WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

MOVEit Exploit-CLOP Ransomware Threat Vector Identification Aided by DNS Intelligence

Table of Contents

Executive Report

The beginning of the month of June, according to CleanINTERNET, marked the emergence of several zero-day attacks targeting vulnerable MOVEit servers to exfiltrate confidential data. MOVEit Transfer is a managed file transfer software that supports file and data exchange. The MOVEit vulnerability gives attackers access to a database and possibly infer information about its structure and content.

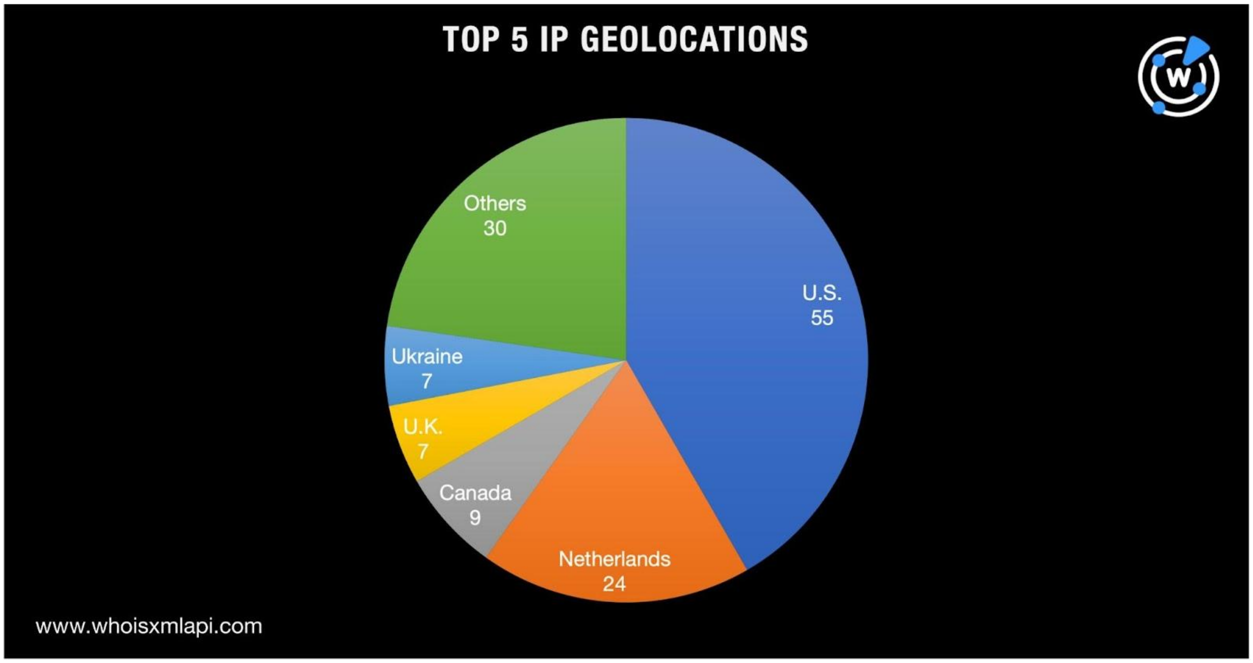
Since then, researchers from various security companies published reports tying the MOVEit vulnerability's exploitation to CLOP ransomware attacks. The WhoisXML API research team obtained a list of 139 indicators of compromise (IoCs) that was then subjected to further analysis using our DNS tools.

Our deep dive into the MOVEit vulnerability-CLOP ransomware IoCs found:

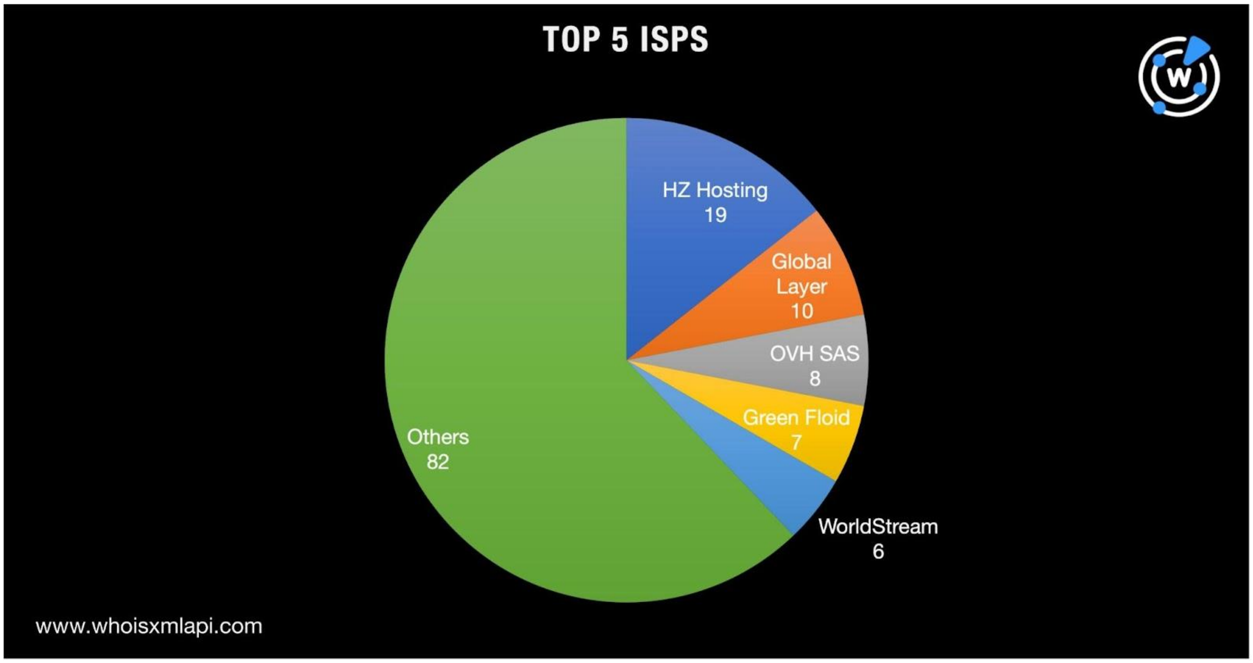
- 34 domains resolving to the dedicated IP addresses identified as IoCs, four of which have been categorized as malicious by our malware check tool
- 10 unique IP addresses that played host to some of the domains identified as IoCs, five of which were dedicated and four were classified as malicious by our malware check tool
- 6,627 domains containing the string ***zoom*** akin to two domains identified as IoCs, 56 of which were tagged malware hosts by our malware check tool

Zooming in on the IP Addresses Identified as IoCs

In-depth reports on MOVEit-enabled CLOP ransomware attacks identified 132 IP addresses as IoCs. A bulk IP geolocation lookup for them showed that they were spread across 16 countries led by the U.S., which accounted for 55 of the IP addresses, followed by the Netherlands (24 IP addresses), Canada (nine IP addresses), and the U.K. and Ukraine (seven IP addresses each).

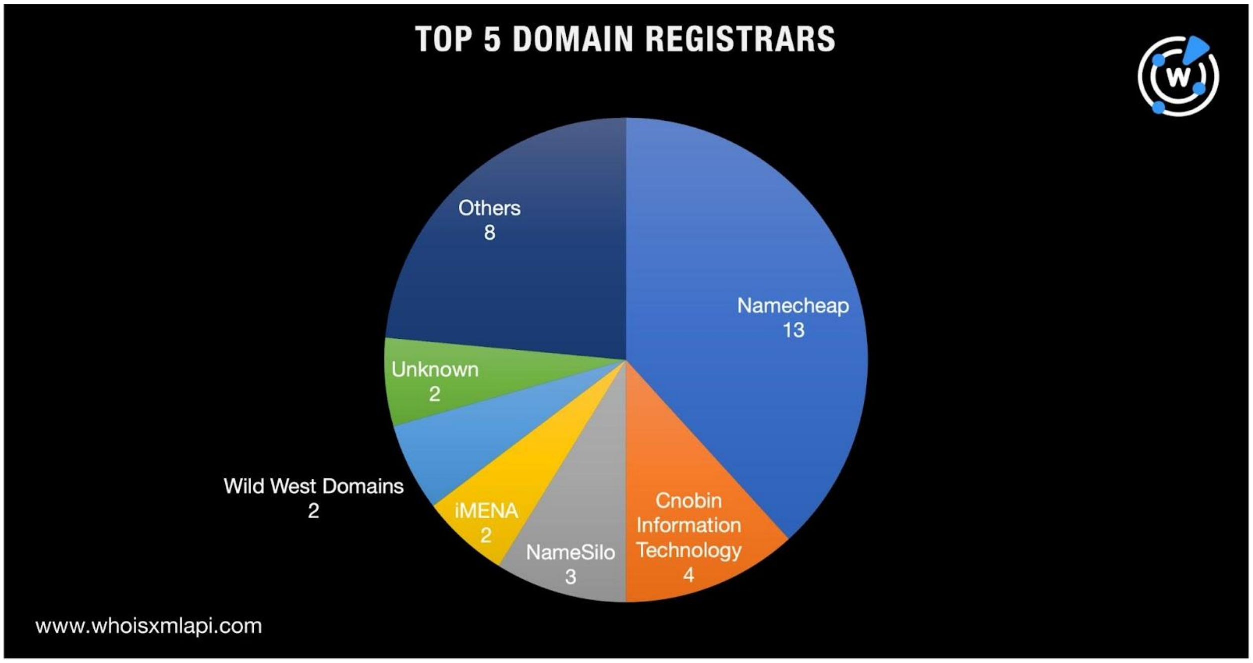


The IoCs were also distributed among 50 ISPs led by HZ Hosting, which accounted for 19 of the IP addresses. Global Layer (10 IP addresses), OVH SAS (eight IP addresses), Green Floid (seven IP addresses), and WorldStream (six IP addresses) rounded out the top 5 ISPs.



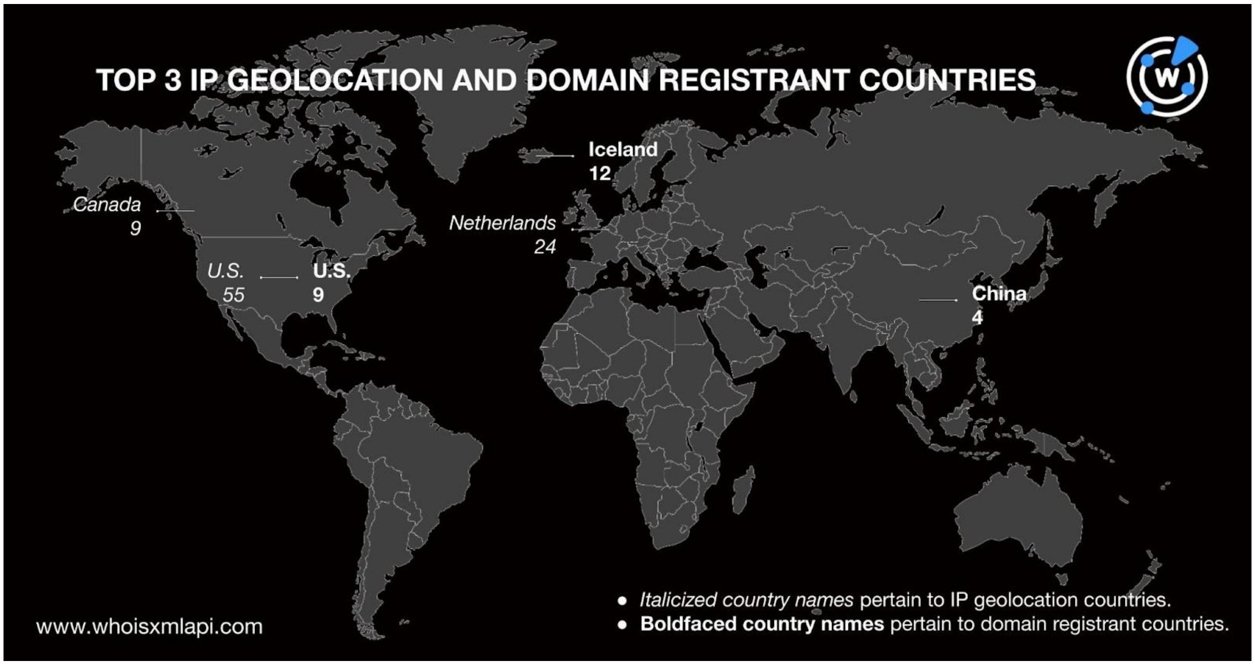
Reverse IP lookups performed on the IoCs revealed that 17 of the 132 were dedicated IP addresses. Altogether, they hosted 34 domains, four of which were dubbed as malicious by a bulk malware check tool.

A bulk WHOIS lookup for the IP-connected domains showed that those with publicly available registrar information were spread across 14 registrars led by Namecheap, which accounted for 13 of the artifacts. Cnobin Information Technology (four domains), NameSilo (three domains), and iMENA and Wild West Domains (two domains each) completed the top 5.



One of the artifacts—tube-plant[.]com—had a publicly viewable personal registrant email address that investigators might wish to further pursue.

The artifacts with publicly available registrant countries cited Iceland as the top registrant country. The nation accounted for 12 of the IP-connected domains but didn't appear as an IP geolocation country.

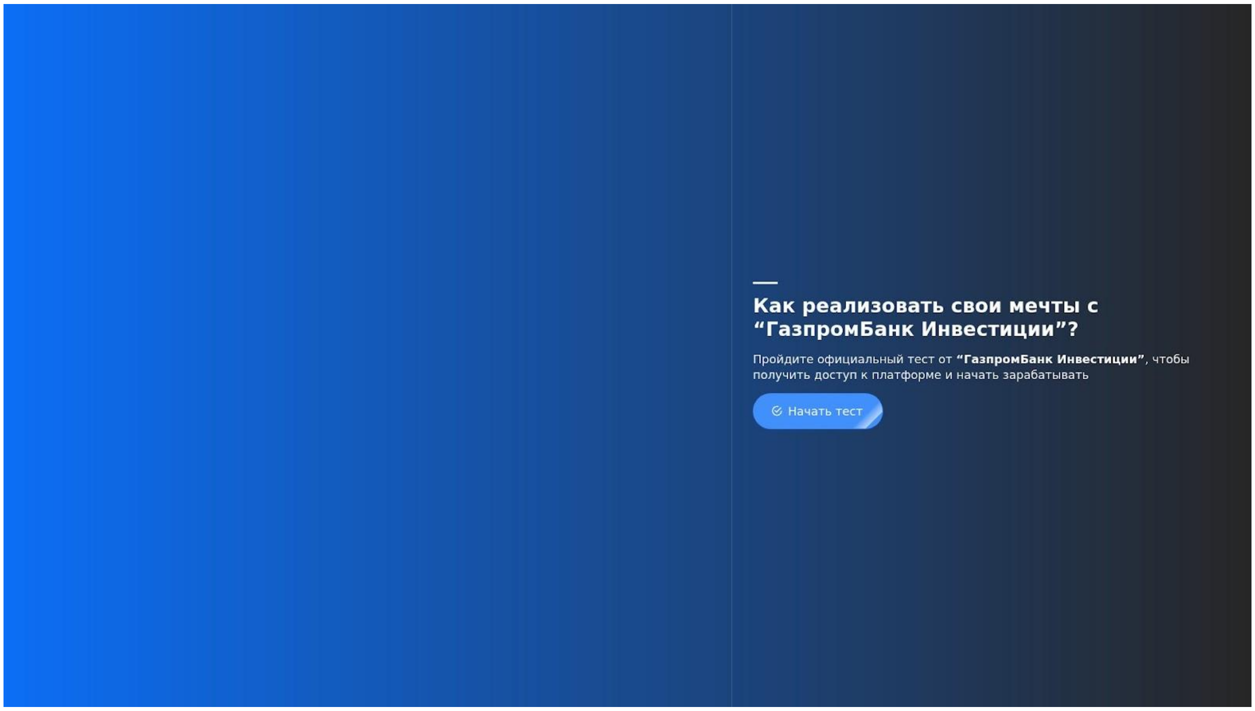

TOP 3 IP GEOLOCATION AND DOMAIN REGISTRANT COUNTRIES
Iceland
12
Canada
9
Netherlands
24
U.S.
55
U.S.
9
China
4
● *Italicized country names* pertain to IP geolocation countries.
● **Boldfaced country names** pertain to domain registrant countries.
www.whoisxmlapi.com

A Closer Look at the Domains Identified as IoCs

Earlier reports about MOVEit-enabled CLOP ransomware attacks also identified seven domains as IoCs. Two of them contained the string ***zoom***—connectzoomdownload[.]com and zoom[.]voyage—but their current WHOIS records didn't bear any similarity with that of zoom[.]com. Apart from not indicating their registrant organization, they were also under NameSilo management unlike zoom[.]com that indicated Zoom Video Communications, Inc. as registrant organization and MarkMonitor, Inc. as registrar.

We looked for other ***zoom***-containing domains created since 1 January 2023 since both IoCs were created in December 2022 to find possibly related artifacts. We found 6,627 such web properties although none of the 6,609 with retrievable WHOIS records could be publicly attributed to Zoom based on the organization their registrants identified.

A bulk malware check for the string-connected domains also revealed that 56 have already been categorized as malware hosts. Of these, only one continued to host live content related to one of the biggest Russian banks and its investment platform. Despite its name, though, it doesn't seem to have anything to do with the videoconferencing platform or viewing parts of the planet.

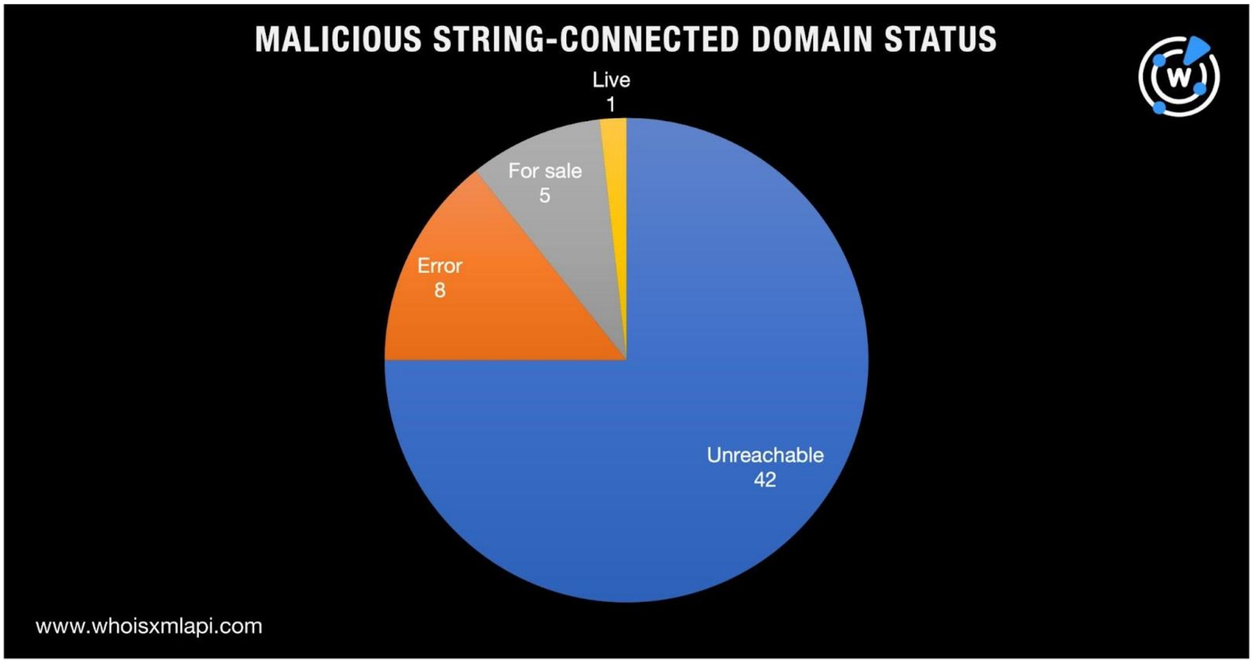


Как реализовать свои мечты с “ГазпромБанк Инвестиции”?

Пройдите официальный тест от **“ГазпромБанк Инвестиции”**, чтобы получить доступ к платформе и начать зарабатывать

Screenshot of zoomplanet[.]online

The rest of the malicious string-connected domains were either unreachable, for sale, or led to error pages.



A bulk WHOIS lookup for the IoCs likewise showed that Cnobin Information Technology was their top registrar, accounting for four domains. In addition, six of them were created in 2022 while the remaining one was much older, created in 1996. Finally, four domain registrants indicated China as their country, followed by the U.S. (two domains) and Canada (one domain).

Next, the IoCs resolved to 10 unique IP addresses, four of which were already part of the published IoC lists. Two of the six remaining IP resolutions were dedicated addresses that played host to five domains. Four of them were identified as malicious based on a bulk malware check. While none of them continued to host live content, it's interesting to note the appearance of the string ***microsoft*** in two of them.

WHOIS lookups for the two malicious IP-connected domains—microsoftclouddownload[.]com and mlcrosoft[.]life—showed they weren't publicly attributable to the company. They were likely used in malicious campaigns targeting Microsoft product users. Note the presence of the string ***download*** in one of them as well akin to the domain connectzoomdownload[.]com that was identified as an IoC.

—

Our foray into the DNS for traces of MOVEit-connected CLOP ransomware attacks led to the discovery of more than 6,600 potentially connected web properties, domains and IP addresses alike.

Our deeper dive also uncovered 65 malicious connected artifacts that organizations can include in their blocklists to enable better cybersecurity.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts and IoCs

IoCs Obtained from AlienVault OTX

IP Addresses

- 84[.]234[.]96[.]104
- 209[.]222[.]103[.]170
- 198[.]27[.]75[.]110
- 96[.]44[.]181[.]131
- 96[.]10[.]22[.]178
- 92[.]118[.]36[.]249
- 92[.]118[.]36[.]213
- 92[.]118[.]36[.]210
- 91[.]223[.]227[.]140
- 91[.]222[.]174[.]68
- 88[.]214[.]27[.]101
- 88[.]214[.]27[.]100
- 82[.]117[.]252[.]97
- 82[.]117[.]252[.]142
- 82[.]117[.]252[.]141
- 81[.]56[.]49[.]148
- 79[.]141[.]173[.]94
- 79[.]141[.]161[.]82
- 76[.]117[.]196[.]3
- 74[.]218[.]67[.]242
- 68[.]156[.]159[.]10
- 54[.]39[.]133[.]41
- 54[.]184[.]187[.]134
- 50[.]7[.]118[.]90
- 5[.]34[.]178[.]31
- 5[.]34[.]178[.]30
- 5[.]34[.]178[.]28
- 5[.]34[.]178[.]27
- 5[.]188[.]206[.]76
- 5[.]149[.]252[.]51
- 5[.]149[.]250[.]90
- 45[.]182[.]189[.]229
- 45[.]182[.]189[.]228
- 45[.]182[.]189[.]200
- 44[.]206[.]3[.]111
- 3[.]101[.]53[.]11
- 23[.]237[.]56[.]234
- 23[.]237[.]114[.]154
- 216[.]144[.]248[.]20
- 213[.]121[.]182[.]84
- 209[.]222[.]98[.]25
- 208[.]115[.]199[.]25
- 20[.]47[.]120[.]195
- 198[.]245[.]13[.]4
- 198[.]199[.]74[.]207
- 198[.]137[.]247[.]10
- 195[.]38[.]8[.]241
- 185[.]81[.]113[.]156
- 185[.]80[.]52[.]230
- 185[.]33[.]87[.]126
- 185[.]33[.]86[.]225
- 185[.]174[.]100[.]17
- 185[.]117[.]88[.]2
- 185[.]104[.]194[.]134
- 173[.]254[.]236[.]131
- 172[.]71[.]134[.]76
- 166[.]70[.]47[.]90
- 162[.]158[.]129[.]79
- 15[.]235[.]83[.]73
- 15[.]235[.]13[.]184
- 148[.]113[.]159[.]213
- 148[.]113[.]159[.]146
- 143[.]31[.]133[.]99
- 142[.]44[.]212[.]178
- 141[.]101[.]68[.]166
- 141[.]101[.]68[.]154
- 107[.]181[.]161[.]207
- 104[.]200[.]72[.]149

- 100[.]21[.]161[.]34
- 93[.]190[.]142[.]131
- 91[.]229[.]76[.]187
- 91[.]222[.]174[.]95
- 91[.]202[.]4[.]76
- 89[.]39[.]105[.]108
- 89[.]39[.]104[.]118
- 84[.]234[.]96[.]31
- 79[.]141[.]160[.]83
- 79[.]141[.]160[.]78
- 66[.]85[.]26[.]248
- 66[.]85[.]26[.]234
- 66[.]85[.]26[.]215
- 63[.]143[.]42[.]242
- 62[.]182[.]85[.]234
- 62[.]182[.]82[.]19
- 62[.]112[.]11[.]57
- 5[.]34[.]180[.]48
- 5[.]34[.]180[.]205
- 5[.]252[.]25[.]88
- 5[.]252[.]23[.]116
- 5[.]188[.]87[.]27
- 5[.]188[.]87[.]226
- 5[.]188[.]87[.]194
- 5[.]188[.]86[.]250
- 5[.]188[.]86[.]114
- 5[.]149[.]250[.]92
- 5[.]149[.]250[.]74
- 5[.]149[.]248[.]68
- 45[.]56[.]165[.]248
- 45[.]227[.]253[.]82
- 45[.]227[.]253[.]6
- 45[.]227[.]253[.]50
- 45[.]227[.]253[.]147
- 45[.]227[.]253[.]133
- 209[.]97[.]137[.]33
- 209[.]127[.]4[.]22
- 209[.]127[.]116[.]122
- 206[.]221[.]182[.]106
- 198[.]12[.]76[.]214
- 194[.]33[.]40[.]104
- 194[.]33[.]40[.]103
- 193[.]169[.]245[.]79
- 188[.]241[.]58[.]244
- 185[.]185[.]50[.]172
- 185[.]183[.]32[.]122
- 185[.]181[.]229[.]73
- 185[.]181[.]229[.]240
- 185[.]174[.]100[.]250
- 185[.]174[.]100[.]215
- 185[.]162[.]128[.]75
- 185[.]117[.]88[.]17
- 185[.]104[.]194[.]40
- 185[.]104[.]194[.]24
- 185[.]104[.]194[.]156
- 179[.]60[.]150[.]143
- 162[.]244[.]35[.]6
- 162[.]244[.]34[.]26
- 148[.]113[.]152[.]144
- 146[.]0[.]77[.]183
- 146[.]0[.]77[.]155
- 146[.]0[.]77[.]141
- 138[.]197[.]152[.]201
- 104[.]194[.]222[.]107

Domains

- zoom[.]voyage
- qweastradoc[.]com
- jirostrogud[.]com
- huntress[.]com
- hiperfdhaus[.]com
- guerdofest[.]com
- connectzoomdownload[.]com

Sample Domains Hosted on the IP Addresses Identified as IoCs

- 097[.]kh[.]ua
- 209-127-116-122[.]plesk[.]page
- 93-190-142-131[.]hosted-by-worldstream[.]net
- canismajor[.]site
- canisminor[.]life
- checkdrvms[.]com
- ciu1x8fy[.]ibxos[.]it
- cnetse[.]com
- cobaltrunner[.]net
- connectfillterdns[.]com
- crackpdud[.]pro
- d2[.]myabandonware[.]com
- digiable[.]net
- fornax[.]life
- fuanshizmo[.]com
- ghustaderzk[.]com
- greenline[.]krd
- ideogencoo[.]vip

Sample Malicious Domains Hosted on the IP Addresses Identified as IoCs

- cnetse[.]com
- digiable[.]net

Sample Domains Containing the String *zoom* Akin to Two Domains Identified as IoCs

- zoomzoom[.]ga
- zoomzoom[.]cc
- zoomzoomz[.]ca
- zoomzoom[.]sbs
- zoomzoom[.]cyou
- zoomzoomllc[.]vg
- zoomzoom[.]co[.]de
- zoomtozoom[.]net
- zoomzoomies[.]de
- zoomzoom[.]click
- zoomzoom850[.]ru
- zoomzoomboom[.]ca
- zoomzoom[.]dating
- zoomzoombkk[.]com
- zoomzoomlab[.]com
- zoomzoommed[.]com
- zoomzoomads[.]com
- zoomifyzoom[.]com
- zoomzoomzurn[.]com
- zoomzoomwifi[.]com
- marrszoomzoom[.]com
- zoomzoomcars[.]shop
- zoombestzoom[.]shop
- airzoomzoom[.]click
- xn--oom-22a[.]de
- zoom[.]ac
- zoomzoomcaleb[.]com
- zoomzoomshoes[.]com
- zoomzoomdenton[.]com
- zoomzoomevents[.]com
- us04webzoomzoom[.]us
- nzoom[.]nl
- zooms[.]vg
- azoom[.]it
- zoomg[.]me
- zoomzoompets[.]com[.]br

- zoomm[.]ca
- xn--zm-8jaa[.]com
- zoomzoomcostume[.]com
- zoom5[.]us
- zoom1[.]vn
- zoomi[.]sk
- zoom[.]zip
- szoom[.]vg
- zooma[.]my
- zoomg[.]in
- ezoom[.]ga
- zoome[.]ga
- zoomg[.]de
- zoomc[.]ml
- szoom[.]ph
- zoomx[.]nl
- zooms[.]mx
- zoom3[.]cn
- zoomg[.]ga
- zoomc[.]ga
- zoomi[.]ch
- aculief-zoomzoom[.]com
- zoomer[.]ph
- zoom4d[.]in
- ipzoom[.]tv
- zoommc[.]ga
- kazoom[.]ch
- oazoom[.]uk
- zoomex[.]fr
- kkzoom[.]ru
- zoom47[.]tk
- zoomon[.]pl
- gazoom[.]me
- yjzoom[.]cn
- zoomag[.]kg
- zoomfr[.]vg
- izoom[.]fun
- zzoom[.]sbs
- ktzoom[.]xn--kprw13d
- zoomzl[.]cn
- zoomfs[.]vg
- vbzoom[.]vg
- edzoom[.]eu
- zoom47[.]ml
- zoome[.]mom
- zoomly[.]pl
- zoomit[.]ph
- zoomna[.]co
- zoom50[.]de
- zoom47[.]gq
- bizoom[.]ca
- mizoom[.]cn
- bgzoom[.]vg
- zooma5[.]ru
- bezoom[.]cn
- quzoom[.]de
- zoomat[.]us
- ezoom[.]app
- zoomzi[.]eu
- zoomik[.]ml
- zoomyx[.]co
- zoomat[.]eu
- x-zoom[.]us
- zoomie[.]ga

Sample Malicious Domains Containing the String *zoom* Akin to Two Domains Identified as IoCs

- zoomm[.]ca
- zoomad[.]us
- zoomupd[.]com
- myzoom[.]tech
- dzooms[.]site
- coudzoom[.]ru
- zoomify[.]pro
- zoomexhk[.]com

- zoom-docs[.]com
- legaczoom[.]com
- zoomchat[.]site
- quozoom[.]click
- zoomsender[.]in
- zoomexbit[.]com
- clientzoom[.]us
- zoomfile[.]tech
- zoom-conf[.]xyz
- zoom-meet[.]site
- zoomvideor[.]com
- zoomsetup[.]tech
- rulezoome[.]live
- zoompanel[.]site

Sample IP Addresses to Which the Domains Identified as IoCs Resolved

- 193[.]42[.]33[.]206
- 92[.]118[.]36[.]213
- 88[.]214[.]27[.]101
- 216[.]239[.]34[.]21
- 216[.]239[.]32[.]21
- 216[.]239[.]36[.]21

Sample Domains Hosted on the Dedicated IP Address Resolutions of the Domains Identified as IoCs

- fastgotosasslst[.]online
- microsoftclouddownload[.]com
- mlcrosoft[.]life

Sample Malicious Domains Hosted on the Dedicated IP Address Resolutions of the Domains Identified as IoCs

- microsoftclouddownload[.]com
- mlcrosoft[.]life