WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact the FBI immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Indicators of Compromise Associated with Ranzy Locker Ransomware

Summary

The FBI first identified Ranzy Locker ransomware in late 2020 when the variant began to target victims in the United States. Unknown cyber criminals using Ranzy Locker ransomware had compromised more than 30 US businesses as of July 2021. The victims include the construction subsector of the critical manufacturing sector, the academia subsector of the government facilities sector, the information technology sector, and the transportation sector.

A majority of victims reported the actors conducted a brute force attack targeting Remote Desktop Protocol (RDP) credentials to gain access to the victims’ networks. Recent victims reported the actors leveraged known Microsoft Exchange Server vulnerabilities and phishing as the means of compromising their networks. The actors attempted to locate important files to exfiltrate, such as customer information, PII related files, and financial records. Ranzy Locker is deployed to encrypt files on compromised Windows host systems (including servers and virtual machines) and attached network shares. The Ranzy Locker executable leaves a ransom note in all directories where encryption occurred demanding the victim pay a ransom in exchange for a
decryption tool. In an example of double extortion techniques, Ranzy actors in some cases have demanded a second ransom from the victim in exchange for not leaking the data on the Internet.

**Technical Details and Indicators**

The FBI identified the following indicators of compromise (IOCs) that we assess are likely associated with Ranzy Locker activity.

**New User Accounts**

The Ranzy Locker actors may establish new accounts on domain controllers, servers, workstations, or the active directories. Newly created accounts with the name “felix” have been observed on at least three victims of the ransomware.

**Ransom Note**

The ransom note for Ranzy Locker has similarities to the wording in both the AKO and ThunderX ransom notes. An example of the notes is below:

```
Ranzy Locker 1.1

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

How to restore my files? -----

For return your files back - contact us and receive universal decryption program
You have only one way for restore your files

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

How to get your files back -----

You have 2 ways for open our website and contact with us:
1. Open via any browser (this way can be blocked so its better to use way 2)
   a. Open any browser.
   b. Open our website: https://ranzylock.hk/RyA0Q240

2. Open via TOR Browser:
   a. Download TOR Browser here: https://www.torproject.org/download/
   b. Open TOR website: https://a8o5b0npnja36kyrjef6xcgycy58dc4fjftj3jr3244bwry21empkuyd.onion/RyA0Q240

!! This page can be open only in TOR Browser.
All instructions how to decrypt your files you can find on our website.

Recovery information ----

key: [redacted]
personal id: [redacted]

The key found in the ransom note is a base64 encoded string, which when decoded reads:

```
{"ext":".ranzy","network":"true/false","subID":"####","lang":"xx-XX."}
```

1 Around October 2020 both AKO and ThunderX rebranded themselves as Ranzy Locker Ransomware.
The .ext extension parameter is typically .ranzy for Ranzy Locker 1.1, and the network parameter is typically set to true. The lang parameter is the language of the computer, such as “en-US.”

The subID parameter is an integer and is the name of the Ranzy Locker executable on the system. For example, if the subid is 0000, then the Ranzy Locker executable’s name is 0000.exe.

**Ransomware Executable**

The name of the Ranzy Locker executable is the subID found in the key on the ransom note. It is a 32-bit portable executable (PE), and all samples observed on different victims have different hash values but identical functionality. The executable requires administrator credentials to run.

Each Ranzy Locker executable contains the same hex encoded strings. Some of these strings are commands used to delete any backups on the system. The table below has the hex string, decoded string, and explanation of the string (if known):

<table>
<thead>
<tr>
<th>Hex Strings</th>
<th>Decoded Strings</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>476C6662616C5C33353335354641352D303745392D343238422D423541352D31433838431423242343838</td>
<td>Global\35355FA5-07E9-428B-B5A5-1C88CAB2B488</td>
<td>GUID/UUID</td>
</tr>
<tr>
<td>726561646D652E747874</td>
<td>readme.txt</td>
<td>Ransom note name</td>
</tr>
<tr>
<td>776D69632E65786520534841444F57434F5059202F66F696E746572616374697665</td>
<td>wmic.exe SHADOWCOPY/nointeractive</td>
<td>Disables shadow copy notification</td>
</tr>
<tr>
<td>776261646D696E2044454C455445203553544454D34154454241434B550</td>
<td>wbadmin DELETE SYSTEMSTATEBACKUP</td>
<td>Deletes system state backups</td>
</tr>
<tr>
<td>776261646D696E2044454C455445203553544454D34154454241434B550</td>
<td>wbadmin DELETE SYSTEMSTATEBACKUP - deleteOldest</td>
<td>Deletes oldest system state backup</td>
</tr>
<tr>
<td>626364656469742E657865202F736574207B6465661756C747D207265636F76657279656E61626C6542404EF6</td>
<td>bcdedit.exe /set {default} recoveryenabled No</td>
<td>Disables auto startup repair</td>
</tr>
<tr>
<td>626364656469742E657865202F736574207B6465661756C747D206266F6F7437461477573706F6C69637920696766F7265616C6661696C75726573</td>
<td>bcdedit.exe /set {default} bootstatuspolicyignoreallfailures</td>
<td>Disables Windows Error Recovery</td>
</tr>
</tbody>
</table>
As these hex strings are present in all Ranzy Locker samples, they provide points for detection such as with YARA. A sample YARA rule can be found here: https://www.tutorialjinni.com/ranzy-ransomware-sample-download.html

**Sample Ranzy Yara Rule:**

```yara
rule Ranzy_Locker_Ransomware {
    meta:
        description = "Ranzy Locker Ransomware"
        date = "2020-11-28"
        hash1 = "393fd0768b24cd76ca653af3eba9bf93c6740a2669b30cf59f8a864c46437a2"
        hash2 = "98691a361d556ba777d0216f7386cd9a9063e716264899431c0afe85a939"
        hash3 = "ade5d0fe2679fb8af652e1440e9990c1a99eb95c25165eb1b1590e33579a79"
        hash4 = "baf122ce1176b41648c4e772b230ee49ed11396270f54ad2c5956113cafeb7b"n        hash5 = "c47f72b297278e9323c16b19761de3eaefc07301b0f9def31adeaf26680000c1c9"
    strings:
        $s1 = "7767361646DE962E6578652044656C65746520536861646F7773202F416C6C202F5175696574" vssadmin.exe Delete Shadows /All /Quiet Deletes all Volume Shadow Copies
        $s2 = "534f4654574152455c4d696e2044656c65746520536861646f773202f416c6c202f5175696574" C:\Program Files\Microsoft SQL Server SQL server path
        $s3 = "433a5C50726F72616D2046696C65735C4D6963726F73666742053514C20536572766572" C:\Program Files (x86)\Microsoft SQL Server SQL server path
        $s4 = "544F465457412044656C65746520536861646F773202F416C6C202F5175696574" SOFTWARE\Microsoft\ERID Registry key
        $s5 = "49444D656C65746520536861646F773202F416C6C202F5175696574" ID
        $s6 = "433A5C50726F72616D2046696C65735C4D6963726F73666742053514C20536572766572" C:\Program Files\Microsoft SQL Server SQL server path
        $s7 = "534f4654574152455c4d696e2044656c65746520536861646f773202f416c6c202f5175696574" C:\Program Files (x86)\Microsoft SQL Server SQL server path
        $s8 = "544F465457412044656C65746520536861646F773202F416C6C202F5175696574" SOFTWARE\Microsoft\ERID Registry key
        $s9 = "49444D656C65746520536861646F773202F416C6C202F5175696574" ID
        $s10 = "433A5C50726F72616D2046696C65735C4D6963726F73666742053514C20536572766572" C:\Program Files\Microsoft SQL Server SQL server path
        $s11 = "534f4654574152455c4d696e2044656c65746520536861646f773202f416c6c202f5175696574" C:\Program Files (x86)\Microsoft SQL Server SQL server path
        $s12 = "544F465457412044656C65746520536861646F773202F416C6C202F5175696574" SOFTWARE\Microsoft\ERID Registry key
        $s13 = "49444D656C65746520536861646F773202F416C6C202F5175696574" ID
        $s14 = "433A5C50726F72616D2046696C65735C4D6963726F73666742053514C20536572766572" C:\Program Files\Microsoft SQL Server SQL server path
        $s15 = "534f4654574152455c4d696e2044656c65746520536861646f773202f416c6c202f5175696574" C:\Program Files (x86)\Microsoft SQL Server SQL server path
        $s16 = "544F465457412044656C65746520536861646F773202F416C6C202F5175696574" SOFTWARE\Microsoft\ERID Registry key
        $s17 = "49444D656C65746520536861646F773202F416C6C202F5175696574" ID
        $s18 = "433A5C50726F72616D2046696C65735C4D6963726F73666742053514C20536572766572" C:\Program Files\Microsoft SQL Server SQL server path
        $s19 = "534f4654574152455c4d696e2044656c65746520536861646f773202f416c6c202f5175696574" C:\Program Files (x86)\Microsoft SQL Server SQL server path
        $s20 = "544F465457412044656C65746520536861646F773202F416C6C202F5175696574" SOFTWARE\Microsoft\ERID Registry key
        $s21 = "49444D656C65746520536861646F773202F416C6C202F5175696574" ID
        $s22 = "433A5C50726F72616D2046696C65735C4D6963726F73666742053514C20536572766572" C:\Program Files\Microsoft SQL Server SQL server path
        $s23 = "534f4654574152455c4d696e2044656c65746520536861646f773202f416c6c202f5175696574" C:\Program Files (x86)\Microsoft SQL Server SQL server path
        $s24 = "544F465457412044656C65746520536861646F773202F416C6C202F5175696574" SOFTWARE\Microsoft\ERID Registry key
        $s25 = "49444D656C65746520536861646F773202F416C6C202F5175696574" ID
        "network":" Ransom note key parameter
        $s26 = "subid":" Ransom note key parameter
        $s27 = "lang":" Ransom note key parameter

    condition:
        any match $s1 or $s2 or $s3 or $s4 or $s5
}
```
In addition to encrypting files and deleting all backups found on the computer, the Ranzy Locker executable attempts to move laterally to other machines on the same network.

**Additional Resources:**

For additional resources related to the prevention and mitigation of ransomware, go to [https://www.stopransomware.gov](https://www.stopransomware.gov) as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) [Joint Ransomware Guide](https://www.cisa.gov). Stopransomware.gov is the U.S. Government’s new, official one-stop location for resources to tackle ransomware more effectively.
Recommended Mitigations:

- Implement regular backups of all data to be stored as air gapped, password protected copies offline. Ensure these copies are not accessible for modification or deletion from any system where the original data resides.
- Implement network segmentation, such that all machines on your network are not accessible from every other machine.
- Install and regularly update antivirus software on all hosts, and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind. Do not give all users administrative privileges.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs for any unusual activity.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Use double authentication when logging into accounts or services.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.
Administrative Note

This product is marked TLP: WHITE. The information in this product may be shared with peers and partner organizations within your sector or community, but not via publicly accessible channels.

Your Feedback Regarding this Product is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:

https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through your FBI Field Office.