FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 MAY 2020

Alert Number

MI-000125-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:GREEN**: Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

Indicators of Compromise Associated with ProLock Ransomware

Summary

As of March 2020, the FBI received notification that the ransomware variant ProLock had infected multiple organizations in the United States to include healthcare organizations, government entities, financial institutions, and retail organizations. ProLock was previously released as PwndLock ransomware in early March 2020. ProLock actors instruct victims to pay the ransom in several days, threatening to release the victims' data on social media and public websites.

Technical Details

ProLock actors gain initial access to victim networks through phishing emails, Qakbot,[1] improperly configured remote desktop protocol (RDP), and stolen login credentials for networks with single-factor authentication. After ProLock actors gain access to a victim's network, they map the network and identify backups, to include Volume Shadow Copies, for deletion and/or encryption.

[1] Qakbot (aka Qbot) is an information-stealing botnet capable of spreading across a network via network shares.

ProLock actors copy portions of a victim's network and exfiltrate the data prior to encryption. ProLock actors use the command line syncing tool RClone to copy files from the victim's network. ProLock actors disguise RClone.exe software as SVChost.exe. ProLock typically encrypts all of the files on a victim's network, appending the file extension ".proLock" or ".pr0Lock" to the original file names after encryption, and deletes the original file.

Ransom Note Details

ProLock actors encrypt the files on the victim's network using RSA-2048 algorithm. After encrypting a victim's files, ProLock actors leave a .txt extension file as a ransom note on the victim computer. The ransom note instructs the victims to visit a TOR page and log in using a unique ID included in the ransom note. The TOR page then displays the ransom price and wallet address for the ransom payment. The ransom note indicates the decryption keys will be stored for one month. The ProLock actors provide an email address victims can use to contact the ProLock actors if the victim cannot connect to the TOR page.

Decryption Tool

The decryption key or "decryptor" provided by the attackers upon paying the ransom has not routinely executed correctly. The decryptor can potentially corrupt files that are larger than 64MB and may result in file integrity loss of approximately 1 byte per 1KB over 100MB. Added coding may be necessary for the decryptor to function.

Indicators of Compromise

The following indicators of compromise have been observed in samples of the ProLock Ransomware:

Encrypted File Extensions

- .proLock
- .pr0Lock
- .proL0ck
- .key
- .pwnd

Subnets of C2 Servers

- 185.212.128.0/21
- 197.210.45.0/21

Ransom Note File

• [HOW TO RECOVER FILES].TXT

Files

• C:\Programdata\WinMgr.xml
• C:\Programdata\WinMgr.bmp
• C:\Programdata\clean.bat
• C:\Programdata\run.bat
• C:\Windows\svchost.exe

Tools used by Attackers

The following applications were leveraged by ProLock actors to conduct the compromise. Some of these applications support legitimate purposes; however, these applications can also be used by threat actors to aid in exploration of an enterprise.

• WinMgr.bmp (MD5: c579341f86f7e962719c7113943bb6e4)
• Rclone.exe (renamed as svchost) (MD5: 7f5e4679edcfae6068ffa2051c4010fa)
• Run.bat
• Wmic
• PowerShell
• 7Zip

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. The FBI is seeking any of the following information that you determine you can legally share, including:

- Recovered executable file
- Complete phishing email file with headers
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- Network and Host Based Log files
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount and if the ransom was paid
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom (if applicable)
- Tor sites used to contact the attackers
- Names of any other malware identified on your system
- Copies of any communications with attackers
- Document use of .icu domains for C2
- Identification of website or forum where data was leaked

Recommended Mitigations

- Backup data regularly, keep offline backups, and verify integrity of backup process.
- Keep software updated. Install software patches so that attackers can't take advantage of known problems or vulnerabilities.
- Use two-factor authentication and strong passwords.
- Audit logs for all remote connection protocols.
- Audit logs to ensure all new accounts were intentionally created.
- Scan for open or listening ports, and Disable SMBv1.
- Consider disabling RDP if it is not being used.

- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
- Monitor Active Directory and local administrators group changes.
- Maintain only the most up-to-date version of PowerShell and uninstall older versions.
- Enable PowerShell logging and monitor for unusual commands, especially execution of Base64 encoded PowerShell.
- Turn off the option to automatically download attachments. To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and disable it.

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 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:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

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.