An Analysis of the Recent Ransomware Families

Adrian (Shuai) Li

Purdue University
li3944@purdue.edu

1 Introduction

The notorious crypto-ransomware infections in the past, such as CryptoLocker[4] and WannaCry[11], can immediately disrupt the access to files or systems after ransomware deployment. With no backups of the compromised systems, the victim has no choice but to pay the ransom and hope the attackers will restore the systems. Additionally, the threat actors pressure victims to pay the ransom demand by stealing the data and threatening to release the stolen data publicly. In the last year, ransomware is still the major malware threat, with 60% of managed service providers seeing attacks in the first half of 2020[5]. The ransomware industry has continued to evolve with more sophisticated new ransomware families and more effective threat actors. We investigate the three most active ransomware families reported by Group–IB in 2020[7]. They stand out to other ransomware families with massive impact by leveraging sophisticated techniques. It is important to recognize the extensive analysis that has been done on these ransomware families by the security companies[1][8][3][13]. Although each ransomware has different source codes, they show some common behaviors when they strike. We summary the behavioral patterns of the chosen ransomware families in Section 3. Finally, we present the characteristics of each ransomware family in Section 4. The major findings of our study include the following.

- Threat actors leverage multiple infection vectors to maximize the damage caused.
- The resources to successfully launch ransomware attacks are abundant. Threat actors can purchase leaked credentials of thousands of servers on underground websites. The ransomware authors can purchase new system vulnerability exploits from the exploit developers.
- Ransomware creators have continued to scale platforms to gain additional partners through the Ransomware as a Service model.
- Ransomware families use common tools and methods to spread across the machines in the enterprise network.
- Ransomware families commonly use a three-tier trust model for encryption.
- In addition to code obfuscation, some ransomware families run the malicious code in a trusted process to achieve defense evasion.

2 The Evolving Sophistication

By utilizing obfuscation techniques, threat actors make the static analysis more difficult for reverse engineers. The most common form of obfuscation is a packed binary that conceals the ransomware until it strikes. Ransomware creators use non-commercial packers that thwart ransomware detection and analysis. Other forms of obfuscation include control flow obfuscation and anti-disassembly obfuscation. This report further investigates the control flow obfuscation since it is leveraged frequently by the Maze ransomware[1]. With sufficient control flow obfuscation, anyone who attempts to analyze the ransomware's assembly code will find endless paths to go from the code and eventually get lost.

Additionally, ransomware as a service model involves a central platform that generates new ransomware samples per victim to the threat actors. The increasingly efficient ransomware generation allows attackers to infect more organizations.

2.1 Obfuscation

A program's control flow is the path/sequence of instructions that the program will execute. The disassembler can visualize a program's control flow as a series of connected blocks. We can distinguish the control flow obfuscation into two categories, absolute jump obfuscation, and call instruction obfuscation.

Absolute Jump Obfuscation. Before talking about this obfuscation form, it is necessary to explain an absolute jump and a conditional jump.

An absolute jump instruction will jump to the indicated address or to the address stored in a register. An absolute jump looks like,

- JMP register: jump to the address stored in the register.
- JMP [address] : jump to the address

In assembly, all branching is done using conditional jumps. We will use the following conditional jump instructions.

- JZ: jump if the flag ZF = 1
- JNZ: jump if the flag ZF =0

Absolute jump obfuscation inserts a series of conditional jumps, but they will ultimately end up at the same destination. In higher-level language, it is equivalent to inserting series of extraneous branchings. Figure 1 shows an example of Absolute Jump obfuscation.

On the left side, at address 004, is a JMP instruction, which will jump the program to address 030. On the right side, the attackers insert a series of conditional jumps. At address 004, the JZ instruction will be followed, and jump the program to 030 if ZF=1. Otherwise, the JNZ instruction at 008 will be executed, and the program jumps to address 020. At address 020, because ZF=0, the JNZ instruction will be executed and eventually jumps the program to 030. It's worth

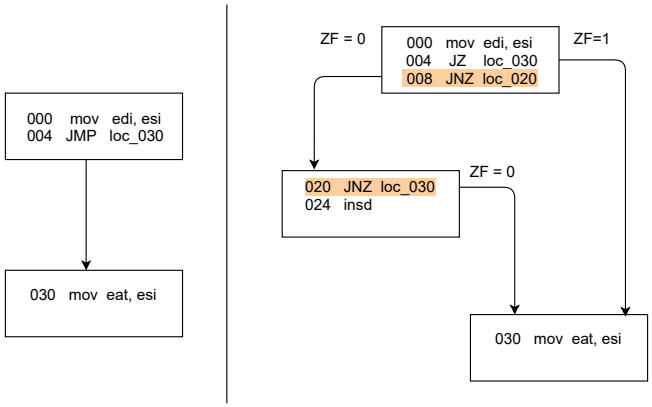

Fig. 1: Absolute jump obfuscaton example

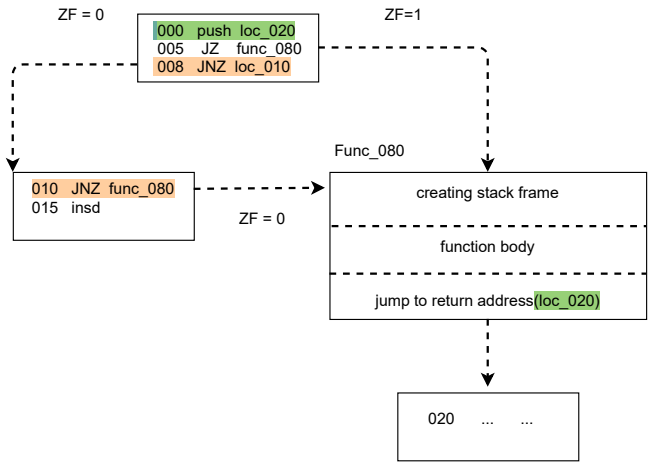

Fig. 2: Call instruction obfuscation example

noting that although the instruction at address 024 will never be reached, IDA will still display it as code. The attackers can insert lots of unreachable instructions like this, making it difficult for the analysts to navigate the program control flow.

Call Instruction Obfuscation. Attackers transform CALL instruction into conditional jumps, making it difficult to identify where functions begin and end. Figure 2 shows an example of call function obfuscation.

At instruction 000, the return address for the function call is pushed to the stack. Then, if ZF=1, JZ instruction jumps the program to the address of the function. The function will allocate space for the function stack frame, execute the function and finally jump to the return address that was pushed at 000.

If ZF=0, JNZ instruction jumps the program to address 010. At address 010, because ZF=0, the JNZ instruction will be executed and eventually jump the program to the same function. Similar to the previous obfuscation type, the instruction at 015 is not reachable. The attackers can apply many unreachable instructions to confuse the control flow.

2.2 Ransomware as a Service

REvil ransomware samples [2] are sold as distribution kits on a dark service platform created by a threat actor called UNKN, who advertised for joining the platform in mid 2019. Since then, many threat actors have joined REvil. Each threat actor operates in isolation, and they can retain 60 to 70 percent of ransom while the rest goes to the platform. The platform provides the threat actors with the ransomware samples per victim and manages the ransom demand and payment. Ransomware as a Service removes the strains of creating sophisticated ransomware. Threat actors can focus on obtaining initial access to the victim's systems and deploying the ransomware once they compromise a privileged account. With the automated platform operation, the attackers can infect more organizations.

3 Ransomware Behaviors

3.1 Infection vectors

Ransomware is typically spread via phishing emails, via compromised malicious websites with exploit kits, or by active adversaries who use tools to scan for systems with weak protection automatically. Note that attackers can combine the infection vectors to maximize the damage. In Section 4.4, we will see how Ryuk ransomware uses the "triple threat" to deliver ransomware to the victim hosts.

Spam email campaigns. The attacker typically sends a themed email with a malicious attachment. The attachment is usually a Word document with a macro that will download ransomware from the attacker's IP address when the victim opens the attachment.

Drive-by download exploit kits. The attackers typically compromise some trusted websites that cater to a particular set of users. Then the attackers place the ransomware on these websites. As a result, unsuspecting users will install ransomware on their systems when they visit the compromised website. There are reports that the threat actors leveraged this method to deliver REvil. They compromised the Italian WinRAR website and replaced the WinRAR installation with a REvil ransomware sample[13]. When the unsuspecting customer clicks the installation link for WinRAR, they will download the REvil ransomware into their systems.

Automated active adversary. The attacker uses tools to scan the internet for systems with vulnerabilities automatically. When such systems are found, the attack exploits the vulnerabilities and gets initial access to the system.

Remote Desktop Protocol (RDP) is a common method used by the attackers to connect to the systems. An open RDP port of the system allows anyone to access this machine from the internet. Nowadays, the attackers need not even carry out a brute-force attack to log in to the machine with an open RDP port. They can purchase the leaked credentials of thousands of servers for just a few dollars on dark resources such as"xDedic" and "UAS RDP Shop"[6].

When REvil was first discovered, it was delivered via exploitation of CVE-2020-14882 (Oracle Weblogic Server vulnerabilities). This vulnerability allows an unauthenticated attacker to compromise and take over Oracle WebLogic Server.

3.2 Privilege Escalation

Running the ransomware requires root/admin privileges. For example, the ransomware needs full privilege to delete sensitive files and to terminate protection software using TASKKILL. Once the threat actors get access to the system, they will use exploits to elevate their privileges. If the attackers have the stolen admin credentials, they can log in to the system with full privileges. Hence, in this section, we assume that the attackers do not possess admin credentials.

EternalBlue EternalBlue is an exploit developed by the U.S. National Security Agency (NSA). Attackers commonly use it to perform privilege escalation. Threat actors typically use the DoublePulsar code injection technique with EternalBlue to execute the ransomware with the highest privileges.

CVE-2018-8453 Win32k Elevation of Privilege Vulnerability. When the Win32k components fail to handle objects in memory properly, there exists a vulnerability such that attackers can exploit it to escalate their privileges. If the exploitation is successful, an attacker can run arbitrary code in kernel mode. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights. There are reports that the threat actors of REvil [13] and Maze [10] exploited this vulnerability to elevate privileges.

Maze also exploits another vulnerability in Win32k (CVE-2016-7255). What's interesting is that the threat actors of Maze did not implement exploits for these vulnerabilities. They use Volodya's exploit for CVE-2016-7255 while transitioning to using PlayBit's exploit for CVE-2018-8453. Volodya and Playbit are two prominent exploit developers who sell their exploits for profit. Checkpoint research lab profiled these two developers and found out that they used multiple platforms (Youtube, Pastebin, and underground forums) to advertise the vulnerabilities[9]. What we learn from this is that ransomware attacks are no longer performed solely by individual cybercriminals. A ransomware infection incident is a joint work between malware authors and exploits developers.

3.3 Propogation

After taking control of the infected system, many attackers attempt to kill all the protection software processes. Then they try to steal the admin's credentials using the Mimikatz tool. Many attackers create a new admin account in the Active Directory to persistently remain foothold in the system.

Next, the attackers leverage a tool called BloodHound to find high-value targets in the domain. Finally, they created a script that automatically copies and executes the ransomware onto the targeted machine, leveraging tools such as Windows Management Instrumentation and PsExec. The script includes a list of targeted machines and their addresses, the ransomware, and a privileged domain account for authentication.

Alternatively, the attackers can create a Group Policy Object in the default domain policy for all computers to execute a task. The task downloads the ransomware and then executes the ransomware.

The attackers can also manually run ransomware on targeted systems, but it takes a much longer time to complete than the automated script. By the time the attackers finish half of the machines, the victim is likely to have started taking action.

3.4 Deleting Backups

Windows offers system recovery via Volume Shadow Service. Windows stores many snapshots of the system - a snapshot is the system's state at a particular time. These snapshots are called volume shadow copies in Windows. With these copies, a system can recover to the previous state before any disruption events.

To prevent the victim recover the system with shadow copies, the attackers destroy any existing volume shadow copies. This is done using a windows utilities called VSSADMIN.EXE. Elevated admin privileges are required to use this utility. Alternatively, the attackers can delete the shadow copies via Windows Management Instrumentation (WMI). Windows includes a command-line utility called WMIC.EXE to access WMI.

3.5 File Encryption

Before encrypting any files, the ransomware recursively searches all the drivers for files to encrypt, including network shared folders. The ransomware encrypts every file except for certain file types and any file containing text from a hard-coded whitelist. The attackers still want certain applications or components intact so that the victim can see the ransom note and pay for the ransom.

All three of the ransomware families use a three-tier trust model for encryption. Figure 3 shows the three-tier model. At the first tier is the global RSA key pair held by the threat actors. The second tier is a per-machine/victim RSA keypair. Typically the machine key pair will be generated by the ransomware on the fly. The private key of the machine key pair is encrypted with the global public key and saved to a local file.

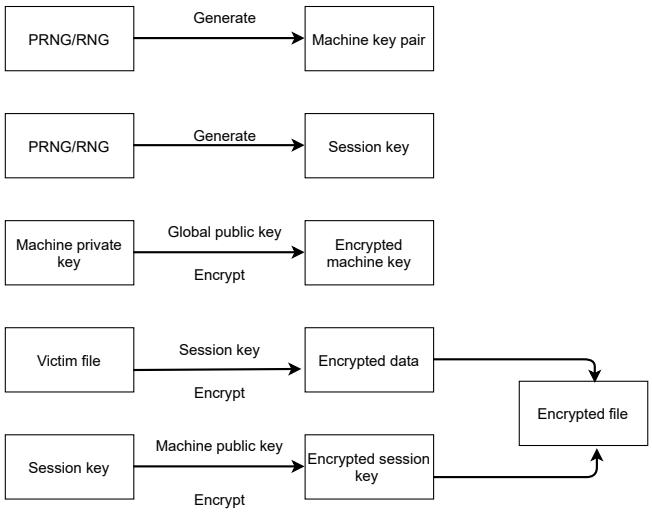

Fig. 3: Three-tier encryption model

The third tier is a session key generated per victim file using some key generation algorithms. The ransomware uses the session keys to encrypt each victim file using some symmetric encryption algorithms. The session keys are encrypted using the second-tier public key, and the results are appended to the encrypted file.

Some ransomware overwrites the original document with the encrypted data, making it impossible to recover original documents with data recovery tools.

Others choose to write the encrypted data to a new file and delete the original document. Some ransomware use CIPHER.exe to prevent the victim from recovering deleted documents from their storage drives.

Finally, ransomware will destroy its session keys.

3.6 Rename

There are several reasons why the ransomware renames the files after encryption,

- Prevent encrypting the files again if the ransomware runs again on the system.
- Make the infection more noticeable to the victim.
- Break the relation between the encrypted files and the Windows Volume Shadow copy. If the ransomware does not delete the shadow copy and the encrypted files have the same name as the original files, the Windows Volume Shadow Copy Service can recover the original files.

4 Ransomware Families

4.1 Overview

An overview of the three ransomware families is shown in Table 1

Table 1: Comparison of tactics and techniques of Maze, REvil and Ryuk

	MAZE	**REvil**	**Ryuk**
Initial access	–Phishing emails –Exploit kits –Automated active attacker	–Phishing emails –Exploit kits –Automated active attacker	–Triple threat Campaign
Privilege escalation	Exploiting –CVE-2016-7255 –CVE-2018-8453	Exploiting –CVE-2018-8453	Exploiting –EternalBlue
Network Infection	–Abusing WMI	–Scripting with PsExec –Creating Group Policy Object	–Not found
Defense evation	–Code obfuscation –Terminating processes –Disable debugger	–Terminating processes –Abusing Powershell	–Terminating processes –Code injection
Persistence	–Creating "startup_vrun.bat" file in the Startup folder	–Not found	–Adding itself to the Run registry key
File scanning &whitelisting	Yes	Yes	Yes
File encryption	Three-tier trust model –RSA-2048 –ChaCha	Three-tier trust model –ECC Curve25519 –Salsa20	Three-tier trust model –RSA –AES
Inhibit system recovery	–Delete volume shadow copies and disable recovery	–Delete volume shadow copies and disable recovery	– Delete volume shadow copies and disable recovery
Discovery & Exfiltration	–Exfiltration Over C2 Channel	–Exfiltration Over C2 Channel	–Not found

4.2 Maze

Maze ransomware attacks made up 12% ransomware attacks in 2020[14]. Maze uses the RaaS model that allows multiple threat groups to operate Maze ransomware attacks independently. Jerome Segura first discovered it in May 2019[12]. Maze authors implemented a data theft mechanism to exfiltrate information from the infected systems. This information is used as leverage for payment. If the victim does not pay the ransom, they will release the information on the internet.

As discussed in Section 2.1, Maze authors use absolute jump obfuscation and call instruction obfuscation to insert unreachable garbage instructions to confuse the reverse engineers. For disassembly to correctly disassemble the ransomware, the analysts need to remove the obfuscations. The general approach is to search for obfuscation patterns and then deobfuscate all located patterns. For example,

the combination of jz/jnz is a pattern for control flow obfuscation. We can search for all the jz/jnz combinations and replace them with jz/jmp. Making the send jump absolute will help the disassembler to skip the unreachable instructions.

Maze ransomware collects information about the compromised machine and encodes it as a unique "fingerprint" of the system. The malware tries to connect to several control hosts. Once connected, the ransomware sends the fingerprint to the C2 hosts and waits for further instructions on possible data exfiltration.

4.3 REvil

REvil, also knowns as Sodinokibi, was first identified in April 2019. REvil makes up 29% of all ransomware attacks in 2020, infecting at least 140 victim organizations since April 2019[14]. It uses the RaaS model and steals the sensitive data from the compromised machines.

REvil can be distributed via phishing emails, via exploit kits, or by active adversary attacks. When the victims download the ransomware into their systems, the ransomware is loaded straight into memory by PowerShell without dropping a Portable Executable file on the disk. In this case, the ransomware attack is performed by the PowerShell process, making it more difficult for protection software to detect the ransomware attack.

REvil uses the three-tier trust model for encryption. Global ECC key pairs held by the attackers. A per machine ECC key pair generated by the ransomware on-the-fly. Finally, the ransomware generates a session key per file for encryption. The session key is encrypted with the machine public key and appended to the encrypted file. The machine private key is encrypted with the Global public key and stored in the system. REvil stores the machine public key and encrypted private key in the recfg registry key.

Table 2: Registry key and values created by REvil

Values	**Description**
pk_key	Machine public key
sk_key	Encrypted machine private key
0_key	Encypted machone private key
rnd_ext	Random file extension
stat	Encrypted host profile information

Table 2 shows the values within the recfg registry key. In addition to pk_key and sk_key, the machine private key is encrypted using a different public key that is hardcoded in the REvil binary. The rnd_ext value contains the random file extension generated at run time. Like Maze ransomware, REvil profiles the compromised host and stores it in a “stat” JSON structure. The “stat” JSON structure is then encrypted with a different hard-coded public key and stored in the registry.

REvil sends the encrypted stat data to multiple C2 servers over HTTPS, making it challenging to analyze the network traffic.

4.4 Ryuk

According to Malwarebytes research lab, Ryuk ransomware infection incidents increased 99 percent over the first quarter of 2019[3]. Ryuk was first discovered in 2018 with the attack against Tribune Publishing and Data Resolution.

Ryuk uses triple threat campaigns to maximize the damage to the victim. The threat actors first send phishing emails with malicious attachments to the victim(s). Once the user opens the attachment, the malicious file attempts to download the Emotet payload from the attackers' IP addresses. The Emonet then drops the TrickBot Trojan, which disables the protect software on the victim machine and performs privilege escalation. Once the attackers take control of the infected system, they run the Ryuk ransomware and attempt to propagate the ransomware to peer endpoints and servers.

Like other ransomware families, Ryuk adds itself to the Run registry key to execute after reboot. Then, it will inject its malicious code into trusted running processes, making protection software believe a trusted application is modifying the documents. Ryuk will iterate each running process in the system except for those in the whitelist and try to inject a code to each process's address space. The injection code holds the core functionality of Ryuk ransomware.

Ryuk uses the three-tier trust model for encryption. However, instead of generating the machine key pair on-the-fly, Ryuk comes with a pre-embedded machine key pair, and the private key is pre-encrypted.

5 Conclusion

We have discussed common stages of ransomware deployment and techniques used in each stage. In particular, we have described infection vectors, privilege escalation, lateral movement, file encryption, and defense evasion. We have considered some new techniques and distribution models that arise and are found in the recent ransomware families.

The next important step is to look at practical security controls and enforcement measures so that the impact of ransomware attacks can be limited. As discussed in this report, many ransomware families exhibit common behaviors and techniques in the entire deployment cycle. It is feasible to come up with practical security recommendations that can potentially protect organizations from ransomware outbreaks.

References

1. Bitdefender: A technical look into maze ransomware. `https://download.bitdefender.com/resources/files/News/CaseStudies/study/318/Bitdefender-TRR-Whitepaper-Maze-creat4351-en-EN-GenericUse.pdf` (2020), Accessed on Feb 2021

2. Clarke, M., Hall, T.: The evolving maturity in ransomware operations. https://i.blackhat.com/eu-20/Wednesday/eu-20-Clarke-Its-Not-FINished-The-Evolving-Maturity-In-Ransomware-Operations-wp.pdf (2020), Accessed on Feb 2021
3. Cohen, I., Herzog, B.: Ryuk ransomware: A targeted campaign breakdown. https://research.checkpoint.com/2018/ryuk-ransomware-targeted-campaign-break/ (2020), Accessed on Feb 2021
4. Cruz, J.D.: Threat refinement ensues with cryptolocker, shotodor backdoor. http://blog.trendmicro.com\\/trendlabs-security-intelligence/threatrefinement-ensues-with-crypto-locker-shotodor-backdoor/ (2020), Accessed on Feb 2021
5. Datto: Datto's global state of the channel ransomware report. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf (2020), Accessed on Feb 2021
6. GROUP-iB: The evolution of ransomware and its distribution methods. https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Ransomware_whitepaper_eng.pdf?mkt_tok=eyJpIjoiTURRd09XRXhZVFpsTXpJMiIsInQiOiJveklIclN0d0dYWXl2ZFQ3XC9ZYVE3VEtcL3lJV0k0WkYzdXNyQkZoajFNWUpnN0FaTTJhaUhBaklDazdhQjRkWVJFVUxqeFhXRzlIZkpZQ2V5bkJzc1hSbkxxa0xXUHFaM2tsUW5CTE85V0JJT0g5NWw5eEFnR2t1TEprVDRcL2s2SCJ9 (2020), Accessed on Feb 2021
7. GROUP-iB: Hi-tech crime trends 2020-2021. https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections/blob/master/Report/Group-IB/Group-IB_Hi-Tech_Crime_Trends_2019-2020_en.pdf (2020), Accessed on Feb 2021
8. Hurley, S.: The many paths through maze. https://www.crowdstrike.com/blog/maze-ransomware-deobfuscation/ (2020), Accessed on Feb 2021
9. Itkin, E., Cohen, I.: Exploit developer spotlight: The story of playbit. https://research.checkpoint.com/2020/graphology-of-an-exploit-playbit/ (2020), Accessed on Feb 2021
10. Loman, M.: How ransomware attacks. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf (2020), Accessed on Feb 2021
11. Mohurle, S., Patil, M.: A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science **8**(5), 1938–1940 (2017)
12. Mundo, A.: Ransomware maze. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/#_ftn1 (2020), Accessed on Feb 2021
13. Securenetwork: Revil/sodinokibi ransomware. https://www.secureworks.com/research/revil-sodinokibi-ransomware (2020), Accessed on Feb 2021
14. Singleton, C., Kiefer, C., Villadsen, O.: Ransomware 2020: Attack trends affecting organizations worldwide. https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/