Published on *The National Law Review* https://natlawreview.com

FBI and DHS/CISA Issue Joint Alert on Mamba Ransomware

Article By:

Linn F. Freedman

The Federal Bureau of Investigations (FBI) recently issued a joint alert with the Department of Homeland Security/Cybersecurity Infrastructure and Security Agency (CISA) that "Mamba ransomware has been deployed against local governments, public transportation agencies, legal services, technology services, industrial, commercial, manufacturing, and construction businesses."

According to the Alert, the hacking group behind the Mamba ransomware attacks is weaponizing an open source tool used for disc encryption—DiskCryptor—to encrypt entire operating systems of victims. Once the operating system has been encrypted, a ransom note appears and demands payment for the decryption key.

The Alert states, "[T]he 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 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 Alert lists the key artifacts, which can be accessed here.

The FBI recommends the following mitigation:

- Regularly back up data, utilize air gap network security measures, and password protect backup copies offline. Ensure that 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.

National Law Review, Volumess XI, Number 98