Cobalt Strike Becomes a Preferred Hacking Tool by Cybercrime, APT Groups

By Kelly Jackson Higgins

Published: 2021-05-19 · Archived: 2026-04-05 17:58:45 UTC

RSA CONFERENCE 2021 - For nearly two decades, the open source Metasploit hacking platform has garnered a mix of enthusiasm and frustration by security teams that both need the tools to test their own networks but also fear cybercriminals or other bad actors could use it against them in attacks.

Metasploit remains popular today among good and bad hackers, but another red-team tool, Cobalt Strike, is increasingly playing a major role in attacks. Attackers are weaponizing the tool for the second stage of attacks to carry payloads (including Metasploit exploits) once they have penetrated the victim's network using customized, cloned, or even purchased versions of Cobalt Strike.

The threat-emulation software suite for penetration testing was created by researcher Raphael Mudge in 2012 and was acquired last year by HelpSystems. Its most popular component by nefarious hackers is Beacon, a payload that operates like an attacker, running PowerShell scripts, logging keystrokes, snapping screenshots, stealing files, and dropping other payloads or malware.

HelpSystems declined to comment for this article.

New data from Sophos that cataloged attacker behavior, tools, techniques, and procedures (TTPs) witnessed by its threat hunters and incident responders last year and through the first part of 2021 shows that Cobalt Strike is one of the top five tools used by attackers. It's also a key element when attackers employ PowerShell commands to camouflage their activity on a victim's network. Nearly 60% of PowerShell exploits employ Cobalt Strike, and some 12% of attacks use a combination of Cobalt Strike and Microsoft Windows tools PowerShell and PsExec. It's also paired with PsExec in nearly a third of attacks, according to Sophos's new "Active Adversary Playbook 2021" report.

"Cobalt Strike lends itself to being deployed by PowerShell" and PsExec, says John Shier, senior security advisor at Sophos. "The code [Cobalt Strike] was leaked online a long time ago, [attackers] know how to use it, and it's an evasion technology" to remain under the radar as an attack escalates and spreads.

In one of its more high-profile uses by attackers, the Russian GRU hacking team behind the SolarWinds supply-chain attack campaign built custom shellcode loaders that dropped Cobalt Strike payloads: the Teardrop and Raindrop malware components of the attack.

Researchers and incident responders at Intel 471 say the malicious use of Cobalt Strike correlates with ransomware's rise in recent years, but it's also used for dropping other types of malware and for stealing data. Among the malware groups using Cobalt Strike: Trickbot, Hancitor, Qbot, SystemBC, Smokeloader, and Bazar.

The researchers today published indicators of compromise that indicate Cobalt Strike is in play with these malware families.

Brandon Hoffman, CISO at Intel 471, says attackers appear to like the features of Cobalt Strike, specifically the Beacon component. "It has so many features built into it from a post-exploit tool perspective; it's a perfect fit for second-stage attack and instead of picking and choosing different pieces of malware, you just trop this tool and all of its features in it," he says.

The tool also contains a "malleable" command and control (C2) function, which allows an attacker to fashion its C2 network to appear like a different threat actor group. "Malleable C2 lets you mimic behavior or make C2 traffic look like almost any legitimate service," he says. So if an organization allows users to stream Pandora, for example, a Malleable C2 could be disguised as Pandora traffic in the victim's network, he says.

"That makes it extremely difficult" to spot an attack, Hoffman says. "Beacon is so customizable."

Even so, there are ways to spot malicious abuse of Cobalt Strike, experts say. Aside from bad guys making mistakes and leaving behind clues or breadcrumbs, you can spot a Cobalt Strike-borne attack unfold if you're monitoring activity: "Because Cobalt Strike is not generally used at the first attack vector, in the middle of an incident response [case] if you see something come in from one of the command-and-control servers it could potentially be Beacon," Hoffman explains. And if you create Yara rules for certain malicious scripts, that can detect it as well.

"Where we saw Cobalt Strike in the wild, some folks had repurposed it for the same malware family," says Hoffman, whose team today published its findings on cybercrime groups deploying Cobalt Strike (including indicators of compromise).

Ransomware Thread

"We've seen a correlation between the rise of Cobalt Strike use [by adversaries] and a rise in ransomware. We're not saying Cobalt Strike is fueling" ransomware, Hoffman says. It's more that ransomware is dropped at the later stages of an attack chain. "Before they get to the ransomware, attackers first have to deploy something like this [Cobalt Strike]." So, spotting that activity before ransomware is installed can save a lot of headache.

Speaking of ransomware, Sophos' IR and threat-hunting data found ransomware in more than 80% of the incidents they investigated. "Ransomware is noisy, it needs to grab attention," which is why those cases were flagged for an investigation, Sophos' Shier says. "[In] a lot of the attacks we stopped, we noticed there had been Cobalt Strike activity" as well, he says.

Researchers at Red Canary also have spotted attackers wielding Cobalt Strike in targeted attacks, including payment card theft and ransomware campaigns. They described incidents where attackers using Bazar malware used Cobalt Strike payloads in advance of their dropping Ryuk ransomware on the victim, all within a two-hour window.

"Cobalt Strike is so common and reliable that adversaries create their own custom tooling to simply deploy the payloads, knowing that they will likely succeed if they can just get the payload past security controls. This

capability demonstrates how Cobalt Strike fits into the threat model for nearly any organization," according to Red Canary's report, which includes details on ways to detect malicious Cobalt Strike activity.

About the Author

Editor-in-Chief, Dark Reading

Kelly Jackson Higgins is the Editor-in-Chief of Dark Reading and VP, cybersecurity editorial at Informa TechTarget, where she leads editorial strategy for the company's three cybersecurity media brands: Dark Reading, SearchSecurity and Cybersecurity Dive. She is an award-winning veteran technology and business journalist with three decades of experience in reporting and editing for various technology and business publications and major media properties. Jackson Higgins was selected three consecutive times as one of the Top 10 Cybersecurity Journalists in the U.S., and was named as one of Folio's 2019 Top Women in Media. She has been with Dark Reading since its launch in 2006.
