A Detailed Walkthrough of Ranzy Locker Ransomware TTPs

Keep up to date with latest blog posts

As we all observed, the number of ransomware attacks increased dramatically in 2021. Since late 2020, the Ranzy Locker ransomware has been responsible for dozens of high-profile breaches. Essentially, Ranzy is a rebranded and improved version of the ThunderX ransomware. Since a free decryption tool of ThunderX is released, Ranzy Locker has been released by the threat actors. Note that the Tor onion URL used by Ranzy was the same as the one previously used by the Ako ransomware. So, it is also a successor of Ako.

Ranzy threat actors also have established a Ransomware as a Service (RAAS) model and utilize the double extortion tactic. In other words, they exfiltrate critical data before encrypting files and threaten the victim with the release of the exfiltrated data to encourage ransom payment.

According to the flash report of the FBI, the Ranzy Locker ransomware gang had compromised over 30 businesses in the U.S. alone as of July 2021. Victims of ransomware are in various sectors, such as manufacturing, government, transformation, and IT.

We provide the tactics, techniques, and procedures (TTPs) used by the Ranzy Locker threat actors in this blog post because detecting and blocking a threat's TTPs is the most effective method of preventing that threat. TTPs enable us to identify potential intrusions and analyze the behavior of threat actors.

Tactics, Techniques, and Procedures (TTPs) used by Ranzy Locker Ransomware

This section presents the malicious behaviors of the Ranzy Locker ransomware group. Our analysis uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 10 framework. See the ATT&CK Matrix for Enterprise v10 for all referenced tactics and techniques.

1. Initial Access

The Initial Access tactic includes techniques used by attackers to gain an initial foothold within a network, such as exploiting vulnerabilities on public-facing web servers.

1.1. ATT&CK T1190 Exploit Public-Facing Application

Ranzy Locker operators leverage known Microsoft Exchange Server vulnerabilities to compromise target systems.

1.2. ATT&CK T1566 Phishing

The Ranzy Locker ransomware is also distributed via phishing campaigns.

1.3. ATT&CK T1078 Valid Accounts

The ransomware gang leverages valid accounts with Remote Desktop Protocol (RDP) to access target systems.

2. Execution

This tactic includes techniques that result in adversary-controlled code running on a local or remote system. The execution technique cannot be detached from other techniques; it is often paired with techniques from all other tactics.

2.1. MITRE ATT&CK T1106 Native API

Adversaries can execute behaviors directly through the native OS application programming interface (API). The Ranzy Locker ransomware leverages Windows API for a variety of operations, such as enumerating shared resources, as explained below.

3. Defense Evasion

Defense evasion techniques are used by adversaries to avoid detection by security controls.

3.1. ATT&CK T1027 Obfuscated Files or Information

The Ranzy Locker ransomware uses Base64 encoding to obfuscate its configuration in the ransom note.

3.2. ATT&CK T1497 Virtualization/Sandbox Evasion

Adversaries may use a variety of techniques to detect and avoid virtualization and analysis environments. This may include altering behavior in response to the detection of artifacts indicative of a virtual machine (VM) environment or sandbox. If the adversary detects a VM environment, they may modify their malware in order to disengage from the victim or conceal the implant's core functions. The Ranzy locker ransomware group uses IsDebuggerPresent API call to detect debuggers by checking if a program is running in debugging mode.

4. Credential Access

4.1. ATT&CK T1110 Brute Force

The ransomware gang acquires valid accounts through brute force.

5. Discovery

Adversaries use the techniques in the Discovery tactic to obtain information about the target environment, such as services, processes, network, files, software, system, accounts, domain, and registry.

5.1. ATT&CK T1083 File and Directory Discovery

The Ranzy Locker ransomware discovers critical files to exfiltrate, such as customer data, personally identifiable information (PII) files, and financial records. It uses GetLogicalDrives API call to enumerate all mounted drives, as also used by the Ryuk ransomware.

5.2. ATT&CK T1135 Network Share Discovery

Ranzi utilizes NetShareEnum API call for discovering shared resources, such as SMB network shares, to encrypt files stored in these resources. This API call is also used by the Conti ransomware. It also sends ARP broadcast requests for network device lookup.

5.3. ATT&CK T1057 Process Discovery

Adversaries get information about running processes to understand software and applications running on the system and shape follow-on behaviors. Ranzy uses Windows Native API calls to enumerate running processes.

5.4. ATT&CK T1120 Peripheral Device Discovery

The Ranzy Locker ransomware scans all drive letters to infect USB drives.

5.5. ATT&CK T1018 Remote System Discovery

Ranzy reads the host file (C:\Windows\System32\drivers\etc\hosts) to discover the hostname to IP address mappings of remote systems.

5.6. T1082 System Information Discovery

The ransomware queries the volume information to determine the disks in the system.

6. Impact

The Impact tactic covers techniques that manipulate, interrupt, or destroy your systems to disrupt availability, compromise integrity, or cover a confidentiality breach.

6.1. ATT&CK T1490 Inhibit System Recovery

Ranzy Locker ransomware attacks utilize multiple procedures to inhibit system recovery:

> First, it disables shadowcopy notifications using wmic.exe, a command-line utility to access Windows Management Instrumentation (WMI)

```
WMIC.exe  SHADOWCOPY /nointeractive
```

> Wbadmin is a built-in Windows tool that allows you to backup and restore your operating system, volumes, files, folders, and programs. Ranzy Locker uses wbadmin to delete system state backups with the following command:

```
wbadmin DELETE SYSTEMSTATEBACKUP
```

It also uses a more specific version of this command to delete the oldest system state backup:

```
wbadmin DELETE SYSTEMSTATEBACKUP - deleteOldest
```

> BCDEdit is a command-line tool for managing Boot Configuration Data (BCD) stores that are used to describe boot applications and boot application settings. Ranzy Locker uses bcdedit.exe twice to disable automatic Windows recovery features by modifying boot configuration data with the following commands, which are also used by REvil (Sodinokibi) and Nefilim ransomware families.

```
bcdedit /set {default} recoveryenabled No

bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

vssadmin (Volume Shadow Copy Service Admin) is another native Windows tool that can display current volume shadow copy backups and all installed shadow copy writers and providers. The Ranzy Locker ransomware abuses vssadmin.exe with the following command to delete all volume shadow copies on the system to prevent recovery, as also used by REvil (Sodinokibi).

vssadmin.exe Delete Shadows /All /Quiet

READ our blog post titled "An Underrated Technique to Delete Volume Shadow Copies - DeviceIoControl" to learn more about four methods used by ransomware threat groups to prevent the recovery of encrypted files from volume shadow copies.

6.2. ATT&CK T1486 Data Encrypted for Impact

Threat actors may encrypt data on target systems or on a large number of systems connected to a network to disrupt the system and network resource availability. They can make stored data unusable by encrypting files or data on local and remote drives, which is a common behavior of ransomware.

Ranzy uses the following encryption schemes.

- Salsa20 to encrypt files.
- RSA to encrypt Salsa20 keys.

Salsa20 is a faster encryption algorithm than RSA. So, they encrypt files with Salsa20, but encrypt the Salsa20 keys with a more secure but slower RSA 2048 bits encryption. This combination is also used by the recent BlackMatter ransomware.

Unfortunately, there is not a public Ranzy Locker ransomware decryption tool as of today.

Ranzy Locker creates a readme.txt file that includes the following instruction. It explains that the files were encrypted and stolen. So, Ranzy is double extortion ransomware like DarkSide.

—=== Ranzy Locker 1.1 ===—

Attention! Your network has been locked.
Your computers and server are locked now.
All encrypted files have extension: .ranzy

—- How to restore my files? —-

All files on each host in your network encrypted with strongest encryption algorithms
Backups are deleted or formatted, do not worry, we can help you restore your files

Files can be decrypted only with private key – this key stored on our servers
You have only one way for return your files back – contact us and receive universal decryption program

Do not worry about guarantees – you can decrypt any 3 files FOR FREE as guarantee

—- Contact us —-

You have two way to contact us:

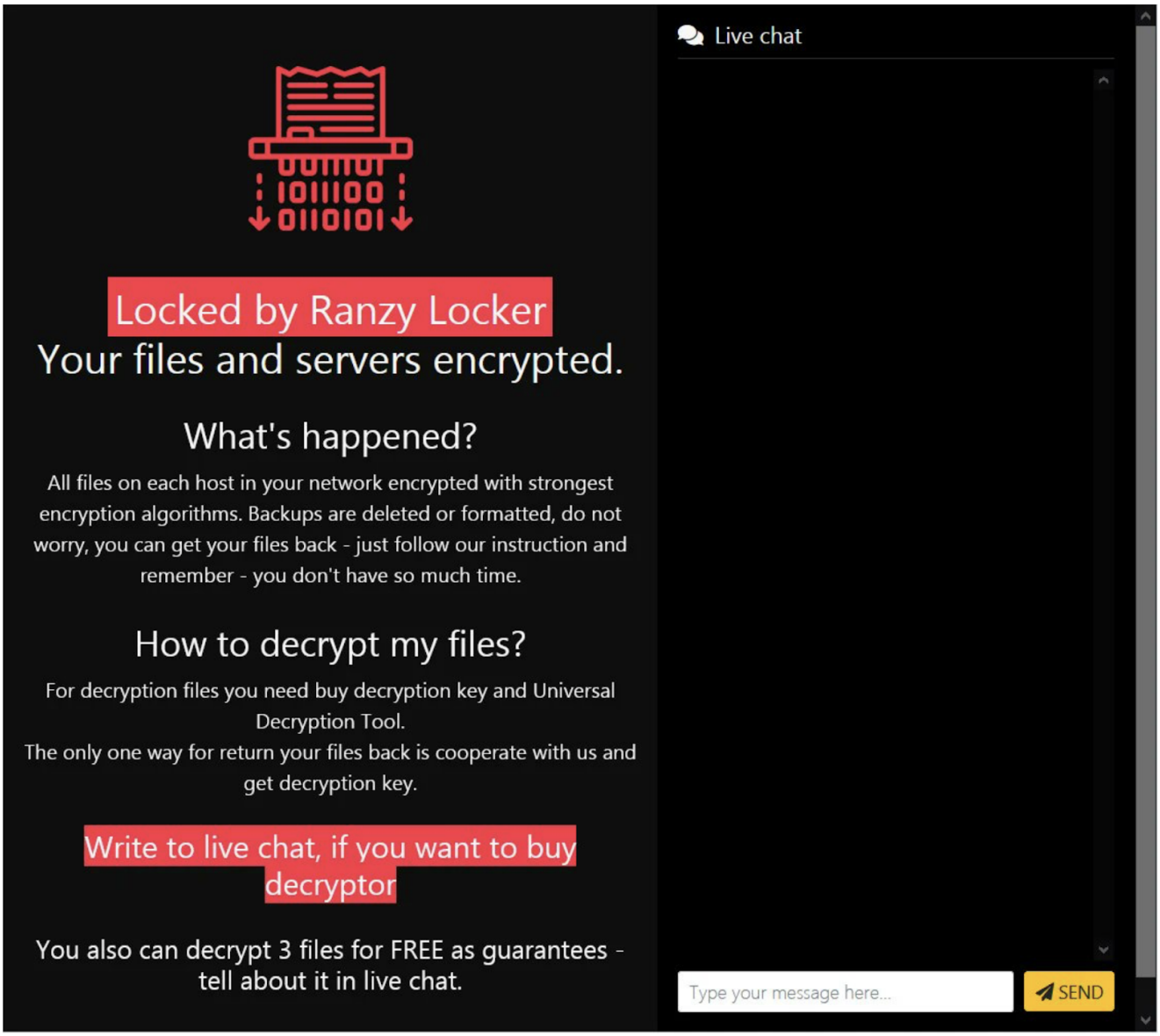
1. Open our recovery-website (can be open in any browser): hxxps://ranzylock.hk/N6CFBPYX

2. In case of link doesnt work open our mirror recovery-website via TOR Browser:
Download TOR Browser here: hxxps://www.torproject.org/download/
Open TOR mirror website:
http://a6a5b4ppnkrio3nikyutfexbc6y5dc6kfhj3jr32kdwbryr2lempkuyd.onion/N6CFBPYX

—- Data Leak Attention —-

!!! All your sensitive data was downloaded to our servers
!!! We are ready to publish this data in our blog with your Company Name, if you will not contact with us by email
!!! Only we can delete your files from our servers
!!! Only we can restore all your files without any LOSS

The Tor onion URL in the ransom note includes a live chat to learn detailed instructions for buying the decryption key.



How Picus Helps Simulate and Prevent the Ranzy Locker Ransomware

We strongly suggest simulating the Ranzy Locker ransomware to test the effectiveness of your security controls using the Picus Security Control Validation Platform. Picus Threat Library includes the following threats for the Ranzy Locker ransomware.

Picus ID	Threat Name
252070	Ranzy Locker Ransomware .EXE File Download Variant-1
845084	Ranzy Locker Ransomware .EXE File Download Variant-2

772539	Ranzy Locker Ransomware .EXE File Download Variant-3
700399	Ranzy Locker Ransomware .EXE File Download Variant-4
445953	Ranzy Locker Ransomware .EXE File Download Variant-5

Ranzy Locker Ransomware IOCs (Indicators of Compromise)

SHA256 Hashes

ade5d0fe2679fb8af652e14c40e099e0c1aaea950c25165cebb1550e33579a79

bbf122cce1176b041648c4e772b230ec49ed11396270f54ad2c5956113caf7b7

c4f72b292750e9332b1f1b9761d5aefc07301bc15edf31adeaf2e608000ec1c9

393fd0768b24cd76ca653af3eba9bff93c6740a2669b30cf59f8a064c46437a2

90691a36d1556ba7a77d0216f730d6cd9a9063e71626489094313c0afe85a939