New ‘Exfiltrator-22’ Post-Exploitation Framework Linked to Former LockBit Affiliates

A recently identified post-exploitation framework offered as a service appears to be operated by former affiliates of the LockBit ransomware, cybersecurity company Cyfirma reports.

Dubbed Exfiltrator-22 or EX-22, the tool was created using the leaked source code of other post-exploitation frameworks, and uses the same command-and-control (C&C) infrastructure as LockBit 3.0.

The malicious tool appears to have been created by skilled developers with knowledge of anti-analysis and defense evasion techniques, who are employing an aggressive marketing strategy, claiming that their solution is fully undetectable.

Exfiltrator-22’s operators, Cyfirma says, are likely operating from Asia and are interested in building their own affiliation program, using a subscription-based payment model: the malware is offered at $1,000 for a month, or $5,000 for lifetime access.

Customers are provided with access to a login panel for the Ex22 server, which is hosted on a bulletproof virtual private server, from where they can remotely control the malware and collect information from the infected devices, update malware configuration, deploy new versions of the tool, and create new campaigns.

“By keeping their operations centralized on a remote server, [the threat actors] can make it more difficult for security

researchers to analyze and identify the source of the malware," Cyfirma says.

Capabilities provided by Exfiltrator-22 include an elevated reverse shell, file download and upload, keylogger, file encryption (ransomware), live connection to the infected device, elevation of privilege, persistence, lateral movement, LSASS credential dumping, hashing, viewing a list of running processes, and exfiltration of authentication tokens.

The framework can bypass User Access Control (UAC), can create scheduled tasks, and allows attackers to check group memberships for the existing user and to select the payload to be executed on the target machine.

The threat actor likely completed the framework's development in November 2022 and started advertising it on a newly created Telegram channel in early December. However, the malware developer continued to work on the tool, and has made several announcements of a new feature being added.

Cyfirma has discovered that the malware developers abuse Akamai's content delivery network (CDN) to host Exfiltrator-22's C&C infrastructure and believes that they likely employ an obfuscation plugin for Tor and domain fronting to hide Tor traffic in legitimate HTTPS connections.

While digging deeper into the framework, Cyfirma discovered that it uses the same domain fronting technique and C&C infrastructure as a LockBit 3.0 sample.

"It can be concluded with high confidence that the threat actors who created EX-22 are highly sophisticated threat actors that are likely to continue to increase the evasiveness of the malware. With continuous improvements and support, EX-22 becomes a go-to alternative for any threat actors planning to purchase tools for the post exploitation phase but do not want to go with the traditional tools due to high detection rates," Cyfirma concludes.

Related: New ‘Alchimist’ Attack Framework Targets Windows, Linux, macOS

Related: Intezer Documents Powerful ‘Lightning Framework’ Linux Malware

Related:‘IceApple’ Post-Exploitation Framework Created for Long-Running Operations

New ‘Exfiltrator-22’ Post-Exploitation Framework Linked to Former LockBit Affiliates