Security recommendations from the FBI in response to LockerGoga and MegaCortex malware

LockerGoga and MegaCortex are currently two of the ransomware strains that cause the biggest damage in 2019.

LockerGoga and MegaCortex are currently two of the ransomware strains that caused the biggest damage in 2019 with a series of large-scale attack campaigns worldwide, causing tens of millions of dollars in damage. These two types of malicious code tend to be used by professional cybercriminal organizations, targeting primarily the business - the object that helps them earn more ransom.

Prior to this situation, the US Federal Bureau of Investigation (FBI) recently issued an "FBI Flash Alert" which warns about threats from LockerGoga, MegaCortex and how they operate, specifically as follows:

1. LockerGoga and MegaCortex are spread mainly through methods of exploiting system vulnerabilities, phishing attacks, SQL injections and the use of stolen login information.
2. Upon successful penetration into a system, malicious agents will install a penetration testing tool called Cobalt Strike. This tool allows them to execute PowerShell scripts, escalate privileges or create spying tools on victim systems.
3. Attackers will stay in the victim's system for a long time until they understand the specifics of the system, and then they deploy ransomware.
4. During ransomware deployment, the attacker will firstly check the processes and services related to the security system. If any security tools and programs are found on the victim's system, they will attempt to

completely disable them.
5. Both ransomware infections use secure encryption algorithms, so it's almost impossible for victims to decode them for free.

FBI recommendation

The following guidelines are recommended by the FBI to minimize the risks posed by LockerGoga and MegaCortex:

1. Ensure that all software and operating systems of all devices in the system are updated to the latest version.
2. Apply additional authentication methods and strong passwords to prevent phishing attacks, login credentials theft, and other fraudulent acts.
3. Monitor all remote servers to prevent an attacker from accessing the intranet.
4. Scan open ports on the network, ready to disconnect access when necessary.
5. Disable SMBv1 because many vulnerabilities and weaknesses exist in this protocol.