FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 March 2021

Alert Number

CU-000143-MW

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

Mamba Ransomware Weaponizing DiskCryptor

Summary

Mamba ransomware has been deployed against local governments, public transportation agencies, legal services, technology services, industrial, commercial, manufacturing, and construction businesses. Mamba ransomware weaponizes DiskCryptor—an open source full disk encryption software— to restrict victim access by encrypting an entire drive, including the operating system. DiskCryptor is not inherently malicious but has been weaponized. Once encrypted, the system displays a ransom note including the actor's email address, ransomware file name, the host system name, and a place to enter the decryption key. Victims are instructed to contact the actor's email address to pay the ransom in exchange for the decryption key.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

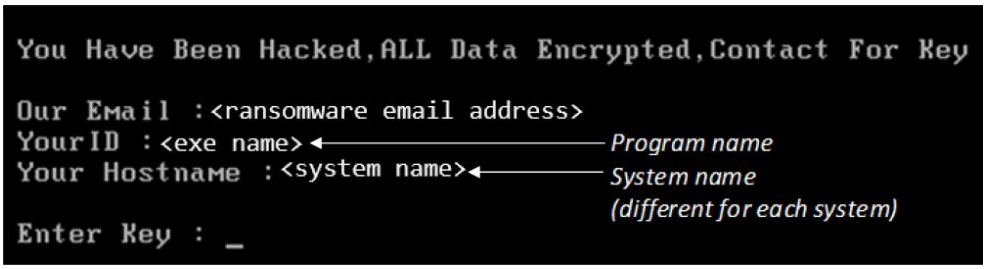

Figure 1 – Example of Mamba ransomware message.

Technical Details

The ransomware program consists of the open source, off-the-shelf, disk encryption software DiskCryptor wrapped in a program which installs and starts disk encryption in the background using a key of the attacker's choosing. The attacker passes the encryption key via the command-line parameter: `[Ransomware Filename].exe <password>`. The ransomware extracts a set of files and installs an encryption service. The ransomware program restarts the system about two minutes after installation of DiskCryptor to complete driver installation. The encryption key and the shutdown time variable are saved to the configuration file (myConf.txt) and is readable until the second restart about two hours later which concludes the encryption and displays the ransom note. If any of the DiskCryptor files are detected, attempts should be made to determine if the myConf.txt is still accessible. If so, then the password can be recovered without paying the ransom. This opportunity is limited to the point in which the system reboots for the second time.

Key Artifacts	
Files	**Description**
$dcsys$	Located in the root of every encrypted drive [i.e. C:\$dcsys$]
C:\Users\Public\myLog.txt	Ransomware log file
C:\Users\Public\myConf.txt	Ransomware configuration file
C:\Users\Public\dcapi.dll	DiskCryptor software executable
C:\Users\Public\dcinst.exe	DiskCryptor software executable
C:\Users\Public\dccon.exe	DiskCryptor software executable
C:\Users\Public\dcrypt.sys	DiskCryptor software executable
C:\Windows\System32\Drivers\dcrypt.sys	Installed DiskCryptor driver

[Ransomware Filename].exe	Portable 32-bit .NET assembly compatible with 32-bit and 64-bit Windows systems which combines DiskCryptor with a simple ransom message upon boot
dcinst.exe	Cryptor installer support
dccon.exe	Console version od DiskCryptor

Services
myCryptoraphyService Runs [Ransomware Filename].exe as a service and is removed once encryption is completed

Recommended Mitigations

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Require administrator credentials to install software.
- If DiskCryptor is not used by the organization, add the key artifact files used by DiskCryptor to the organization's execution blacklist. Any attempts to install or run this encryption program and its associated files should be prevented.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication where possible.
- Regularly, change passwords to network systems and accounts, and avoid reusing passwords for different accounts. Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.

- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on awareness and training. 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).

Reporting Notice

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. Regardless of whether your organization decided to pay the ransom, the FBI urges you to report ransomware incidents to the FBI's Internet Crime Complaint Center (IC3) (https://ic3.gov). Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under U.S. law.

Administrative Note

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

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