Scouring the DNS for Traces of Bumblebee SEO Poisoning

Table of Contents

Executive Report

Google ad or search engine optimization (SEO) poisoning has long been a favored threat actor tactic to spread malware. A recent Secureworks study of Bumblebee, which comes in the guise of a software installer, proved that once again.

Bumblebee could potentially affect millions of users given that it takes advantage of some of today's most widely used enterprise applications—Zoom, Cisco AnyConnect, ChatGPT, and Citrix Workspace.

The Secureworks report published 31 indicators of compromise (IoCs)—two domains and 29 IP addresses—which the WhoisXML API research team expanded to identify as many potential Bumblebee attack vectors as possible. Our foray into the DNS revealed:

- 18 domains that shared some of the IoCs' IP hosts, two of which turned out to be malicious
- 1,955 domains that contained the string ***appcisco.*** akin to one of the domains identified as an IoC and the strings ***cisco.***, ***chatgpt.***, ***zoom.***, and ***citrix.*** that represented the names of the software the threat actors abused, three of which turned out to be malware hosts

Behind the IoCs

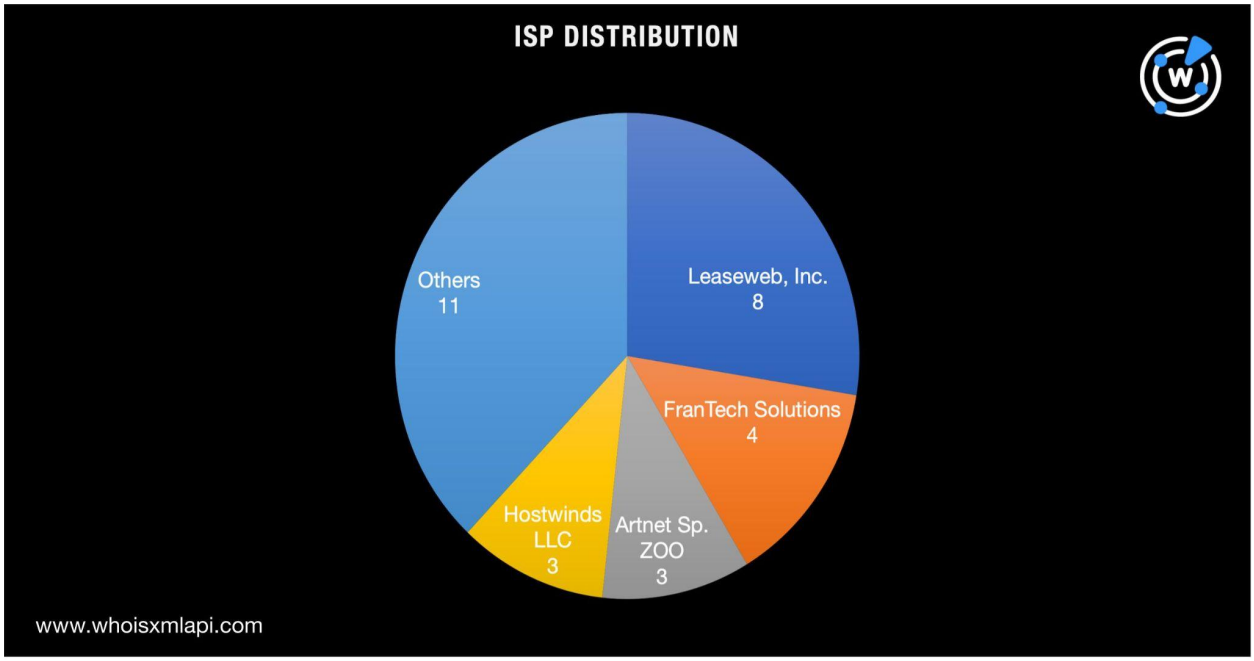
The Secureworks study listed these Bumblebee IoCs.

DOMAINS	IP ADDRESSES
• appcisco[.]com • baveyek[.]com	• 173[.]44[.]141[.]131 • 23[.]82[.]140[.]131

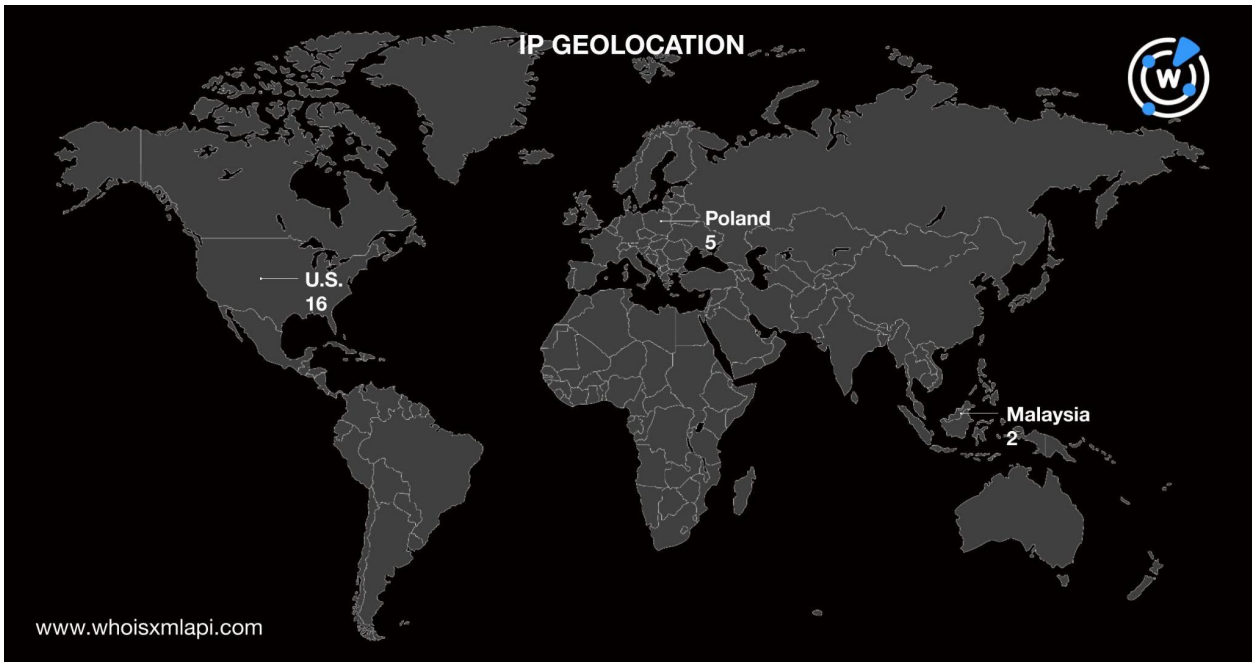
	• 172[.]93[.]193[.]3 • 23[.]81[.]246[.]22 • 95[.]168[.]191[.]134 • 104[.]168[.]175[.]78 • 172[.]93[.]193[.]46 • 157[.]254[.]194[.]104 • 37[.]28[.]157[.]29 • 23[.]106[.]124[.]23 • 194[.]135[.]33[.]182 • 54[.]38[.]139[.]94 • 192[.]119[.]65[.]175 • 107[.]189[.]8[.]58 • 205[.]185[.]114[.]241 • 104[.]168[.]171[.]159 • 103[.]144[.]139[.]159 • 91[.]206[.]178[.]204 • 198[.]98[.]58[.]184 • 172[.]241[.]27[.]120 • 23[.]106[.]223[.]197 • 23[.]108[.]57[.]83 • 54[.]37[.]131[.]232 • 23[.]82[.]128[.]11 • 160[.]20[.]147[.]91 • 103[.]175[.]16[.]10 • 45[.]61[.]187[.]225 • 91[.]206[.]178[.]68 • 193[.]109[.]120[.]252

WHOIS lookups for the two domains identified as IoCs showed that both were purchased from Namecheap, Inc. in February 2023. Both domain names' registrants indicated Iceland as their country.

A bulk IP geolocation lookup, meanwhile, for the 29 IP addresses identified as IoCs showed they were managed by 10 ISPs led by Leaseweb, Inc., which accounted for eight of the hosts. FranTech Solutions followed with a 14% share. Completing the top 3 ISPs were Artnet Sp. ZOO and Hostwinds LLC with a 10% share each.



The IP geolocation searches also revealed the hosts were spread across nine countries led by the U.S., which accounted for 16 IP addresses. Completing the top 3 geolocations were Poland and Malaysia with five and two IP addresses each.



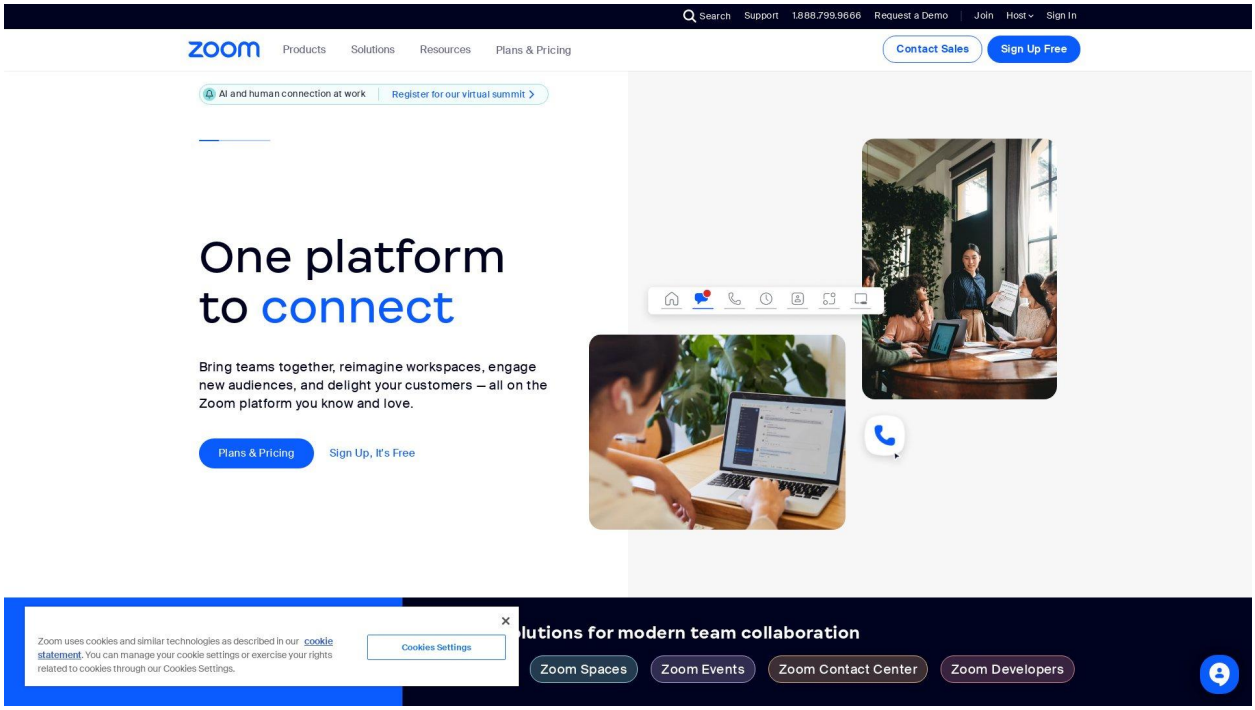
Interestingly, while the domain registrants indicated Iceland as their country, none of the IP addresses identified as IoCs were geolocated in the nation.

Bumblebee DNS Connections

Pivoting off the IP addresses identified as IoCs, reverse IP lookups revealed that 18 of hosts didn't have active IP resolutions while the remaining 11 were dedicated. They also uncovered 18 domains hosted on the dedicated IP addresses, two of which turned out to be malicious. One of the malicious web properties—newsoftup[.]com—remained accessible though the page required further configuration.

Screenshot of newsoftup[.]com

The in-depth Bumblebee analysis stated that the threat actors misused the names of four software providers in their campaigns—Cisco, ChatGPT, Zoom, and Citrix. To identify other possible Bumblebee attack vectors, we looked for domains containing the strings ***cisco.***, ***chatgpt.***, ***zoom.***, and ***citrix.*** via Domains & Subdomains Discovery. Our searches led to the discovery of 1,955 domains. Three of them turned out to be malware hosts. Appcisco[.]us was unreachable as of this writing, zoom[.]cyou was parked, and zoom[.]com[.]de continued to host live content.

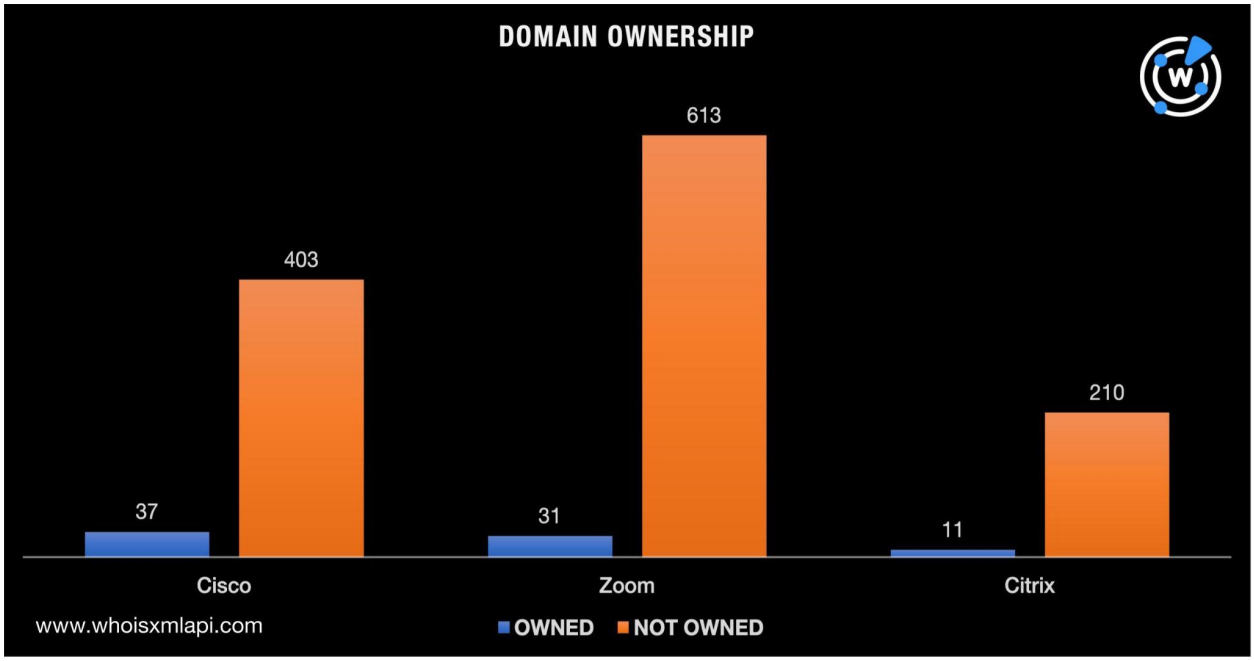


Screenshot of zoom[.]com[.]de

While zoom[.]com[.]de looks exactly like the official Zoom website zoom[.]com, it couldn't be publicly attributed to the company based on its WHOIS record details.

As a final step, we sought to determine how many of the 1,900+ brand-containing domains were owned by the companies whose names appeared as strings in them. Note that the openai[.]com (ChatGPT's owner) domain's WHOIS record has been redacted so we excluded the ***chatgpt.***-containing domains from our analysis. To attribute ownership, we used the registrant email address for the ***cisco.***- and ***citrix.***-containing domains and the registrant organization for the ***zoom.***-containing domain names.

Our deep dive revealed that only 6% of the total brand-containing domain volume could be publicly attributed to Cisco, Zoom, and Citrix. In particular, Cisco only owned 37 of the 1,305 domains. Zoom and Citrix, meanwhile, only controlled 31 and 11 of the domain names, respectively.



—

Not all the websites that sport a company's logo and are hosted on look-alike domains are worth trusting, as in those the Bumblebee malware operators used, if you go beyond the surface. A simple WHOIS record detail comparison for zoom[.]com and zoom[.]com[.]de, for instance, revealed that the latter is likely cybersquatting. The same could be true for the other 1,200+ domains containing the Cisco, Zoom, and Citrix brand names that couldn't be publicly attributed to the companies if further DNS scrutiny is applied to them.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Domains That Shared the IoCs' IP Hosts

- 157-254-194-104[.]plesk[.]page
- barnco-agricola[.]com
- d157029[.]artnet[.]gda[.]pl
- festive-cannon[.]157-254-194-104[.]plesk[.]page
- fs3vjo97f[.]dubbed1686[.]cf
- hollistechhelp[.]com
- hwsrv-1039376[.]hostwindsdns[.]com
- hwsrv-1040739[.]hostwindsdns[.]com
- hwsrv-1041841[.]hostwindsdns[.]com

- jovial-blackwell[.]157-254-194-104[.]plesk[.]page

Sample Malicious IP-Connected Domain

- newsoftup[.]com

Sample Domains That Contained the Strings *appcisco.*, *cisco.*, *chatgpt.*, *zoom.*, and *citrix.*

- appcisco[.]us
- cisco[.]xn--io0a7i
- cisco[.]nyc
- cisco[.]cc
- cisco[.]xn--vuq861b
- cisco[.]space
- cisco[.]org[.]ru
- cisco[.]cymru
- cisco[.]pk
- cisco[.]ac[.]mw
- cisco[.]al
- cisco[.]off[.]ai
- cisco[.]net[.]pl
- cisco[.]gy
- cisco[.]lol
- cisco[.]org[.]ki
- cisco[.]co[.]tt
- cisco[.]security
- cisco[.]bar
- cisco[.]pics
- cisco[.]re
- cisco[.]pub
- cisco[.]moscow
- cisco[.]asia
- cisco[.]promo
- chatgpt[.]market
- chatgpt[.]media
- chatgpt[.]builders
- chatgpt[.]software
- chatgpt[.]pk
- chatgpt[.]loans
- chatgpt[.]cricket
- chatgpt[.]sexy
- chatgpt[.]org[.]uk
- chatgpt[.]diamonds
- chatgpt[.]clothing
- chatgpt[.]pro[.]vn
- chatgpt[.]vg
- chatgpt[.]wf
- chatgpt[.]moscow
- chatgpt[.]mg
- chatgpt[.]me[.]uk
- chatgpt[.]republican
- chatgpt[.]reviews
- chatgpt[.]soy
- chatgpt[.]hockey
- chatgpt[.]maison
- xn--chtgpt-jua[.]se
- chatgpt[.]jp
- chatgpt[.]zone
- zoom[.]football
- zoom[.]co[.]pl
- zoom[.]associates
- zoom[.]pictures
- zoom[.]mortgage
- zoom[.]czest[.]pl
- zoom[.]xn--5tzm5g
- zoom[.]sexy
- zoom[.]date
- zoom[.]moscow
- zoom[.]lighting
- zoom[.]realty

- zoom[.]salon
- zoom[.]accountants
- zoom[.]school
- zoom[.]review
- zoom[.]org[.]cn
- zoom[.]net
- zoom[.]co[.]gg
- zoom[.]yoga
- xn--oom-5ez[.]com
- xn--zom-1lz[.]com
- zoom[.]black
- zoom[.]industries
- zoom[.]photo
- citrix[.]wang
- citrix[.]ms
- citrix[.]pub
- citrix[.]ninja
- citrix[.]engineering
- citrix[.]nyc
- citrix[.]world
- citrix[.]cx
- citrix[.]agency
- xn--citr-oza8916b[.]com
- citrix[.]work
- citrix[.]fr
- citrix[.]se
- citrix[.]ae
- citrix[.]today
- citrix[.]llc
- citrix[.]si
- citrix[.]jobs
- citrix[.]io
- citrix[.]info
- citrix[.]ovh
- citrix[.]surf
- citrix[.]partners
- citrix[.]me
- citrix[.]tokyo

Sample Malicious String-Connected Domains

- appcisco[.]us
- zoom[.]com[.]de