FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

5 MAY 2020

Alert Number

MU-000126-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 to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

Latest Tactics, Techniques, and Procedures Associated with Ryuk Ransomware and Recommended Mitigation

Summary

Unknown cybercriminals have targeted more than 1,000 US and international businesses with Ryuk ransomware since approximately August 2018. Once the victim has been compromised, Ryuk encrypts all the network's data files and the actors demand sums of up to $24 million worth of Bitcoin (BTC) in exchange for a decryptor program. Ryuk's targets are varied, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. While Ryuk impacts a range of industries, attacks have had a disproportionate impact on logistics companies, technology companies, healthcare organizations, and municipalities.

Technical Details

Ryuk first appeared in August 2018 as a derivative of Hermes 2.1 ransomware, which first emerged in late 2017 and was available for sale on the open market as of August 2018. Ryuk still retains some aspects of the Hermes code. For example, all of the files encrypted by Ryuk contain the "HERMES" tag but in some infections the files have

`.ryuk` to the filename, while others do not. In other parts of the ransomware code, Ryuk has removed or replaced features of Hermes, such as the restriction against targeting specific Eurasia-based systems.

The exact infection vector may vary, but typically Ryuk has been deployed as a payload from Trickbot and/or Emotet banking Trojans. Further details regarding Trickbot can be found in FBI FLASH Alert Number MC-000100-MW, dated 22 October 2018.

While negotiating the victim network, Ryuk actors will commonly use commercial off-the-shelf products such as Cobalt Strike and PowerShell Empire in order to steal credentials. Both frameworks are very robust and are highly effective dual-purpose tools, allowing actors to dump clear text passwords or hash values from memory with the use of Mimikatz. This allows the actors to inject malicious dynamic-link library (DLL) into memory with read, write, execute (RWX) permissions. In order to maintain persistence in the victim environment, Ryuk actors have been known to use scheduled tasks and service creation.

Ryuk actors will quickly map the network in order to enumerate the environment to understand the scope of the infection. In order to limit suspicious activity and possible detection, the actors choose to live off the land and, if possible, use native tools such as `net view`, `net computers`, and `ping` to locate mapped network shares, domain controllers, and active directory. In order to move laterally throughout the network, the group relies on native tools such as PowerShell, Windows Management Instrumentation (WMI), Windows Remote Management (WinRM), and Remote Desktop Protocol (RDP). The group additionally will use third party tools such as Bloodhound.

Once dropped, Ryuk uses AES-256 to encrypt files and an RSA public key to encrypt the AES key. The Ryuk dropper drops a .bat file that attempts to delete all backup files and Volume Shadow Copies (automatic backup snapshots made by Windows), preventing the victim from recovering encrypted files without the decryption program.

In addition, the attackers will attempt to shut down or uninstall security applications on the victim systems that might prevent the ransomware from executing. Normally this is done via a script, but if that fails, the attackers are capable of manually removing the applications that could stop the attack. The `RyukReadMe` file placed on the system after encryption provides either one or two email addresses, using the end-to-end encrypted email provider Protonmail, through which the victim can contact the attacker(s). While earlier versions provide a ransom amount in the initial notifications, Ryuk users are now designating a ransom amount only after the victim makes contact.

The victim is told how much to pay to a specified BTC wallet for the decryptor and is provided a sample decryption of two files.

Initial testing indicates that the `RyukReadMe` file does not need to be present for the decryption script to run successfully but other reporting advises some files will not decrypt properly without it. Even if run correctly, there is no guarantee the decryptor will be effective. This is further complicated because the `RyukReadMe` file is deleted when the script is finished. This may affect the decryption script unless it is saved and stored in a different location before running.

Indicators

The following are new tactics, techniques, and procedures that have been observed in samples of Ryuk malware since the previous FBI Ryuk FLASH released in May 2019:

Precursors to Deployment of Ryuk Ransomware

- Ryuk actors will commonly use Cobalt Strike. Many of the payload settings in the framework are malleable to help prevent detection. Should the actors decide to use the default Cobalt Strike Agent, environments whose Operating Systems and Browsers are up to date should be able to detect the beacon traffic commonly seen over destination port 443. The default User Agent String for the Cobalt Strike Agent is shown on the next page.

  User-Agent:

  ```
  Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
  Trident/5.0; XXXX)
  ```

  The above User Agent String is consistent with a Windows 7, IE 9.0 environment. If the host environment is not that specific combination of OS and browser, this traffic should be flagged as potentially malicious. **Please note** - *User Agent Stings are trivial to spoof, so the above example should not be used as an automated IOC without testing in your environment for false positives.*

- To move laterally throughout the network, the group relies on the tools Windows Management Instrumentation (WMI), Windows Remote Management (WinRM), and Remote Desktop Protocol (RDP).

In environments where WMI and WinRM are not commonly used, monitoring logs will help detect suspicious activity.

Systems that have RDP disabled by default, or Group Policy Object, should monitor for changes in firewall settings via built in commands such as:

```
netsh advfirewall
```

Detect modified registry keys allowing actors access remotely via Terminal Services using the string:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
```

The aforementioned TTPs are by no means inclusive, nor entirely unique to the Ryuk actors, but highlight known tools and techniques used by the group prior to deploying the Ryuk ransomware through the domain via psexec / batch scripts or Group Policy Object.

Commands Used by Ryuk

- Ryuk leverages the iCACLS command to avoid permission issues. The iCACLS command gives the ability to display or change Access Control Lists (ACLs) for files and folders on the file system. Ryuk leverages iCACLS by using the following command:

```
icacls "M:\*" /grant Everyone: F /T /C /Q
```

- Ryuk is commonly seen using the vssadmin command, which administers settings for System Restore. Ryuk uses the vssadmin to delete all shadow copies using the following command:

```
cmd.exe /c "vssadmin.exe Delete Shadows /all /quiet"
```

- Ryuk also uses Windows Management Interface Command (WMIC) to delete shadow copies using the following command:

```
cmd /c "WMIC.exe shadowcopy delete"
```

- Ryuk uses the following commands to disable the built-in Windows Automatic Startup Repair:

```
cmd.exe /c "bcdedit /set {default} recoveryenabled No &bcdedit /set
{default}"
cmd.exe /c "bootstatuspolicy ignoreallfailures"
```

Ryuk file formats

While not the sole file format, Ryuk often uses a 12-character naming convention for the unpacked version of the executable that runs on the victim network. Other commonly used naming conventions include a three-character repetition with the middle character capitalized such as xXx.exe, vVv.exe, or yYy.exe; or a pattern of a single digit or letter such as 1.exe, 2.exe, r.exe, etc. The Ryuk file originally pulled into the network is a packed executable. Usually this version is deleted after the secondary version is unpacked. This file usually has a format of a few alphanumeric characters followed by a dash and a number. For example, `fx1-232.exe` or `r2-114.exe`.

Host Based Indicators		
Mutex:	efkrm4tgkl4ytg4, FakeMutex	
Registry:	Key Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
	Value:	svchos
	Date Type:	REG_SZ
File:	Depending on the Windows version, one of the following: C:\users\Public\sys C:\Documents and Settings\Default User\sys	
Ransom note Files:	RyukReadMe.txt" and numerous encrypted filed, which were not renamed, but have the "HERMES" tag followed by an encrypted key at the end of the file (alternatively filed with the .RYK extension	

Network Indicators (not common)	
HTTP GET request:	GET /Lfkgnt5lkgngl3knfl3.php?UI=v9&ID=1140 HTTP/1.1;
User-Agent string:	Microsoft Internet Explorer
IP address:	5.188.231.138

Recommended Mitigations

A key step to limit damage and lower risk to your environment is to establish and maintain a solid foundation of industry best practices, which can help mitigate the threat and reduce your organization's attack surface. Mitigation steps for a malware such as Ryuk involve two different components: those steps that can be taken to prevent the ability of the malware to execute in the first place, and those that should be taken to restore the network's health going forward.

Prevention: The same basic network hygiene principles can be applied to dealing with Ryuk as with many other malware families. Those steps include:

- Enact multifactor authentication wherever possible.
- Ensure network segmentation.
- Ensure all file backups are located offline and have been tested for restoration success.
- Disable RDP and other remoting options except where absolutely necessary and incorporate additional security such as multifactor authentication for those necessary cases.
- Incorporate a SIEM or other log aggregation mechanism to build a history of logged activity. Alert on actions detected in logs such as:
    - New user created in Active Directory;
    - RDP sessions to server machines from non-IT department machines;
    - New machines identified on the network in daily network scans;
    - PowerShell scripts executing, especially encoded script execution.
- Use known indicators of Trickbot or Emotet activity to serve as an early warning sign that the network is compromised and possibly a future Ryuk victim.
- In environments where services and software are tracked and monitored, abnormalities across the domain may identify outlying services or scheduled tasks.
- Detection is also possible by auditing Windows Event logs, to include but not limited to System, Security and PowerShell.
- Domains that use PowerShell frequently for administrative tasks should flag scripts that have been encoded such as base64 encoding. When possible, enable script block logging for PowerShell.

Remediation: After a Ryuk attack occurs, determining the initial point and method of compromise is critical to preventing recurrence since there are two components to the ransomware: 1) the initial network compromise and exploitation and 2) the persistence mechanism of the ransomware. A single workstation offline during remediation can result in a second Ryuk infection.

The FBI recommends that any victims of Ryuk take the following steps in addition to the previous mitigation steps, including, but not limited to:

- Scan system backups for registry persistence.
- Scan system backups for other malware infections, particularly Trickbot and/or Emotet.
- Execute a network-wide password reset.
- Continue to monitor firewall traffic for known Trickbot and Emotet communications as well as for known exploit kit traffic.

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, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that 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 have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks. If you or your company is found to be a victim of Ryuk ransomware, the FBI is seeking any of the following information that you determine you can legally share, including:

- Recovered executable file;
- Copies of the *read me* file – DO NOT REMOVE the file or decryption may not be possible;
- Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally);

- Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally);
- Malware samples;
- Log files (Windows Event Logs from compromised systems, Firewall logs, etc.);
- Any PowerShell scripts found having executed on the systems;
- Any user accounts created in Active Directory or machines added to the network during the exploitation ;
- E-mail addresses of the attackers;
- A copy of the ransom note;
- Ransom amount and whether or not the ransom was paid;
- Bitcoin wallets used by the attackers;
- Bitcoin wallets used to pay the ransom (if applicable);
- Names of any other malware identified on your system;
- Copies of any communications with attackers.

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 www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail 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:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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.