TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

7 MARCH 2022

FLASH Number

CU-000163-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 your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

RagnarLocker Ransomware Indicators of Compromise

Summary

The FBI first became aware of RagnarLocker in April 2020 and subsequently produced a FLASH to disseminate known indicators of compromise (IOCs) at that time. This FLASH provides updated and additional IOCs to supplement that report. As of January 2022, the FBI has identified at least 52 entities across 10 critical infrastructure sectors affected by RagnarLocker ransomware, including entities in the critical manufacturing, energy, financial services, government, and information technology sectors. RagnarLocker ransomware actors work as part of a ransomware family[1], frequently changing obfuscation techniques to avoid detection and prevention.

[1] Ransomware family is a group of binaries associated to several ransomware variants or actor groups.

Technical Details

RagnarLocker is identified by the extension ".RGNR_<ID>," where <ID> is a hash of the computer's NETBIOS name. The actors, identifying themselves as "RAGNAR_LOCKER," leave a .txt ransom note, with instructions on how to pay the ransom and decrypt the data. RagnarLocker uses VMProtect, UPX, and custom packing algorithms and deploys within an attacker's custom Windows XP virtual machine on a target's site.

Ragnar Locker uses Windows API GetLocaleInfoW to identify the location of the infected machine. If the victim location is identified as "Azerbaijani," "Armenian," "Belorussian," "Kazakh," "Kyrgyz," "Moldavian," "Tajik," "Russian," "Turkmen," "Uzbek," "Ukrainian," or "Georgian," the process terminates.

RagnarLocker checks for current infections to prevent multiple transform encryption of the data, potentially corrupting it. The binary gathers the unique machine GUID, operating system product name, and user name currently running the process. This data is sent through a custom hashing algorithm to generate a unique identifier: <HashedMachineGuid>-<HashedWindowsProductName>-<HashedUser>-<HashedComputerName>-<HashedAllDataTogether>.

RagnarLocker identifies all attached hard drives using Windows APIs: CreateFileW, DeviceIoControl, GetLogicalDrives, and SetVolumeMountPointA. The ransomware assigns a drive letter to any volumes not assigned a logical drive letter and makes them accessible. These newly attached volumes are later encrypted during the final stage of the binary.

RagnarLocker iterates through all running services and terminates services commonly used by managed service providers to remotely administer networks. The malware then attempts to silently delete all Volume Shadow Copies, preventing user recovery of encrypted files, using two different methods:

- >vssadmin delete shadows /all /quiet
- >wmic.exe.shadowcopy.delete

Lastly, RagnarLocker encrypts all available files of interest. Instead of choosing which files to encrypt, RagnarLocker chooses which folders it will *not* encrypt. Taking this approach allows the computer to continue to operate "normally" while the malware encrypts files with known and unknown extensions containing data of value to the victim. For example, if the logical drive being processed is the C: drive, the malware does not encrypt files in the following folders:

- Windows

- Windows.old
- Mozilla
- Mozilla Firefox
- Tor browser
- Internet Explorer
- $Recycle.Bin
- Program Data
- Google
- Opera
- Opera Software

Also, when iterating through files, the malware does not encrypt files with the following extensions:

- .db
- .sys
- .dll
- .lnk
- .msi
- .drv
- .exe

Indicators

The following IOCs are associated with RagnarLocker ransomware, as of January 2022.

RagnarLocker IOCs as of January 2022		
IP address	**Context**	**Timeframe**
185.138.164.18	IP accessing confluence server	2021-09-03 10:53:56 - 2021-09-21 18:46:40
185.172.129.215	IP accessing confluence server	2021-09-01 20:49:56 - 2021-09-03 10:45:50
45.144.29.2	IP accessing confluence server	2021-09-12 21:34:13 -02021-09-16 14:28:19
23.106.122.192	IP seen with updt32.exe proxy malware	2021-09-27 20:07
45.90.59.131	IP resolution for secanalytics C2 domain	2021-09-17 16:27
149.28.200.140	IP address involved in PSCP activity	2021-09-10 19:20

IP address	Context	Timeframe
193.42.36.53	IP address resolution for windows-analytics-prod12ms[.]com	2021-10-01 14:41
45.63.89.250	IP address belonging to ctlmon.exe - GOTROJ malware	2021-09-11 13:13
190.211.254.181	IP address involved in data exfiltration	2021-10-27 11:30:35
142.44.236.38	IP address involved in data exfiltration	2021-11-03 8:16
37.120.238.107	IP address involved in data exfiltration	2021-10-19 21:22:48 - 2021-10-26 13:12:56
95.216.196.181	C2 embedded in malware (snmp.dat and bash.dat and esync.exe)	2021-11-11 19:20
162.55.38.44	C2 embedded in malware (snmp.dat and bash.dat and esync.exe)	2021-11-11 19:20
116.203.132.32	C2 embedded in malware (snmp.dat and bash.dat and esync.exe)	2021-11-11 19:20
49.12.212.231	C2 embedded in malware (snmp.dat and bash.dat and esync.exe)	2021-11-11 19:20
193.42.39.10	seen as argument to inetinfo.exe	2021-11-22 17:12
193.111.153.24	(ssl-secure-com2048[.]com) - bash, snmp, 7z, and psexec downloaded from this domain	2021-11-18 20:38
178.32.222.98	IP address involved in data exfiltration	2021-10-30 16:25
23.227.202.72	IP address involved in data exfiltration	2021-11-26 14:18:21 - 2021-12-14 11:12:19
159.89.163	NA	2021-06-05
50.201.185.11	NA	2021-03-26 19:28 UTC +3
47.35.60.92	NA	2021-09-03 11:40 UTC +3
108.26.193.165	NA	2021-05-13 14:01 GMT +3
108.56.142.135	NA	2021-03-25 17:16:55 GMT +1
198.12.81.56	NA	2021-10/11
198.12.127.199	NA	2021-10/11
45.91.93.75	NA	2021-03-18

IP address	Context	Timeframe
217.25.93.106	NA	2021-03-21
45.146.164.193	NA	2020-10-05
89.40.10.25	NA	2020-10-10
5.45.65.52	NA	NA
79.141.160.43 (URL: izugz.envisting.xyz)	NA	2021-05-24

Bitcoin Addresses:	Timeframe
19kcqKevFZhiX7NFLa5wAw4JBjWLcpwp3e	2021-04-30
1CG8RAqNaJCrmEdVLK7mm2mTuuK28dkzCU	2021-03
151Ls8urp6e2D1oXjEQAkvqogSn3TS8pp6	2021-02-27

Email Addresses:	Timeframe
ShingXuan7110@protonmail.com	2021-040-03
scanjikoon@yahoo.com	2021-05-25
alexeyberdin17@gmail.com (linked by SMS)	NA
titan_fall572cool@gmail.com	NA
Vivopsalrozor@yahoo.com	NA
Gamarjoba@mail.com	NA
back.shadow98@gmail.com (cookie-linked)	NA
michael.shawn.brown2@gmail.com	NA
Alexey_Berdin@list.ru	NA
sh0d44n@gmail.com	NA
alexeyberdin437@gmail.com	NA
alexeyberdin38@gmail.com	NA
alexeyberbi@gmail.com	NA

Information Requested:

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, or fund illicit activities. Paying the ransom also does not guarantee a victim's files will be recovered. However, the FBI understands when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization decides to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators and analysts with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks.

The FBI may seek the following information:

SHORT TERM ITEMS

- Copy of the ransom note (screen shot/picture/text file).
- Any discovered malicious IPs with time stamps/time zones (unusual RDP connections/unusual VPN connections/beacons to malicious IPs).
- Virtual currency addresses/amount of demand.
- Any malicious files (executables/binaries).
- Summary of timeline of events (dates of initial observation/malicious activity).
- Evidence of data exfiltration.

LONG TERM ITEMS

- Brief summary of where the IOCs came from.
- Incident response report.
- Copy of any communications with malicious actors.
- Forensic images and memory captures.
- Host and network logs.
- Any available decryptor.
- Scope of impact (amount of loss).

Recommended Mitigations:

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device. This information should not be accessible from the compromised network.

- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Use multi-factor authentication with strong passwords, including for remote access services.
- Keep computers, devices, and applications patched and up-to-date.
- Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords and settings.
- Consider adding an email banner to emails received from outside your organization.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Implement network segmentation.

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 Government's official one-stop location for resources to tackle ransomware more effectively.

CISA's Ransomware Readiness Assessment (RRA) is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

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, and 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**. Subject to standard copyright rules, the information in this product may be shared without restriction.