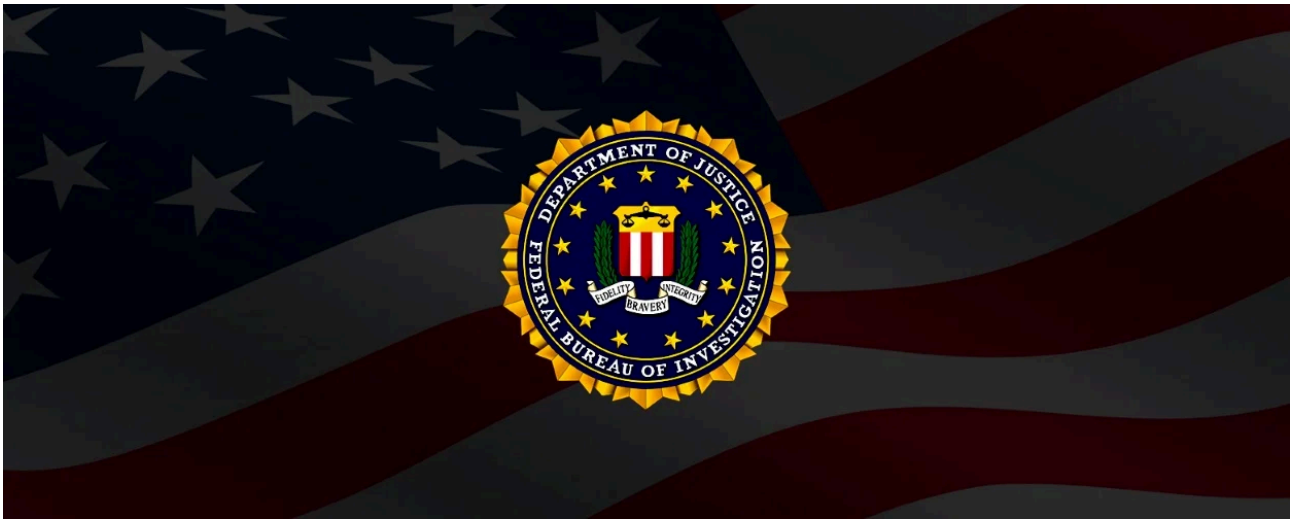
FBI Issues Alert For LockerGoga and MegaCortex Ransomware

By Lawrence Abrams

Published: 2019-12-23 · Archived: 2026-04-10 03:03:28 UTC



The FBI has issued a warning to private industry recipients to provide information and guidance on the LockerGoga and MegaCortex Ransomware.

Both LockerGoga and MegaCortex are ransomware infections that target the enterprise by compromising the network and then attempting to encrypt all its devices.

In an FBI Flash Alert marked as TLP:Amber and seen by BleepingComputer, the FBI is warning the private industry regarding the two ransomware infections and how they attack a network.

"Since January 2019, LockerGoga ransomware has targeted large corporations and organizations in the United States, United Kingdom, France, Norway, and the Netherlands. The MegaCortex ransomware, first identified in May 2019, exhibits Indicators of Compromise (IOCs), command and control (C2) infrastructure, and targeting similar to LockerGoga."

According to the alert, the actors behind LockerGoga and MegaCortex will gain a foothold on a corporate network using exploits, phishing attacks, SQL injections, and stolen login credentials.

Once a network is compromised, the threat actors will install the penetration testing tool called Cobalt Strike. This tool allows the attackers to deploy "beacons" on a compromised device to "create shells, execute PowerShell scripts, perform privilege escalation, or spawn a new session to create a listener on the victim system."

When a network is compromised, the actors will be resident on the network for months before they deploy the LockerGoga or MegaCortex ransomware infections.

While the FBI had not said what these attackers are doing during this period, the actors are probably exfiltrating data, deploying information-stealing trojans, and further compromising workstations and servers.

Once the network has been harvested of anything of value, the attackers will deploy the LockerGoga or MegaCortex infections so that they begin to encrypt the devices on the network. This will generate a final revenue source for the attackers.

During the ransomware deployment, the FBI states the actors will execute a kill.bat or stop.bat batch file that terminates processes and services related to security programs, disables Windows Defender scanning features, and disable security-related services.

The threat actors will also use a variety of LOLBins and legitimate software such as 7-Zip, PowerShell scripts, wmic, nslookup, adfind.exe, mstds.exe, Mimikatz, Ntsdutil.exe, and massscan.exe.

Unfortunately, both of these ransomware infections use a secure encryption algorithm, which means it is not possible to decrypt them for free.

FBI's recommended mitigations

The FBI offers guidance and mitigation advise that business owners should utilize to minimize their risk to the LockerGoga and MegaCortex ransomware.

The most important mitigation provided by the FBI is to make sure you "backup data regularly, keep offline backups, and verify integrity of backup process."

By having a working and verified backups, especially offline backups, ransomware is not a threat as you can always restore your data.

Other mitigations suggested by the FBI include:

- Make sure all installed software and operating systems are kept updated. This helps to prevent vulnerabilities from being exploited by the attackers.
- Enable two-factor authentication and strong passwords to block phishing attacks, stolen credentials, or other login compromises.
- As publicly exposed remote desktop servers are a common way for attackers to first gain access to a network, businesses should audit logs for all remote connection protocols
- Audit the creation of new accounts.
- Scan for open or listening ports on the network and block them from being accessible.
- Disable SMBv1 as numerous vulnerabilities and weaknesses exist in the protocol.

- Monitor the organization's Active Directory and administrator group changes for unauthorized users.
- Make sure you are using the most up-to-date PowerShell and uninstall any older versions.
- "Enable PowerShell logging and monitor for unusual commands, especially execution of Base64 encoded PowerShell"

This guidance is general enough that it applies to all ransomware infections and should be followed by all organizations and even consumers.

Source: https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/