FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

02 MAY 019

Alert Number
MC-000103-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 has been **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indicators of Compromise Associated with Ryuk Ransomware

Summary

Unknown cybercriminals have targeted more than 100 US and international businesses with Ryuk ransomware since approximately August 2018. Ryuk encrypts files on network shares and an infected computer's filesystem. Once the victim has been compromised, the actors encrypt all the network's files and demand sums of up to $5 million worth of Bitcoin (BTC) in exchange for a decryptor program. Ryuk's targets are varied and indiscriminate, but attacks focus on organizations with high annual revenues in hopes of extracting larger ransoms from the victims. While Ryuk is generally undiscerning about victims, attacks have had a disproportionate impact on logistics companies, technology companies, and small municipalities.

Technical Details

Ryuk first appeared as a derivative of Hermes 2.1 ransomware, which first emerged in late 2017 and available for sale on the open market as of August 2018. Ryuk still retains some aspects of Hermes code. For example, all of Ryuk's files contain the "HERMES" tag but some of the files have .ryk added to the filename, while others do not. In other parts of the ransomware code, Ryuk has removed or replaced features of its predecessor, such as the restriction against targeting specific Eurasian-based systems.

The exact infection vector remains unknown as Ryuk deletes all files related to the dropper used to deploy the malware. In some cases, Ryuk has been deployed secondary to Trickbot and/or Emotet banking Trojans, which use Server Message Block (SMB) protocols to propagate through the network and can be used to steal credentials. In one case, the ransomware appears to have used unsecured or brute

forced Remote Desktop Protocols (RDPs) to gain access. After the attacker has gained access to the victim network, additional network exploitation tools may be downloaded, including PowerShell Empire, the Microsoft Sysinternals tool psexec, or the penetration testing tool Cobalt Strike.

Once executed, Ryuk establishes persistence in the registry, injects into running processes, looks for network connected file systems, and begins encrypting files. Ryuk utilizes AES-256 to encrypt files and uses an RSA public key to encrypt the AES key. The Ryuk dropper drops a .bat file which tries 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. The "RyukReadMe" file the ransomware places on the system after encryption provides two email addresses, using end-to-end encrypted email providers Protonmail and/or Tutanota, 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 attacker(s) tell the victim how much to pay to a specified BTC wallet for the decryptor and will provide a sample decryption of two files.

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. More importantly, paying the ransom does not guarantee that a victim's files will be recovered. For instance, with this variant, testing shows success when running the decryption as 'admin'. Additionally, initial testing reports that the "RyukReadMe" file does not need to be present for the decryption script to run successfully but other reporting advises that 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 by the fact that the "RyukReadMe" file is deleted when the script is finished which may affect the decryption script unless it is saved and stored in a different location before running. In all cases, the FBI encourages organizations to contact their local field office immediately to report a ransomware event.

Indicators:

The following indicators of compromise have been observed in samples of Ryuk malware.

Host Based Indicators:

- Mutex: "efkrm4tgkl4ytg4", "FakeMutex"

- Registry:
  - KeyName: "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"
  - Numerous identical "ransom note" files:
    - "RyukReadMe.txt"
    - Numerous encrypted files, which were not renamed, but have the "HERMES" tag followed by an encrypted key at the end of the file;
  - Some malware samples add '.RYK' to the end of encrypted filenames

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

Information Requested:

If you or your company is found to be a victim of Ryuk ransomware, the FBI is seeking any information, 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
- Images of infected systems
- Malware samples
- Log files
- 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

Recommended Mitigations

Determining the initial point and method of compromise is critical to preventing reoccurrence since there is both the initial network compromise and exploitation and the persistence mechanism of the ransomware itself. There have been victims who experience a second Ryuk infection after remediation because a single workstation was offline when remediation occurred.

The FBI recommends that any victims of Ryuk take the following steps, to include, 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
- Enact multifactor authentication
- Ensure network segmentation
- Ensure all file backups are located offline

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

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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

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.