Talos

2022 YEAR IN REVIEW

GENERAL THREAT LANDSCAPE

DOWNLOAD THE FULL REPORT HERE

Talos observed several major trends across the threat landscape in 2022. Based on telemetry and case studies across Cisco Talos Incident Response engagements, we observed threat actors incorporating cracked/leaked versions of popular red-teaming tools; using living-off-the-land binaries (LoLBins), such as PowerShell and Microsoft PS Exec; and an increase in USB attacks.

DUAL-USE TOOLS

Developing malicious tools is resource intensive and potentially allows a threat actor to be tracked. To sidestep these steep costs and provide an additional layer of anonymity, many adversaries turn to offensive and red-team frameworks to support a range of actions across an attack lifecycle.

Cobalt Strike continues to remain a popular option for cyber threat actors (Figure 1). This legitimate network defense tool and threat emulation software has a range of capabilities, including reconnaissance, post-exploitation activity, and a variety of attack simulations, making it a highly functional tool for adversaries.

Talos and the security community have been dealing with Cobalt Strike for years, continuously developing better and more robust detections. Throughout the year, we also saw threat actors adapt to these developments by turning to additional offensive frameworks, such as Sliver and Brute Ratel (Figure 2).

Additionally, Talos discovered two separate offensive frameworks developed by threat actors for their own purposes, called "Manjusaka" and "Alchimist." Alchimist is already being used in the wild, and although we haven't observed widespread usage of Manjusaka as of this writing, it has the potential to be adopted by threat actors globally.

LIVING-OFF-THE-LAND BINARIES

Living-off-the-land binaries (LoLBins) are legitimate utilities and tools that are pre-installed on an operating system and are commonly abused by adversaries. Since these are inherently

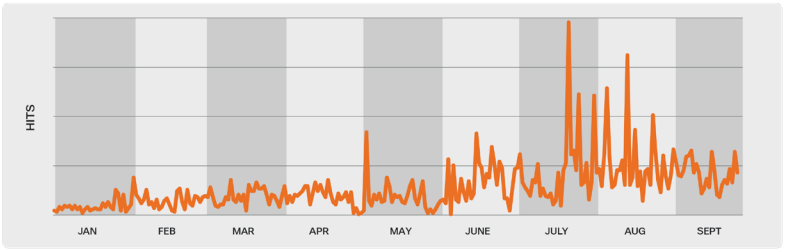

Figure 1. *Cisco Secure Endpoint detections for Cobalt Strike-named pipe usage.*

Cobalt Strike

- A legitimate network defense tool and threat emulation software that has a range of capabilities, including reconnaissance, post-exploitation activity, and a range of attack packages, making it a highly functional tool for adversaries.
- Beacon is Cobalt Strike's payload for generating attacks and creating outbound traffic over HTTP, HTTPS, or DNS. Cobalt Strike beacons can be compared with Meterpreter, which is part of the Metasploit framework, and used by penetration testers and offensive security researchers when delivering their services.

Brute Ratel

- A legitimate sophisticated red-teaming tool released in 2020 as an attack simulation tool. It has since been leveraged by threat actors to facilitate various stages of the attack lifecycle.
- Brute Ratel is specifically designed to avoid detection by endpoint detection and response (EDR) and antivirus (AV) solutions.

Sliver

- An open-source red-teaming framework and attack simulation tool that can be used to perform security testing. Sliver's implants are dynamically compiled with asymetric encryption keys per binary and supports C2 over a number of protocols (mTLS, HTTP, DNS).
- Sliver implants are supported on MacOS, Windows, and Linux. Sliver features multiple functionalies, including staged and stageless payloads, dynamic code generation, named pipe pivots, in-memory .NET assembly execution, and much more.

Figure 2. *Comparison of common dual-use tools.*

GENERAL THREAT LANDSCAPE

trusted tools used for routine activities, network defenders may miss attacks leveraging LoLBins when monitoring for malicious behavior. We continue to see adversaries leverage legitimate tools and utilities in all stages of an attack to support their operations.

According to our telemetry, 4 of the 25 most active Cisco Secure Endpoint Behavioral Protection signatures are related to PowerShell, highlighting threat actors' consistent reliance on using this native Windows utility for malicious purposes (Figure 3). Adversaries commonly use PowerShell to support a broad range of activities, including installing adware like ChromeLoader, downloading cryptocurrency miners, or exploiting vulnerabilities in software such as Elasticsearch.

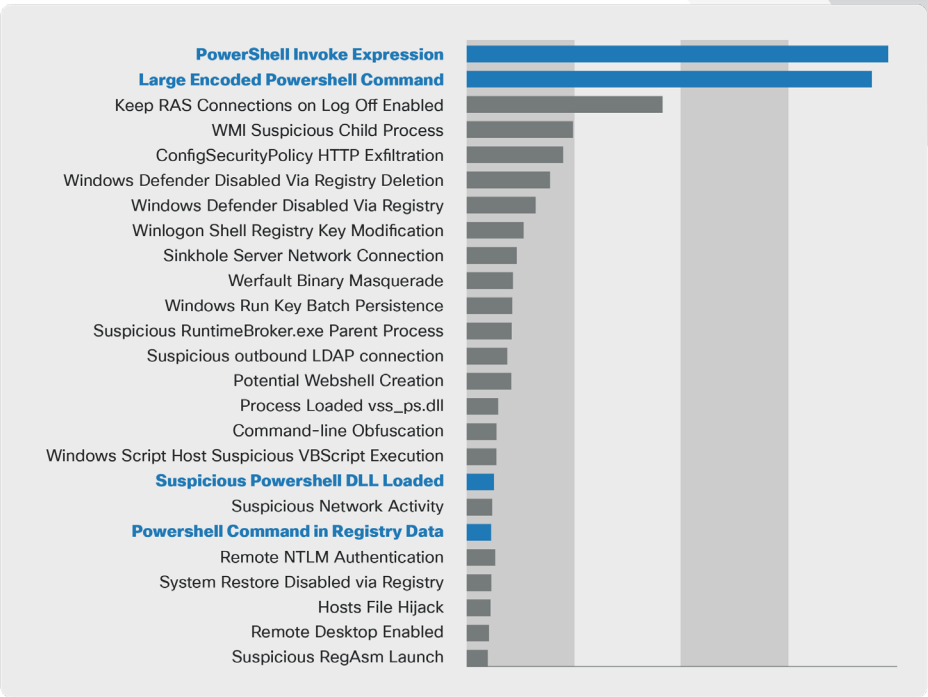

Figure 3. *Top 25 most active Cisco Secure Endpoint Behavioral Protection signatures.*

USB THREATS

Spreading malware via removable storage devices dates back to the days of floppy disk drives. Throughout 2022, Talos observed an uptick in detections in Cisco Secure Malware Analytics for various behaviors associated with USBs and external drives, highlighting adversaries' continued use of this old but effective tactic. Those behaviors include executables being written to a USB drive or setting hidden attributes for files on a USB drive to stay undetected (Figures 4 and 5).

The increase can partly be explained by the Raspberry Robin malware, which spreads between devices using shared USB drives. However, APT groups have also been observed using USB drive access as part of their attacks.

2022 has shown us that USB attacks are back and that adversaries will adapt their tactics to take advantage of enterprises shifting their attention away from older attack vectors.

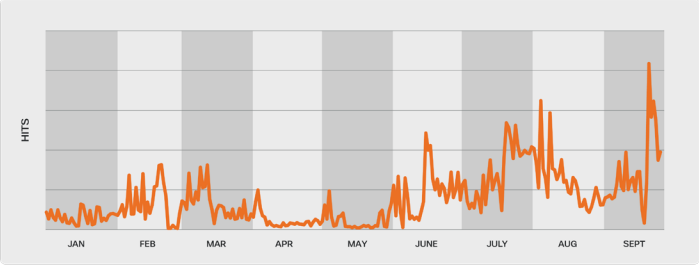

Figure 4. *Cisco Secure Malware Analytics detections for executables written to USB.*

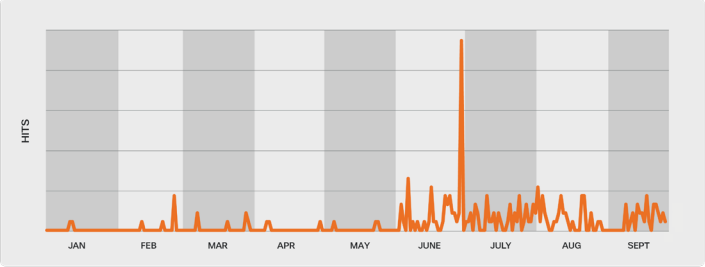

Figure 5. *Cisco Secure Malware Analytics detections for setting hidden attributes for files on a USB.*

