Detecting Cobalt Strike: Government-Sponsored Threat Groups

secureworks.com/blog/detecting-cobalt-strike-government-sponsored-threat-groups

Counter Threat Unit Research Team

TIN WOODLAWN used a customized version of Cobalt Strike to evade configuration-based detections, but a combination of strategic and tactical countermeasures identifies the activity.
Thursday, August 5, 2021 *By: Counter Threat Unit Research Team*

During a focused investigation into malicious use of the legitimate Cobalt Strike penetration testing tool, Secureworks® Counter Threat Unit™ (CTU) researchers explored how government-sponsored threat groups leverage it during intrusions. These groups use various tactics to operate with stealth.

Secureworks incident responders observed the TIN WOODLAWN cyberespionage group using a modified version of Cobalt Strike to evade countermeasures that rely on the default configuration for detection. CTU™ research indicates that this group is likely operated or tasked by the Vietnamese government to steal intellectual property and trade secrets. The threat actors have also targeted individuals deemed to be of interest to the Vietnamese government, including journalists and political opponents.

TIN WOODLAWN uses Cobalt Strike extensively during intrusions, often delivering it via spearphishing emails containing malicious document attachments. These documents include macro code that registers a scheduled task. This scheduled task uses the Windows mshta utility to download a Cobalt Strike Beacon PowerShell stager that executes in memory. This method avoids writing a portable executable to disk, making in-memory detection the only way to identify this phase of the intrusion.

CTU researchers observed TIN WOODLAWN deploying a custom stager that created a named pipe, using a command-line parameter as the pipe name. CTU researchers dubbed this stager 'CommaChameleon' because it uses the '-comma' PowerShell command-line switch. This switch is short for the '-command' switch string, which indicates that a PowerShell command follows. As of this publication, TIN WOODLAWN is the only threat group known to use the shortened command-line switch and a randomized uppercase and lowercase spelling (e.g., POWersHEll -cOmmA).

The stager waits for an RC4-encrypted executable payload to be written to the named pipe and then injects the payload into a legitimate Windows executable randomly selected from a hard-coded list in the stager code. In one campaign, Cobalt Strike injected the Windows esentutl.exe Extensible Storage Engine utility with an RC4-encrypted Mimikatz credential harvesting payload for credential theft.

Cobalt Strike can offer a threat actor anonymity because it is so widely used. Custom implementations may indicate activity by a sophisticated threat actor trying to evade security controls. In this incident, TIN WOODLAWN's custom stager evaded detections for generic Cobalt Strike stagers, downloaded and executed a secondary payload in-memory to minimize host artifacts, and injected an encrypted portable executable into a Windows utility process instead of leveraging the standard Cobalt Strike shellcode.

Table 1 maps the observed TIN WOODLAWN's techniques to the MITRE ATT&CK® framework.

Observed activity	MITRE ATT&CK mapping

Phishing campaigns	Phishing: Spearphishing Attachment
Establishing persistence	Scheduled Task/Job: Scheduled Task Create or Modify System Process: Windows Service
Defense evasion	Signed Binary Proxy Execution: Mshta Process Injection: Portable Executable Injection
Remote code execution	Command and Scripting Interpreter: PowerShell
Credential harvesting	OS Credential Dumping: LSASS Memory

Table 1. MITRE ATT&CK techniques used by TIN WOODLAWN.

Direct observation of TIN WOODLAWN's techniques allowed CTU researchers to combine strategic countermeasures that detect generic behaviors with tactical countermeasures that identify customized activity. The resulting detections indicated this was targeted activity by a targeted government-sponsored threat actor rather than the work of an opportunistic cybercriminal. By integrating these countermeasures into the Secureworks Taegis™ XDR platform, CTU researchers and network defenders can identify attempts by government-sponsored threat actors to weaponize Cobalt Strike in targeted environments. Preview Taegis XDR to explore more coverage for MITRE ATT&CK techniques.

This blog is part of a series. Watch for an upcoming post on the use of Cobalt Strike by penetration testers.

Other posts in this series: