US Government Warns Organizations of LockBit 3.0 Ransomware Attacks

The Federal Bureau of Investigation (FBI), the Cybersecurity and Information Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) this week issued an alert on the LockBit 3.0 ransomware operation.

Since January 2020, LockBit has functioned based on the ransomware-as-a-service (RaaS) model, targeting a broad range of businesses and critical infrastructure entities and using a variety of tactics, techniques, and procedures (TTPs).

Also referred to as LockBit Black, LockBit 3.0 has a more modular architecture compared to its previous variants, and supports various arguments that modify its behavior after deployment.

To hinder analysis and detection, LockBit 3.0 installers are encrypted, and can only be executed if a password is supplied, the FBI, CISA, and MS-ISAC explain in a joint advisory.

The malware also supports specific arguments for lateral movement, can reboot systems in Safe Mode, and performs a language check at runtime to avoid infecting systems that use specific language settings, such as Arabic (Syria), Romanian (Moldova), Tatar (Russia), and others.

In observed LockBit 3.0 attacks, initial access is obtained via remote desktop protocol (RDP) compromise, drive-by attacks, phishing, compromised credentials, and the exploitation of vulnerabilities in public-facing applications.

The malware then attempts to escalate privileges, gathers system information, terminates specific processes and services, launches commands, enables automatic logon for persistence, and deletes logs, recycled files, and system volume information copies.

The ransomware uses a hardcoded list of credentials to move laterally into the network, and can also spread via Group Policy Objects and PsExec, over the Server Message Block (SMB) protocol.

LockBit 3.0 then encrypts all files on local and remote devices, drops a ransom note, and changes the wallpaper and icons to its branding. After the process is completed, the malware may delete itself from the machine.

As part of the observed attacks, LockBit 3.0's operators exfiltrated sensitive data using a custom tool called Stealbit, an open-source command line cloud storage manager, and public file sharing services.

Numerous freeware and open-source tools may also be used in attacks, for network reconnaissance, remote access, data exfiltration, and credential dumping. PowerShell and batch scripts, along with Metasploit and Cobalt Strike implants have been observed as well.

Organizations are advised to implement best security practices to mitigate the risks associated with ransomware, including by adopting a recovery plan, using strong passwords for all accounts, implementing phishing-resistant multi-factor authentication, keeping all systems and applications updated, implementing network segmentation, reviewing abnormal activity on their networks, creating backups of all data, disabling unused ports and services, auditing user accounts, and installing and maintaining a modern security solution.

Related: New 'Exfiltrator-22' Post-Exploitation Framework Linked to Former LockBit Affiliates

Related: Russian National Arrested in Canada Over LockBit Ransomware Attacks

Related: LockBit Ransomware Site Hit by DDoS Attack as Hackers Start Leaking Entrust Data

US Government Warns Organizations of LockBit 3.0 Ransomware Attacks