JUNIPER NETWORKS | Engineering Simplicity

White Paper

RANSOMWARE TACTICS AND DETECTION STRATEGIES

A Deep Dive into Cyber Extortion

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Security administrators are expected to defend enterprise networks and their users from ransomware. Understanding the various types of ransomware and their propagation methods is the first step in this process. This white paper offers a deep dive into ransomware and explains how Juniper Networks® Advanced Threat Prevention (ATP) can stop such attacks in their tracks.

Introduction

Ransomware, which takes a system or its data hostage, and demands payment before returning control to the owner; is one of the most pervasive and destructive threats facing organizations and individuals today.

While ransomware has evolved and taken on many different forms over the years; its objective remains the same: extort ransoms from victims. Understanding how ransomware and its various propagation methods work is critical to blocking attacks and protecting your enterprise.

Ransomware strains have begun to differentiate themselves by both vertical and geography. As of 2020, many vendors report that Sodinokibi, Ryuk, and Phobos/Dharma are the top ransomware strains, while others still see Cryptolocker, Wannacry, and Cryptowall as dominant. MedusaLocker is also rising in prominence.

Another notable trend in 2020 is the rise of Ransomware as a Service (RaaS), which coincides with ransomware payments doubling roughly every quarter.

Remote Desktop Protocol (RDP) compromise, e-mail phishing, and software vulnerability exploitation are the three most common vectors of ransomware infection, although popular SaaS applications like Dropbox, Office 365, and Salesforce are also being targeted. Windows is the dominant target, but MacOS, iOS, and Android are not immune.

Ransomware Categories

Various versions of ransomware have evolved, each distinguished by the techniques they use. These attacks fall under four basic categories:

Application-Level Lockers—This category blocks victims from accessing their operating systems or applications. Reveton is the classic example of this type of ransomware. It prevents users from logging in and displays a note claiming to be from a law enforcement agency demanding payment of a "fine" to unlock the computer.

Other versions, such as Manifesto or Ransom Locker, display a ransom note and prevent users from doing anything on their computer. Since this type of ransomware operates at the application level, it can hijack the browser and prevent users from going to any other site until a ransom is paid.

System-Level Lockers—This type of ransomware overwrites a system's Master Boot Record (MBR) with its own mini kernel, rendering the computer useless (except to pay the ransom). Petya and PetrWrap are examples of this method; others include HDDCryptor, GoldenEye, and Satana.

Growth in Ransomware

Although ransomware is not new, it has grown exponentially over the past few years given the success of recent campaigns. Table 1 shows that we have gone from almost nothing in 2012 to a plethora of ransomware in 2017.

File Encryptors—Extremely popular among cyber criminals, this type of ransomware encrypts user files and data and demands a ransom for the decryption key. There are many notable versions of this ransomware, including Cryptowall, TeslaCrypt, Cerber, TeslaCrypt, Radamant, KeRanger, and WannaCrypt0r.

Fake Ransomware—This method does not actually encrypt data or hold any resource captive. Instead, it plays off the popularity of other ransomware, using scare tactics to trick victims into paying.

Doxware—This approach to ransomware threatens to publish the victim's files. Ransoc, one of the earliest doxware strains, told victims that their computers contained child pornography or violated intellectual property laws, and they would be reported to the authorities if they did not pay.

Chimera is another famous example of doxware, hitting German companies in 2015. Chimera encrypted files and demanded ransom, accompanied by a warning that if victims did not pay, "we will publish your personal data, including photos and videos, and your name on the internet."

Wipers—Data wipers delete all data on a system and demand payments to restore it. In some cases, the data is exfiltrated and backed up remotely before the ransom demand is made, making it possible to retrieve data. In other cases, the data is "undeleted" locally using any of various methods, or simply not restored at all.

Hybrid Ransomware—Hybrid ransomware combines multiple malware methodologies wherein ransomware—typically a file encryptor—is merely one method of attack. This can result in wormable ransomware that first arrives as part of a Trojan delivery system.

Table 1: Statistics from CyberEdge 2020 Cyberthreat Defense Report

Year	2017	2018	2019
% organizations hit by ransomware	55%	56%	62%
% organizations that paid ransom	39%	45%	58%

Key Reasons for Ransomware Growth

Several key factors are driving the continued growth of ransomware:

- **High Value of User Data**—Victims depend on the data taken hostage to run their day-to-day business operations. If they have no backup, their only recourse is to pay the ransom in hopes of recovering the data.
- **Time Pressure**—In most cases, time is on the side of the attacker. A hospital or airline, for example, can't abide a nonfunctional IT infrastructure for even a short period of time. To make matters worse, many ransomware attacks push victims to pay quickly; amounts increase and files start getting deleted as time passes.
- **Success Rates of Previous Campaigns**—According to some sources, the ransomware economy raked in more than
- $390 million in 2016, infecting an average of 90,000 victims a day. Projections say it will continue to grow.
- **Availability of Cryptocurrency**—Cyber criminals have to launder proceeds from their ransom collections, and crypto currency makes that easier. Bitcoin is the cryptocurrency of choice among cyber criminals; even though Bitcoin transactions are public, it is virtually impossible to track the parties involved.
- **Exploit Kits**—The availability of very successful exploit kits, mainly Angler, Nuclear, Neutrino, and RIG, make it relatively painless for ransomware actors to deliver their payloads over proven infection methods.

Infection Vectors

E-Mail

E-mail remains the most popular method of delivering ransomware. Using a very convincing message, cyber criminals can entice victims to open an e-mail attachment or click on a link that leads to infection.

E-Mail Attachment

Infected attachments are usually MS Word documents purporting to be something important to the recipient, like a shipment notification. However, the document actually contains a malicious obfuscated Visual Basic (VB) script, which will either embed the ransomware binary in its own data, decrypt it, write it to disk, and launch it; or it will reach out to a website to download the ransomware binary and execute it.

The Locky campaign was particularly successful at attaching a malicious JavaScript code to e-mails inside a zip file. The script files have file extensions that appear to be legitimate documents, enticing the victim to open them. The script would then download the ransomware from the Internet and launch it into the system.

In some cases, attachments will attempt to take advantage of a vulnerability in the handler application. For example, a malicious PDF could attempt to exploit an unpatched or zero-day vulnerability in Adobe Acrobat Reader, drop the ransomware binary, then execute it. The same goes for Microsoft Office documents. This approach has grown less popular lately due to the low number of known vulnerabilities that are unpatched.

Sometimes, Office or PDF attachments contain nothing but links to websites that host the ransomware. This method is also falling from favor because it requires victims to interact with the downloaded file and agree to execute it, which raises suspicions.

E-Mail Links

Mainly associated with phishing attacks, links have also been used to get victims to download ransomware, albeit with limited success.

Drive-By Infections Using Exploit Kits

In a drive-by attack, a user merely visiting a website can be infected with ransomware—no interaction required. Threat actors will either compromise a website and inject code to redirect visitors to the exploit kit, or resort to malvertising. In both cases, the user's browser is redirected to an intermediate site containing JavaScript that will identify vulnerabilities, either in the browser or its plugins, and deliver a payload that will trigger the exploitation. The exploit is either in JavaScript, Adobe Flash, or Silverlight, depending on the versions installed in the browser. Once successful, the exploit kit downloads and executes a ransomware binary.

Direct Web Downloads

Ransomware can also be downloaded directly from the Web when users are tricked into installing a nifty new text editor or PC cleaner, which is ransomware in disguise.

Wormable Exploits

The WannaCry mass infection in May 2017 introduced yet another method of infection. "Ransomworms" attack computers directly from the Internet using a vulnerability in the SMB file-sharing protocol, dropping ransomware in the form of an encrypted DLL.

Trojan Downloaders

Ransomware can also be downloaded by malicious Trojans such as Upatre, Bedep, and Nemucod. Upatre and Nemucod typically spread through e-mail attachments. To defend against such attacks, it is critical they be stopped at the earliest kill chain phase possible.

Remote Desktop Protocol Compromise

RDP is a way to remotely access a computer system, commonly used for systems administration and for Virtual Desktop Infrastructure (VDI). RDP vulnerabilities give attackers direct control over target systems, making compromise simple.

SaaS Application compromise

Cloud-hosted applications are also vulnerable to ransomware. Password reuse means that login credentials for SaaS applications can often be found in existing data dumps, allowing attackers to log into SaaS applications and either change settings to deny legitimate access or encrypt/delete data found there. In both cases, ransom is typically demanded in order to re-enable access.

Ransomware Encryption Process

A typical ransomware encryption process will use a combination of public and private key algorithms. The private key algorithm encrypts the files themselves, while the public key algorithm encrypts the file encryption keys.

The operation works as follows:

Encryption

1. When the ransomware is executed, it reaches out to its Command and Control (C&C) server with the victim's computer identification.
2. The C&C server generates a pair of public and private keys specific to the victim's computer and responds with the public key. The corresponding private key is safely stored on the C&C server. It is worth noting here that some ransomware bypasses these first two steps by including the public key in the ransomware binary itself, which is custom-built on the fly for the intended victim.
3. The ransomware enumerates all the files it needs to encrypt using a hardcoded list of data file extensions.
4. The ransomware generates a set of private symmetric keys locally to encrypt the files. Symmetric keys are used for both encryption and decryption; in some cases, one key per file is generated, while in others it could be one key per file extension or just one key for the entire set, depending on the paranoia of the author.
5. The ransomware uses the private key algorithm and the symmetric private keys to encrypt the files.
6. Then the private encryption keys themselves are encrypted using the public key from step two; the result is stored in the victim computer's key store.
7. The ransom note is displayed, sometimes with an incentive to pay quickly.

Decryption

1. Once the malware operator receives payment, the private key from the C&C server is sent to the ransomware decryptor code.
2. This private key is then used to decrypt the symmetric private keys used earlier to encrypt the files stored in the local key store.
3. The symmetric private keys decrypt and recover the original data files.

Earlier versions of ransomware, like CryptoWall 2.0, were not as sophisticated and used the public key directly to encrypt data files. As it evolved, Cryptowall 3.0 eventually adopted the process above, combining public/private keys and symmetric keys. Cerber uses a combination of RSA public/private keys and RC4 keys. Typically, a combination of Advanced Encryption Standard (AES) and Rivest Cipher 4 (RC4) encryption algorithms are used with varying ciphers.

Juniper ATP Appliance: Detecting Ransomware

Ransomware can be identified using either network-based or endpoint-based detection. We will focus on network-based detection and, more specifically, how the Juniper Networks Advanced Threat Prevention Appliance detects these advanced threats.

The advanced detection fabric of the Juniper ATP Appliance includes multiple detection and analytics capabilities that work together to quickly identify targeted ransomware attacks. These capabilities are summarized below.

Object Analysis Pipeline

All files analyzed by the Juniper ATP Appliance go through a multistage detection pipeline within its SmartCore analytics engine, which is comprised of the following components:

- **Static AV Engine**—Leverages top-tier antivirus technology with frequent signature updates to detect known viruses.
- **Reputation Engine**—Provides reputation-based detection where file hashes, signers, and other metadata about the file and the context around its source are compared to our threat intelligence knowledge base.
- **Behavioral Engine**—Performs dynamic analysis of the object's behavior in a sandbox environment and applies machine learning models to the observed behavior.
- **Emulation Engine**—Emulates files containing scripts as an alternative to full behavioral analysis.
- **Yara Engine**—Allows application of Yara rules to files as well as memory dumps obtained during behavioral analysis.

Network Analysis Pipeline

Traffic visible to the Juniper ATP Appliance also goes through a couple of steps before files are extracted for analysis:

- **Snort Rules**—All traffic is subjected to snort rules from Juniper Threat Labs as well as third-party sources.
- **Chain Heuristics**—All suspicious traffic is flagged and submitted to a browser-based dynamic analysis environment where heuristic rules are applied to identify malicious traffic such as exploit kit redirects.

Use Cases

The detection methods for ransomware are usually tailored to the delivery mechanism employed. This section will review each delivery mechanism above and drill down into the methods used by the Juniper ATP Appliance to detect them.

E-Mail Attachments

E-mail traffic using either a journaled account or Bcc mailbox is monitored by the Juniper ATP Appliance. In both cases, it extracts all e-mail attachments and submits them to the SmartCore Object Analysis Pipeline (OAP), which extracts all links (including links inside attachments) and submits them to the SmartCore Reputation Engine (SRE). The Juniper ATP Appliance also integrates with Office365 and Gmail, providing seamless remediation capabilities by blocking or quarantining malicious e-mails.

If ransomware is being delivered via a PDF, Office document, malicious JavaScript, or executable file attached to an e-mail, the Juniper ATP Appliance uses all elements of the OAP to identify the threat.

Locky is a popular example of ransomware downloaded by an e-mail attachment. The attachment itself is either a JavaScript file inside a zip file or a Word document with a VBA macro claiming to be an invoice or a shipment notification.

The Juniper ATP Appliance detects the JavaScript zipped attachments as Exploit.Script.

The Juniper ATP Appliance detects the Word documents as TROJAN_NEMUCOD.DC or TROJAN_DONOFF.DC.

If the e-mail contains a link to the ransomware, the Juniper ATP Appliance submits the link to the SRE, which has the ability to:

- Perform a reputation lookup of the URL or domain and assess the risk
- Perform a crawl of the URL and assess the risk based on the content returned
- Perform predictive analysis based on past history of the site or URL to estimate the likelihood the site will be malicious in the future

Example: Potential victims receive a phishing e-mail purporting to be from Microsoft alerting them to recent suspicious activity and encouraging them to visit their recent activity page.

E-mail SHA256: 5b18f7f958a39cc37b36f9766bfe2c12d5d28854695ba8c14f598f1070ad9cf6

This phishing e-mail has a link to "http://voperforseanx[.]top/site/ chrome_update.html" which, when visited, results in a Cerber Ransomware (5855d6b239620e53c8c60acee3d0960b84fbb75f2f9b20b2ccf721a8fc5a88a2) being downloaded.

The Juniper ATP Appliance detects this threat and classifies it as a phishing incident.

Exploit Kits

Usually, exploit kits redirect users to a series of webpages designed to assess which component of the browser is most vulnerable and deliver the appropriate exploit. The final payload may be totally encrypted.

A user visits simply-vegan.org, a site which has been compromised with an iframe injection by the pseudo darkleech campaign.

The iframe redirects the user to mobilalibey.com, which hosts the RIG landing page. The landing page JavaScript assesses the user's environment and detects a vulnerable version of Adobe Flash player. The browser is instructed to download the proper Flash exploit, which in turn downloads the Cerber ransomware disguised as a final payload.

In this case, the Juniper ATP Appliance detects and correlates between two components of the attack: the redirection to the RIG exploit kit is detected as an IN event and the download of the Flash exploit is detected as a DL event. Both are combined in a single incident as EXPLOIT_RIGV.CY.

Direct Web Downloads

In this example of direct download, the threat actors use some social engineering tactics to make the Google Chrome user believe the website they are visiting requires a new font that the browser does not have. They prompt the user to download the font in the form of an executable font installer for Chrome. Once downloaded and launched, the ransomware springs into action.

In this case, several elements of the OAP are able to detect this threat as RANSOM_GENASOM.DC.

Wormable Exploits

The WannaCry pandemic focused the public's attention on the devastating effects that a worm leveraging a vulnerability can have, spreading like wildfire and deploying advanced ransomware. In this case, the vulnerability in the Windows file sharing protocol SMBv1 was exploited via what is known as the EternalBlue exploit. This exploit was allegedly developed by the NSA as a cyber weapon and stolen by the Shadow Brokers group, then disclosed to the public. Even though a patch was available and exploits were publicized, many systems remained unprotected and fell victim to WannaCry.

Over the network, the ransomware WannaCrypt0r was transferred as an encrypted DLL. The Juniper ATP Appliance detects this attack in the OAP as EXPLOIT_ETERNALBLUE.CY.

Recommended Steps to Stop Ransomware

In order to protect against ransomware, Juniper recommends taking the following precautions:

- Patch your systems early. Threat actors prey on the window of opportunity between the time a vendor discloses fixes for a particular vulnerability and the time computers are patched. With automation, some cyber criminal groups have become very quick at integrating new capabilities into their exploit kits.
- Back up your data frequently and test the backup periodically to avoid unpleasant surprises the day you need to restore.
- Invest in staff training on social engineering tactics used by cyber criminals to avoid opening the wrong attachments or clicking on a bad link.
- A combination of RDP gateways and expedient patching will make an organization less vulnerable to RDP. However, best practices call for not exposing RDP directly to the internet—even through a gateway—and using VPNs or similar technologies to restrict access.

- Multi-Factor Authentication is strongly recommended, especially for use with SaaS applications. Where possible, restricting access to your organization's SaaS tenant instance to authorized organization IP addresses can also provide significant defense. A cloud-based solution such as the Juniper Networks vSRX Virtual Firewall can serve as an access node to the wider organizational Secure SD-WAN fabric, providing a secure way to restrict access to that tenant to those users who have successfully authenticated to, and gained use of, the organization's Secure SD-WAN fabric.
- Do not rely exclusively on prevention methods that tend to lag behind new threats. Make sure you deploy detection methods to root out any advanced threat already in your network which could be "hired" to install ransomware.
- Provide your security operations center (SOC) team with a platform that allows correlation of incidents across multiple security devices. Alert fatigue is a major reason backdoor attacks remain undetected for a long time.

Conclusion

As ransomware attacks evolve, their specific strategies, tactics, and technology components will evolve as well. Juniper Threat Labs will continue to monitor and analyze these developments to ensure that the Juniper ATP Appliance detection technologies are continually enhanced and optimized to protect customers from these attacks.

By following the recommended steps above and leveraging the Juniper ATP Appliance, enterprises can win the fight against ransomware and protect their users.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity