KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification| Sliver toolkit used as an alternative to Cobalt Strike

Tracker ID: TN0902 **Date:** 13/Sep/2022 **Category:** Malware **Industry:** All **Region**: All

Background

Threat actors are abandoning the Cobalt Strike suite of penetration testing tools in pursuit of similar but lesser-known frameworks. Sliver, a cross-platform open-source toolkit, is emerging as a viable substitute for Brute Ratel. Nation-state threat actors, cybercrime groups directly supporting ransomware and extortion, and other threat actors are now exploiting and integrating the Sliver command-and-control (C2) infrastructure for infiltration and escape detection.

Sliver is an open-source framework available on GitHub that was first made public and promoted to security professionals in late 2019. It includes many common C2 Framework features such as support for multiple concurrent operators, numerous listener types, user-developed extensions, and payload generation. It has been used by threat actors since December 2020.

Sliver includes a number of built-in methods and post-exploitation functionalities. One of the most common underlying techniques used by C2 operators and frameworks is process injection, which allows arbitrary code to be executed into the address space of another live process. In terms of process injection instructions, the default Sliver code achieves this without deviating from common implementations. Common artifacts include unique HTTP header combinations and JARM hashes, which are active fingerprinting methods for TLS servers.

The tool employs the following commands: migrate (to migrate into a remote process), spawndll (to load and run a reflective DLL in a remote process), sideload (to load and run a shared object (shared library/DLL) in a remote process), inject a Metasploit Framework payload into a process with the command msf-inject, .NET assemblies can be loaded and launched in a child process with the command execute-assembly, The toolkit also employs extensions and aliases (Beacon Object Files (BFOs),.NET apps, and other third-party tooling) for command injection. PsExec is also used by the framework to execute commands that allow for lateral movement. The C2 framework's canonical, unmodified codebase is used to generate sliver payloads (shellcode, executables, shared libraries/DLLs, and services). Extracting configurations from Sliver malware payloads with little context is beneficial since the framework needs to de-obfuscate and decode them before using them.

Threat actors have devised alternatives as Cobalt Strike defences have become more robust. The Go-based Sliver security testing tool, developed by BishopFox cybersecurity professionals, is increasingly being used in attacks by hackers, including state-sponsored groups and cybercrime gangs. One gang identified as DEV-0237, aka FIN12, has been linked to multiple ransomware developers. In the past, the threat actor has distributed ransomware payloads from a range of ransomware operators, including Ryuk, Conti, Hive, Conti, and BlackCat, using malware such as BazarLoader and TrickBot.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Sliver toolkit used as an alternative to Cobalt Strike

MITRE ATT&CK Tactics

Initial Access, Execution, and Command and Control.

Detection Methods

- Threat hunters can set up listeners to detect anomalies on the network for Sliver infrastructure as the Sliver C2 network supports several protocols (DNS, HTTP/TLS, MTLS, and TCP), accepts implants/operator connections, and can host files to imitate a legitimate web server.
- If the shellcode isn't obfuscated, detection engineers can develop rules for the shellcode payload that is incorporated in the loader or loader-specific detections [like Bumblebee].

Recommendations

- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically
- Ensure secure handling of emails that come from outside sources and data acquired from the Internet. Apply mail filtering settings to ensure blocking spoofed emails, spam, and emails with malware.
- Avoid opening untrusted links and email attachments without first verifying their authenticity. Check the sender's email address to confirm its legitimacy.
- Establish a data recovery strategy and routinely backup your files to a secure offsite place. The ability to rescue your data after a ransomware assault is guaranteed by routine data backups.
- Use strong passwords, change them frequently, and implement multi-factor authentication.
- To prevent servers from connecting arbitrarily to the internet to browse or download data, check your perimeter firewall and proxy and block suspicious activity. Such limitations aid in preventing the download of malware and C2 activity, including mobile devices.
- Prevent remote procedure call (RPC) and service message block (SMB) communication along endpoints whenever possible. This limits lateral movement and other attack activities.
- Organizations should verify that their security tools are running in optimum configuration and perform regular network scans to ensure a security product protects all systems.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Sliver toolkit used as an alternative to Cobalt Strike

References

- Microsoft Security Experts, Looking for the 'Sliver' lining: Hunting for emerging command-and-control frameworks, Microsoft, 24th August 2022, External Link (microsoft.com)
- Ionut Ilascu, Hackers adopt Sliver toolkit as a Cobalt Strike alternative, 25th August 2022, External Link (bleepingcomputer.com)

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia