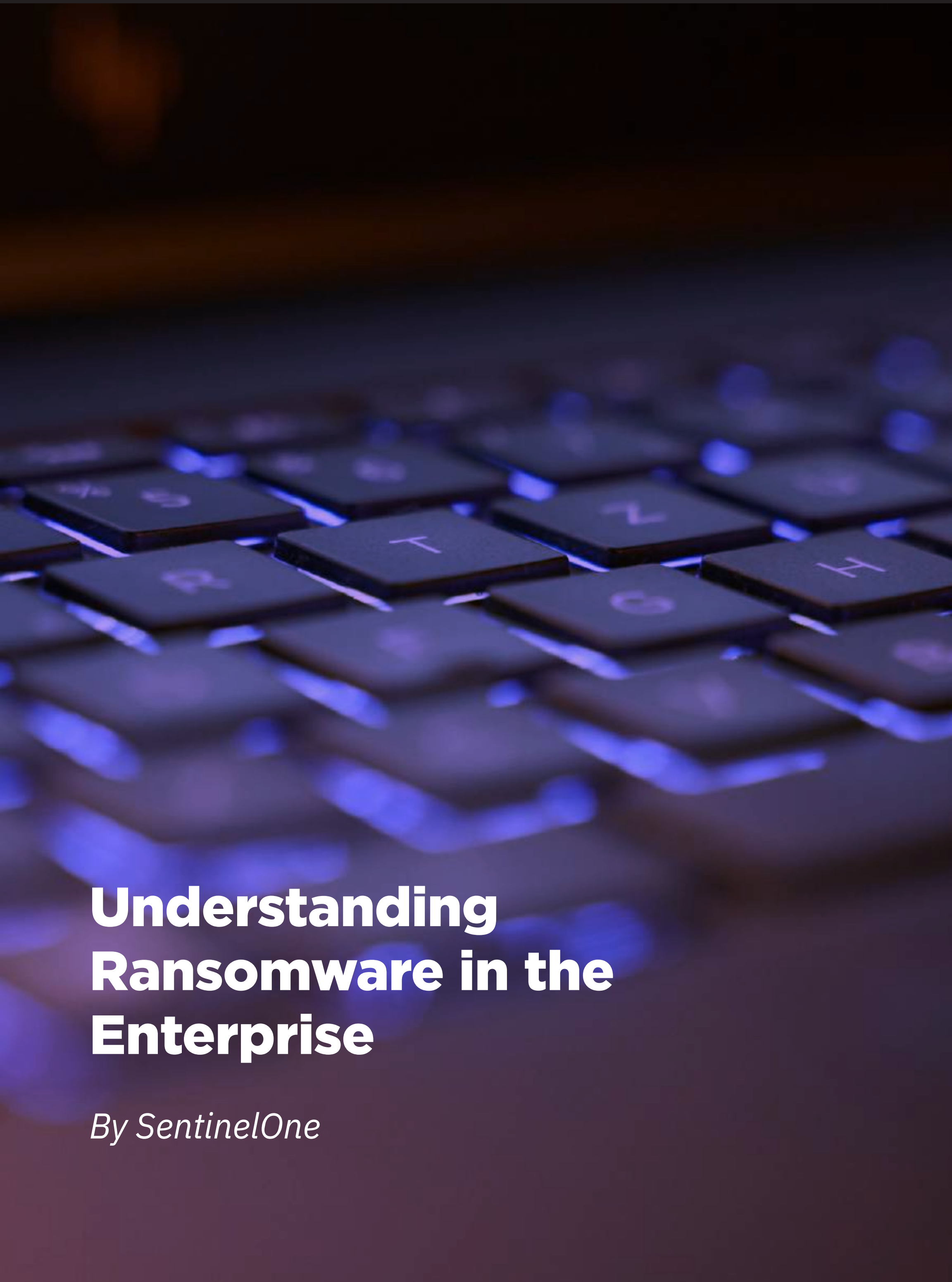
SentinelOne



Understanding Ransomware in the Enterprise

By SentinelOne

Contents

Introduction

Ransomware is a form of malicious software that, when deployed on a device, encrypts a user's sensitive data. In order to secure a decryption key or initiate a decryption process, the victim is required to pay a ransom to the attacker, usually in the form of cryptocurrency such as Bitcoin. The amount demanded by attackers can vary, with ransoms typically in the range of $200 to over $10,000 per endpoint, depending on the size of the enterprise and the value of the data held for ransom.

Ransomware, in concept, can be traced back to the late 1990s and early 2000s with the rise in popularity of "FakeAV" or fake system utilities which "find" false infections or non-existent system issues, then demand (aka extort) fees in order to enable "removal" of these fake artifacts. Eventually, these morphed into threats like PGPCoder and similar. These threats have much in common with modern ransomware, but there was still a weakness in the chain in the form of payment collection, processing, and management. When attackers had to rely on more tangible means of payment through legitimate conduits like Western Union, Perfect Money, and wire transfers, there was far more risk involved. These payment systems were easily traceable and prone to various points of failure.

The rise of cryptocurrency was the answer ransomware and other malware developers had been waiting for. Bitcoin and similar technologies allow for a far simpler, more streamlined and dynamic payment architecture for criminals, who could now use these blockchain-based currencies to control ransom demands over time, and collect and manage all payments digitally. Bitcoin, Litecoin, Monero and others also greatly obfuscate transactions, making it more difficult for law enforcement to tie transactions directly to individuals. Once cyber criminals fully embraced cryptocurrencies, ransomware was propelled into the model we see today.

Aside from demanding payment to decrypt files, ransomware operators may also threaten to publicly leak the victim's data if payment is not made. This complicates the scenario in multiple ways: aside from dealing with the immediate problem of restoring access to files and services, organizations may have to declare a breach incident to regulators, could face regulatory fines, face reputation loss, legal action from clients, and the risk of sensitive data or IP leaking to competitors. All these complications could remain in play regardless of whether the victim actually pays the initial ransom demand.

The SentinelOne Complete Ransomware Guide will help you understand, plan for, respond to and protect against this now-prevalent threat. This guide offers examples, recommendations and advice to ensure you stay unaffected by the constantly evolving ransomware menace.

Understanding the Ransomware Threat

Methods of Infection

Understanding how ransomware infects and spreads is the key to avoiding falling victim to an attack. Post-infection, ransomware can spread to other machines or encrypt network filers in the organization's network. In some cases, it can spread across organizational boundaries to infect supply chains, customers and other organizations.

All of the following can be vectors of infection for ransomware attacks:

1. Phishing
2. Compromised Websites
3. Malvertising
4. Exploit Kits
5. Downloads
6. Messaging Applications
7. Brute Force via RDP

Phishing

Still the most common method for attackers to initially infect an endpoint with ransomware is through phishing emails. Increasingly targeted, personalised and specific information is used to craft emails to gain trust and trick potential victims into opening attachments or clicking on links to download malicious files. Malicious files can look indistinguishable to normal files, and attackers may take advantage of a default Windows configuration that hides the file's true extension. For example, an attachment may appear to be called 'filename.pdf', but revealing the full extension shows it to be an executable, 'filename.pdf.exe'.

Files can take the form of standard formats like MS Office attachments, PDF files or JavaScript. Clicking on these files or enabling macros allows the file to execute, starting the process of encrypting data on the victim's machine.

Compromised Websites

Not all ransomware attacks have to be packaged in a maliciously-crafted email. Compromised websites are easy places to insert malicious code. All it takes is for an unsuspecting victim to visit the site, perhaps one they frequent often. The compromised site then reroutes to a page that prompts the user to download a newer version of some software, such as the web browser, plugin, or media player. If clicked, the ransomware is either activated directly or runs an installer that downloads and runs the ransomware.

Malvertising

If a user has an unpatched vulnerability in his or her browser, a malvertising attack can occur. Using common advertisements on websites, cybercriminals can insert malicious code that will download the ransomware once an advertisement is displayed. While this is a less common ransomware vector, it still poses a danger since it doesn't require the victim to take any overt action such as downloading a file and enabling macros.

Exploit Kits

Angler, Neutrino, and Nuclear are exploit kits that have been widely used in ransomware attacks. Exploit kits are a type of malicious toolkit with pre-written exploits that target vulnerabilities in browser plugins like Java and Adobe Flash. Common ransomware like Locky and CryptoWall have been delivered through this vector on booby-trapped sites or through malvertising campaigns.

Downloads

Any file or application that can be downloaded can also be used for ransomware. While downloadables on illegal file-sharing sites are ripe for compromise, there is also potential for attackers to exploit legitimate websites to deliver an infected executable. All it takes is for the victim to download the file or application and then the ransomware is injected.

Messaging Applications

Through messaging apps like Facebook Messenger, ransomware can be disguised as scalable vector graphics (SVG) to load the file that bypasses traditional extension filters. Since SVG is based on XML, cybercriminals are able to embed any kind of content they please. Once accessed, the infected image file directs victims to a seemingly legitimate site. After loading, the victim is prompted to accept an install, which if completed distributes the payload and goes on to the victim's contacts to continue the impact.

Brute Force Via RDP

Attackers use ransomware like SamSam to directly compromise endpoints using a brute force attack through Internet-facing RDP servers. Remote Desktop Protocol enables IT admins to access and control a user's device remotely, but this presents an opportunity for attackers to exploit it for criminal use.

Attackers can search for vulnerable machines using tools like Shodan and port scanners like Nmap and Zenmap. Once target machines are identified, attackers may gain access by brute-forcing the password to log on as an administrator. A combination of default or weak password credentials and open source password-cracking tools such as "Aircrack-ng", "John The Ripper", and "DaveGrohl" help achieve this objective. Once logged on as a trusted admin, attackers have full command of the machine and are able to drop ransomware and encrypt data. They may also be able to disable endpoint protection, delete backups to increase likelihood of payment or pivot to achieve other objectives.

Ransomware continues to evolve, with ransomware-as-a-service now growing in popularity. Malware authors sell custom-built ransomware to cyber criminals in exchange for a percentage of the profit. The buyer of the service decides on the targets and the delivery methods. This division of labour and risk is leading to increasingly targeted malware, innovation in delivery methods and ultimately a higher frequency of ransomware attacks.

Common, Prevalent and Historic Ransomware Examples

Ransomware comes in all shapes and sizes. Over the last five years we have seen a wide variety of ransomware, with new ones appearing regularly. Below are just a few examples.

WannaCry

WannaCry hit a number of high profile businesses around the world in 2017, including Renault, FedEx and Britain's national health service. It infected Windows computers, encrypting files and crippling many businesses and public organizations such as the National Health Service in the U.K. WannaCry used an innovative attack vector, exploiting a vulnerability in the Windows implementation of the Server Message Block (SMB) protocol which helps various nodes on a network communicate. The worm component spread the infection by scanning for IP addresses of other computers.

GandCrab

GandCrab was released at the end of January 2018 and quickly rose in popularity among cybercriminals, mainly due to its innovative affiliate scheme. It was the first ransomware to be observed using the Dash cryptocurrency for payments rather than the more popular Bitcoin. GandCrab is distributed via the Rig and GrandSoft exploit kits, as well as via email campaigns and compromised websites. Information released by the malware authors stated that "In one year, people who worked with us have earned over US $2 billion," and it is estimated to have infected over a million victims to date. Notably, GandCrab checks for the existence of a keyboard with Russian layout and aborts if found.

Maze

Maze was initially observed in May 2019. Becoming more prevalent throughout 2019, authors claimed credit for attacks on both Allied Financial as well as the City of Pensacola Florida. Maze added a new trick to the ransomware extortion racket, by first exfiltrating the victim's data before encryption. This allows the attacker extra leverage to ensure payment: if the ransom demand is not met, the attackers dump part of the victim's sensitive data to a public repository. The data may contain confidential intellectual property, or more commonly PII of the victim's customers, thus setting up the possibility of further financial penalties in the form of severe reputation loss and/or lawsuits.

RobinHood

The RobinHood (aka 'RobbinHood') ransomware was previously used in the high-profile infection encrypting computers of large government entities like the City of Grenville and the City of Baltimore. The ransomware does not spread within the network. It drops all Windows shares, which likely means that the ransomware is pushed on each machine individually after the initial network breach. Whilst the ransomware does not appear sophisticated, it is typically deployed as part of a well-planned and orchestrated network intrusion, and consequently results in high payouts with individual ransoms set per machine.

Cerber

Cerber emerged in early 2016 as a highly-exclusive RaaS. It differed from more common 'public' ransomware services in terms of vetting clients and the granting of affiliate access. The platform was designed to offer ransomware distributors efficiency and automation, making operation, management and payment processing and manipulation very streamlined. Delivery was typically achieved via spam/phish email or drive-by downloads, though it was also seen used in conjunction with various exploit kits (e.g., RIG). Cerber is also known for additional features such as discovery and theft of cryptocurrency wallets.

Ryuk

Ryuk has been responsible for numerous high-profile attacks over the last few years. This includes a 2018 attack on the Los Angeles Times. It has also been associated with (though not exclusively) the Lazarus group (DPRK). Ryuk is known to be particularly aggressive in terms of speed-of-encryption as well as additional measures to cripple defenses and recovery options on machines. Ryuk, like other ransomware families, will attempt to terminate processes known to be associated with endpoint security products. This is in addition to the deletion of backup Volume Shadow Copies (VSS). Such features are not exclusive to Ryuk; however, combined with the prolific nature of Ryuk's infections, it has proven to be a powerful and dangerous combination. Over the years, the actors behind Ryuk have collected millions of dollars in profit.

CryptoLocker

CryptoLocker was first reported in late 2013 and was one of the first to employ the encryption/ransom technique. Originally, it also gave victims only 72 hours to make payment before the decryption key was permanently deleted. CryptoLocker made a point of targeting businesses specifically, and file encryption was focused on business application files belonging to Microsoft Office and Adobe products. Famously, one of CryptoLocker's early victims was the Swansea Police, who themselves were forced to pay a ransom to recover their own data.

TeslaCrypt

TeslaCrypt was detected in February 2015. Originally, it targeted computer game data such as games saves and player profiles. Early versions of TeslaCrypt were also found to be decryptable by security researchers. Newer variants of TeslaCrypt were not focused on game-related data and also encrypted JPEG, PDF, and other file types and closed the programming flaw that made it possible to create public decryptors.

Locky

Locky was first discovered in February 2016. Distributed through malicious email attachments, it encrypts files and renames them with the .locky extension. Locky ransomware also deletes any VSS backup ‘shadow’ copies of original files made by the Windows operating system and changes the computer’s desktop wallpaper to an image file displaying the ransom message with details of how to pay.

NotPetya

NotPetya hit the news in 2017, rapidly spreading to affect a wide range of organizations across 65+ countries, drawing comparisons with the WannaCry attack. While it shows characteristics similar to ransomware, NotPetya is more akin to a wiper, which is generally regarded as a kind of malware responsible for destroying data on the target’s hard disk. NotPetya infects the master boot record (MBR) and prevents any system from booting. Even if the ransom is paid, however, the damage from NotPetya is irreversible, so it is likely that the actor’s aim was to sabotage the infected system rather than gaining money out of it.

Samsam

Samsam ransomware was first seen in 2015 and has been increasingly used in targeted attacks on healthcare, schools, and other networks containing valuable sensitive information. Samsam is unique because it infects servers directly using a vulnerability in Red Hat’s JBoss enterprise products. Attackers use tools like JexBoss, an open-source penetration testing tool, to identify unpatched vulnerabilities in JBoss application servers. Having gained access to a system, the operators move laterally from the entry point to identify more hosts and manually deploy more ransomware. Samsam deletes shadow copies after encrypting the original files.

CryptoWall

Cryptowall was first discovered in June 2014, and primarily distributed through emails with ZIP attachments in order to bypass blacklisting from anti spam email security solutions. A commonly used trick with CryptoWall ransomware is to rename an .exe file as a .scr or .pif file, and then zip it, as Windows usually will still execute such files normally. Users may suspect that a .exe could be malicious, but few users are aware of other executable extensions. CryptoWall encrypts files and deletes any VSS or shadow copies to prevent data recovery.

REvil

Used in targeted ransomware attacks throughout 2019, REvil ransomware hit one of America’s largest data center providers, CyrusOne. It is also believed to have been used in the Travelex breach on New Years Eve, 2020, when criminals demanded a ransom of $3m. With the apparent retirement of Gandcrab, affiliates are looking for a new tool and this is increasingly looking like a similar affiliate set up. It may build on GandCrab source code and business model, but REvil campaigns can differ in skills and tools due to the different affiliates operating these campaigns.

Snake

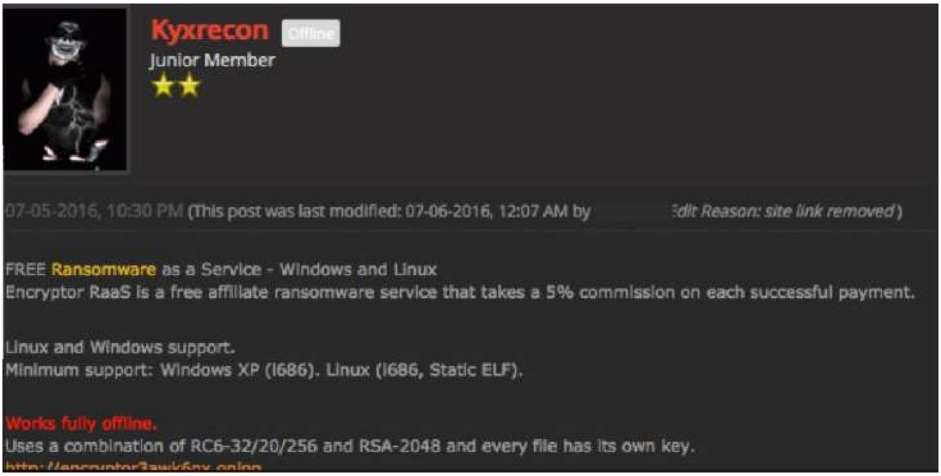
First appearing in January 2020, Snake (aka Ekans) ransomware is written in Golang and is capable of cross-platform infections. Large-scale targeted campaigns have hit healthcare organizations across the world, with a sustained campaign occurring throughout May 2020. Snake has been known to target ICS systems and supporting environments. Snake infections come equipped with a hard-coded process ‘kill list’ to terminate any process or applications that either interfere with its encryption routines or the collection of data.

Early Snake campaigns included many ICS-specific processes in these lists, leading many to view Snake as an ICS-specific threat. That is not entirely the case, as the kill-list can be customized for any environmental requirements. As with other recent variants of ransomware, Snake attempts to also exfiltrate victim data prior to encryption. Victims that refuse to comply with the ransom demand within 48 hours are threatened with a data leak.

The Ransomware as a Service (RaaS) Model

Throughout 2019 and into 2020 there was an increasing trend by some of the above as well as new ransomware families of selling ransomware as a service to other cybercriminals. In particular, Maze, REvil, NetWalker, Nephilim, Project Root, SMAUG and others began following the RaaS model.

This model is far from new, however. Between 2014 and 2015 RaaS services gained a great deal of momentum, at least in the context of non-exclusive and lower-tier ransomware families. Starting with TOX, a whole new generation of RaaS offerings offered non-skilled criminals a way into the thriving ransomware economy. TOX quickly imploded under the high-demand of interested criminals, as well as the attention from the security industry. However, many new services were quick to pick up on the trend. Services such as Ransom32, Nemes1s, SATAN, Encryptor RAAS, and more quickly rose up to fill the demand.



Kyxrecon Offline
Junior Member
★★

07-05-2016, 10:30 PM (This post was last modified: 07-06-2016, 12:07 AM by Edit Reason: site link removed)

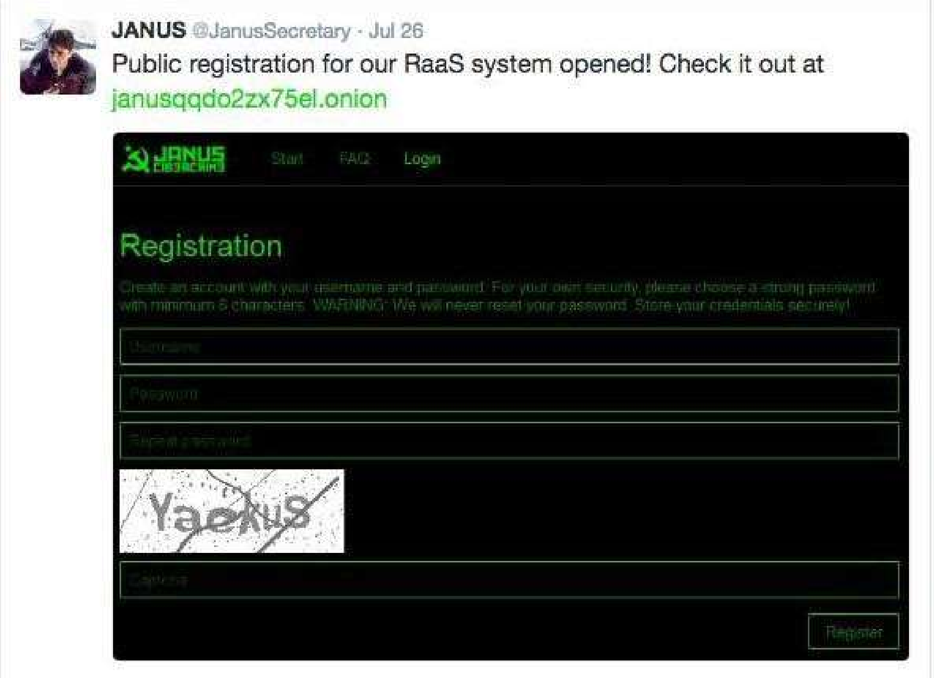
FREE Ransomware as a Service - Windows and Linux
Encryptor RaaS is a free affiliate ransomware service that takes a 5% commission on each successful payment.

Linux and Windows support.
Minimum support: Windows XP (I686). Linux (I686, Static ELF).

Works fully offline.
Uses a combination of RC6-32/20/256 and RSA-2048 and every file has its own key.
http://encryptor3awk6px.onion

Eventually more sophisticated efforts embraced the RaaS model as well. For example Petya started out as a highly-destructive and closed ransomware ecosystem.

However, they eventually opened up the system as a full public RaaS, allowing anyone to create an account and generate their own Petya or Mischa payloads for zero cost up front. These services eventually evolved into GoldenEye.



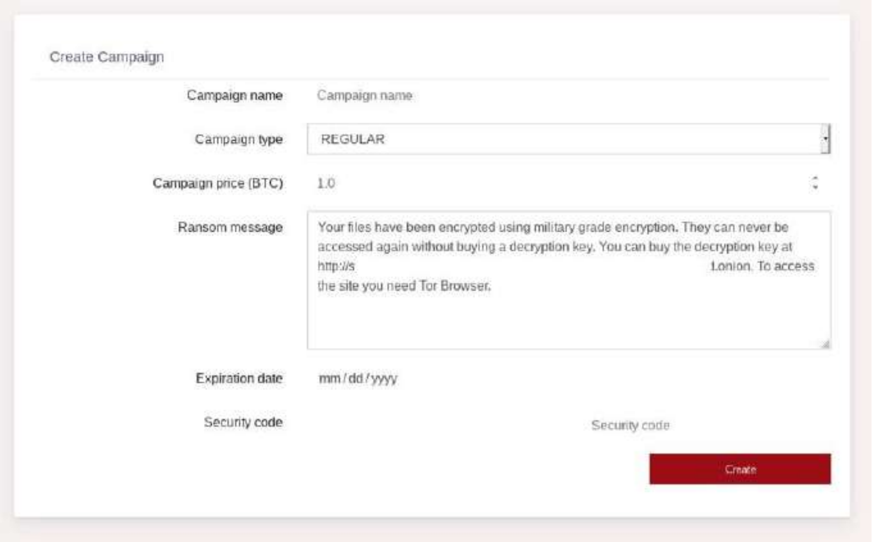
JANUS @JanusSecretary · Jul 26

Public registration for our RaaS system opened! Check it out at janusqqdo2zx75el.onion

Registration

Create an account with your username and password. For your own security, please choose a strong password with minimum 6 characters. WARNING: We will never reset your password. Store your credentials securely!

Although the idea of RaaS has an established history, it has become increasingly preferred during 2019/2020. RaaS services offer an attractive way for enterprising criminals to create, distribute, and manage their ransomware and subsequent profits with almost no barrier to entry. Buying ransomware as a service requires no prior coding or development knowledge, provides instant results and is cheap to launch. Typically, these services either require an up front payment from clients or a share of the profits once the victims pay.

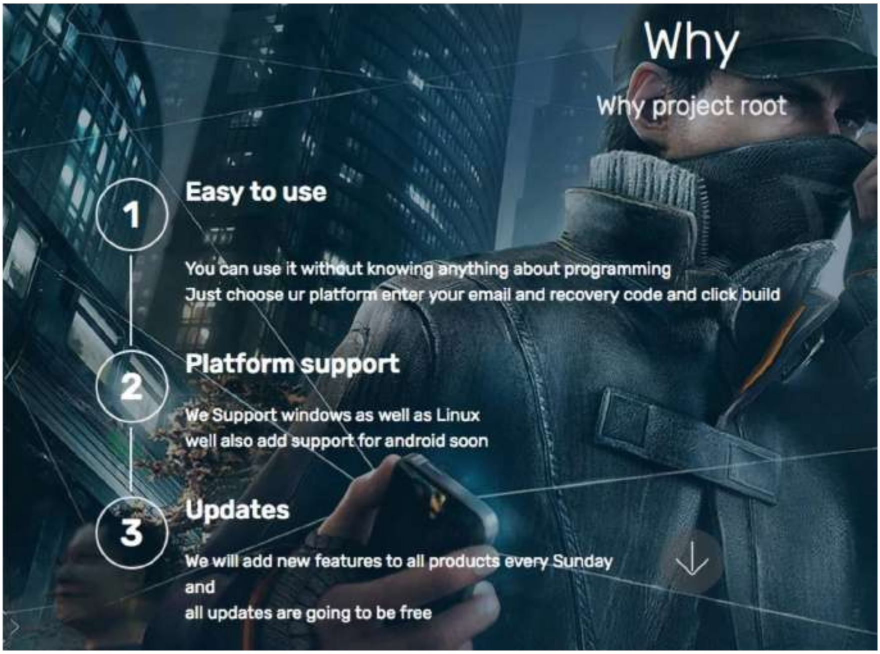


Create Campaign

Campaign name	Campaign name
Campaign type	REGULAR
Campaign price (BTC)	1.0
Ransom message	Your files have been encrypted using military grade encryption. They can never be accessed again without buying a decryption key. You can buy the decryption key at http://s 1onion. To access the site you need Tor Browser.
Expiration date	mm / dd / yyyy
Security code	Security code

Image of a panel from SMAUG RaaS

For ransomware developers the benefits are that they do not need to directly concern themselves with either the risk or the trade-craft of finding and infecting targets. This division of labor and craft means criminals with different areas of expertise and interest can effectively combine their skills to make attacks more efficient and more profitable.



Why

Why project root

1 Easy to use

You can use it without knowing anything about programming
Just choose ur platform enter your email and recovery code and click build

2 Platform support

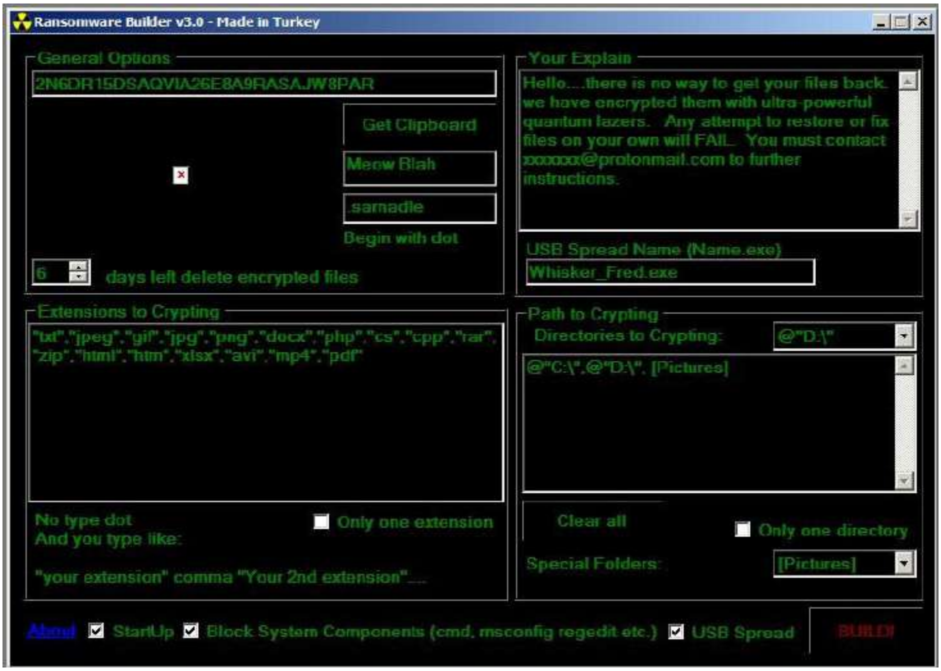
We Support windows as well as Linux
well also add support for android soon

3 Updates

We will add new features to all products every Sunday
and
all updates are going to be free

Image from Project Root Raas advertisement

Another tier worth mentioning in the RaaS discussion is that of generic ransomware “builders’ or kits. These are sort of the ‘bargain bin’ intersection of ransomware and RaaS models. They allow unskilled attackers to generate their own ransomware payloads, but they do not include any of the hallmark features of a full RaaS. These kits are simply applications that output new ransomware binaries. Many are based on open-source ransomware “experiments” (for example, Hidden Tear).



2N6DR15DSAQVIA26E8A9RASAJW8PAR

Meow Blah

.samadle

Begin with dot

6 days left delete encrypted files

Hello....there is no way to get your files back. we have encrypted them with ultra-powerful quantum lazers. Any attempt to restore or fix files on your own will FAIL. You must contact xxxxxx@protonmail.com to further instructions.

USB Spread Name (Name.exe): Whisker_Fred.exe

"txt","jpeg","gif","jpg","png","docx","php","cs","cpp","rar","zip","html","htm","xlsx","avi","mp4","pdf"

No type dot
And you type like:

"your extension" comma "Your 2nd extension"....

□ Only one extension

Directories to Crypting: @"D:\"

@"C:\",@"D:\", [Pictures]

□ Only one directory

Special Folders: [Pictures]

☑ StartUp ☑ Block System Components (cmd, msconfig regedit etc.) ☑ USB Spread

The Ransomware “Kill Chain”

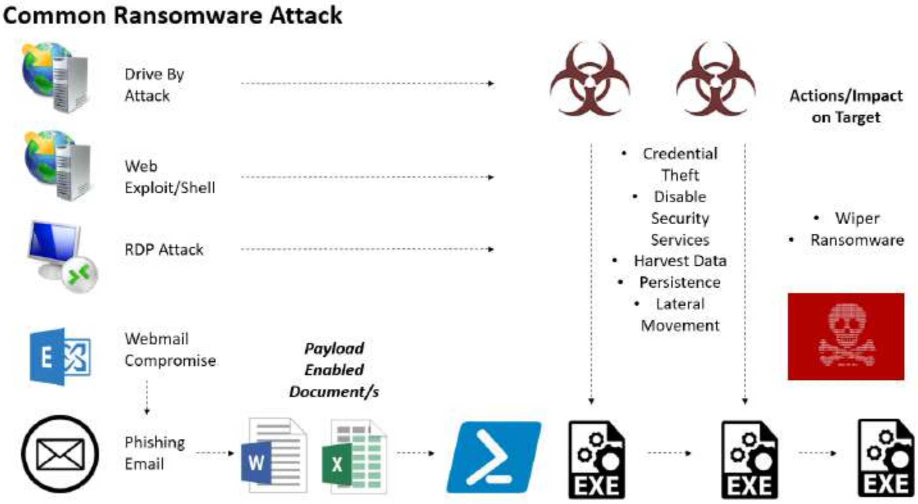
Ransomware, while unique from other malware, still exhibits several tell-tale signs which can indicate that an attack is underway. The MITRE ATT&CK framework provides a common language for defenders to better understand the elements of attack, detect an attack and prepare for it by discovering if they could defend against such a threat.

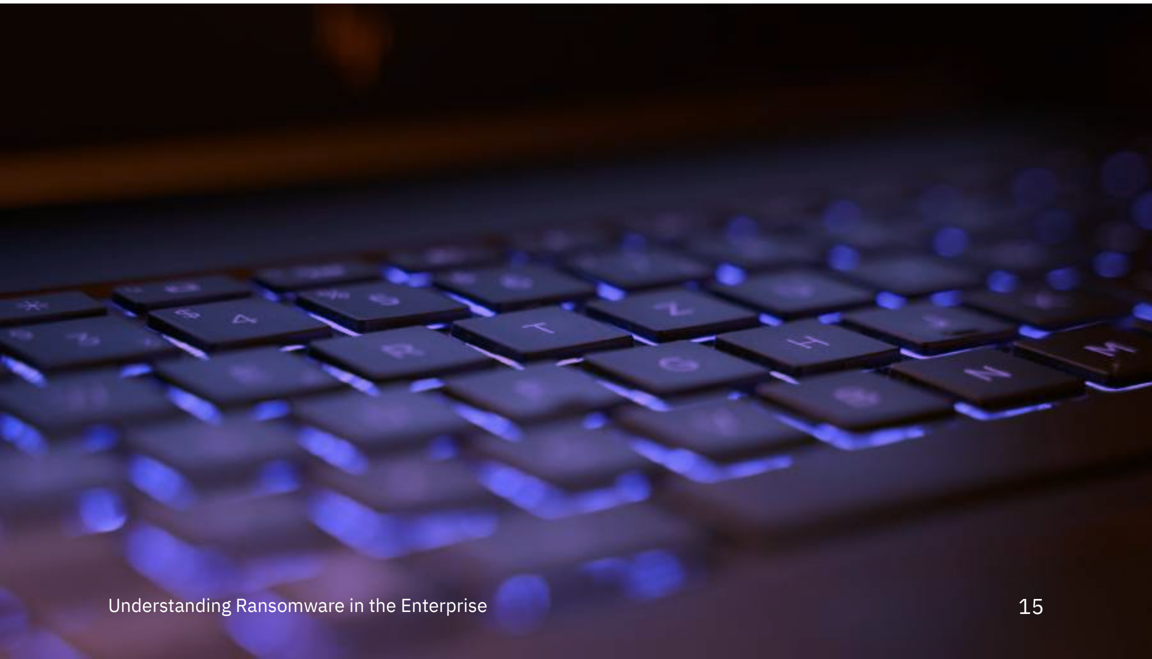
In line with the MITRE ATT&CK framework, the following offers a high level flow of events in a typical ransomware attack.

- TA0001 **Initial Access:** The adversary is trying to get into your network.
- TA0002 **Execution:** The adversary is trying to run malicious code.
- TA0003 **Persistence:** The adversary is trying to maintain their foothold.
- TA0004 **Privilege Escalation:** The adversary is trying to gain higher-level permissions.
- TA0005 **Defense Evasion:** The adversary is trying to avoid being detected.
- TA0006 **Credential Access:** The adversary is trying to steal account names and passwords.

- TA0007 **Discover:** The adversary is trying to figure out your environment.
- TA0008 **Lateral Movement:** The adversary is trying to move through your environment.
- TA0009 **Collection:** The adversary is trying to gather data of interest to their goal.
- TA0011 **Command and Control:** The adversary is trying to communicate with compromised systems to control them.
- TA0010 **Exfiltration:** The adversary is trying to steal data.
- TA0040 **Impact:** The adversary is trying to manipulate, interrupt, or destroy your systems and data.

A common high level attack may look similar to the following:





Planning for a Ransomware Incident

You should prepare for a possible ransomware incident by creating all the relevant components for an incident response management process. You need to consider specific ransomware responses and recognize that existing IR plans might not be applicable to ransomware incidents due to the combined possibilities of encryption, loss of access to critical system files and services and data breach notification issues.

Development throughout 2019 and early 2020 made it clear that most ransomware infections would now need to be treated as possible full data breaches, including all the regulatory and legal requirements around breach notification and open disclosure. This includes understanding relevant regulatory fines and penalties such as GDPR, and tying that assessment into risk management processes and calculations. The permanent inaccessibility and damage to important files may also lead to specific challenges that need to be considered in order to restore business continuity.

With that context in mind, there are six key elements which should be considered when planning and preparing for a ransomware incident:

Incident Response Policy

When writing an effective incident response policy to deal with ransomware, the six-step SANS process for incident handling provides a useful place to start. Considering what you would do if you were attacked forms the basis of the policy and gives you a framework to follow in response.

The six steps of the Incident Response Policy are:

- Preparation phase:
  - How are staff trained and prepared? What tools and resources are they armed with to respond to ransomware incidents? Consider awareness and education for users here.
- Identification phase:
  - How do you recognize and detect a ransomware incident? How do you go about understanding the strain of ransomware, attack vector, attack group and real motivation, through gathering data and performing initial analysis?

- Containment phase:
    - With ransomware it is imperative that infected systems are quickly contained to limit the damage. How will you contain the incident from spreading to network shares and other connected devices? Actions to consider include:
        - Shutting the system down
        - Turning off the system's port at the switch
        - Utilizing network access control (NAC) to isolate the system
        - Implementing the quarantine feature of your EDR solution
- Eradication phase:
    - How will you perform a forensic analysis of data to determine the cause of the incident, remove the ransomware from infected devices, patch vulnerabilities and update protection? Ransomware might not be the only malware on the system, just the noisiest. Consider that the detected attack may be a pivot or diversion, so include wider forensic analysis and methods to assign attribution in order to uncover and respond to what might be a wider campaign.
- Recovery phase:
    - How will you return to normal operation? Reimaging or restoring from backup may not work if the ransomware lay dormant during the last image or backup cycle, or if part of the ransomware attack was to seek and destroy back-ups. With ransomware you should consider
        - How to identify and decrypt using communities like Nomoreransom
        - How to quickly and easily rebuild affected devices and servers
        - Whether payment is an option. Can you pay, do you have access to Bitcoin, do you need a middleman?
- Post-Incident phase:
    - After the incident is resolved, what can you learn to prevent it from happening again in the future?
        - How will you document the incident? Detail improvements to IR plans, additional security controls, preventative measures or new security initiatives.
        - How can you monitor to stop repeat performances or further connected activities? What IOCs do you need to collect and how do you use them in any monitoring technology?
        - How can you improve and update organizational threat intelligence feeds?
        - How will you understand and quantify the financial impact on the organization, in terms of manhours, business down time, regulatory fines and possibly ransoms paid?

We discuss responses to these challenges in the Responding to a Ransomware Incident section later in this guide.

Recruitment

Teams assembled to deal with ransomware may need specific skills, knowledge and access to relevant system tools and technologies in order to effectively detect, investigate and respond. This may include outsourced help as well as non-technical staff like executives, PR and media teams. You may need links to legal teams, regulators and law enforcement as specific responses like paying the ransom need to be considered.

Define Roles and Responsibilities

Prepare documentation that clearly states the roles, responsibilities and processes. Clarity makes for timely action and eliminates confusion in a time-sensitive ransomware infection.

Create a Communication Plan

The entire response team should know who to contact, why and when during an incident. What information will be required in the first stages of a detection? Specific contact details and information requirements need to be documented to ensure the right people can be contacted quickly and effectively.

Test Your Incident Response Plan

Perform a risk assessment and prioritize security issues, identify which are the most sensitive assets and what are the critical security incidents the team should focus on. Rollplay, table top and test the incident response plan to identify any weaknesses proactively. As the old military strategy says, “no plan survives contact with the enemy”.

Review and Understand Policies

Review and consider changes and updates to existing policies and procedures to ensure they are fit for purpose relating to ransomware. Examples with available templates include:

- Acceptable Use Policies.
- Asset Control Policies
- Audit Policy
- Logging Policy
- Evidence Collection Policy

- Linkage to Other Policies
  - Information Security Policy
  - Information Security Assurance Policy
  - Physical Security Policy

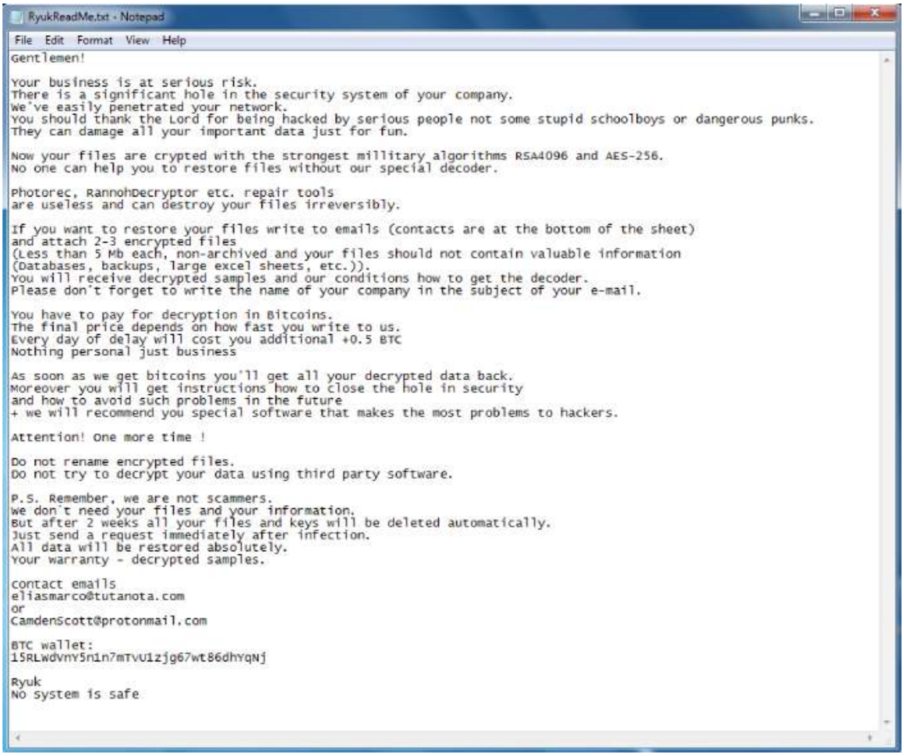
Responding to a Ransomware Incident

Being a victim of a ransomware attack, losing files and experiencing downtime is damaging. If you handle the aftermath badly, however, reputational damage could be long-lasting or even business ending. Using the SANS process for incident handling we will explore the response to ransomware.

- Identification
- Containment
- Eradication
- Recovery
- Post-Incident

Identification

Ransomware is often detected when it's in the process of encrypting files or shares, or worse, when it announces itself in the form of a ransom note.



```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk
No system is safe
```

Just because an organization has identified an infected device, or a device that is responsible for encrypting files, it doesn't necessarily mean that it is the only device affected.

The detection starts a race against time to identify any and all parts of the network that have been infected or that could become infected with ransomware. If the ransomware is wormable and exploits a vulnerability, then there is a strong possibility of multiple infections as the same vulnerability may exist in other devices on the network. Security teams need to identify the source rapidly to prevent further damage, and they must make sure the process doesn't repeat when backups are restored. Isolating the infected parts of the network and stopping any encryption currently underway reduces the potential impact and damage to the organization.

Identification is more than detecting that you have been attacked. Further analysis of the situation is needed to inform the best course of action for containment, eradication and recovery. The analysis needs to answer two key questions:

- What is the specific variant of ransomware?
- How did the ransomware enter the organization?

Each variant of ransomware can have a different message that is displayed to the user and the message text itself may vary. The message displayed on the infected computer can be very helpful in determining which variant of ransomware is involved. Any displayed messages should be captured by taking a screenshot or photo with another device.

Ransomware Identification

It is essential to identify the specific variant of ransomware within your environment. As highlighted in the Common, Prevalent and Historic Ransomware Examples section, there are many varieties of ransomware with new ones or adaptations emerging regularly. Each variant has different or unique capabilities which need to be understood to truly contain the spread. As we have seen, some ransomware variants like SAMSAM and RobinHood enable attackers to move laterally and exfiltrate data.

Initial Root Cause Analysis

Organizations need to establish how ransomware was introduced to their networks to support the containment phase. This does not need to be a full blown root cause analysis, which normally takes place in the recovery phase, but incident responders need to be sure that when they do contain the ransomware and move onto recovery, the attackers don't just repeat their actions and encrypt files again.

In the Methods of Infection section above, we detailed a number of infection vectors. Identification determines actions like searching for and destroying unopened emails containing the malware, patching vulnerabilities where possible and isolating systems where not, as well as blocking access to websites and removing devices or revoking user access to the network and file shares.

Containment

Once a part of your network has been identified or suspected as having been infected with ransomware, the devices should be immediately removed from your network, or isolated from communicating with the rest of your network or the wider internet through network protocols like Wifi. Having an EDR solution allows for the isolation of the machine and blocking of communication channels used for moving to file shares or propagation to other endpoints. Without shutting down the machine, this allows intelligence to be gathered and forensic and sample analysis to aid in deeper understanding of the ransomware campaign.

If you don't have an EDR solution, or you cannot quickly establish the root cause of the ransomware, you may have to consider shutting down the endpoint and taking file shares and connected systems offline, terminating all access or using NAC to block access.

Eradication

Once you are confident the ransomware outbreak is contained, the next step is to eradicate it. You have to be confident that no residual files are hidden on the system that may be able to re-infect devices. If you have an EDR solution installed on the endpoint device, this may be as easy as initiating a rollback. If you are confident based on identification and analysis that your backups are clean and uncompromised, you can use this to rebuild. Alternatively, you may be left with no other option than to replace machines that have been affected.

For other network locations, such as mailboxes or file shares, you need to clean those locations, search for and remove any unopened malicious emails or code, and set up close monitoring using details uncovered from your analysis to prevent the attack from re-emerging. Consider keeping devices connected to mailboxes isolated until you can determine they are clean from infection and change passwords to prevent use of any credentials scraped during the attack.

Recovery

Once you understand the ransomware variant, root cause and the extent of the attack and affected systems, you can attempt to recover.

To recover from ransomware you have five options:

- Rollback the device
- Restore from backup
- Decrypt files using a decryption tool
- Do nothing, simply rebuild affected systems
- Negotiate and pay the ransom

Rollback the Device

Some EDR solutions such as SentinelOne provide a one-click solution to eradication and recovery through a feature known as rollback. Be sure that your EDR solution also guards against the deletion of shadow copies seen in ransomware variants like RobinHood. Rollback is by far and away the simplest, least disruptive solution to a ransomware attack and can be accomplished in minutes.

Restore from Backup

If backups are available, predating the ground zero of the ransomware attack, you can restore endpoints and file shares from this date. Backups should be archived and removed and organizations should not rely on local network backups or disk images as these can be encrypted by the ransomware, or destroyed by targeted attacks prior to infection.

Decrypt Files Using a Decryption Tool

Identification of the ransomware variant can allow decryption if neither rollback nor backups are available. Communities like No More Ransom help infected users to regain access to their encrypted files or locked systems without having to pay. They curate a repository of keys that can decrypt data locked by different types of ransomware. The number of decryptors available now is into the hundreds; unfortunately, the recent flurry of ransomware variants means that there are many strains of ransomware for which no decryptor is available.

Do Nothing, Rebuild Affected Systems

To be absolutely sure that ransomware is removed from the system, you can wipe the infected devices and rebuild the operating system from the ground up. If your devices and the encrypted files are not mission critical or do not contain irreplaceable data, then this is an option especially if you can quickly rebuild devices and servers. However, be aware of the possibility that data may have also been exfiltrated and could be publicly dumped or obtained by competitors (see Maze ransomware mentioned earlier).

Negotiate and Pay the Ransom

If you have run out of options, your files cannot be recovered and the encrypted systems are not easily replaced and critical to the operation of your business and reputation, you may not have any choice but to pay. If the ransomware also involved a data breach, with company data exfiltrated, you may also be pressured into paying to avoid sensitive data being leaked publicly and to competitors.

In general, SentinelOne does not recommend paying ransomware attackers as it supports the ransomware business model and encourages more criminals to join in and multiply the number of attacks. It also supports organized crime and cash gained here will be used across a wider network of organised crime. Even in the case of a combined ransomware attack and data breach, there is no guarantee that paying the ransom will ensure any exfiltrated data will not still be sold to others or leaked to competitors, the media or the general public. You have to consider that data exfiltrated by threat actors is now "out there" and access to it is beyond your control, regardless of whether or not you choose to pay the attackers.

If you do decide to pay, you may need the services of a data recovery specialist or a negotiator and access to crypto currency such as Bitcoin, Monero or Dash.

Post-Incident

Your incident is resolved, but how can you prevent this happening in the future and what lessons did you learn during incident response?

Post incident, you need to gather data together into a report to establish what detection and security controls were in place and why they were not able to prevent the infection. The review should include recommendations and developments of new techniques to respond, detect, analyze or prevent similar incidents in the future.

The reporting should also include quantifying the financial impact on the organization, in terms of manhours, business down time, regulatory fines and possibly ransoms paid.

Prevention: Reducing Your Attack Surface

Ransomware attacks are not going away; in fact, the increasing diversity and total volume enabled by RaaS and affiliate schemes along with the low risk and lucrative returns only serves to suggest that ransomware will continue to evolve and increase in sophistication for the foreseeable future.

Examples like DopplePaymer ransomware employ lightning-fast payloads to perform over 2000 malicious operations on the host in less than 7 seconds. This means that legacy detection and response methods are failing to prevent infections and defenders response to ransomware often starts after the ransomware has achieved its objectives.

In order to become more effective in preventing ransomware, try to implement as many of the following recommendations as possible, where appropriate for your business environment.

To reduce your attack surface, first you have to understand and have visibility into it.

Threat Intelligence

How well do you know your attack surface? Prevention starts with intelligence on possible adversaries TTPs. Access to feeds and research powers your defences and helps you to understand and control your attack surface.

Highly organized crimeware groups such as Dridex and Trickbot have demonstrated success at scale utilizing ransomware as their primary attack vectors. Where they once relied primarily on banking fraud, their operations have noticeably shifted. This has attracted many new startup groups attempting to emulate their success. The proliferation of RaaS (Ransomware as a service) operations have undoubtedly wreaked havoc on many corporate networks.

However, there appears to have been an escalation amongst the groups struggling for dominance in the burgeoning ransomware services. The operators are no longer content with holding a network hostage. They are now seeking major payouts. The operators rifle through networks for days and weeks on end attempting to map the data points and find the juiciest data targets that will provide them with the best leverage for a payout.

Ransomware operators are now attempting to perfect their extortion schemes. Recent statistics put out by the FBI in the RSA presentation, attributed $61 million dollars to the group operating the RYUK ransomware. This figure accounted for operations conducted only between February 2018 and October 2019.

The operators of Maze and Revil (sodinokibi) are leveraging media and data leak sites in order to further threaten and humiliate victims into paying out their extortionist demands. Many groups such as DoppelPaymer, Clop, Netwalker, ATO and others have followed suit with leak sites. As the payouts continue, the attacks are not likely to go away anytime soon. The groups are now armed with substantial capital to further their attacks and further improve their products.

Discovery and Inventory

Ransomware criminals take advantage of the challenges and vulnerabilities created by BYOD, IoT and digital transformation initiatives using technologies like social, mobile, cloud, and software defined networks. Remote work forces demanding the ability to work from anywhere, any time whilst accessing company data and using cloud applications also create challenges and increase your attack surface. Visibility into who and what is on your network is crucial.

To control and take action, aim for continuous discovery and fingerprinting of all connected devices using active and passive discovery to identify and create a real time inventory of even intermittently connecting devices. This will help you to find and control rogue endpoints.

Software vulnerabilities allow attackers to use exploit kits to distribute ransomware. Supplementing endpoint discovery with an understanding of what operating systems, software and versions you have on which endpoints and servers is important to any patch management process.

Can you answer these questions?

- Which devices are connected to my environment?
- Which devices were connected in my environment?
- When was a device last seen or first seen in my environment?
- Which devices are unmanaged and unprotected?
- What is a device’s IP? MAC? Manufacturer? Type?
- Does this device have a specific port open?
- What information does the device report on this port?
- In which network (behind which GW) is it connected?
- What applications are installed on connected endpoints?
- Are there any unauthorized applications running in the organization?

Control Vulnerabilities and Harden Configuration

After you understand what devices are in your environment and what programs are installed on them, you need to control access, mitigate vulnerabilities and harden these endpoints and the software on them.

Centrally managing the evaluation and enforcement of device configuration and compliance is important to reducing your attack surface. Non-compliant devices should be reconfigured and hardened. Enforcing VPN connectivity, mandatory disk encryption, and port control will reduce the attack surface for ransomware.

Patch management is key, but with thousands of new vulnerabilities appearing every year, no organization is realistically going to patch every single one. Having a risk-based structured approach is best, but no approach is infallible.

Having centrally-managed application control allows security teams to control all software running within the endpoint environment and protect against exploits of unpatched vulnerabilities. It allows authorization of new software and prevents other, unauthorized, malicious, untrusted, or unnecessary applications from executing.

Control Human Vulnerabilities

Often with ransomware the weakest link is us, the human. The main entry vector is still email or visiting risky websites. Phishing, spear phishing and whaling is becoming more sophisticated and targeted, loaded with maldocs or ransomware links that tempt even vigilant users to click.

Having a programme of staff education and training is important to create a culture of suspicion and vigilance, sharing real world examples with staff and testing resilience is important, but even the best of us have the weakest of moments. You can reduce risk but you cannot eliminate it with training alone.

You can improve your email security with products that include features such as:

- Url scanning of inbound or archived email which does not allow clicks on target sites until the site can be checked for malware
- Detecting weaponized attachments in the mailbox and redirecting to a sandbox before delivery
- Protection against impersonation, social engineering, typosquatting and masking

Ransomware only has rights to change and encrypt files if the infected user does. Controlling user access to critical network resources is necessary to limit exposure to this and ensure lateral movement is made more difficult.

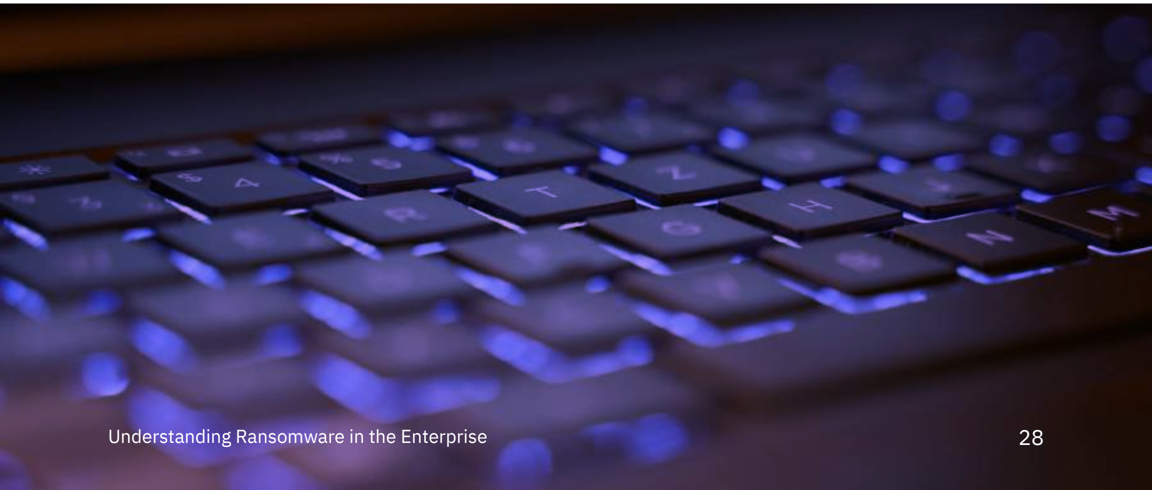
Therefore, it is critical to ensure privileges are current and up to date and that users can only access appropriate files and network locations required for their duties.

Monitoring and controlling user behaviour on and off the network will allow alerts and actions to automatically respond to suspicious deviations to server, file share or unusual areas of the network. Recording data, credential usage and connections by endpoints can highlight productivity change or possible security breach signals. Tools like EDR are available to record every file execution and modification, registry change, network connection and binary execution across an organization's connected endpoints, enhancing threat visibility to speed up action.

Improve Endpoint Security

Almost all organizations have endpoint security; however, to prevent ransomware, static detection and antivirus is no longer enough. Having advanced features in your endpoint protection and the ability to perform endpoint management and hygiene from a centralized management system is increasingly important.

Good endpoint security should include multiple static and behavioural detection engines, using machine learning and AI to speed up detection and analysis. It is also important to have exploit protection, device control, access control, vulnerability and application control. The addition of endpoint detection and response (EDR) into the mix provides forensic analysis and root cause and immediate response actions like isolation, transfer to sandbox and rollback features to automate remediation are important considerations. Having these features in one platform and one agent capable of protecting all devices and servers will ensure centralized visibility and control for your cyber security team across your entire endpoint estate.



How Can SentinelOne Help?

SentinelOne provides one platform to prevent, detect, respond, and hunt ransomware across all enterprise assets. See what has never been seen before. Control the unknown. All at machine speed.

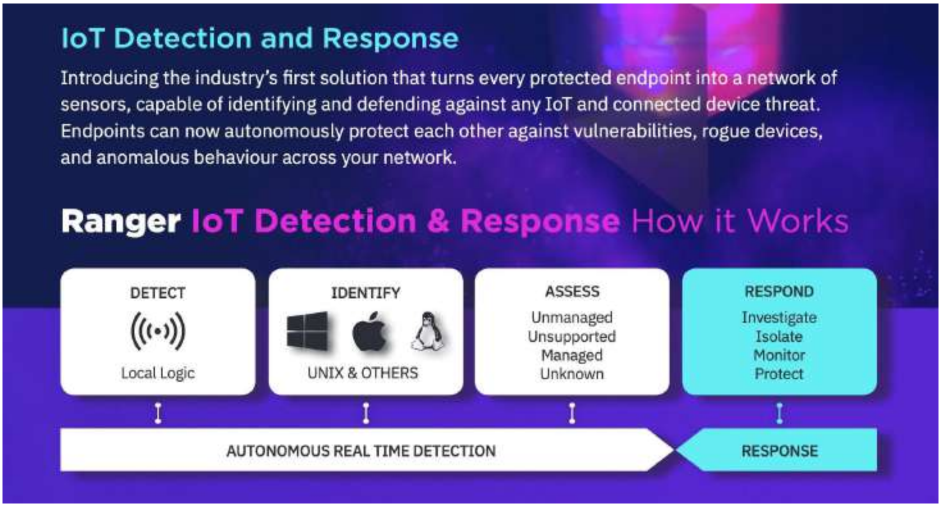
Prepare

Virtual Patching and Exploit Shield

SentinelOne prevents reliance on the traditional patching process. SentinelOne can dramatically reduce your attack surface by identifying out-of-date applications and immediately deploying an Exploit Shield policy to "wrap" a vulnerable application.

IoT Discovery & Control

With no additional agents or hardware to install, SentinelOne can automate device discovery, access and control. SentinelOne can automatically generate and maintain live device asset inventory of every endpoint, including IoT, IP, mobile and industrial control devices connecting to your network. It can fingerprint operating systems, device configuration and applications, push protection and enforce compliance, all from one management console.



IoT Detection and Response

Introducing the industry's first solution that turns every protected endpoint into a network of sensors, capable of identifying and defending against any IoT and connected device threat. Endpoints can now autonomously protect each other against vulnerabilities, rogue devices, and anomalous behaviour across your network.

Ranger IoT Detection & Response How it Works

DETECT
Local Logic

IDENTIFY
UNIX & OTHERS

ASSESS
Unmanaged
Unsupported
Managed
Unknown

RESPOND
Investigate
Isolate
Monitor
Protect

AUTONOMOUS REAL TIME DETECTION

RESPONSE

Protect

SentinelOne's multi-layered approach has been very effective in preventing ransomware infections. It features:

A Static AI engine trained on millions of malware and ransomware samples. It is able to detect and quarantine unique, never-seen-before ransomware downloaded from links in email campaigns or drive-by dropper websites.

A Behavioral AI engine which monitors all running processes, network communications, and interprocess communication to ensure system integrity. By logging all the changes made on the system and automatically correlating these events to a TrueContextID, SentinelOne is able to group all the variations of related processes together. Malicious activity, when detected, results in the entire process group getting killed and quarantined.

Next-Generation server and workload protection that is purpose-built for containers, including managed or unmanaged Kubernetes systems. Behavioral AI and autonomous response capabilities are available across all major Linux platforms, physical and virtual, cloud native workloads, and containers, providing prevention, detection, response, and hunting for today and tomorrow's cyber threats. SentinelOne's server and workload protection is infrastructure agnostic and can be deployed either in containers themselves, or in the machines that host them, in servers or in the cloud.

Respond

ActiveEDR

Forensic work is done by the single SentinelOne agent on the endpoint. Stories are already assembled using TrueContext, so the security analyst can save time and focus on reviewing full, contextualized stories to understand the root cause quickly. The technology can autonomously attribute each event on the endpoint to its root cause without any reliance on cloud resources.

ActiveEDR knows the full story, so it will mitigate ransomware at run time, before encryption begins. Other response actions can be used to isolate suspected targets based on root cause analysis, or tracking email mailboxes to the users devices.

Rollback

SentinelOne offers a unique rollback function, powered by protected copies of Volume Shadow Copy Services (VSS) available on Windows. Security teams can rollback any files that may have been encrypted before the Agent killed the process group to the latest version backed up by VSS. This highly effective and lightweight process obviates the need for restores from external backup solutions or full re-image of the system.

Recover

Warranty

SentinelOne believes that your next-generation endpoint protection solution should give you complete confidence that your sensitive data is protected against ransomware and other sophisticated attacks.

SentinelOne is so confident in its technology that it offers a warranty to ensure no ransomware attack will go undetected and cause irreparable damage. In the event that your organization must pay the ransom, SentinelOne Endpoint Protection Platform (EPP) customers covered by the SentinelOne Ransomware Warranty will be reimbursed up to $1,000 USD per affected endpoint if we're unable to keep you safe from a ransomware attack, up to a maximum of $1,000,000 USD per company.

Thank you

Daniel Card (PWNDEFEND), Mark Watkinson, Phil Stokes, Jim Walter, Joshua Platt, Migo Kedem and many more.

Tomorrow's Threats Require a New Enterprise Security Paradigm

REAL TIME Endpoint Protection

Multiple patented AI algorithms protect against the widest array of threat vectors. Eliminate dependency on connectivity, cloud latency, and human intervention. On-device AI prevents known and unknown threats in real time.

ACTIVE Detection & Response

Devices self-defend and heal themselves by stopping processes, quarantining, remediating, and even rolling back events to surgically keep endpoints in a perpetualy clean state. Hunt more and pivot less.

CLOUD DELIVERED IoT Discovery & Control

SentinelOne Ranger transforms every device into a sentinel, mapping and enforcing the enterprise IoT footprint. Hunt rogue devices, ensure vulnerability hygiene, and segment devices with dynamic policies.

NATIVE Cloud Security

Deploy autonomous workload protection across cloud, container, and server workloads. The building blocks of your secure cloud transformation are visibility, file integrity monitoring, protection and compliance.

Stay protected. Get a free demo today!

Get a Free Demo