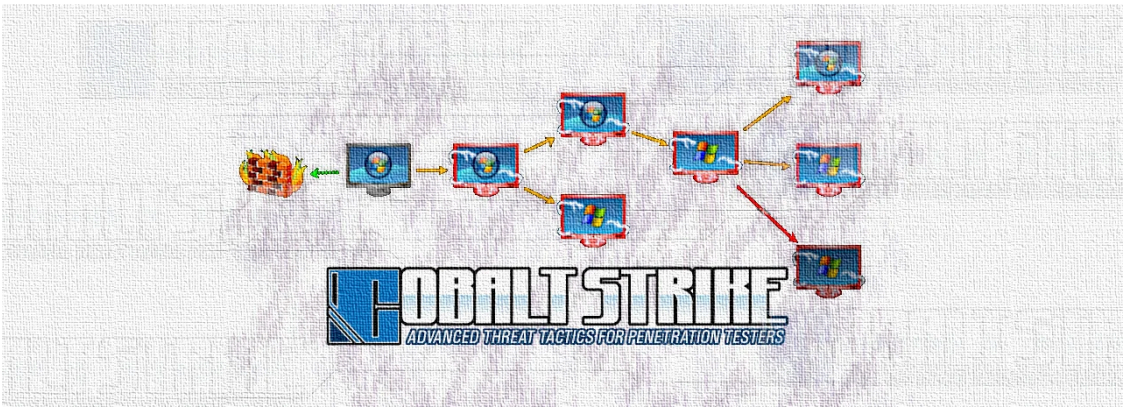
Threat Actors Use Older Cobalt Strike Versions to Blend In

By Ionut Ilascu

Published: 2019-06-18 · Archived: 2026-04-05 23:10:41 UTC

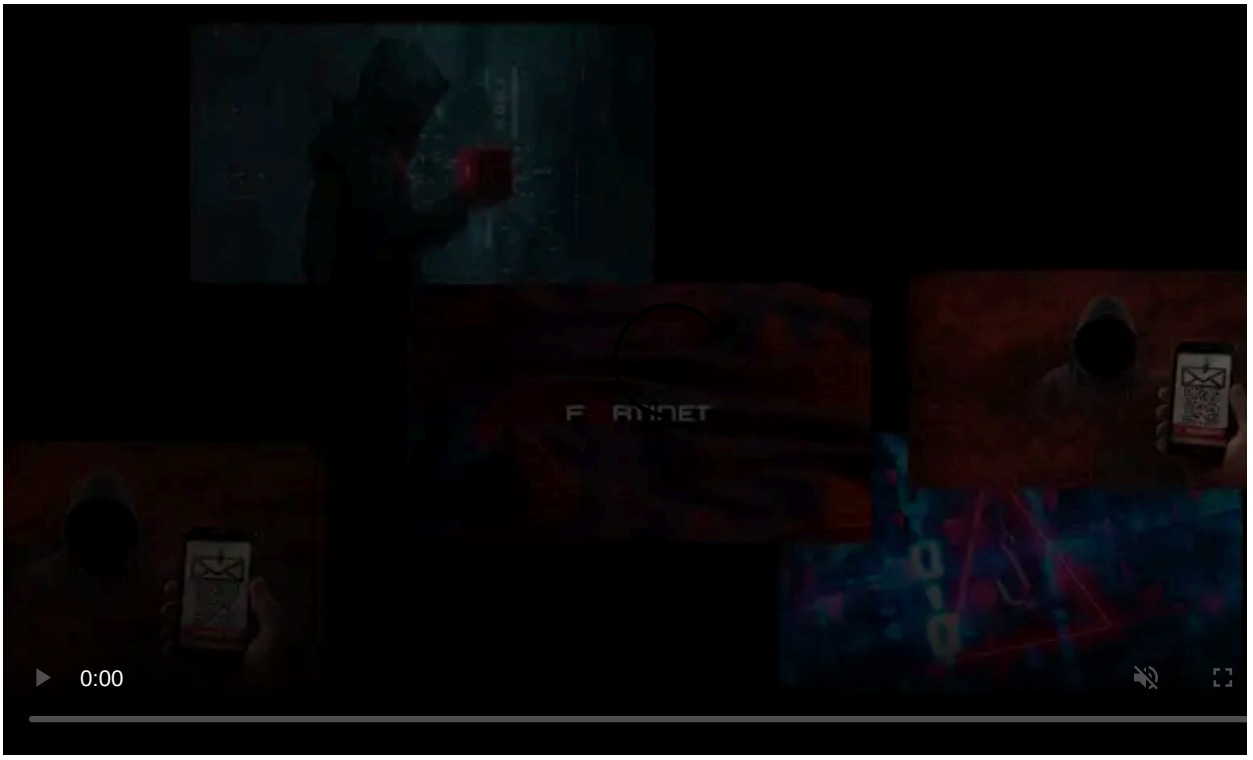


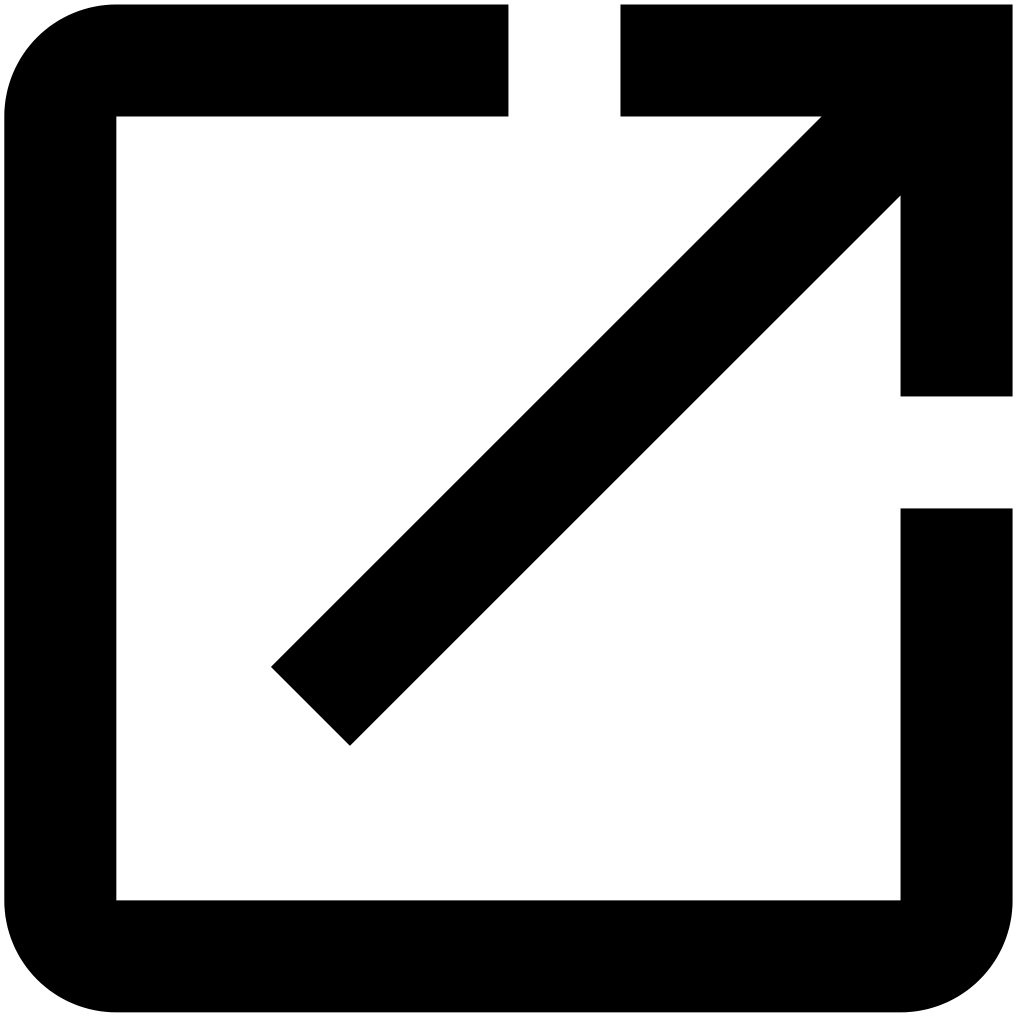
Plenty of outdated Cobalt Strike servers exist in the wild, helping cybercriminals or giving security professionals the upper hand when testing corporate defenses; and they can be easily identified to stifle intrusions of any purpose.

The developer of Cobalt Strike, Strategic Cyber, released version 3.13 of the framework in early January and 3.14 in May. Yet there are tens of servers running an older version of the platform, some of which may have been obtained illegally and deployed for malicious intentions.

Restricted availability

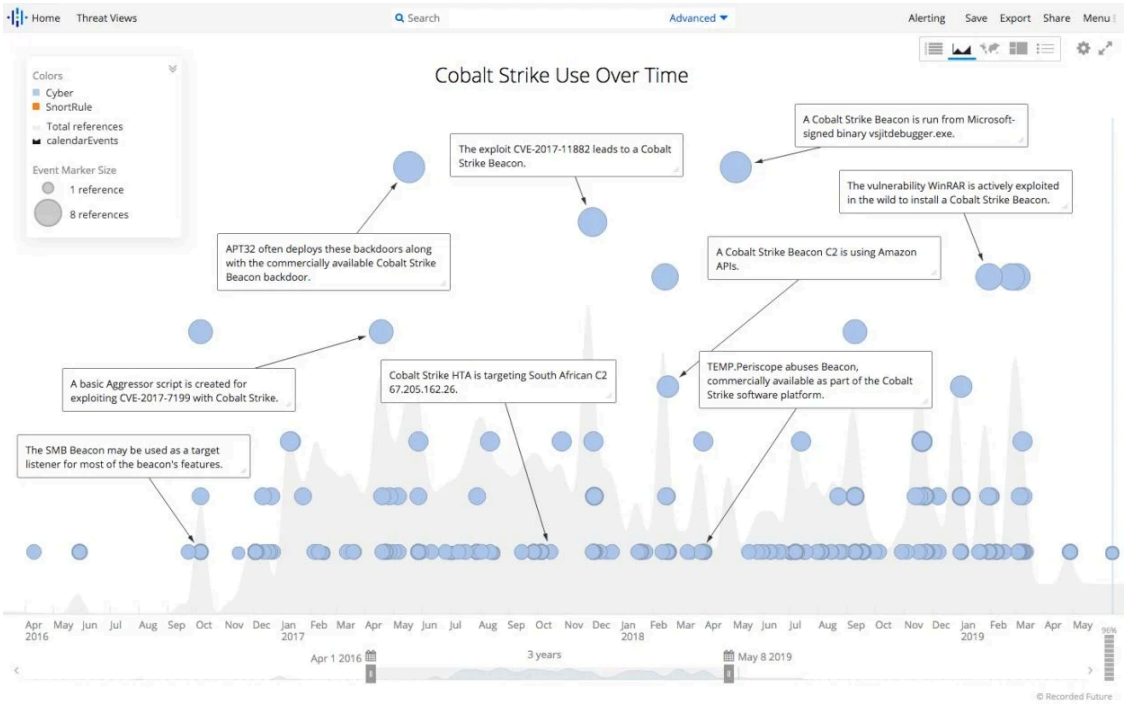
Cobalt Strike is an adversary simulation platform intended for assessing a network's security against an advanced threat actor. Simply put, its purpose is solely for lawful and ethical security testing.


0:00



Apart from its expensive price (per-user license is $3,500 for one year, renewable for $2,500), there are restrictions in place to prevent it from falling into a real adversary's hands. This includes customer screening, limited availability outside the U.S. and Canada, and controlled exporting.

These measures, however, are not always sufficient to stop a determined threat actor from applying for and getting a trial version of Cobalt Strike or obtaining a licensed copy. Some users on hacker forums offered $25,000 to anyone in the US that could get them a genuine copy of the product.



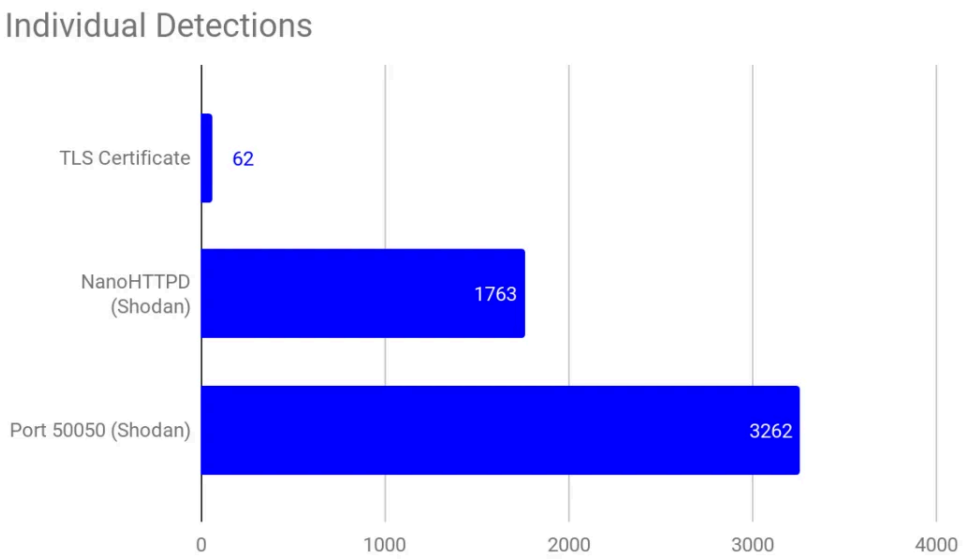
Cracked versions of the software can also be found online (the newest we've seen is for trial version 3.13), but they often pack backdoors or fail to include all the features of the original. These cracked versions cannot be updated.

Identifying unpatched servers

Network defenders should be able to detect and deflect Cobalt Strike activity regardless of the motive behind it. To this end, Recorded Future's Insikt Group scanned the internet searching for clues that may indicate an unpatched server.

By combining multiple methods for detecting the software in the wild, the researchers told BleepingComputer that they were able to discover 104 servers they believe were running Cobalt Strike "based on moderately-high to high confidence detections."

Insikt Group applied methods already documented by Strategic Cyber. One way, which works for all versions of the framework, is to look for the default security certificate from the developer. If the admin does not make a change, it is a pretty reliable sign pointing to Cobalt Strike.



Recorded Future detections January 2019 to May 2019

Another hint is the DNS server in the framework, which responds with a fake IP address (0.0.0.0) when active. This is not unique, though, but could be combined with other methods to increase confidence in the detection.

An open controller port number 50050/TCP may also indicate a Cobalt Strike Team Server, as it would be unexpected to find it on other types of servers.

Last on the official list of indicators is a "404 Not Found" HTTP error, which was is unique to the NanoHTTPD web servers running on Cobalt Strike 3.13 and earlier.

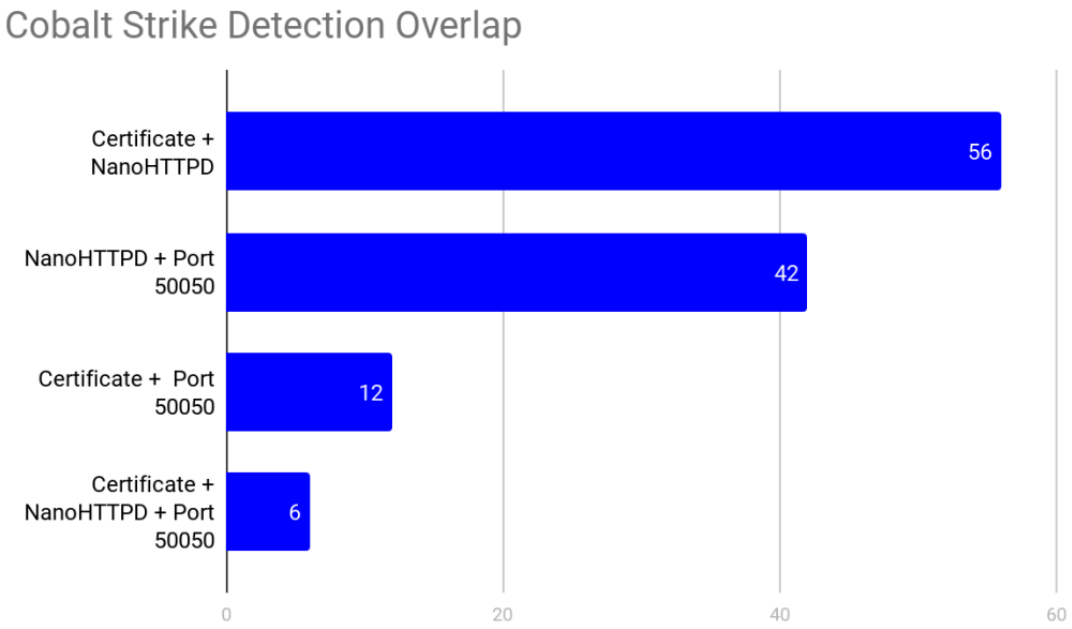
An unofficial mark in NanoHTTPD that also gave away the presence of an outdated Cobalt Strike server is the presence of "a null space in the HTTP response where “HTTP/1.1” is followed by a blank space (0x20) not found in other web server responses."

```
0030  ff ff e9 13 00 00 48 54  54 50 2f 31 2e 31 20 32   ·····HT TP/1.1 2
0040  30 30 20 4f 4b 20 0d 0a  43 6f 6e 74 65 6e 74 2d   00 OK · Content-
0050  54 79 70 65 3a 20 74 65  78 74 2f 68 74 6d 6c 0d   Type: te xt/html·
0060  0a 44 61 74 65 3a 20 46  72 69 2c 20 33 20 4d 61   ·Date: F ri, 3 Ma
0070  79 20 32 30 31 39 20 31  34 3a 30 30 3a 30 39 20   y 2019 1 4:00:09
0080  47 4d 54 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   GMT··Con nection:
0090  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 43 6f 6e    keep-al ive··Con
00a0  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 35 0d 0a   tent-Len gth: 5··
00b0  0d 0a                                              ··
```

A fix was delivered with version 3.13, as shown in the official release notes: "removed extraneous space from HTTP status responses."

For a year and a half, security outfit Fox IT used this method to identify Cobalt Strike Servers, "with high confidence" before it was fixed.

Defenders can take advantage of these techniques to enable proactive protections on the network against an older Cobalt Strike release, which would likely cater to criminal activity.



Although there may still be room for error, mixing the various detection methods should provide high confidence results. The use of the default TLS certificate, though, remains the surest way to identify a Cobalt Strike server.

Fingerprinting TLS negotiations

Another technique to detect Cobalt Strike system is to inspect suspicious network traffic in search for specific markers relating to the TLS negotiation between a server and a client. TLS fingerprints like protocol version, accepted ciphers, and elliptic curve information can be used to identify connections to the server.

JA3, an open-source method for profiling SSL/TLS connections can help with signatures for both clients and servers. The project (and other sources) provides fingerprints for the TLS data exchange by the client beacon (which uses the Windows socket to initiate communication) and servers running on Kali Linux.

This detection method can be thwarted by using a proxy for the connections but such a scenario is not common so it is a reliable technique to find Cobalt Strike servers, especially in combination with the other solutions.

Mingling in

The techniques described in the report from Recorded Future may be for unpatched versions of the security testing framework but it does not mean they make for outdated detection routines.

To keep a low profile, attackers often prefer running an older release if other bad actors have not moved to a newer version. Another reason may be that customizations could be lost when upgrading to a new build.

If a pirated version is used, the threat actor would have to wait for a cracked copy of a newer release.

"The use of cracked versions of Cobalt Strike or deployment of standard Cobalt Strike instances causes a blending together of threats, making attribution difficult. Additionally, by running cracked versions of the framework, actors can blend in with older versions of Cobalt Strike," explains Recorded Future.
