VULNERABILITY BULLETINS

FBI Releases Indicators of Compromise Associated with RagnarLocker Ransomware

TLP:WHITE

Mar 07, 2022

Health-ISAC is issuing a vulnerability bulletin regarding the United States Federal Bureau of Investigation's release of Indicators of Compromise (IOCs) associated with RagnarLocker ransomware. The FBI first became aware of RagnarlLocker in April 2020 and subsequently produced a Flash to disseminate known indicators of compromise (IOCs). This FLASH provides updated and additional IOCs to supplement that report.

As of January 2022, the FBI has identified numerous entities across several critical infrastructure sectors affected by RagnarLocker ransomware, including energy, financial services, government, and information technology sectors. RagnarLocker ransomware affiliates operate as a family and frequently change obfuscation techniques to avoid detection and prevention.

Health-ISAC is sharing these IOCs to increase sector awareness. Organizations are encouraged to ingest these IOCs manually if no automatic ingestion systems are implemented. For Health-ISAC members who have implemented the Health-ISAC Indicator Threat Sharing (HITS) program, the IOCs related to this alert have been automatically imported into your environment.

All members are encouraged to review the FBI FLASH (CU-000163-MW): RagnarLocker Ransomware Indicators of Compromise, which has been attached to this alert.

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

Reference(s)	IC3
Report Source(s)	FBI

Recommendations
FBI recommends network defenders apply the following mitigations to reduce the risk of compromise by RagnarLocker ransomware:

- 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.

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.

Release Date
Mar 07, 2022

Threat Indicator(s)

IP(s):
79[.]141[.]160[.]43

149[.]28[.]200[.]140
23[.]227[.]202[.]72
45[.]63[.]89[.]250
49[.]12[.]212[.]231
108[.]56[.]142[.]135
193[.]42[.]39[.]10
45[.]90[.]59[.]131
37[.]120[.]238[.]107
198[.]12[.]81[.]56
185[.]138[.]164[.]18
45[.]144[.]29[.]2
198[.]12[.]127[.]199
45[.]91[.]93[.]75
193[.]111[.]153[.]24
116[.]203[.]132[.]32
47[.]35[.]60[.]92
185[.]172[.]129[.]215
23[.]106[.]122[.]192
108[.]26[.]193[.]165
193[.]42[.]36[.]53
217[.]25[.]93[.]106
50[.]201[.]185[.]11
190[.]211[.]254[.]181
142[.]44[.]236[.]38
162[.]55[.]38[.]44
178[.]32[.]222[.]98
45[.]146[.]164[.]193
95[.]216[.]196[.]181
89[.]40[.]10[.]25
5[.]45[.]65[.]52

Email(s):
alexeyberdin437[@]gmail[.]com
titan_fall572cool[@]gmail[.]com
ShingXuan7110[@]protonmail[.]com
sh0d44n[@]gmail[.]com
alexeyberbi[@]gmail[.]com
Alexey_Berdin[@]list[.]ru
alexeyberdin17[@]gmail[.]com
alexeyberdin38[@]gmail[.]com
michael[.]shawn[.]brown2[@]gmail[.]com
Vivopsalrozor[@]yahoo[.]com
Gamarjoba[@]mail[.]com

scanjikoon[@]yahoo[.]com
back[.]shadow98[@]gmail[.]com

Alert ID c7e0ec4d

View Alert

Tags RagnarLocker ransomware

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**