

TLP: WHITE



FBI *FLASH*

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

25 Oct 2021

FLASH Number

CU-000153-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP: WHITE**

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

TLP: WHITE

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):

Hex Strings	Decoded Strings	Explanation
476C6F62616C5C333533353546 41352D303745392D343238422 D423541352D31433838434142 3242343838	Global\35355FA5-07E9-428B- B5A5-1C88CAB2B488	GUID/UUID
726561646D652E747874	readme.txt	Ransom note name
776D69632E6578652053484144 4F57434F5059202F6E6F696E74 6572616374697665	wmic.exe SHADOWCOPY /nointeractive	Disables shadow copy notification
776261646D696E2044454C4554 452053595354454D5354415445 4241434B5550	wbadmin DELETE SYSTEMSTATEBACKUP	Deletes system state backups
776261646D696E2044454C4554 452053595354454D5354415445 4241434B5550202D64656C657 4654F6C64657374	wbadmin DELETE SYSTEMSTATEBACKUP - deleteOldest	Deletes oldest system state backup
626364656469742E657865202F 736574207B64656661756C747 D207265636F76657279656E616 26C6564204E6F	bcdedit.exe /set {default} recoveryenabled No	Disables auto startup repair
626364656469742E657865202F 736574207B64656661756C747 D20626F6F74737461747573706 F6C6963792069676E6F7265616 C6C6661696C75726573	bcdedit.exe /set {default} bootstatuspolicyignoreallfailures	Disables Windows Error Recovery

76737361646D696E2E65786520 44656C65746520536861646F77 73202F416C6C202F5175696574	vssadmin.exe Delete Shadows /All /Quiet	Deletes all Volume Shadow Copies
433A5C50726F6772616D20466 96C65735C4D6963726F736F667 42053514C20536572766572	C:\Program Files\Microsoft SQL Server	SQL server path
433A5C50726F6772616D20466 96C65732028783836295C4D69 63726F736F66742053514C2053 6572766572	C:\Program Files (x86)\Microsoft SQL Server	SQL server path
534F4654574152455C4D696372 6F736F66745C45524944	SOFTWARE\Microsoft\ERID	Registry key
4944	ID	
7B5041545445524E5F49447D	{PATTERN_ID}	
7B4558547D	{EXT}	
7B5549447D	{UID}	
22657874223A22	"ext":	Ransom note key parameter
226B6579223A22	"key":	Ransom note key
226E6574776F726B223A22	"network":	Ransom note key parameter
227375626964223A22	"subid":	Ransom note key parameter
226C616E67223A22	"lang":	Ransom note key parameter

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:
rule Ranzy_Locker_Ranomware {
meta:
description = "Ranzy Locker Ranomware"
reference = "https://labs.sentinelone.com/ranzy-ransomware-better-encryption-among-new-features-of-thunderx-derivative/"
date = "2020-11-20"
hash1 = "393fd0768b24cd76ca653af3eba9bfff93c6740a2669b30cf59f8a064c46437a2"
hash2 = "90691a36d1556ba7a77d0216f730d6cd9a9063e71626489094313c0afe85a939"
hash3 = "ade5d0fe2679fb8af652e14c40e099e0c1aeea950c25165cebb1550e33579a79"
hash4 = "bbf122cce1176b041648c4e772b230ec49ed11396270f54ad2c5956113caf7b7"
hash5 = "c4f72b292750e9332b1f1b9761d5aefc07301bc15edf31adeaf2e608000ec1c9"
strings:
$s1 = "776261646D696E2044454C4554452053595354454D53544154454241434B5550" ascii // 'wmic.exe SHADOWCOPY /nointeractive'
$s2 = "776D69632E65786520534841444F57434F5059202F6E6F696E746572616374697665" ascii // 'SOFTWARE\Microsoft\ERID'

```

```

$s3 = "76737361646D696E2E6578652044656C65746520536861646F7773202F416C6C202F5175696574" ascii //
'vssadmin.exe Delete Shadows /All /Quiet'
$s4 = "776261646D696E2044454C4554452053595354454D53544154454241434B5550202D64656C6574654F6C64657374"
ascii // 'wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest'
$s5 = "534F4654574152455C4D6963726F736F66745C45524944" ascii // 'SOFTWAREMicrosoftERID'
$s6 =
"626364656469742E657865202F736574207B64656661756C747D20626F6F74737461747573706F6C6963792069676E
6F7265616C6C6661696C75726573" // 'bcdedit.exe /set {default} bootstatuspolicyignoreallfailures'
$s7 = "7B5549447D" ascii // '{UID}'
$s8 = "7B5041545445524E5F49447D" ascii // '{PATTERN_ID}'
$s9 = "726561646D652E747874" ascii // 'readme.txt'
$s10 = "226E6574776F726B223A22" ascii // '"network":'
$s11 = "226C616E67223A22" ascii // '"lang":'
$s12 = "7B4558547D" ascii // '{EXT}'
$s13 = "476C6F62616C5C33353335354641352D303745392D3433238422D423541352D314338384341423242343838" //
'Global35355FA5-07E9-428B-B5A5-1C88CAB2B488'
$s14 = "433A5C50726F6772616D2046696C65735C4D6963726F736F66742053514C20536572766572" ascii //
'C:\ProgramFiles\Microsoft SQL Server'
$s15 = "433A5C50726F6772616D2046696C65732028783836295C4D6963726F736F66742053514C20536572766572" ascii
// 'C:\Program Files (x86)\Microsoft SQL Server'
$s16 = "227375626964223A22" ascii // '"subid":'
$s17 = "22657874223A22" ascii // '"ext":'
$s18 = "226B6579223A22" ascii // '"key":'
// seq encrypt
$seq1 = { 8b 46 50 8d 4d a4 83 7d d4 10 53 8b 1d 14 80 41 00 89 45 a4 8d 45 c0 0f 43 45 c0 51 50 6a 00
6a 01 6a 00 ff 35 e8 1c 42 00 ff d3 85 c0 0f 84 b9 00 00 00 8b 46 68 8d 4d a4 83 7d ec 10 57 89 45 a4
8d 45 d8 0f 43 45 d8 33 ff 51 50 6a 00 47 57 6a 00 ff 35 e8 1c 42 00 ff d3 85 c0 0f 84 8a 00 00 00 c6
45 fc 02 33 db 8b 45 e8 8b 4d d0 03 c1 6a 0f 5a 89 5d b8 89 55 bc 88 5d a8 89 7d a4 3b c2 76 15 88 5d
a0 8d 4d a8 ff 75 a0 50 e8 78 02 00 00 8b 4d d0 89 5d b8 83 7d d4 10 8d 45 c0 51 0f 43 45 c0 8d 4d a8
50 e8 ca de ff ff 83 7d ec 10 8d 45 d8 ff 75 e8 0f 43 45 d8 8d 4d a8 50 e8 b3 de ff ff 8d 45 a8 50 8d
4e 70 e8 b8 d8 ff ff 8d 4d a8 e8 3f bf ff ff 8d 4d d8 e8 37 bf ff ff 8d 4d c0 e8 2f bf ff ff b0 01 eb
12 8d 4d d8 e8 23 bf ff ff 8d 4d c0 e8 1b bf ff ff 32 c0 e8 3f f1 }
//seq recon
$seq2 = { 8b 75 08 33 ff 8b 55 0c 33 c0 89 b5 68 fb ff ff 89 bd ac fb ff ff c7 85 b0 fb ff ff 07 00 00
00 66 89 85 9c fb ff ff 89 7d fc 39 7a 10 0f 84 da 00 00 00 6a 02 0f 57 c0 8d 8d 84 fb ff ff 58 66 0f
13 85 bc fb ff ff 66 89 85 b4 fb ff ff e8 6e ac ff ff 83 78 14 10 72 02 8b 00 50 ff 15 18 82 41 00 8d
8d 84 fb ff ff 89 85 b8 fb ff ff e8 8f a8 ff ff 68 87 69 00 00 ff 15 0c 82 41 00 bb 01 04 00 00 66 89
85 b6 fb ff ff 53 8d 85 c4 fb ff ff 57 50 e8 fd 2d 00 00 83 c4 0c 8d 7d cc 33 c0 6a 08 59 6a 08 6a 20 f3
ab 8d 45 cc 50 53 8d 85 c4 fb ff ff 50 6a 10 8d 85 b4 fb ff ff 50 ff 15 1c 82 41 00 85 c0 75 45 8d 85
c4 fb ff ff 50 8d 8d 6c fb ff ff e8 7f a8 ff ff 8b d0 c6 45 fc 01 8d 8d 84 fb ff ff e8 26 ab ff ff 50
8d 8d 9c fb ff ff e8 88 bf ff ff 8d 8d 84 fb ff ff e8 c8 c2 ff ff 8d 8d 6c fb ff ff e8 f5 a7 ff ff 8d
85 9c fb }
condition:
uint16(0) == 0x5a4d and filesize > 80KB and 10 of ($s*) and 1 of ($seq*)
}

```

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> as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) [Joint Ransomware Guide](#). 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.