Cobalt Strike, a penetration testing tool abused by criminals

By Malwarebytes Labs

Published: 2021-05-31 · Archived: 2026-04-05 22:33:35 UTC

If you were to compose a list of tools and software developed by security and privacy defenders that ended up being abused by the bad guys, then Cobalt Strike would unfortunately be near the top of the list. Maybe only Metasploit could give it a run for the first place ranking.

Metasploit—probably the best known project for penetration testing—is an exploit framework, designed to make it easy for someone to launch an exploit against a particular vulnerable target. Metasploit is notorious for being abused, yet modules are still being developed for it so that it continues to evolve. Cobalt Strike is in the same basket. Cobalt Strike offers a post-exploitation agent and covert channels, intended to emulate a quiet long-term embedded actor in the target's network.

What is Cobalt Strike?

Cobalt Strike is a collection of threat emulation tools provided by HelpSystems to work in conjunction with the Metasploit Framework. Cobalt Strike, and other penetration testing tools, were originally created for network defenders to train them to understand vulnerabilities and possible avenues of infection by cyber criminals. These tools are meant to simulate intrusions by motivated actors, and they have proven to be very good at this. So, while "white hat" hackers were developing tools to more easily emulate "black hat" activities, few considered how these tools might be turned against someone. (The terms "white hat" and "black hat" are also falling out of favor, as cybersecurity professionals adopt "red team" and "blue team" descriptors to describe offensive and defensive security teams.)

Establishing a foothold

Lately, we have seen targeted attacks by both state-sponsored threat actors and ransomware peddlers. What we mainly see in the ransomware field is an increasing amount of manual infections. For example, by using brute force methods and exploiting vulnerabilities to break into networks. We have seen a significant uptick in these methods in 2020 and beyond. As a follow-up to these more manual types of attacks, as opposed to spray-and-pray phishing attacks, we are seeing threat actors who have compromised a server, loading tools like Cobalt Strike Beacon onto the system. Cobalt Strike Beacon provides encrypted communication with the C&C server to send information and receive commands. Those commands can include instructions to download malware. After doing this, they can use Cobalt Strike to map out the network and identify any vulnerabilities as well as deploy implants, backdoors, and other tools to accomplish lateral movement eventually leading to complete network infection.

Building out grip on the compromised network

So how this usually goes, is an infection occurs, be it phishing, manual breaches by brute forcing a port, or even an exploit. Once an endpoint has been compromised, the actor looks to compromise a server on the

network. There are numerous ways to accomplish this, in fact last year we saw the ZeroLogon vulnerability used against domain admin servers, which essentially gave full admin rights to a criminal within seconds! Once the server is infected, Cobalt Strike is installed and it's at this point, that more advanced network monitoring, vulnerability identification and a bunch of other advanced features, become available to the criminal. Now armed with more capabilities, the attacker can more quickly and completely compromise endpoints across the network, eventually launching ransomware, sometimes after all the juicy data saved on the network has been collected and exfiltrated.

Cobalt Strike is pricey

New Cobalt Strike licenses cost $3,500 per user for a one year license. License renewals cost $2,585 per user, per year. But why would a cybercriminal worry about such costs? Criminals who are using these tools do not just buy them from the vendors anyway. In many cases, leaked and older versions of Cobalt Strike are being used and in some cases, sophisticated threat actors, e.g. the group behind Trickbot, are building their own versions of Cobalt Strike, modified for their special needs and purposes.

The dilemma

This whole situation creates a strange moral grey area when you consider that tools developed by the good guys as a method of defense against the bad guys, are now being used by the bad guys to infect the customers of the good guys. There is a fair amount of discussion among security professionals whether or not it is a good idea to continue the free and unregulated development and release of these penetration testing tools. Especially when some of them are almost indistinguishable from actual black hat tools. As well as a lot of finger pointing about whose responsibility it is to make sure these tools aren't used for crime. But also how could we do that, or is it already too late?

The need for pen-testing

While we can see why major corporations deploy red teams to perform penetration testing, we also wonder whether it is right to develop the malware for the threat actors. One could argue that using the latest and newest actual forms of malware should be adequate to test whether your defenses are up to par.

As it stands now, we have ended up with a situation where there are paid, dedicated researchers who spend all day working on new tools for penetration testing and intrusion. Which may very well end up being used by the criminals themselves. There are likely far less, if any, full time malware tool developers who have the resources, time, and experience to create something of the same magnitude. So at the end of the day, the weapons created by the white and grey hats, may be causing more harm than good in the long run because of a lack of control.

The problem it causes

Pen-testing is limited to the companies that can afford it and feel the need to do it. By using it they are not only adding to their own protection, which is their prerogative, but as a side-effect they are enabling the development of more advanced penetration software.

Combine that with an industry where some penetration testers prefer the situation where organizations are unable to defend themselves against these tools because it creates more business for penetration testing companies if they can't defend themselves effectively. If you pass the test every time with flying colors, you will start to doubt the effectiveness of said test.

This is the problem we currently have with penetration tools being hijacked by criminals. The organizations that employ penetration testers are involuntary enablers, who are protected from this threat while also being the main drivers of development and providers of resources. On the other side of the spectrum there are those who aren't aware of the threat, and will be the biggest victims once these tools fall into the hands of criminals.

As long as the consultants build new, more powerful tools, and don't pay attention where the outdated and discarded tools end up, your neighbor can end up under attack by the tools you paid to develop. You are probably safe from the attack, but dozens of others, many in industries who can't afford a consultant to test their security, are not safe, and in fact, are at a greater risk than before you brought in your consultant.
