Detecting Cobalt Strike: Cybercrime Attacks

secureworks.com/blog/detecting-cobalt-strike-cybercrime-attacks

Counter Threat Unit Research Team

Countermeasures that detect malicious Cobalt Strike activity enabled a compromised organization to mitigate a GOLD LAGOON intrusion before the threat actors deployed ransomware. Wednesday, August 4, 2021 *By: Counter Threat Unit Research Team*
Many cybercriminals that operate malware use the ubiquitous Cobalt Strike tool to drop multiple payloads after profiling a compromised network. Cobalt Strike is a commercially available and popular command and control (C2) framework used by the security community

as well as a wide range of threat actors. The robust use of Cobalt Strike lets threat actors perform intrusions with precision.

Secureworks® Counter Threat Unit™ (CTU) researchers conducted a focused investigation into malicious use of Cobalt Strike to gain insights about when and how the tool has been used. This knowledge can help to secure organizations that may be targeted by threat actors with diverse motives.

Understanding a threat actor's end goal is important. For example, the financially motivated GOLD LAGOON threat group leverages the Qakbot botnet to deploy Cobalt Strike. CTU™ researchers frequently observe GOLD LAGOON deploying Cobalt Strike to Qakbot-infected hosts that are identified as members of an Active Directory domain. The threat actors then use Cobalt Strike to move laterally throughout the network, establish persistence, and ultimately facilitate damaging post-intrusion ransomware attacks. GOLD LAGOON provides access to other threat groups that deploy various ransomware families in compromised environments.

The value of early detection is highlighted by two similar incidents. In the first incident, Secureworks incident responders helped the victim recover from a REvil ransomware attack. The organization did not have an endpoint detection and response (EDR) solution that identified the preceding Qakbot and Cobalt Strike activity, which enabled the threat actors to achieve their objectives. In the second incident, Secureworks Taegis™ XDR countermeasures detected and alerted on the malicious Qakbot and Cobalt Strike activity in the environment, enabling network defenders to respond quickly to contain and mitigate the intrusion before ransomware was deployed.

In this second incident, a user opened an Excel 4.0 macro worksheet attached to a phishing email. The attachment downloaded and installed Qakbot. Qakbot profiled the infected host, sent the profiled data to its C2 servers, and then downloaded and executed Cobalt Strike Beacon. The threat actor used Cobalt Strike Beacon's remote code execution capability to execute the ping utility. Ping identified additional accessible servers within the network. The threat actor deployed Cobalt Strike Beacon on those targets and then executed arbitrary commands on those systems via the Rundll32 execution utility. One of these commands attempted to discover domain administrator accounts.

This process of deploying Cobalt Strike Beacon to additional servers from a compromised host lets network defenders detect the service established on the remote host, the admin share launching content, and the resulting command execution:

- By default, Cobalt Strike always leverages the Rundll32 utility for command execution.
- Cobalt Strike always launches Rundll32 as a service via the 'ADMIN$' share on the remote host.
- The binary that Cobalt Strike uses to launch Rundll32 via the 'ADMIN$' share always has a filename that is exactly seven alphanumeric characters.

The threat actor also installed Cobalt Strike PowerShell stagers on servers accessed when moving laterally through the compromised network. These stagers allowed the Cobalt Strike Beacon payload to execute in memory. Cobalt Strike PowerShell stager's default execution pattern is always configured to launch as a service and is invoked from the command line with the parameters "/b /c start /b /min powershell -nop -w hidden". The stager executes and decodes a byte sequence in memory to launch Cobalt Strike via a reflected loaded library.

Table 1 maps the observed GOLD LAGOON techniques to the MITRE ATT&CK® framework.

Observed activity	MITRE ATT&CK mapping
Phishing campaigns	Phishing: Spearphishing Attachment
Remote code execution	Command and Scripting Interpreter: Windows Command Shell Signed Binary Proxy Execution: Rundll32 Command and Scripting Interpreter: PowerShell
Network reconnaissance	Remote System Discovery Account Discovery: Domain Account
Lateral movement	Remote Services: SMB/Windows Admin Shares
Defense evasion	Process Injection: Proc Memory Deobfuscate/Decode Files or Information
Establishing persistence	Create or Modify System Process: Windows Service

Table 1. MITRE ATT&CK techniques used by GOLD LAGOON.

The availability of unauthorized Cobalt Strike versions on the dark web means that threat actors can abuse it. Network defenders must attempt to answer the "friend or foe" question when they detect Cobalt Strike in their environment, as the tool can be used for both legitimate and malicious purposes. Taegis XDR, which is continually updated with intelligence gained through CTU research, helps organizations differentiate noise, legitimate use, and actionable alerts. Preview Taegis XDR to explore more coverage for MITRE ATT&CK techniques.

Other posts in this series: