New Snort, ClamAV coverage strikes back against Cobalt Strike

By Jonathan Munshaw

Published: 2020-09-21 · Archived: 2026-04-05 14:48:52 UTC

Monday, September 21, 2020 00:01

By Nick Mavis. Editing by Joe Marshall and Jon Munshaw.

Cisco Talos is releasing a new research paper called "The Art and Science of Detecting Cobalt Strike."

We recently released a more granular set of updated SNORT® and ClamAV® detection signatures to detect attempted obfuscation and exfiltration of data via Cobalt Strike, a common toolkit often used by adversaries.

Cobalt Strike is a "paid software platform for adversary simulations and red team operations." It is used by professional security penetration testers and malicious actors to gain access and control infected hosts on a victim network. Cobalt Strike has been utilized in APT campaigns and most recently observed in the IndigoDrop campaign and in numerous ransomware attacks.

What's New?

This paper is a coverage narrative, discussing and sharing the challenges and solutions to creating coverage for Cobalt Strike attacks. We decided it wasn't simply enough to provide coverage — we wanted to use this as an opportunity to show our readers what Cobalt Strike is, how it operates, and the mindset it takes to craft effective Snort and ClamAV signatures. This was a tough but worthy journey for Talos. More than 50 new signatures between Snort and ClamAV were created, and combined with prior coverage, covers the following core set of Cobalt Strike modules:

- Raw shellcode generator
- Staged/stageless executable generator
- HTML application attack generator
- Scripted web delivery
- Signed java applet attack
- Smart java applet attack
- System profiler

So what?

Cobalt Strike is notorious and often synonymous with cyber attacks. As noted in Talos' Quarterly Report: Incident Response trends in Summer 2020, Cobalt Strike accounted for 66 percent of all ransomware attacks Cisco Talos Incident Response responded to this quarter. It's a prolific platform for both red teams and malicious actors. Cobalt Strike's strength comes from the many answers it offers to difficult questions an attacker might have. Deploy listeners and beacons? No problem. Need to create some shellcode? Easy. Create staged/stagless executables? Done. Given Cobalt Strike's versatility, it's no wonder why Talos is noticing a trend for attackers to lean more upon Cobalt Strike and less upon commodity malware.

Ready to jump in?

There's a lot to learn in this paper. We delve deep into how Cobalt Strike operates. This is vital to a security researcher, as we focused on specific elements to craft effective coverage. As you read, you'll see our thought processes as we created our Cobalt Strike coverage.

It's important to understand the technical aspects of the threat you're addressing. However, crafting coverage is a nuanced art. Keying in on the specific technical condition is vital, but coverage should be broad enough to catch the threat along with preventing evasion tactics and catch other attacks. To make matters worse, coverage needs to be effective, but also humane to sensors that will be doing all of the inspection while minimizing false positives. It can be a very difficult balance to strike. This is why we created "The art and science of detecting Cobalt Strike" — not only to highlight Cisco Talos' Cobalt Strike coverage, but to give back to our security community. We're proud of our coverage, but we also hope to assist readers in understanding the art of effective detection. By unveiling the details of Cobalt Strike detection, we hope our journey to coverage helps you craft your own when thinking about how to address threats.
