacy ransomware – which was highly automated and largely untargeted – the workflow in today's attacks is largely manual. A threat actor skilfully navigates around defences, customising the attack's tools, techniques and procedures (TTPs) against each and every organisation, based on the victim's environment and assessed value.

Against such a threat, having the best technological defences is necessary, but insufficient. The combination of human attackers and advanced technologies needs a like-for-like defence. No defence is complete without expert hunters to track and stop these attacks.

(Crowdstrike Global Threat Report 2021)

Successful ransomware needs to gain access to a target system, encrypt the files there, and demand a ransom from the victim. Implementation details can change. However, every ransomware variant shares the same core three stages:

Step 1. Infection and Distribution Vectors

Ransomware, like any malware, gains access to an organisation's systems in different ways, but tend to prefer a few specific infection routes.

One of these is phishing emails. A malicious email may contain a link to a website hosting a malicious download, or an attachment that has downloader functionality built in. If the email recipient falls for the phish, then the ransomware is downloaded and executed on their computer.

Another popular pathway takes advantage of services such as the Remote Desktop Protocol (RDP). With RDP, an attacker who has stolen or guessed an employee's login credentials can use them to authenticate and remotely access a computer within the enterprise network. With this access, the attacker can directly download the malware and execute it on the machine under their control.

Others may attempt to infect systems directly, like how WannaCry exploited the EternalBlue vulnerability. Most ransomware variants have multiple infection vectors.

Step 2. Data Encryption

After ransomware has gained access to a system, it can begin encrypting its files. Since encryption functionality is built into an operating system, this simply involves accessing files, encrypting them with an attacker-controlled key, and replacing the originals with the encrypted versions.

Most ransomware variants are cautious in their selection of files to encrypt to ensure system stability. Some variants will also take steps to delete backup and shadow copies of files, making recovery without the decryption key more difficult.

Step 3. Ransom Demand

Once file encryption is complete, the ransomware is prepared to make a ransom demand. It is not uncommon to have a display background changed to a ransom note, or text files placed in each encrypted directory containing the ransom note.

Typically, these notes demand a set amount of cryptocurrency in exchange for access to the victim's files. If the ransom is paid, the ransomware operator will either provide a copy of the private key used to protect the symmetric encryption key or a copy of the symmetric encryption key itself. This information can be entered into a decryptor program (also provided by the cybercriminal) that can be used to reverse the encryption and restore access.

Ransomware kill chain

The term "kill chain" is used in the Cybersecurity community to describe the steps in a cyber-attack. It is helpful to understand these steps so that they can be individually addressed. Stopping ransomware at any point on this chain can completely disable - or at least limit - the damage.

Ransomware typically goes through the following stages of a kill chain to complete an attack:

1 Initial vector infection: Typically, a small dropper file is introduced to an endpoint machine via a malicious website or email attachment.

2 The ransomware code itself is downloaded, installed, hidden, and executed on an endpoint machine.

3 The ransomware code does a quick inventory (directory structure, registry, etc.) of the target machine.

4 If the machine appears to be a likely target, the ransomware code reaches out to a Command & Control server on the Internet for encryption keys to be used.

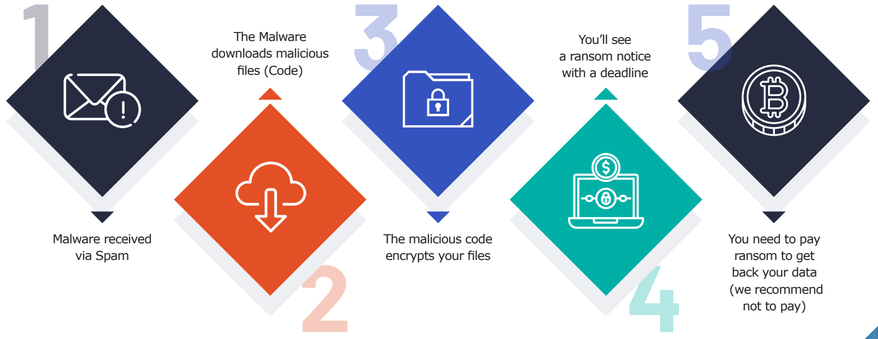
5 The software waits for a period of inactivity, and then begins quietly encrypting accessible files on the local drive and any network drives accessible to the user.

6 The software uses SMB or Domain Controller attacks to infect other machines, to continue the process.

EMIS connecting healthcare

CYBERFORT

How Ransomware Works



Ransomware distribution

The main attack vectors are:

- Email including attachments and URLs
- Compromised RDP and VPN access
- Vulnerabilities in enterprise networking equipment
- Infected websites/links through social media or malware-infected advertising
- Other malware (loaders/stealers) that can infect already-compromised systems with ransomware

EMIS
connecting healthcare

CYBERFORT

What you can do

As leaders of organisations and security practitioners and professionals, we have to protect and defend. Leave the attacking to the government agencies, police, and security services who have the means, intelligence, and the legal and political backing to fight the cyber criminals.

Below are some of the most advocated and best practices to adopt to become more Ransomware resilient:

Prevention and Detection Measures

- Ensure all critical assets are identified. Check all systems that critical data touches as it is stored, processed, or transported through our systems and our suppliers
- Audit the network and challenge unidentified connections and services
- Disable internet-facing systems, services and ports that are not required
- Perform regular vulnerability scans
- Patch systems regularly and prioritise based on criticality
- Harden remote access with layered controls. Closing RDP and patching VPNs can be key to preventing easy access points used to launch ransomware attacks
- Deploy endpoint security software to all endpoints and servers
- Increase the level and regularity of cyber security awareness training. Target teams and vary the level of awareness training
- Ensure everyone knows how to raise an incident or report suspicious activity
- Use network segmentation to subdivide the network. Conventional vlans/subnet configuration doesn't prevent ransomware spread
- Use least-privilege access for all systems and services – use a privileged account management (PAM) tool if necessary
- Allow only authorised software to run

Respond and Recovery Measures

- Ensure Network and Data Flows are documented. This will be needed to work with First Responders
- Monitor the network and endpoints using IDS, EDR, and SIEM
- Make continuous, comprehensive backups and make sure these are offline and immutable
- Have repeatable, rehearsed, and documented processes for restoring computers from clean system images
- Practice restoring systems from backups
- Create a ransomware incident playbook and response plan
- Use the critical asset list to determine what needs to be restored and the order of priority

Cybersecurity practitioner: what to focus on

- Lock down endpoints and prohibit usage of user-installed software - or at least monitor it. Don't allow PowerShell use by end users on Windows endpoints.
- Keep up with Operating System patches and updates on end user machines. Make sure malware signatures are up to date in Endpoint Detection and Response (EDR), and Antivirus (AV). Also maintain currency with firewall rules, intrusion detection systems, and email protection systems.
- Consider an automated Sandboxing tool, or use VirusTotal to detonate possible malware before users can download it.
- Install a secondary keyboard mapping for Cyrillic keyboards on endpoints and servers. To avoid infecting themselves, many ransomware programmers have their code check for Cyrillic keyboards and will not execute on a machine with those keyboards installed.
- Use a Secure DNS provider to block the connections out to known Command & Control Servers on the Internet. Default DNS services provided by your Internet Service Provider (ISP) are typically insecure.
- Block unauthorised connections to the internal network by default.
- Ensure Wireless separation of guest users and corporate usage.
- Maintain multigenerational offline backups of all endpoint and server data and test restoration of backup data regularly.
- Keep up with Operating System patches and updates on file servers and Domain Controllers. Use network segmentation or micro-segmentation to limit network domain access and use Group Access Policies to limit server access. This helps to isolate an attack to one user.
- Continuously collect, monitor, and analyse logs to detect active attacks as quickly as possible. Have a quarantine process in place to isolate infected machines and servers quickly. Baseline typical network and server behaviour to be able to spot unusual activity.
- Understand and manage risk introduced into your systems by third parties including partners, suppliers, user owned devices (BYOD), and customers.

End Users: what to focus on

There are steps that all staff can take to help protect themselves against ransomware attacks. Share the following suggestions with your team.

- Make sure your computer is kept up to date, and follow guidance by your IT staff.
- Don't open unexpected attachments. It's often safer to upload a document or spreadsheet to a file storage system and open it in your browser instead of on your desktop.
- Don't click on suspicious links in emails. If you get an email from a known entity (your bank, for example), type the URL into the browser yourself. Don't trust the link in the email!
- Forward any suspicious emails to the address designated by your IT team to be checked.
- Keep up-to-date with cyberattack techniques with regular cyber-awareness training.
- Do not install unauthorised software. Let your IT team know any software requirements so that they can provide safe, licensed software.
- Don't use your work computer for personal Internet browsing. Even legitimate websites can sometimes be compromised by hackers.
- If you get a warning asking you to install browser add-ons or notifications, do not select it.
- If a ransomware screen pops up, you notice unusual changes in files in your computer, or your computer slows down, you may have an active Ransomware infection.

  You need to act quickly. Disconnect the ethernet cable or disconnect from WiFi, and immediately power down your computer.

  Don't follow the usual software shut-down process. Use the power switch.

  Don't restart your computer - take it to your IT team to fix it instead.

Where and how to get help

The best course of action is to work with a security partner on an 'incident response retainer'. An Incident Response Retainer (IRR) is a service agreement that allows organisations to get external help with cybersecurity incidents.

IRRs are provided by data forensics and incident response (DFIR) specialists and service providers, and vendors offering incident response tools, who have in-house incident response teams. When you purchase a service from a tool vendor, you will typically receive access to their technology as well as incident response services.

There are two main types of retainers:

- **No-cost retainer** – an on-demand agreement with a vendor or service provider that specifies how they will help the organisation respond to an incident if and when an incident occurs. The agreement specifies a service level agreement (SLA), nature of services provided, a procedure for declaring incidents, and a cost per incident, which is paid only if the service provider renders services.
- **Prepaid retainer** – an incident response agreement in which the organisation pre-pays the service provider for a certain number of hours, typically per month or per quarter, which can be used to respond to cyber incidents, with an agreed SLA. If the hours are not used in full, the service provider will typically offer other valuable security services, such as penetration testing or security education for the organisation's staff.

If you take out Cyber Insurance, your broker or insurer will have a panel of incident response partners to work with and often include negotiated rates. The main advantage of a prepaid retainer is that you can use the partner to prepare playbooks for ransomware. You can also test your capabilities, and find ways to improve them, by rehearsing the response and recovery actions.

Depending on the severity of the attack, the National Cyber Security Centre (NCSC) will assist or point you to recommended partners which are published on their website. The NCA (National Crime Agency) are also a go-to organisation in these circumstances.

When dealing with this type of incident there are regulatory and legal aspects to consider in terms of breach notification (ICO) and how that's handled. If your own legal team aren't experts in data breach law, factor in the services of a legal firm who specialise in advising organisations on it. If news becomes public, media relations need to be managed. Legal advisers can play an important part in recommending how to communicate with people affected, and the relevant regulators.

EMIS connecting healthcare

CYBERFORT

To Pay or Not to Pay:

With Ransomware it is a moral dilemma, as well as a legal one. Many organisations do pay!

The official advice will be not to pay the ransom. But, when under threat and with time against you, paying up may be a necessary evil. Consider the following points when you're choosing the best course of action:

- Can you afford the time it takes to recover and get your critical services back up and running?
- What do your investors and shareholders want to do, and what will they tolerate to keep the business running?
- Consider the safety of the customers, if the data is leaked. What are the implications for them?
- Will the authorities and regulators try and punish your organisation for paying the ransom, which could fund criminals, or nation states?

  Bitcoin is usually used to pay ransoms. It can take weeks to set up BitCoin accounts to handle the amounts involved in extortion demands. This is down to Anti Money Laundering controls (AML, KYC) that rule Bitcoin exchanges. This can mean more delays to payments, or more money spent, if you need to ask a broker with verified-accounts to help broker the deal.

There is a lot to prepare. Robust security means resilience. This involves practice, testing, rehearsals, and constant vigilance. You can't hesitate in doing everything you can to prevent, detect, respond to, and recover from ransomware.

References:

Crowdstrike Global Threat Report 2021

TechMonitor Black FogGLobal Ransomware Report May 2021

Comodo SSL Store Ransomware Blog

Get in touch to find out more

cyberfortgroup.com

emishealth.com