Tracking Cobalt Strike Servers Used in Cyberattacks on Ukraine

ironnet.com/blog/tracking-cobalt-strike-servers-used-in-cyberattacks-on-ukraine

Back to IronNet Blog

Threat Research

By IronNet Threat Research Team with lead contributions by Peter Rydzynski and Brent Eskridge, Ph.D

May 8, 2022

On April 18, 2022, CERT-UA published alert #4490, which describes a malicious email campaign targeting Ukraine. The email attempts to deploy a Cobalt Strike beacon on the victim's system through the use of a MS Office macro. In the alert, CERT-UA provides a list of indicators of compromise (IoCs), including a list of IP addresses and domains used in the attack that are known to be Cobalt Strike command and control (C2) servers.

IronNet Threat Research regularly monitors the internet for malicious C2 servers, including Cobalt Strike. As a result of this monitoring, we have a longitudinal dataset on the C2 servers hosted on the IP addresses and domains referenced in the alert starting in May 2021. This report provides an analysis of this data in an attempt to inform the community on the observed patterns of these IoCs and other indicators that may be related to those referenced in the alert.

Cobalt Strike: Malleable Profiles

One of the ways Cobalt Strike operators obfuscate communications between a beacon planted on a victim system and the C2 server is through the use of a malleable profile. A malleable profile allows the operator to configure the beacon communication to masquerade as benign network traffic. Some of the settings that can be modified are:

- the sleep time between callbacks to the C2 server,
- jitter in the callback sleep time,
- the user agent used in the communication, and
- the URI used in the HTTP request to the C2 server.

While these malleable profiles are useful in obfuscating communications, they can also be used as an approximate fingerprint when analyzing a Cobalt Strike C2 server. While most actors use open source malleable profiles or a malleable profile generator, which makes attribution or clustering challenging, a server's profile can be combined with other attributes to identify patterns. A full discussion of malleable profiles is beyond the scope of this report, but there are numerous descriptions available elsewhere (link, link).

Two of the profiles that were seen in the campaign targeting Ukraine were a JQuery profile and a minimal defender bypass profile. JQuery is a popular choice of emulation amongst threat actors; however, the minimal defender bypass profile is something that we've only noticed in the past few months and only in this campaign.

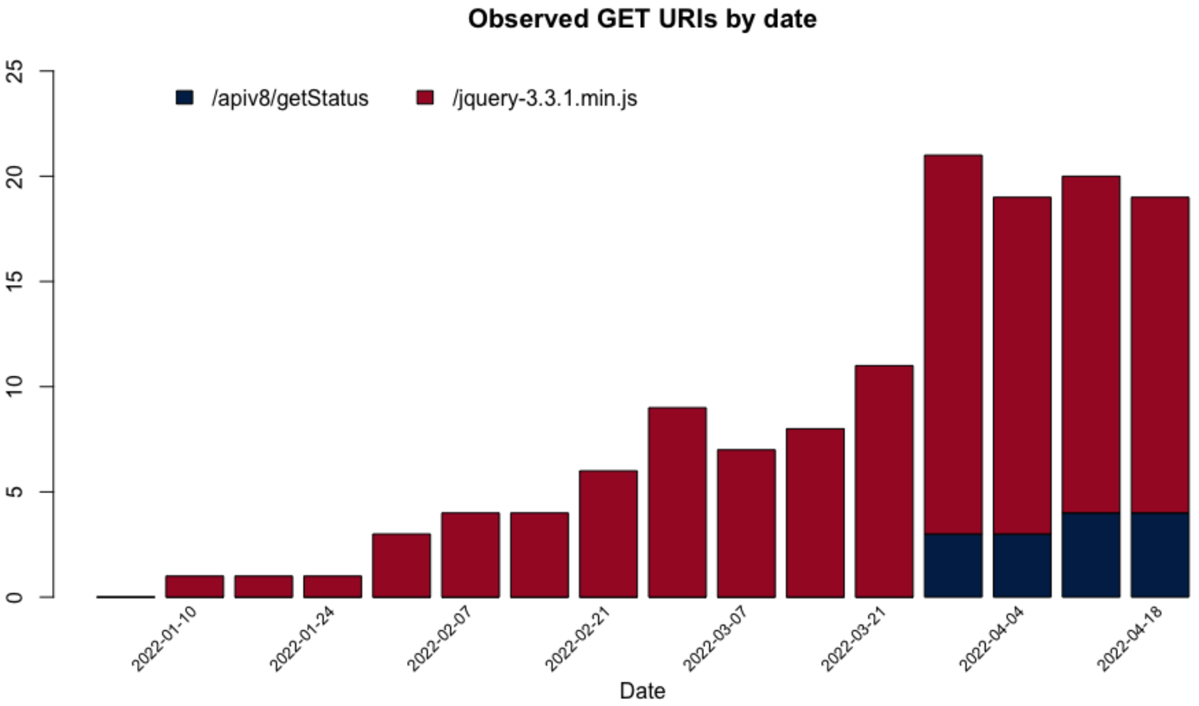
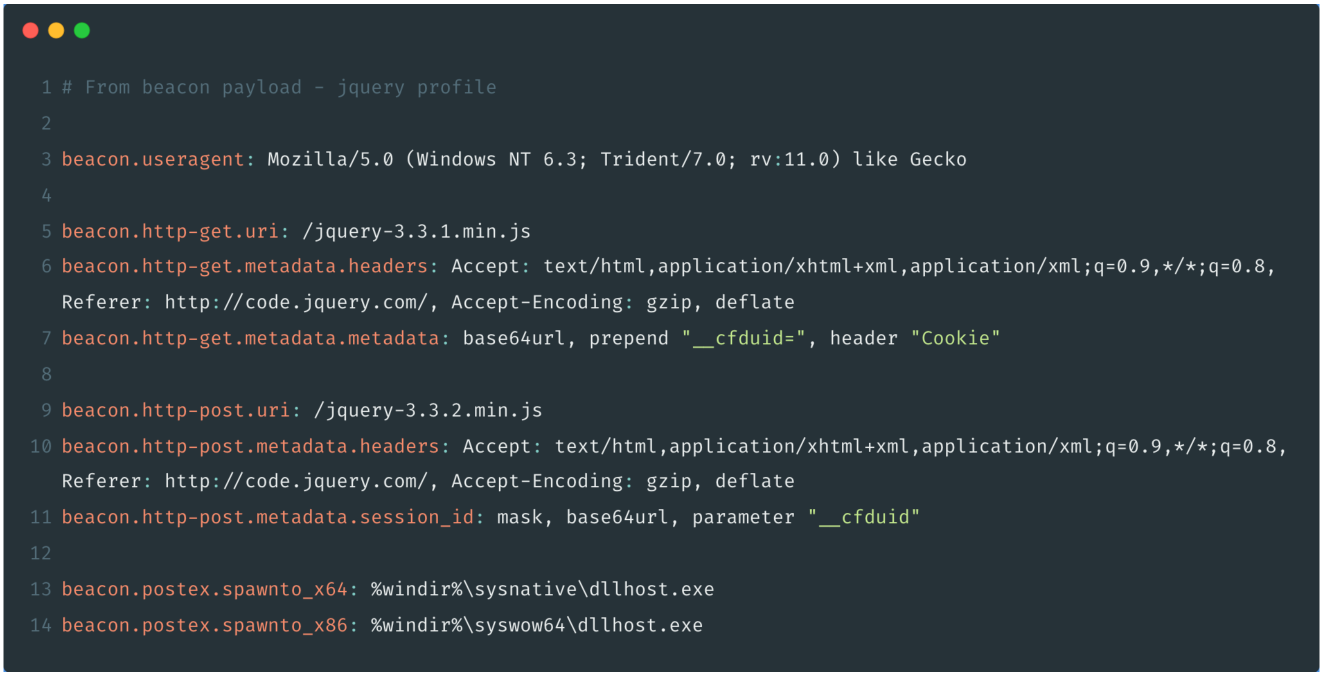


Figure 1 - Malleable profile GET URI's observed in the IoCs since May 2021

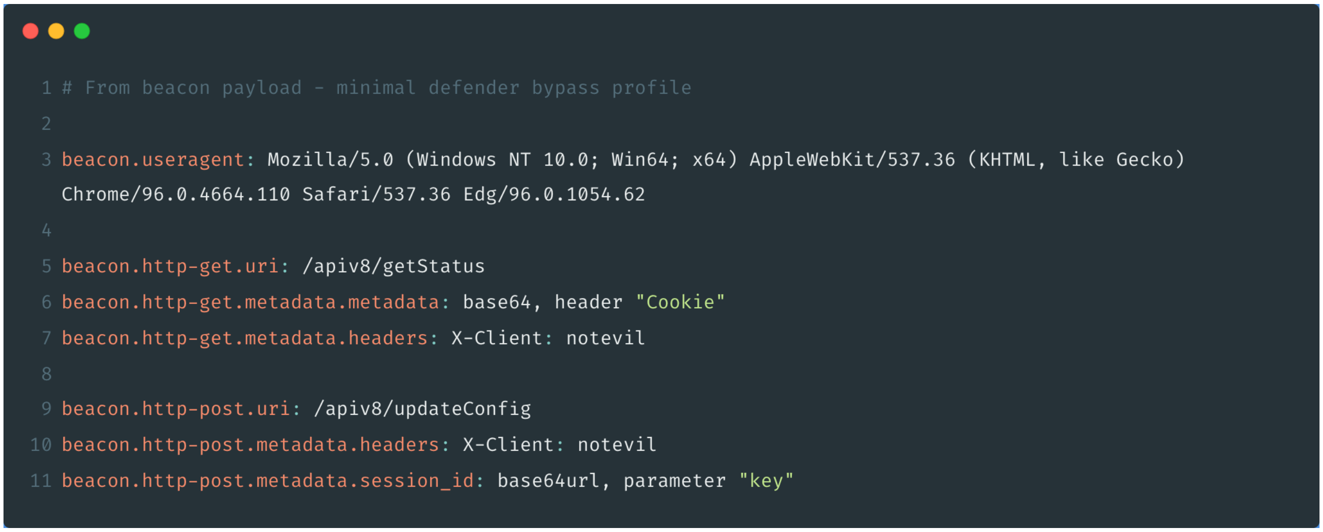
Of the options available in malleable profiles, the request uniform resource indicator (URI) is the most varied and the most useful for attempting to fingerprint, or at least categorize, C2 servers using the malleable profile. In total, eight different URIs were observed in use by the C2 servers mentioned in the CERT-UA alert, indicating that there were at least eight different malleable profiles used. Of particular interest are the two profiles observed in 2022, which overlap with Russia's invasion of Ukraine and the associated cyber attacks. The URIs associated with these profiles are shown in Figure 1.



```
# From beacon payload - jquery profile

beacon.useragent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko

beacon.http-get.uri: /jquery-3.3.1.min.js
beacon.http-get.metadata.headers: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8, Referer: http://code.jquery.com/, Accept-Encoding: gzip, deflate
beacon.http-get.metadata.metadata: base64url, prepend "__cfduid=", header "Cookie"

beacon.http-post.uri: /jquery-3.3.2.min.js
beacon.http-post.metadata.headers: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8, Referer: http://code.jquery.com/, Accept-Encoding: gzip, deflate
beacon.http-post.metadata.session_id: mask, base64url, parameter "__cfduid"

beacon.postex.spawnto_x64: %windir%\sysnative\dllhost.exe
beacon.postex.spawnto_x86: %windir%\syswow64\dllhost.exe
```

Figure 2 - A malleable profile found online that closely matches the one observed in use on numerous C2 servers described in the Ukrainian CERT alert

The profile with the `/jquery-3.3.1.min.js` URI is the more common of the two profiles, both in this particular set of IoCs and in IronNet's full data set of Cobalt Strike C2 servers (see Figure 2). This particular malleable profile can be found on the internet and is listed as a reference for designing Cobalt Strike malleable profiles. As such, use of this profile makes attribution difficult since it is used everywhere.



```
# From beacon payload - minimal defender bypass profile

beacon.useragent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 Edg/96.0.1054.62

beacon.http-get.uri: /apiv8/getStatus
beacon.http-get.metadata.metadata: base64, header "Cookie"
beacon.http-get.metadata.headers: X-Client: notevil

beacon.http-post.uri: /apiv8/updateConfig
beacon.http-post.metadata.headers: X-Client: notevil
beacon.http-post.metadata.session_id: base64url, parameter "key"
```

Figure 3 - A malleable profile found online that is intended to be hidden behind an Nginx redirector that matches observed C2 servers described in the Ukrainian CERT alert

The second profile, which is referred to as the *minimal defender bypass profile* and has the `/apiv8/getStatus` URI, can also be found on the internet, but its observed use is far more rare than the previous one (see Figure 3). These servers were the first observations we have had of this profile. At first, we thought this was due to the relative novelty of the profile. However, further inspection indicates the profile is intended to be used behind an Nginx redirector to hide the C2 server from fingerprinting.

Both of these profiles used in the most recent attacks are pre-made and provide a low effort configuration cost. We often see malleable profiles that are customized versions of profiles found on the internet. For example, the domain `klycnmik[.]com`, which uses the same jQuery URI, has been observed in use by Cobalt Strike servers associated with Emotet.

Cobalt Strike: Watermarks

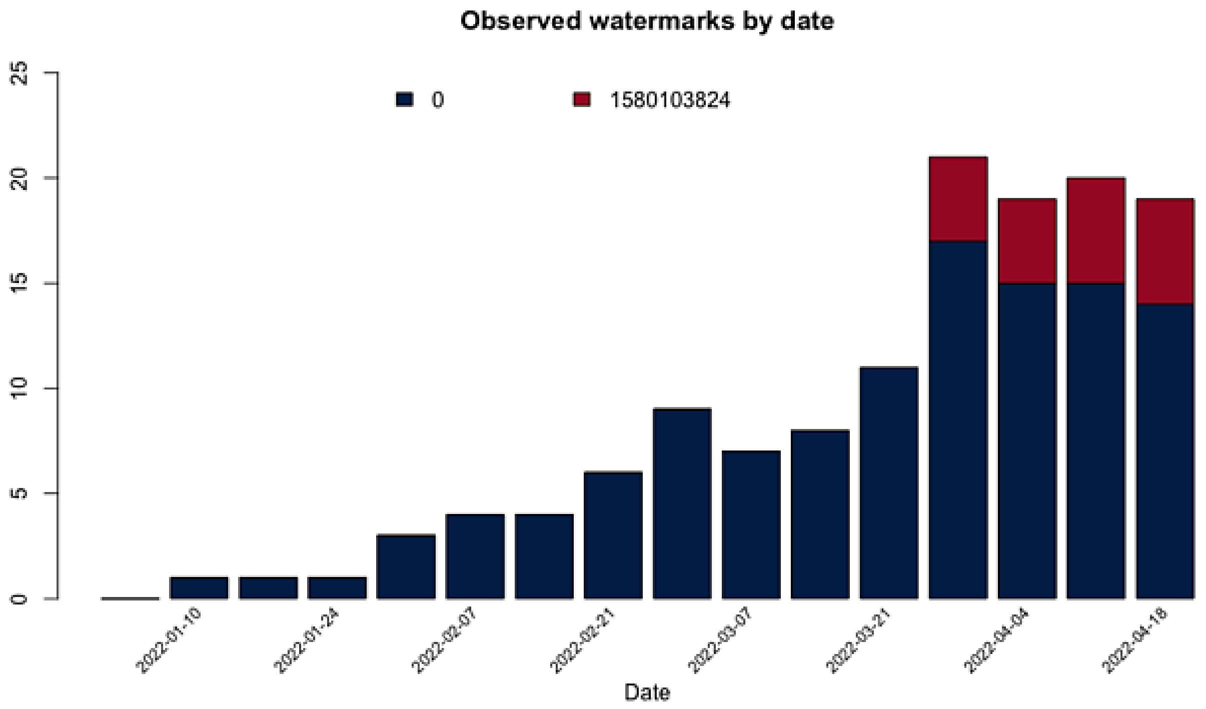


Figure 4 - Cobalt Strike watermarks observed in the IoCs since May 2021

Another means of categorizing and analyzing Cobalt Strike C2 servers is through the use of the server's watermark. Each payload deployed by a server contains a watermark, which is a unique number associated with the Cobalt Strike license. But since stolen or cracked copies of Cobalt Strike are frequently used by threat actors, using a watermark as a fingerprint isn't foolproof. For example, a watermark value of 0 indicates a cracked version. Unsurprisingly, this is the most commonly found watermark in our data. Despite this, watermarks can still be used for analysis. The watermarks we observed being used by the IoCs described by CERT-UA are shown in Figure 4. The watermark of particular interest here is `1580103824`. It is shared by all the C2 servers using the `/apiv8/getStatus` URI, which was specifically noted in the CERT-UA alert. While C2 servers with different profiles and configurations could potentially have this same watermark, we rarely observe this watermark, but have seen an increase in recent weeks. Note that this watermark is very similar (one digit differs) from one associated with a hacked version of Cobalt Strike that is frequently found on dark web forums.

Of the five domains that share the rare URI and watermark, only four are mentioned in the CERT-UA alert. These are: `axikok[.]com` , `blopik[.]com` , `dezword[.]com` , and `verofes[.]com` . The fifth observed domain, `furfen[.]com` , is not mentioned in the CERT-UA alert, but has, in addition to our own scans, been observed by other sources to be a Cobalt Strike C2 server. While a URI and watermark is insufficient to confirm that this server is related to the others, further analysis detailed below lends more credence to the argument that they are related.

NGINX

We found the use of the minimal defender bypass profile to be of particular interest, not because it was used, but because they took the time to lock down the C2 communications, but left the staging wide open. The profile is intended to be used with a redirector to prevent the C2 server from being fingerprinted with conventional methods. This is a fairly common technique that is not unique to Cobalt Strike and has been utilized by threat actors for quite some time. Redirectors are positioned between the C2 server and the beacon to hide the true location of the C2 server. They are often configured to only redirect specific traffic from a beacon to the C2 server and to direct the remaining traffic to a legitimate server, making the detection of these servers challenging.

Cobalt Strike Infrastructure

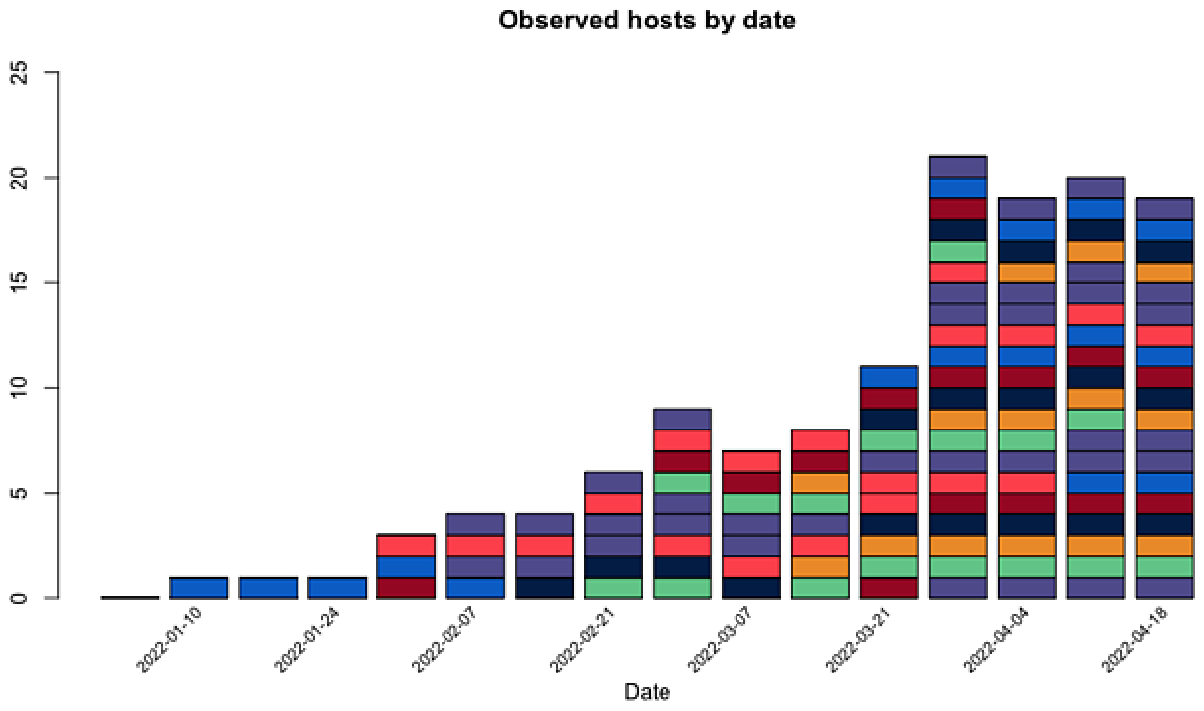


Figure 5 - Observation dates of the IoCs mentioned in the Ukrainian CERT alert since May 2021 (organized by unique domain or IP address)

Apart from server configurations, there are a number of interesting relationships between the infrastructure of the C2 servers mentioned in the alert. Over the course of the last 15 months, there were three distinct clusters of activity for the IoCs described in the Ukrainian CERT alert. The distribution of observations for the cluster observed in 2022 is shown in Figure 5. In this cluster, 35 different domains were observed, but, as discussed above, they share many similarities such as profiles and watermarks.

The vast majority of the hosts listen on either port 80 (HTTP), 443 (HTTPS), or both, as would be expected. One server, `axikok[.]com` primarily listened on 8443 (HTTPS), but did have port 8080 (HTTP) opened intermittently.

According to our data, the C2 servers in the alert are all hosted in one of four hosting providers: HostKey, HostKey B.V., Endurance International, and UAB Nacionalinis Telekomunikaciju, with 33 of the 40 hosted by HostKey as far back as June 2021. As for the domains themselves, all of the domains used in the most recent campaign were registered to one of three registrars: Eranet, WEBCC, and NiceNIC, with 26 of the 30 domains registered at Eranet since January 10, 2022.

Next Steps

It’s clear that the ease of use and flexibility that Cobalt Strike provides is one of the main reasons that it remains so prevalent amongst threat actors. Reflecting on the analysis of our dataset matched with the indicators provided in the UA CERT alert, there are a few open questions remaining. First, we see less sophisticated threat actors still deploy Cobalt Strike servers with little to no OPSEC, allowing even the most basic detections of C2 frameworks. Thus, will threat actors continue to forgo OPSEC concerns as long as they continue to dominate victims with high success rates?

Second, we wonder whether the majority of threat actors will utilize open source malleable profiles or a malleable profile generator like C2 Concealer that takes static attributes from a list and combines them to a single profile? Furthermore, do threat actors take into consideration the environment they are targeting when selecting a malleable profile, or are they simply choosing a popular service they know will thwart most defenders? Answers to these questions will be beneficial to detecting Cobalt Strike servers in the future.

Additional IOCs

IronNet observed the following domains present in Cobalt Strike beacon payloads being served up by the same Cobalt Strike servers mentioned in the Ukrainian CERT alert.

- `furfen[.]com`

- `Klycnmik[.]com`
- `Shizij[.]com`
- `ngrety[.]com`
- `korunder[.]com`
- `vedingumbr[.]com`
- `jenevabaiden[.]com`
- `zeronyk[.]com`
- `shevronf[.]com`
- `dunclikf[.]com`
- `nentundo[.]com`
- `gelmutol[.]com`
- `axelkim[.]com`
- `gookju[.]com`

IronNet Threat Intel API

Interested in these indicators? The IronNet Threat Research team regularly scans the internet for malicious C2 frameworks. If you are interested in receiving these indicators as a threat intelligence feed, contact our team by clicking the button below.

Email us

About Ironnet

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Back to IronNet Blog