FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

19 NOV 2020

Alert Number
MU-000140-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, 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.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order 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 criminals. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with Ragnar Locker Ransomware

Summary

The FBI first observed Ragnar Locker[1] ransomware in April 2020, when unknown actors used it to encrypt a large corporation's files for an approximately $11 million ransom and threatened to release 10 TB of sensitive company data. Since then, Ragnar Locker has been deployed against an increasing list of victims, including cloud service providers, communication, construction, travel, and enterprise software companies. The FBI is providing details of Ragnar Locker ransomware to assist with understanding the code and identifying the activity. Ragnar Locker actors first obtain access to a victim's network and perform reconnaissance to locate network resources, backups, or other sensitive files for data exfiltration. In the final stage of the attack, actors manually deploy the ransomware, encrypting the victim's data.

Technical Details

The Ragnar Locker ransomware family[2] is frequently changing obfuscation techniques to avoid detection and prevention. The Ragnar Locker ransomware is identified by the extension ".RGNR_<ID>," where <ID> is a hash of the computer's NETBIOS name. Furthermore, the actors, identifying themselves as "RAGNAR_LOCKER," leave a .txt ransom note, with instructions on how to pay

[1] Ragnar Locker, also written as RagnarLocker and Ragnar_Locker, has no association with Ragnarok ransomware.
[2] Ransomware family is a group of binaries associated to several ransomwares or actor groups.

the ransom and decrypt the data. Ragnar Locker has used VMProtect, UPX, and custom packing algorithms. Ragnar Locker has been deployed within an attacker's custom Windows XP virtual machine on a target's site.

Ragnar Locker uses Windows API GetLocaleInfoW to get the infected machine's current locale. If the victim's locale is found to be "Azerbaijani," "Armenian," "Belorussian," "Kazakh," "Kyrgyz," "Moldavian," "Tajik," "Russian," "Turkmen," "Uzbek," "Ukrainian," or "Georgian," the process will terminate.

```
00401F0E    mov dword ptr ss:[ebp-108],eax    [ebp-108]:L"Azerbaijani"
00401F14    lea eax,dword ptr ss:[ebp-6C]
00401F17    mov dword ptr ss:[ebp-104],eax    [ebp-104]:L"Armenian"
00401F1D    lea eax,dword ptr ss:[ebp-D8]
00401F23    mov dword ptr ss:[ebp-100],eax    [ebp-100]:L"Belorussian"
00401F29    lea eax,dword ptr ss:[ebp-28]
00401F2C    mov dword ptr ss:[ebp-FC],eax     [ebp-FC]:L"Kazakh"
00401F32    lea eax,dword ptr ss:[ebp-38]
00401F35    mov dword ptr ss:[ebp-F8],eax     [ebp-F8]:L"Kyrgyz"
00401F3B    lea eax,dword ptr ss:[ebp-94]
00401F41    mov dword ptr ss:[ebp-F4],eax     [ebp-F4]:L"Moldavian"
00401F47    lea eax,dword ptr ss:[ebp-C]
00401F4A    mov dword ptr ss:[ebp-F0],eax     [ebp-F0]:L"Tajik"
00401F50    lea eax,dword ptr ss:[ebp-48]
00401F53    mov dword ptr ss:[ebp-EC],eax     [ebp-EC]:L"Russian"
00401F59    lea eax,dword ptr ss:[ebp-58]
00401F5C    mov dword ptr ss:[ebp-E8],eax     [ebp-E8]:L"Turkmen"
00401F62    lea eax,dword ptr ss:[ebp-18]
00401F65    mov dword ptr ss:[ebp-E4],eax     [ebp-E4]:L"Uzbek"
00401F6B    lea eax,dword ptr ss:[ebp-A8]
00401F71    mov dword ptr ss:[ebp-E0],eax     [ebp-E0]:L"Ukrainian"
00401F77    lea eax,dword ptr ss:[ebp-80]
```

Figure 1 _ Code Snippet

The ransomware also checks for current infections to prevent multiple encryption transforms 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>.

The Ragnar Locker ransomware identifies all attached hard drives, whether assigned a drive letter or not, 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.

Ragnar Locker iterates through all running services and terminates services commonly used by managed service providers to remotely administer networks.

The list of services terminated includes:						
vss	sql	memtas	mepocs	sophos	dfs	splashtop
veeam	backup	pulseway	logme	logmein	mysql	connectwise

Ragnar Locker also terminates the following running processes:				
sql	mysql	veeam	oracle	ocssd
dbsnmp	synctime	agntsvc	isqlplussvc	xfssvccon
mydesktopservice	ocautoupds	encsvc	firefox	tbirdconfig
mydesktopqos	ocomm	dbeng50	sqbcoreservice	excel
infopath	msaccess	mspub	onenote	outlook
powerpnt	steam	thebat	thunderbird	visio
winword	wordpad	EduLink2SIMS	bengine	benetns
beserver	pvlsvr	beremote	VxLockdownServer	postgres
dfssvc.exe	SavService.exe	OWSTIMER	SAVAdminService	wsstracing
Fdhost	dfsrs.exe	sophos	WSSADMIN	swc_service.exe

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, Ragnar Locker encrypts all available files of interest. Instead of choosing which files to encrypt, Ragnar Locker 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
- Tor browser
- Internet Explorer
- Mozilla
- Mozilla Firefox
- $Recycle.Bin
- ProgramData

- 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

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.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Use multi-factor authentication with strong passwords.
- Keep computers, devices, and applications patched and up-to-date.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at CyWatch can be contacted by phone at (855) 292-3937 or by email at CyWatch@fbi.gov. 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. Press inquiries should be directed to the FBI's national Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback on the Value of 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 FBI CYWATCH.