Identifying Rogue Cobalt Strike Servers: A Recorded Future Approach | Recorded Future

By THE RECORDED FUTURE TEAM

Archived: 2026-04-05 15:49:30 UTC

What Is Cobalt Strike?

It all began with cybersecurity professionals realizing that sometimes the best defense is a good offense. As the principle of “deny all” has become increasingly difficult to implement at scale, more organizations have begun looking to tools and techniques designed to penetrate information systems in order to identify gaps in security.

Cobalt Strike is one such tool. Designed and distributed by D.C.-based Strategic Cyber, Cobalt Strike was, and is to this day, meant to specifically aid in red team operations, giving friendly “bad guys” the means of quickly replicating what sophisticated hackers might set up on their own.

Over time, as distribution grew, these tools began to fall into the wrong hands. Malicious hackers and nation-states downloaded trials of Cobalt Strike and found ways to crack the software, or gain access to the full version.

Fortunately, researchers began to notice quirks about some Cobalt Strike servers. Chief among them was an inability for some versions of Cobalt Strike to receive updates from the central servers at Strategic Cyber. Unpatched versions became increasingly recognizable.

Recorded Future combined several disparate detection methods and tested their combined effectiveness on samples of suspected Cobalt Strike servers, demonstrating how using multiple methods could increase the certainty of identification.

Cobalt Strike Hits the Market

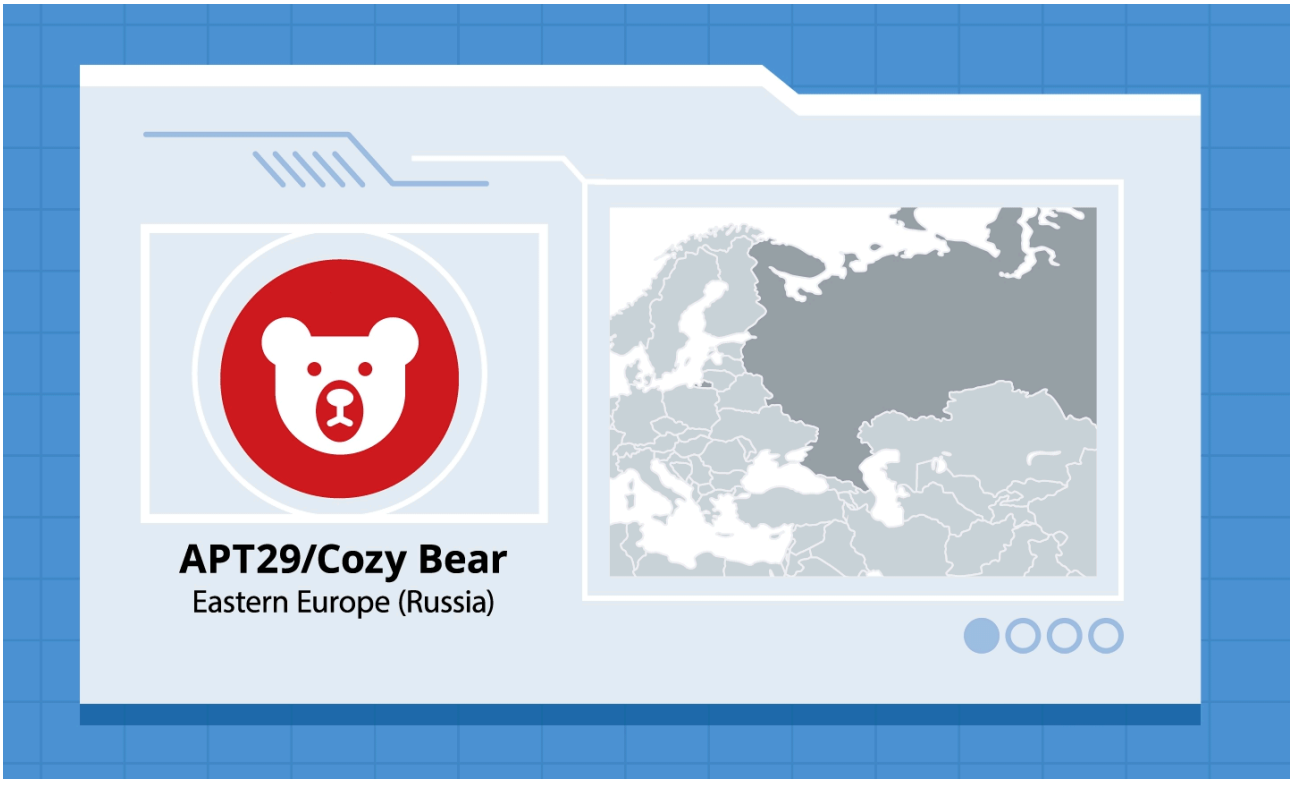
When Cobalt Strike first hit the market in 2012, distribution of the software was carefully controlled. Strategic Cyber realized the potential for it to be used for harm and vetted users in addition to charging significant fees. Soon, red teams around the world were using Cobalt Strike to conduct authorized penetration tests, helping organizations identify flaws in their information systems.

Despite the controls in place, Cobalt Strike eventually fell into the wrong hands. The trial available for immediate download was cracked and unauthorized copies began to emerge in dark web marketplaces.

Proliferation of the software continued worldwide, but it was difficult to know which servers were being used for authorized testing and which were being used for criminal or other destructive activity. The problem of identifying Cobalt Strike as a possible red team trying to demonstrate gaps in network defense was further complicated by Cobalt Strike servers in the wild that could actually do harm

Falling Into the Wrong Hands

Notorious organizations known to have used Cobalt Strike include APT29 (Cozy Bear), Magic Hound, and Winnti. Malicious IP addresses known to be responsible for sending phishing campaigns have also been found to be associated with Cobalt Strike server certificates.

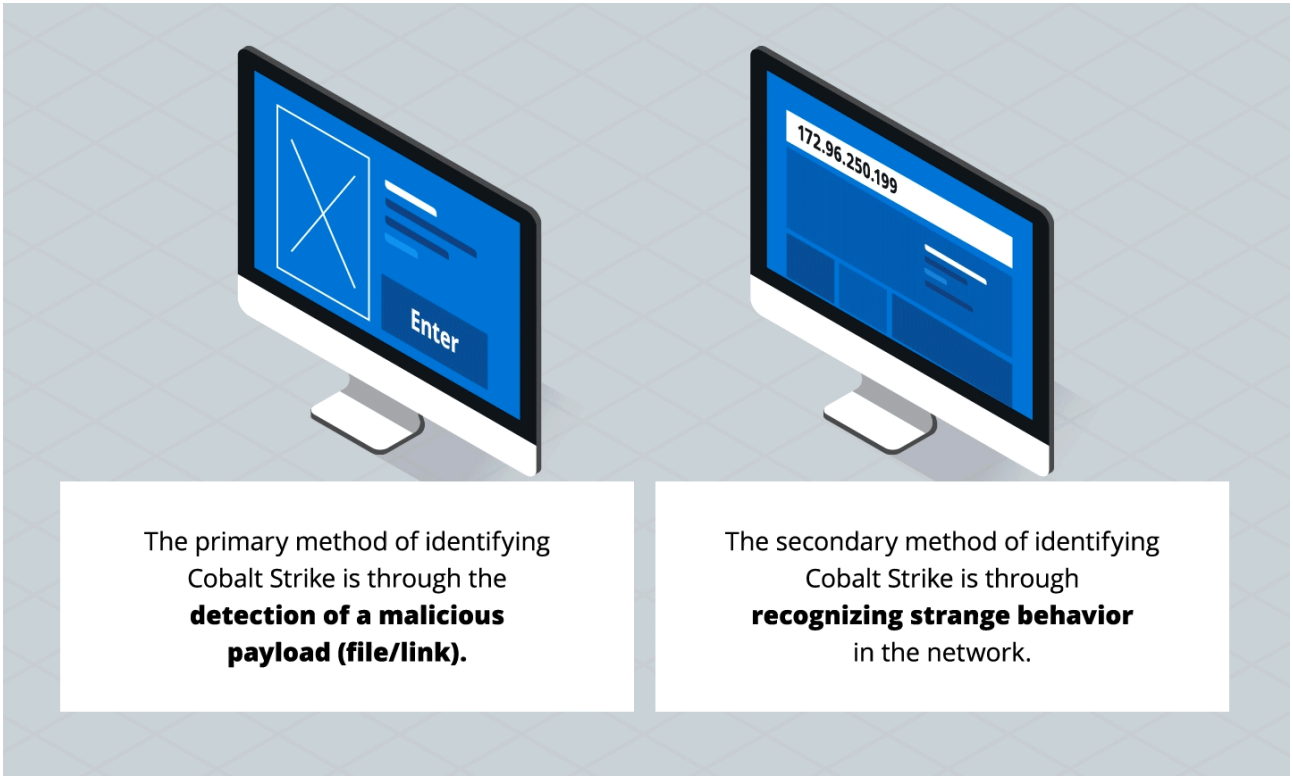


Discovering Methods of Detection

Because cybersecurity teams need to be able to detect Cobalt Strike servers regardless of who is using them and what those actors intend to do when they access a network, they have developed useful methods of detecting Cobalt Strike.

The primary method begins with detection of a malicious payload (file/link). In this scenario, existing security infrastructure like a SIEM or alert system will notify the security team that a malicious payload has entered (or is attempting to enter) the network. Threat analysts can then trace the origin of the payload and look for a Cobalt Strike certificate associated with the email server and related systems.

Attackers using Cobalt Strike may also be discovered as they move throughout a network. A security team may notice improper privilege escalation or lateral movement that calls for a closer look. Upon inspection, the actions can be tied to a certain IP address or domain and these can be analyzed for associations with Cobalt Strike.



Validating Methods of Detection

Strategic Cyber recognized the growing threat of unlicensed copies of Cobalt Strike being in the wild and got to work on a solution:

- In January 2019, Cobalt Strike in release notes identified an anomaly with “removed extraneous space from HTTP status responses.”
- In February 2019, Cobalt Strike released a study highlighting multiple techniques to ID Cobalt Strike servers, including an HTTP 404 Not Found response anomaly.

Meanwhile, independent researchers were also looking for a solution:

- In February 2019, researchers at Fox-IT in the Netherlands published a study based on a null space in an HTTP response from NanoHTTPD servers. They identified the exact anomaly, which Cobalt Strike did not provide.
- Later in February 2019, researchers at Knownsec in China released a blog based on Fox-IT’s study, which was mentioned by Cobalt Strike earlier that month.

- Other known methods of detection included checking the TLS certificate and looking for an open port 50050.

Taking all methods of detection into consideration, Recorded Future validated a highly effective method of detecting Cobalt Strike, which can be accomplished by combining methods of assessing the connection to a malicious IP or domain.

Analysts using this method can cleverly combine specific aspects of unpatched (and therefore, potentially illicit) Cobalt Strike servers and cross-reference the IP addresses of those servers against threat intelligence to develop a level of confidence about both the presence of Cobalt Strike and the likelihood of the party behind Cobalt Strike being malicious.

The Value of Combining Methods

Prior to Recorded Future validating this research, there was a widespread perception that identifying Cobalt Strike servers was highly resource intensive. That kind of thinking could inhibit those in small and medium-sized businesses from taking steps to detect the servers and protect their organizations. Now, by combining a few simple methods, cybersecurity managers at any organization are better equipped to find Cobalt Servers and prevent attacks.

Security Teams at the Forefront

As security teams adopt the methods discussed in the report (and as Cobalt Strike continue to roll out patches for legitimate servers), the gulf between legitimate and pirated versions widens, exposing more harmful Cobalt Strike servers and empowering security teams to guard against them.

Ultimately, the story of Cobalt Strike shows that cybersecurity is less about thinking along strictly defensive or offensive lines. Each has its importance. The challenge and where the fight is won is in the transition from offense to defense and defense to offense.

Source: https://www.recordedfuture.com/blog/identifying-cobalt-strike-servers