FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

19 January 2022

FLASH Number

CU-000161-MW

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

This FLASH has been released **TLP:WHITE**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

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

Indicators of Compromise Associated with Diavol Ransomware

Summary

The FBI first learned of Diavol ransomware in October 2021. Diavol is associated with developers from the Trickbot Group, who are responsible for the Trickbot Banking Trojan. Diavol encrypts files solely using an RSA encryption key, and its code is capable of prioritizing file types to encrypt based on a pre-configured list of extensions defined by the attacker. While ransom demands have ranged from $10,000 to $500,000, Diavol actors have been willing to engage victims in ransom negotiations and accept lower payments. The FBI has not yet observed Diavol leak victim data, despite ransom notes including threats to leak stolen information.

Technical Details

Diavol creates a unique identifier for victim computers via the generation of a System or Bot ID with the following format:

[hostname]-[username]_W[windows_version].[32CharacterString] (example BOT ID follows:)

```
EXAMPLEHOSTNAME-EXAMPLEUSERNAME_W617601.6A8DA4GEEV11E43V85556FE984GG94W1G
```

The Bot ID generated by Diavol is nearly identical to the format used by TrickBot and the Anchor DNS malware, also attributed to Trickbot. Once the Bot ID is generated, Diavol attempts to connect to a hardcoded command and control (C2) address. If the registration to the botnet is successful, the infected device connects to the C2 again to request updated configuration values. Diavol encrypts files and appends the ".lock64" file extension to the encrypted files. The file contents are encrypted using Microsoft CryptoAPI functions and then written to the new encrypted file. Diavol can also terminate processes and services.

Indicators

Once files are encrypted, the desktop background color is changed to black, and the following message is stored in a BMP file and displayed: **"All your files were encrypted. For more information see README-FOR-DECRYPT.txt."** Files are encrypted with the ".lock64" extension and the ransom note is dropped into the folders. A readme file dropped on victims' machines directs them to a TOR website to obtain a decryption key.

After successful execution of the malware, Diavol can be found in the following directories:

Diavol indicators as of 12/2021			
Directories	**Whitelisted File Extensions**	**Whitelisted Files**	**Whitelisted Paths**
%ProgramData% %UserProfile%	.exe	readme_for_decrypt.txt	%WINDIR%
	.sys	locker.txt	%PROGRAMFILES%
	.dll	unlocker.txt	%PROGRAMW6432%
	.lock64		%TEMP%
	.restore		

Diavol's malicious executables further contained the following PDB path:
D:\Development\Master\onion\locker.divided\LockMainDIB\Release\LockMainDIB.pdb

The following is an example of a ransom note used by Diavol, as of December 2021:

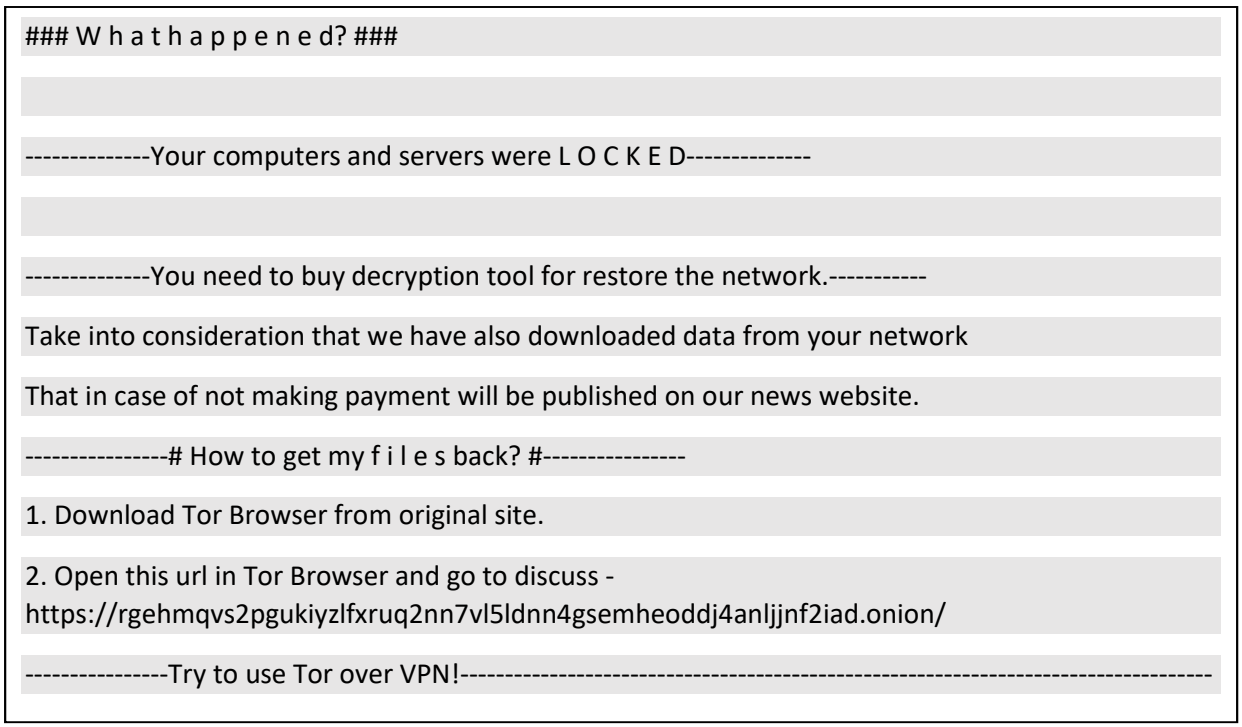

Figure 1: Diavol Ransom Note

Information Requested

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, Bitcoin wallet information, the decryptor file, and/or a benign sample of an encrypted file. The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees and customers. The FBI may be able to provide threat mitigation resources to those impacted by Diavol ransomware. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to promptly report ransomware incidents to your local field office. Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law.

Recommended Mitigations

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- Implement network segmentation and maintain offline backups of data to ensure limited interruption to the organization.
- Regularly back up data, password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Install and regularly update antivirus software on all hosts, and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind. Do not give all users administrative privileges.
- Disable unused ports.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Require administrator credentials to install software.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

Additional Resources

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the Government's official one-stop location for resources to tackle ransomware more effectively.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. 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.

Administrative Note

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