THREAT BULLETINS

Mamba Ransomware Weaponizing DiskCryptor

TLP:WHITE

Mar 24, 2021

On March 23, 2021, the FBI disseminated "Mamba Ransomware Weaponizing DiskCryptor" Flash Report (CU-000143-MW). The FBI Flash report contains specific and actionable intelligence Health-ISAC members can use to improve their cyber security posture. The data is provided in order to help cyber security professionals and system administrators guard against the persistent malicious actions of nation state and criminal cyber actors.

The summary of the FBI FLASH is provided below. The FLASH is attached.

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 which is an open source full disk encryption software used 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.

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. Subsequently, 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

Report Source(s)	FBI

Recommendations

- 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).

Alert ID 4cae0d2a

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags FBI Flash

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

For Questions or Comments Please email us at toc@h-isac.org

FBI 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 may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**