SOPHOS

THE RISE OF ENTERPRISE RANSOMWARE

Ransomware attackers are becoming increasingly sophisticated and professional in their approach. They're targeting larger organizations, infecting hundreds of computers within them, and demanding higher ransoms. Furthermore, the costs incurred from the downtime of these attacks are skyrocketing; crippling organizations in the process.

But what has caused this shift in focus towards larger enterprises? Who and what are the main threats? And what security solutions should be in place to safeguard against these types of attacks?

This paper examines the enterprise ransomware landscape, outlines the key threats, and highlights the critical security technologies that every IT setup should include to combat the rise of enterprise ransomware.

A Sophos Whitepaper October 2019

What is enterprise ransomware?

Enterprise ransomware is ransomware is targeted at mid- and large-sized organizations. Public sector organizations, including local government and school districts, are frequent victims. However, private enterprises are also targeted. By attacking organizations with deeper pockets, cybercrooks are looking to increase their financial gains without increasing effort.

This shift towards larger prey has be coined as enterprise ransomware.

A brief history

One of the earliest forms of enterprise ransomware was the infamous SamSam virus. SamSam has secured over US$6million revenue for cybercriminals since its emergence in late 2015. Targeted at medium to large organizations, the largest ransom fee paid by a victim was in excess of US$64,000 – a significantly large amount compared to most ransomware families at the time.

While it is now considered to be dead, SamSam set the benchmark for successful enterprise ransomware. Since then, deadlier copycats are appearing and are demanding higher ransoms than ever. BitPaymer, a particular deadly strain, is known to have plundered in excess of a staggering US$20million from its victims.

The results of enterprise ransomware been devastating with, in some instances, entire cities being held to ransom.

What has caused the shift towards enterprise ransomware?

In terms of execution, you could say that ransomware attacks have come full circle. Early attacks were manual and targeted specific organizations. However, the evolution of technology and near omnipresence of the internet in society led attackers to automate attacks to maximize the probability of success, resulting in the scalable Cryptolocker, Locky, and Teslacypt ransomware variants.

However, with automation comes predictability.

Once you realize that an unexpected email message with a zipped file attachment more likely than not contains something bad, you can take steps to block all emails with zipped file attachments. If you know attackers are likely to use vulnerabilities in Microsoft Word or Excel to infect machines, you patch those applications and operating systems. For good measure, you might disallow users from opening those types of documents if they're downloaded from the internet, or create rules that prevent users from enabling scripting technology like Office macros.

Most mainstream endpoint solutions and firewalls have incorporated these technologies and can now stop these attacks efficiently and effectively.

Attackers are additionally having logistical challenges managing high-volume attacks aimed at low value smaller businesses who struggle to access and pay with Bitcoin, the predominant cryptocurrency used in ransomware demands.

Attackers have therefore reverted to manual, coordinated, highly targeted and therefore unpredictable approaches which are far harder to detect and block. Attacks typically focus on a single organization with the aim of infecting as many internal systems as possible – ultimately bringing the victim to their knees.

This blended threat approach, coupled with access to now highly sophisticated technologies, is proving a deadly concoction for large corporations.

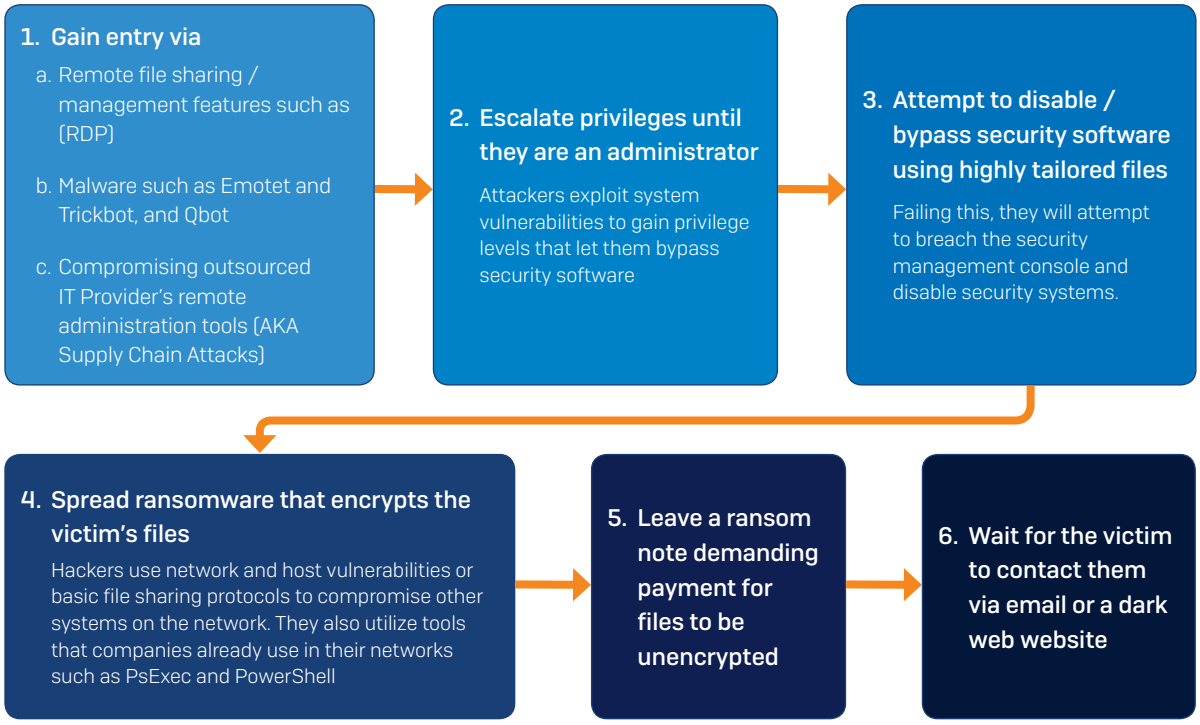
Traditional Ransomware	Enterprise Ransomware
Targets many smaller organizations in each attack	Targets a single medium to large sized organization at a time
Automated, 'fire and forget'	Manual attack
Spread to as many machines as possible	Controlled deployment using admin tools – corrupt as many machines as possible within organization
No particular timing	Timed for maximum impact
WannaCry, NotPetya	BitPaymer, SamSam, Dharma

What does an enterprise ransomware attack look like?

Enterprise ransomware attacks differ quite considerably from 'traditional' automated approaches and typically:

- Take longer to unfold: there's a higher dwell time as the attackers manually traverse the network towards targets
- Are harder to recover from as the attackers take time to:
  - Ensure backups are, in some way, permanently removed
  - Understand the business and attack the most impactful assets
  - Gain deep administrative access to the environment – domain admin, etc. making them much harder to kick out
- Are carefully priced – in some cases the attackers access finance systems first so they know exactly how much the business can afford to pay

A typical enterprise ransomware attack looks like this:



Consequences for falling victim to these attacks can be severe. In addition to the significant downtime and lost business productivity is the ransom demand itself. Ryuk has been known to ask in excess of $5million for encrypted files to be unlocked.

The art of deployment

Enterprise Ransomware is typically deployed using one or a combination of worms, exploiting RDP and manipulating post exploitation tools.

RDP

RDP and other desktop sharing tools like virtual network computing (VNC) are innocuous and highly useful features of most operating systems that allow staff to access and manage systems remotely.

Unfortunately, without the proper safeguards in place, it also provides a convenient inroad for attackers and is commonly exploited by enterprise ransomware. Access is often achieved by use of brute force hacking tools which try hundreds of thousands of login/password combinations until they get the right one and compromise your network.

Malware

Enterprise ransomware is typically deployed by malware that acts as a vehicle for attacks. While there are an innumerable number of malware variants, we've listed the most commonly associated with enterprise ransomware attacks.

Emotet
Emotet first appeared in 2014. Starting off as a Trojan that silently stole banking credentials, it has since evolved into a highly sophisticated platform for distributing other kinds of malware.

Emotet generally arrives on the back of a spam campaign. The emails encourage you to click on a malicious document. Emotet spam began as emails with malicious document attachments but have since evolved into emails with links to malicious documents hosted on websites.

Qbot
QBot (or QakBot) is a multi-purpose network worm with backdoor functions. It spreads over network shares and removable drives. It can steal credentials, information, download additional files and open a backdoor on the infected system. It is typically delivered via an exploit kit.

TrickBot
First seen in late 2016, TrickBot is a banking Trojan which steals banking credentials and posts to its command-and-control server (C2). It is typically delivered via an email spam attachment or exploit kit.

PowerShell Exploitation

Modern attacks aren't just viruses or worms these days. More and more, SophosLabs sees attackers making use of built-in features of Windows to perform the majority of their attack. PowerShell, a scripting tool that's part of Windows, is heavily used by attackers to circumnavigate poor endpoint defenses.

Post Exploitation Tools

Enabled by software tools, post exploitation refers to the operations that take place once a system has been compromised. Essentially, these operations will enable the attacker to determine the value (by gathering intel on data etc.) of the compromised system and ultimately maintain control of it at a later date. These tools were designed for security researchers to emulate cyber-attacks but are being exploited by hackers to great detriment and are very common deployment method during Enterprise Ransomware attacks.

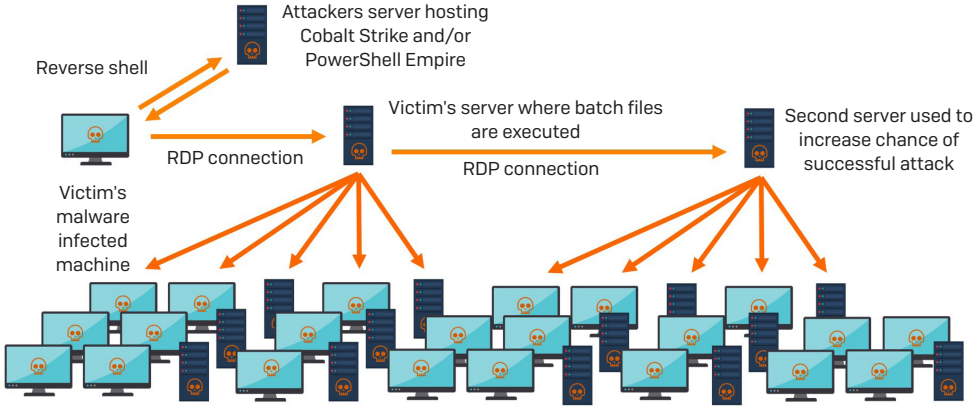
PowerShell Empire

Designed in 2015 as a legitimate penetration testing tool, PowerShell Empire enables continued exploitation once an attacker has gained access. It can be then be used to escalate privileges and harvest data and sensitive information. It can also be used to create malicious documents and files for social engineering attacks such as phishing.

Cobalt Strike

Much like Empire, Cobalt Strike is a commercial, full-featured, penetration testing tool designed to emulate an assailant on a network. Attackers use Cobalt Strike to host their C2 servers, and then deploy malware on company networks through Cobalt "beacons."

Typical enterprise ransomware deployment diagram



Know your enemy

While there are an innumerable number of enterprise ransomware variants, the most successful and well-known strains to date are Ryuk, BitPaymer and MegaCortex. While these examples vary in their scope and complexity, they share many commonalities in their methods.

Ryuk

Photo Credit: Adam B. Morgan, Wikipedia Commons.

Emerging in 2018 and drawing its name from a character in the anime series 'Death Note,' Ryuk represents an evolution in ransomware that's either learning from, building on, stealing from, or paying homage to the targeted malware that's gone before.

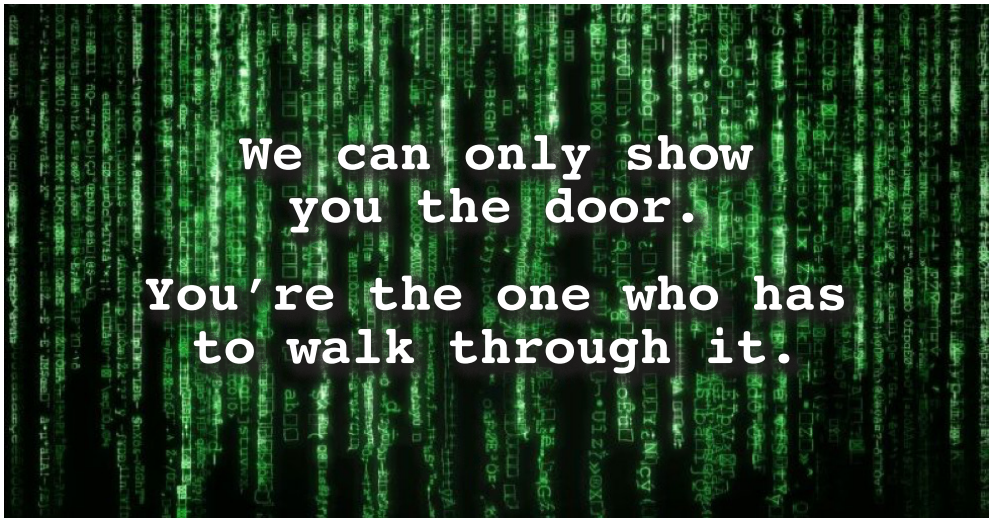
When it's run, Ryuk drops and executes its payload before covering its tracks by deleting itself. The payload cloaks itself by injecting itself into processes run by NT AUTHORITY, taking care to avoid csrss.exe, explorer.exe, and lsass.exe.

To maximize the damage it can cause, the malware tries to shut down a long list of processes and services, such as those associated with security software, before it begins encrypting files.

By excluding particular directories from its encryption, the malware leaves web browsers and basic operating system components untouched. Victims are left with just enough elbow room to read a ransom note, buy some cryptocurrency, and pay a ransom, but not much else.

Hackers using Ryuk work hard to achieve administrator access because it allows their software to cause so much damage – enough that many victims have no option but to pay five- or six-figure ransoms. In fact, in August 2018, Ryuk was known to have made more than US$600,000 inside two weeks.

MegaCortex

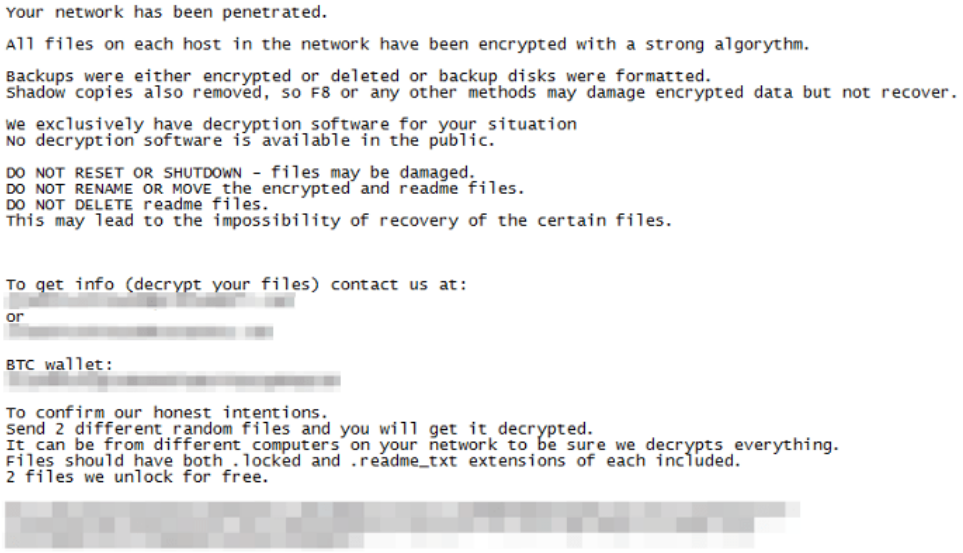


Emerging in early 2019, MegaCortex is a particularly deadly strain that targets enterprise networks and the workstations on them. Dubbed a 'company destroyer,' the ransomware encrypts all accessible Windows endpoints and servers. Attacks are highly tailored to each victim with a three-hour window for execution.

MegaCortex leverages both automated and manual components and appears to involve a high amount of automation to infect a greater number of victims. In attacks Sophos has investigated, the attackers used Cobalt Strike to invoke a meterpreter reverse shell in the victim's environment. From the reverse shell, the infection chain uses PowerShell scripts, batch files from remote servers, and commands that only trigger the malware to drop encrypted secondary executable payloads (that had been embedded in the initial dropped malware) on specified machines.

The group behind MegaCortex interestingly have a fascination with 'The Matrix' films (the name is actually a misspelled homage to the faceless, bureaucratic corporation where the character Neo worked in the first Matrix movie). Ransom notes often read like it was written in the voice and cadence of Lawrence Fishburne's character, Morpheus.

BitPaymer



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at:
[redacted]
or
[redacted]

BTC wallet:
[redacted]

To confirm our honest intentions.
Send 2 different random files and you will get it decrypted.
It can be from different computers on your network to be sure we decrypts everything.
Files should have both .locked and .readme_txt extensions of each included.
2 files we unlock for free.

[redacted]
```

Rearing its ugly head in 2017, BitPaymer is arguably the deadliest of the aforementioned due to its effectiveness and staggering ransom demands which have been known, in some cases, to be in excess of US$1million per victim.

Unique to BitPaymer is its notorious ability to cover its tracks. BitPaymer starts off as a regular ..exe (program) file, but when running, the malware copies itself into not one but two alternate data streams (ADS) where it exists as a sub-component of otherwise empty files.

The malware then transfers control into the new copies of itself in ADS and deletes the more obvious .exe file in which it arrived.

Furthermore, while most ransomware sticks to encrypting your data files, steering clear of your application directories and program files such as .exe files and DLLs, BitPaymer favours a more aggressive approach. The malware encrypts your apps and program files along with your data, although it carefully avoids the Windows folder to avoid messing with the operating system itself.

Beyond ransom fees – the true cost of enterprise ransomware

While it is the typically extortionate ransom fees that make the headlines, both the cost of the downtime inflicted by enterprise ransomware and the reputational damage to businesses are largely understated.

In May 2019, The City of Baltimore was held hostage by ransomware. The attackers demanded 13 Bitcoins – worth around US$100,000. While this fee is staggering, the cost of downtime eclipses this and is estimated to have cost the city more than US$18 million as the attack took down voicemail, email, a parking fines database, and a system used to pay water bills, property taxes and vehicle citations. Real estate transactions were also shut down.

Such downtime of course inflicts heavy reputational damage with corporate security strategies thrown into question and data integrity doubted.

It is therefore of the utmost importance to remain ahead of the game and put in place steps to combat enterprise ransomware.

Best practices to stop enterprise ransomware attacks

There are many methods of mitigation recommended for all types of ransomware, including patching early and often and enabling file extensions. Here are five best practices you can implement to mitigate against enterprise ransomware attacks specifically.

Lock down remote management

RDP is the most commonly utilized deployment method for enterprise ransomware attacks. Locking down your organization's RDP access and other management protocols is one of the most effective steps you can take to secure against targeted ransomware attacks.

There are numerous ways you can do this, such as require users be on a VPN before they can access RDP, or restrict access to known IP addresses. Your organization's firewall should be able to implement both methods.

Back up regularly and keep a recent backup copy offline and offsite

There are dozens of ways other than ransomware that files can suddenly vanish, such as fire, flood, theft, a dropped laptop, or even an accidental delete. Encrypt your backup and you won't have to worry about the backup device falling into the wrong hands.

Monitor your network 24/7

Enterprise ransomware attackers are meticulous when it comes to attacking at the right time of day (or night). To minimize the attack window, it is essential to monitor your network at all times and put in place steps to detect and respond to threats as soon as they are discovered.

One way of achieving this is by implementing a Managed Threat Response (MTR) service. MTR fuses machine learning technology and expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate more sophisticated and complex threats (synonymous with enterprise ransomware attacks).

Educate your workforce

Nearly every strain of enterprise ransomware attack includes a phishing element. Helping your employees to understand how to spot these bogus communications is critical in circumventing malicious access to your networks.

One way of doing this is by setting up regular simulated attacks and monitoring the performance against them. This will allow you to gauge your enterprise's phishing attack readiness and ultimately the level of training required to prepare your employees.

Review the deployment and configuration of your IT cybersecurity implementation

Enterprises often have sufficient technology in place to safeguard against enterprise ransomware attacks, but it rarely deployed or configured in the most optimal way to do its job properly.

Proper deployment and configuration is key to reducing the surface area of attack and minimizing the risk and potential scope of propagation.

General best practices to stop ransomware

The tips above will enable you to safeguard against enterprise ransomware specifically, but there several measures you can take to protect yourself against ransomware attacks in general.

1. **Patch early, patch often.** The sooner you patch, the fewer holes there are to be exploited.
2. **Enable file extensions.** Enabling extensions makes it much easier to spot file types that wouldn't commonly be sent to you and your users, such as JavaScript.
3. **Open JavaScript (.JS) files in Notepad.** Opening a JavaScript file in Notepad blocks it from running any malicious scripts and allows you to examine the file contents.
4. **Don't enable macros in document attachments received via email.** A lot of infections rely on persuading you to turn macros back on, so don't do it!
5. **Be cautious about unsolicited attachments.** If in doubt, leave it out.
6. **Monitor administrator rights.** Constantly review admin and domain admin rights. Know who has them and remove those who do not need them.
7. **Stay up to date with new security features in your business applications**
8. **Use strong passwords.** We recommend making them impersonal, at least 12 characters long, using a mix of upper and lower case and adding a sprinkle of random punctuation Ju5t.LiKETh1s

For further information on the general best practices to stop ransomware, download our white paper entitled How to Stay Protected Against Ransomware.

How Sophos helps to keep your enterprise secure

To stop enterprise ransomware, you need to have effective, advanced protection in place at every stage of an attack.

Stopping attacks get into your network

Sophos XG Firewall is packed with technology to help protect your organization from ever-evolving ransomware attacks. In particular, XG Firewall includes one of the best performing and most effective IPS engines on the market, and provides a simple and elegant solution to lockdown your RDP servers.

XG Firewall offers flexible and easy segmentation tools like zones and VLANs to secure your LAN and reduce the risk of lateral movement, reducing surface area of attack and minimizing the risk and potential scope of propagation.

Securing your endpoints and protecting your servers

Should hackers somehow access your network, Intercept X uses multiple layers of defense to stop ransomware in its tracks. Anti-exploit technology stops the delivery of ransomware, deep learning blocks ransomware before it can run, and CryptoGuard prevents the malicious encryption of files, rolling them back to their safe state. The endpoint detection and response (EDR) functionality within Intercept X additionally detects advanced ransomware attacks that may have gone unnoticed and search for indicators of compromise across your network.

Furthermore, Sophos Managed Threat Response (MTR) enables 24/7 threat response actions to be identified and executed utilizing a fusion of machine and machine intelligence.

Educating on phishing techniques

Sophos Phish Threat sends simulated phishing attacks to your organization, testing preparedness against real world attacks. Emails can be customized to your organization and industry and have been carefully localized for multiple languages. Detailed feedback lets you see how many users failed, overall susceptibility to attacks, and more.

For more information on ransomware visit sophos.com/ransomware.

Try Sophos XG Firewall for free at

sophos.com/xg-firewall

Try Sophos Intercept X for free at

sophos.com/intercept-x

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-10-04 WP-NA (GH)