Bumblebee Malware Loader Threat Analysis

By Michael Lamb

Published: 2022-09-16 · Archived: 2026-04-05 17:42:32 UTC

Executive summary

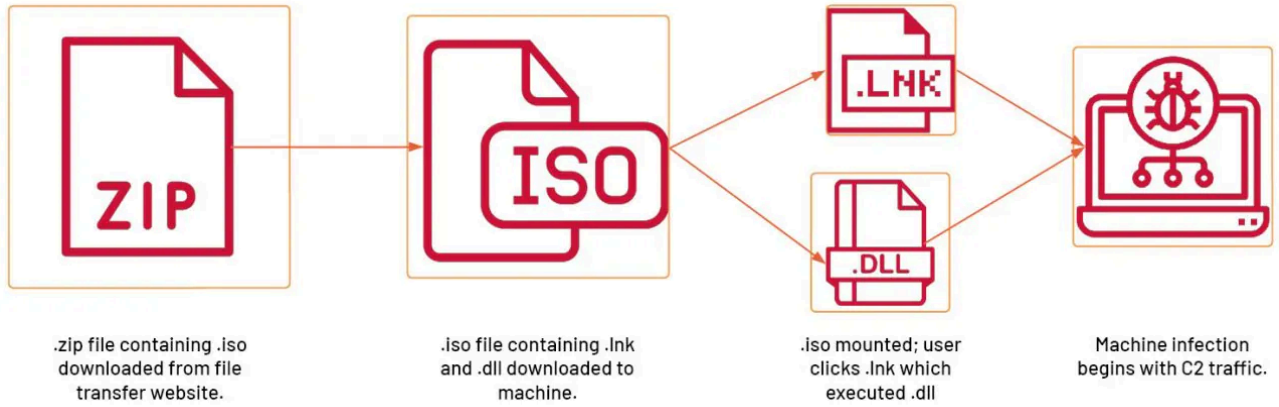
This year Google's TAG (Threat Analysis Group) published an article referring to a new Threat Actor Group called "EXOTIC LILY". This group is believed to be an Initial Access Broker with strong links to the Wizard Spider group which operates the Conti ransomware variant.

In an interesting analysis, Google TAG noted a new delivery method abusing file transfer sites like TransferXL and WeTransfer, which lured users to download a .zip file. Inside the .zip file was an .iso which, when clicked would auto-mount to a Windows system containing a .lnk shortcut file and .dll file.

Further analysis revealed that the .dll file is a new variant of loader which is executed by the command embedded into the .lnk file.

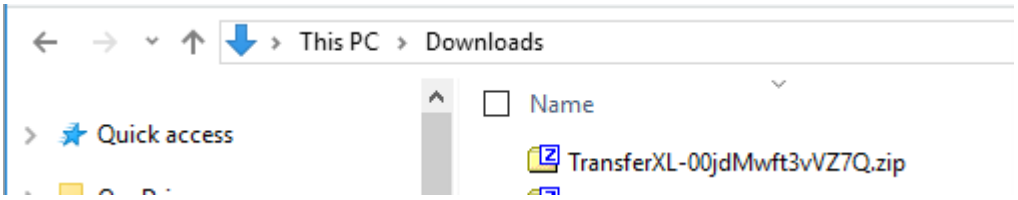
Aspire's SOC team undertook further analysis of the campaign by retrieving a copy of the network packet capture from the SANS Internet Storm Center. We uncovered evidence of cobalt strike activity, suspicious C2 connections displaying evidence of defence evasion and suspicious connections to AWS Virtual Machine Infrastructure.

Bumblebee delivery & execution mechanism overview

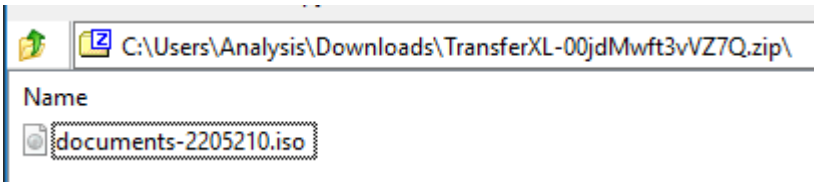


Bumblebee breakdown

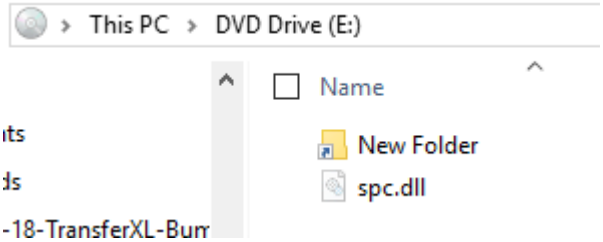
The bumblebee loader is delivered as a zip file, downloaded via an e-mail lure from TransferXL:



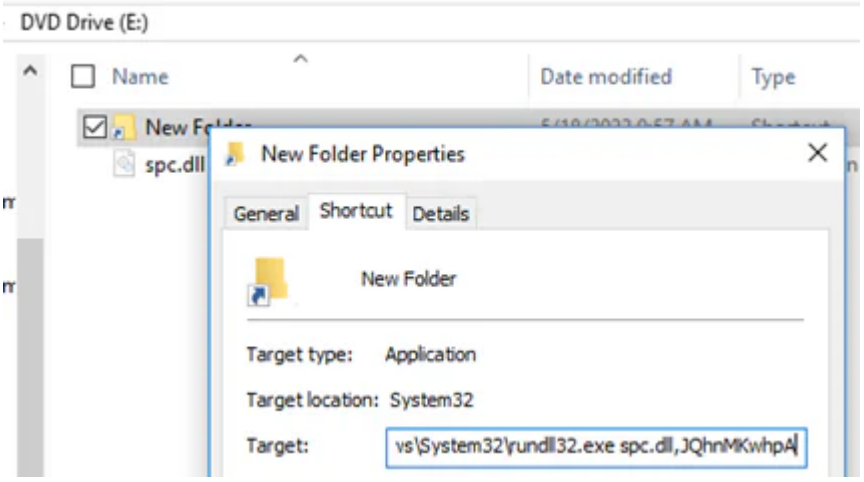
Upon opening the zip file you will find an .iso file which mounts when double clicked:



Inside the mounted .iso you will find a shortcut file and a .dll file (spc.dll)



Inspecting the shortcut reveals an [execution tactic utilising rundll32.exe]



Rundll32.exe takes the .dll and the entry point as two arguments to execute the DLL.

Traffic analysis with Brim

Brim is a desktop application providing a SIEM-like interface to take in PCAP files and convert them to Zeek logs, as well as running the file through the Suricata NIDS engine to produce alert events for suspicious activity.

Brim can be used to pivot from zeek data points, open Wireshark for deeper analysis, enrich with VirusTotal and visualise data in charts and graphs.

Host identification

There was only one host and username on the PCAP, which made scoping the potentially infected host easier.

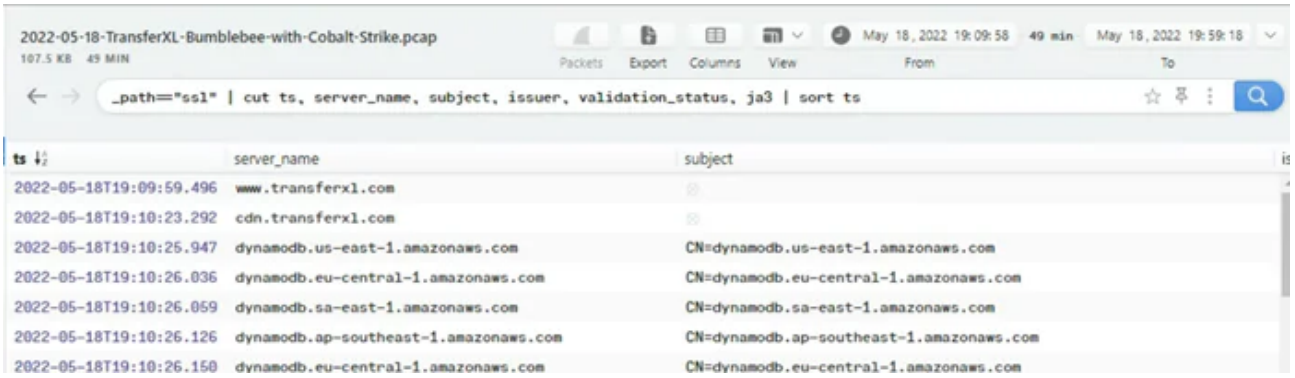
Hostname: DESKTOP-D8FSF3

Domain: STUDIOPLUS.COMPANY

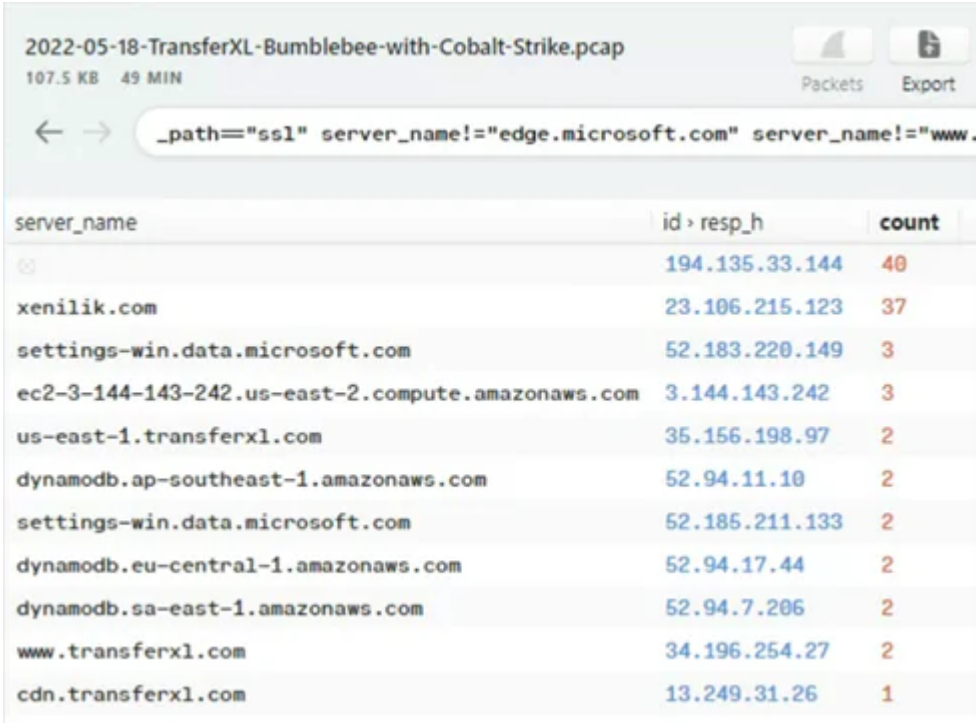
Username: Jacob.macnuttey

HTTPS traffic

A quick filter on the SSL traffic shows us communications with the TransferXL domain (transferxl[.]com) initially. By ordering the traffic by time (Earliest to Latest) we can then start to spot suspicious domains that we might want to investigate more by pivoting into other Zeek logs.



Another perspective of the SSL traffic is to sort by count of destination host, this shows the majority of the traffic in this packet capture was to xenilik[.]com. What's more interesting at this point of our analysis, is that there are more connections directly to 194[.]135[.]33[.]144 over Port 443… This could be our Command and Control (C2) connections.



server_name	id › resp_h	count
	194.135.33.144	40
xenilik.com	23.106.215.123	37
settings-win.data.microsoft.com	52.183.220.149	3
ec2-3-144-143-242.us-east-2.compute.amazonaws.com	3.144.143.242	3
us-east-1.transferxl.com	35.156.198.97	2
dynamodb.ap-southeast-1.amazonaws.com	52.94.11.10	2
settings-win.data.microsoft.com	52.185.211.133	2
dynamodb.eu-central-1.amazonaws.com	52.94.17.44	2
dynamodb.sa-east-1.amazonaws.com	52.94.7.206	2
www.transferxl.com	34.196.254.27	2
cdn.transferxl.com	13.249.31.26	1

Suricata alerts

When you load a packet capture into Brim, the file will be analysed by the integrated Zeek and Suricata engines which in turn generates the Zeek log files as well as any Suricata (NIDS) alerts to assist in generating leads to investigate.

In the case of this packet capture, there were only 3 alert categories, which didn't generate any immediate leads with regards to command and control, file download of exfiltration.

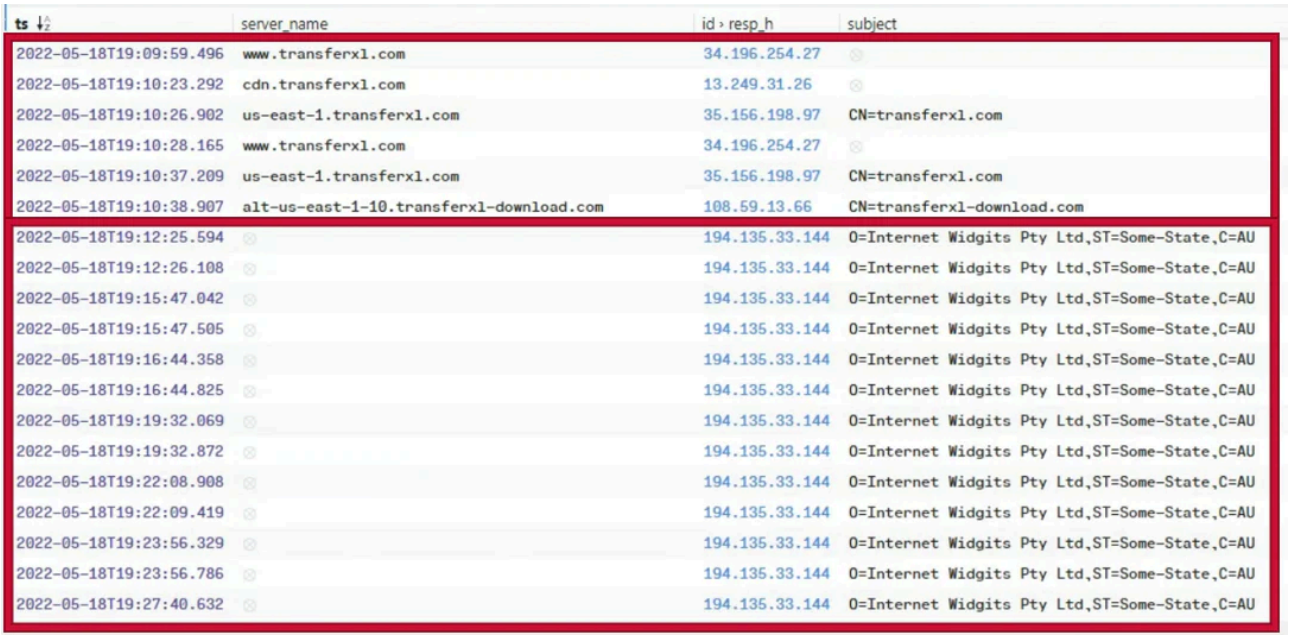
alert › severity	alert › category	count
1	Attempted Administrator Privilege Gain	115
3	Not Suspicious Traffic	40
3	Generic Protocol Command Decode	2

Conclusions

With the traffic filtered down to interesting traffic i.e. not CDN, not googletagmanager etc. we get a clear view of the timeline.

The first section of traffic shows the download from TransferXL, the second section of traffic shows C2 traffic related to bumblebee loader, utilising a self-signed certificate.

TransferXL download & C2 traffic



ts	server_name	id › resp_h	subject
2022-05-18T19:09:59.496	www.transferxl.com	34.196.254.27	
2022-05-18T19:10:23.292	cdn.transferxl.com	13.249.31.26	
2022-05-18T19:10:26.902	us-east-1.transferxl.com	35.156.198.97	CN=transferxl.com
2022-05-18T19:10:28.165	www.transferxl.com	34.196.254.27	
2022-05-18T19:10:37.209	us-east-1.transferxl.com	35.156.198.97	CN=transferxl.com
2022-05-18T19:10:38.907	alt-us-east-1-10.transferxl-download.com	108.59.13.66	CN=transferxl-download.com
2022-05-18T19:12:25.594		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:12:26.108		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:15:47.042		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:15:47.505		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:16:44.358		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:16:44.825		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:19:32.069		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:19:32.872		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:22:08.908		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:22:09.419		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:23:56.329		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:23:56.786		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
2022-05-18T19:27:40.632		194.135.33.144	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU

C2 JA3 hash (The pitfall of JA3 hashes)

JA3 hashes can be really useful, as they aid in identifying the client application that made the SSL connection. With that said, some C2 frameworks will rely on underlying default libraries (Python) or an operating system socket, which means the hash cannot be used as a reliable IOC.

When analysing the JA3 hash of the SSL handshake, Aspire uncovered that this is being reported as an IoC in many sources and historical articles related to other threat actors. The JA3 hash in this case actually identifies that the C2 used a Windows 10 socket, which means that the hash cannot be used to uniquely identify the handshake as an indicator of malicious traffic. This could in theory by a method of evasion.

A full list of default hashes can be found below:

- Win10-socket: c12f54a3f91dc7bafd92cb59fe009a35
- Win10-socket-SNI: 3b5074b1b5d032e5620f69f9f700ff0e
- Win10-powershell: fc54e0d16d9764783542f0146a98b300
- Win10-powershell-SNI: 54328bd36c14bd82ddaa0c04b25ed9ad
- Win10-iexplore: be6155e945a3e59a1dd0841b86f6c945
- Win10-iexplore-SNI: 10ee8d30a5d01c042afd7b2b205facc4
- Win2016-socket: 043c543b63b895881d9abfbc320cb863
- Win2016-socket-SNI: 7c410ce832e848a3321432c9a82e972b
- Win2016-powershell: 17b69de9188f4c205a00fe5ae9c1151f
- Win2016-powershell-SNI: 235a856727c14dba889ddee0a38dd2f2
- Win2016-iexplore: 4f2e9c50db9bd107439136bd24740c0d
- Win2016-iexplore-SNI: f88610704d61a237aa9e5e0849573998

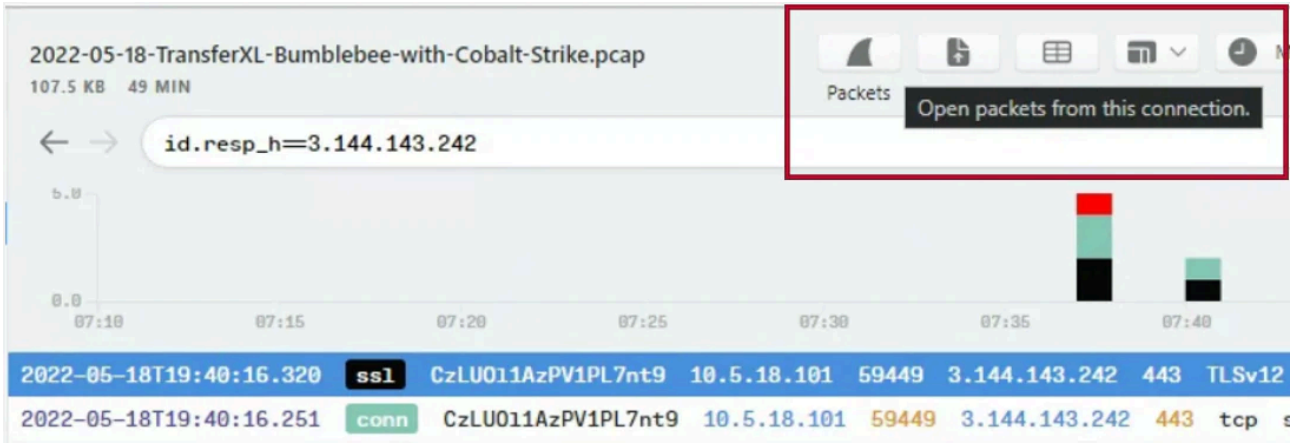
The above list should be used to baseline your environment. Credit to Jeff Atkinson who shared this list in the Bro Workshop 2019 at Geneva.

Suspicious AWS EC2 connections

As highlighted by MTA's analysis, we also noted the suspicious connections to an AWS EC2 Virtual Machine.

2022-05-18T19:32:02.241		194.135.33.144
2022-05-18T19:35:40.744		194.135.33.144
2022-05-18T19:35:41.192		194.135.33.144
2022-05-18T19:37:46.174		194.135.33.144
2022-05-18T19:37:46.613		194.135.33.144
2022-05-18T19:37:47.591	ec2-3-144-143-242.us-east-2.compute.amazonaws.com	3.144.143.242
2022-05-18T19:37:48.560	ec2-3-144-143-242.us-east-2.compute.amazonaws.com	3.144.143.242
2022-05-18T19:40:03.606		194.135.33.144
2022-05-18T19:40:04.069		194.135.33.144
2022-05-18T19:40:16.320	ec2-3-144-143-242.us-east-2.compute.amazonaws.com	3.144.143.242
2022-05-18T19:42:02.933		194.135.33.144

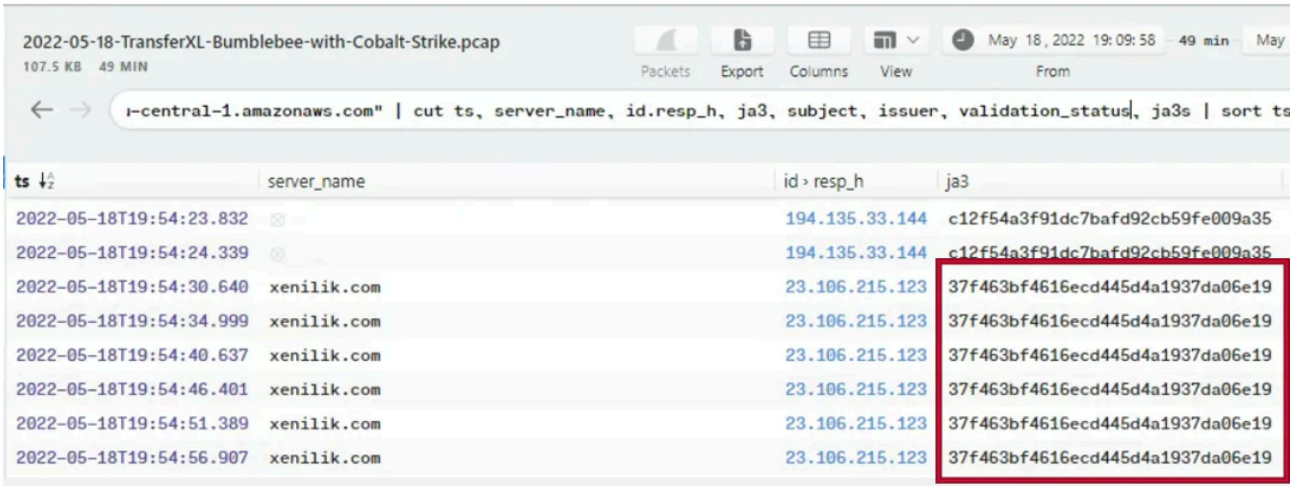
Whilst Brim offers a powerful capability to see the raw packets in Wireshark at a click of a button to inspect the data in more detail, the traffic is SSL and thus cannot be inspected in this case.



What we can do is calculate the total bytes sent and received (Approx. 7.7MB), this traffic could be related to the threat actor in some way, so should be deemed an IOC of low confidence.

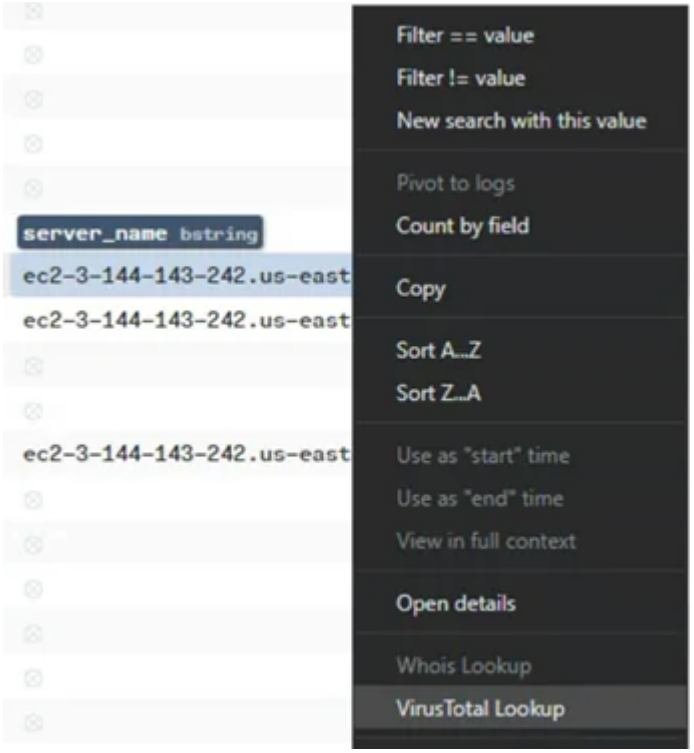
Cobalt Strike traffic

We re-visited the high amount of connections to xenilik[.]com (23[.]106[.]215[.]123), when cross-referencing the JA3 hash, this hash is a high confidence IOC for cobalt strike.



Enrichment

One final feature of Brim we leveraged, was the ability to enrich the data with VirusTotal by right clicking elements like IP Addresses and domain names to perform a VT lookup. One key takeaway was that the detection rate was very low, with no key context around what the entities were related to i.e. Cobalt Strike or C2 or malware etc.



Source: https://www.aspirets.com/blog/bumblebee-malware-loader-threat-analysis/