heige

141 Followers About

ZoomEye Behavior Mapping For Office Word 0day (CVE-2021–40444) Original Attacker

heige 1 day ago · 11 min read

Author: Heige (a.k.a Superhei) of KnownSec 404 Team https://twitter.com/80vul
09/12/2021

[Note: The ZoomEye search data in the article is based on the results of the query on September 11, and the target data has been overwritten and updated]

Before starting the article, please read the following articles to facilitate understanding of related theories:

“Behavior Mapping” in Cyberspace https://80vul.medium.com/behavior-mapping-in-cyberspace-one-net-cleans-apt-and-botnet-c2s-ed49a9b7d426
One ZoomEye Query Cleans BazarLoader C2s https://80vul.medium.com/one-zoomeye-query-cleans-bazarloader-c2s-4b49a71ec10d

For related information about CVE-2021–40444, you can refer to the security bulletin issued by Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444 Our purpose is to carry out the survey and mapping of the organization that used this 0day to attack in the first place, so we can start with the information related to the attacker’s IOCs at the time. We noticed that Trend Micro security researchers have released relevant information:

https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day--

cve-2021-40444--hits-windows--tr.html

From their article, I saw the C2 server used by the attacker at the time:

> *hxxps://joxinu[.]com*
> *hxxps://dodefoh[.]com*
> *hxxp://pawevi[.]com/e32c8df2cf6b7a16/specify.html*

Let's search with ZoomEye: https://www.zoomeye.org/searchResult?q=dodefoh.com%20joxinu.com%20pawevi.com Fortunately, I found the corresponding data results. The relevant information is extracted as follows:

> *IP:45.147.229.242 Germany, Frankfurt, Operator:combahton.net*
> *ZoomEye Update time:2021–09–06 22:01*
> *CobaltStrike Beacon:*
> *C2 Server: dodefoh.com,/hr.html,joxinu.com,/ml.html*
> *C2 Server: dodefoh.com,/ml.html,joxinu.com,/hr.html*
> *Spawnto_x86: %windir%\\syswow64\\rundll32.exe*
> *Certificate:*
> *Subject: CN=dodefoh.com*
> *Issuer: C=GB,ST=Greater Manchester,UnknownOID=2.5.4.7,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA*
>
> *IP:104.194.10.21 United States, Piscataway, Operator:versaweb.com*
> *ZoomEye Update time:2021–07–14 01:40*
> *CobaltStrike Beacon:*
> *C2 Server: dodefoh.com,/tab_shop_active,joxinu.com,/tab_shop_active*
> *C2 Server: dodefoh.com,/tab_shop_active,joxinu.com,/ce*
> *Spawnto_x86: %windir%\\syswow64\\rundll32.exe*
> *Certificate:*
> *Subject: CN=zikived.com*
> *Issuer: C=GB,ST=Greater Manchester,UnknownOID=2.5.4.7,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA*
>
> *IP:45.153.240.220 Germany, Frankfurt Operator:combahton.net*
> *ZoomEye Update time:2021–08–29 15:25*
> *Banner:Comply with Apache default page content*
> *Certificate:*

> *Subject: CN=pawevi.com*
> *Issuer: C=US,O=Let's Encrypt,CN=R3*

From the above information, we can determine:

1, 45.147.229.242 and 104.194.10.21 are CobaltStrike servers
2. pawevi.com bound to 45.153.240.220 is an Apache WEB service. Judging from the IOCs provided by Trends, it should be a remote page loaded with the payload.

It can be seen that the banner of CobaltStrike has been modified and configured. According to our "**behavior mapping**" concept, these unique modified information are the "behavior characteristics" we want to find.

45.147.229.242

> *HTTP/1.1 404 Not Found*
> *Date: Mon, 6 Sep 2021 14:01:21 GMT*
> *Server: Microsoft-IIS/8.5*
> *Content-Type: text/plain*
> *Cache-Control: max-age=1*
> *Connection: keep-alive*
> *X-Powered-By: ASP.NET*
> *Content-Length: 0*
>
> *Certificate*:
> *Subject: CN=dodefoh.com*
> *Issuer: C=GB,ST=Greater Manchester,UnknownOID=2.5.4.7,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA*

104.194.10.21

> *HTTP/1.1 404 Not Found*
> *Cache-Control: max-age=1*
> *Connection: keep-alive*
> *X-Powered-By: ASP.NET*
> *Content-Length: 0*
> *Date: Tue, 13 Jul 2021 17:40:00 GMT*
> *Server: Microsoft-IIS/8.5*

> *Content-Type: text/plain*
>
> *Certificate:*
> *Subject: CN=zikived.com*
> *Issuer: C=GB,ST=Greater Manchester,UnknownOID=2.5.4.7,O=Sectigo Limited,CN=Sectigo RSA Domain Validation Secure Server CA*

Combining the banner and certificate content through some test analysis, finally determined a relatively accurate ZoomEye Dork:

> *“HTTP/1.1 404 Not Found” +”Connection: keep-alive” +”X-Powered-By: ASP.NET” +”Content-Length: 0" +”Server: Microsoft-IIS” +”Content-Type: text/plain” +”ST=Greater Manchester” -kong*

[ps:After our research, the behavior used by this attacker is probably disguised as Kong API Gateway (https://github.com/Kong/kong), so this is why there is a condition of “-kong”]

https://www.zoomeye.org/searchResult?q=%22HTTP%2F1.1%20%20404%20Not%20Found%22%20%2B%22Connection%3A%20keep-alive%22%20%2B%22X-Powered-By%3A%20ASP.NET%22%20%2B%22Content-Length%3A%200%22%20%2B%22Server%3A%20Microsoft-IIS%22%20%2B%22Content-Type%3A%20text%2Fplain%22%20%2B%22ST%3DGreater%20Manchester%22%20-kong

A total of 319 results, mainly distributed in the United States, a few in Germany, and 1 in the Netherlands.

The domain name statistics extracted from the Subject in the certificate:

> *badiwaw.com -> 2*
> *barovur.com -> 2*
> *bemesak.com -> 1*
> *beyezil.com -> 3*
> *boatver.com -> 2*
> *bucudiy.com -> 2*

buloxo.com -> 1
bulozeb.com -> 2
buremih.com -> 2
cajeti.com -> 1
capuxix.com -> 2
cegabox.com -> 1
cohusok.com -> 1
comecal.com -> 2
comhook.com -> 1
cubigif.com -> 2
cujicir.com -> 1
cuyuzah.com -> 2
dahefu.com -> 1
damacat.com -> 2
dapapev.com -> 1
davevud.com -> 1
derotin.com -> 2
digised.com -> 1
dihata.com -> 2
dimuyum.com -> 2
dirupun.com -> 2
docrule.com -> 1
dodefoh.com -> 1
etcle.com -> 2
fepaza.com -> 2
finegeo.com -> 2
flexzap.com -> 2
fonazax.com -> 3
formpi.com -> 1
ganobaz.com -> 1
gerepa.com -> 1
gihevu.com -> 1
gisopow.com -> 1
gohaduw.com -> 2
govahuk.com -> 2
gucunug.com -> 1

hacoyay.com -> 2
hakakor.com -> 2
hakenu.com -> 2
hayitad.com -> 2
hejalij.com -> 1
hesovaw.com -> 2
hexihan.com -> 2
hireja.com -> 2
hitark.com -> 1
hiwiko.com -> 1
hizewad.com -> 2
hoguyum.com -> 2
howiwo.com -> 2
hubnick.com -> 1
hubojo.com -> 2
hufamal.com -> 1
hulixo.com -> 2
innohigh.com -> 1
jafiha.com -> 2
jecubat.com -> 2
jegufe.com -> 1
jenupe.com -> 1
jikoxaz.com -> 1
jinoso.com -> 2
jumpbill.com -> 1
kayohe.com -> 2
kedorux.com -> 1
keholus.com -> 2
kelowuh.com -> 1
kidukes.com -> 2
kizuho.com -> 2
koviluk.com -> 1
koxiga.com -> 3
kuhohi.com -> 1
kuwoxic.com -> 1
kuyeguh.com -> 1

> *lajipil.com -> 2*
> *landhat.com -> 1*
> *laputo.com -> 2*
> *lessfox.com -> 1*
> *lifige.com -> 1*
> *lostzoom.com -> 1*
> *lozobo.com -> 2*
> *luherih.com -> 2*
> *maloxob.com -> 2*
> *masaxoc.com -> 2*
> *mebonux.com -> 1*
> *mevepu.com -> 2*
> *meyalax.com -> 1*
> *mgfee.com -> 2*
> *mibiwom.com -> 2*
> *moduwoj.com -> 1*
> *nacicaw.com -> 1*
> *nagiwo.com -> 1*
> *nemupim.com -> 3*
> *neoalt.com -> 2*
> *newiro.com -> 1*
> *newodi.com -> 1*
> *nokuje.com -> 2*
> *nupahe.com -> 2*
> *nuzeto.com -> 1*
> *nuzotud.com -> 1*
> *pathsale.com -> 1*
> *pavateg.com -> 2*
> *paxobuy.com -> 2*
> *payufe.com -> 3*
> *pazovet.com -> 2*
> *pecojap.com -> 2*
> *pigaji.com -> 1*
> *pilagop.com -> 2*
> *pipipub.com -> 2*
> *plushawk.com -> 1*

pobosa.com -> 2
pofafu.com -> 1
pofifa.com -> 2
prorean.com -> 2
quickomni.com -> 1
raniyev.com -> 3
rasokuc.com -> 2
refebi.com -> 2
rinutov.com -> 2
riolist.com -> 2
rivuha.com -> 2
ronedep.com -> 1
roxiya.com -> 2
rucajit.com -> 1
rurofo.com -> 1
rusoti.com -> 2
sazoya.com -> 4
scalewa.com -> 3
secost.com -> 1
sexefo.com -> 2
showero.com -> 2
showmeta.com -> 1
showmod.com -> 1
sidevot.com -> 2
slicemia.com -> 1
somerd.com -> 1
sopoyeh.com -> 2
stacknew.com -> 1
surfell.com -> 1
tafobi.com -> 1
talkeve.com -> 2
tamunar.com -> 2
tepabaf.com -> 2
tepiwo.com -> 1
tifiru.com -> 1
tonbits.com -> 1

tophal.com -> 2
tosayoj.com -> 1
touchroof.com -> 3
tryddr.com -> 1
trywd.com -> 2
tucosu.com -> 2
upfros.com -> 1
vigave.com -> 1
vinayik.com -> 1
vumedoj.com -> 2
waceko.com -> 2
wezaju.com -> 2
wideri.com -> 2
wigeco.com -> 1
wingsst.com -> 1
winohak.com -> 2
wiwege.com -> 2
wordten.com -> 1
wudepen.com -> 2
wukeyos.com -> 1
wuluxo.com -> 2
xagadi.com -> 1
xesoxaf.com -> 1
xisiyi.com -> 1
xivuli.com -> 2
xoxalab.com -> 1
xudivum.com -> 1
yazorac.com -> 2
yedawu.com -> 1
yeruje.com -> 1
yeyidun.com -> 2
yipeyic.com -> 1
yisimen.com -> 2
yiyuro.com -> 2
yodofed.com -> 2
yowofe.com -> 1

```
yuxicu.com -> 4
zedoxuf.com -> 2
zeheza.com -> 2
zikived.com -> 2
zikojut.com -> 2
zojuya.com -> 2
zokotej.com -> 2
zosohev.com -> 1
zovipiy.com -> 1
zulomuw.com -> 2
zuveye.com -> 2
```

The number distribution is relatively scattered, the letter composition of the domain name is very similar, and it feels like it was registered after being generated by the program.

JARM hash:

```
07d14d16d21d21d00042d41d00041de5fb3038104f457d92ba02e9311512c2 : 29
07d14d16d21d21d07c42d41d00041d58c7162162b6a603d3d90a2b76865b53 : 31
07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1 : 7
```

C2 Server list in CobaltStrike Beacon configuration information:

```
IP -> C2 Server -> total
23.106.215.137:443 -> laputo.com,/fr -> 1
23.19.227.178:443 -> gohaduw.com,/us.html -> 2
23.82.140.162:443 -> kidukes.com,/as -> 1
-> kidukes.com,/br -> 1
172.241.27.70:443 -> scalewa.com,/sm.html -> 40
23.106.223.184:443 -> hacoyay.com,/be -> 1
192.254.79.154:443 -> riolist.com,/av -> 32
23.108.57.230:443 -> pilagop.com,/an.html -> 1
192.198.89.242:443 -> zeheza.com,/ro -> 2
45.147.231.12:443 -> waceko.com,/FAQ.html -> 2
23.81.246.18:443 -> showero.com,/bn -> 9
-> showero.com,/lt -> 9
108.177.235.13:443 -> koviluk.com,/copyright.html -> 2
```

23.92.212.54:443 -> gerepa.com,/ce -> 2
209.222.98.225:443 -> showero.com,/bn -> 48
-> showero.com,/lt -> 49
104.243.33.123:443 -> pazovet.com,/dhl.js -> 2
108.62.141.5:443 -> touchroof.com,/modcp,focuslex.com,/modcp -> 32
172.93.105.162:443 -> mevepu.com,/modules.css -> 2
172.98.197.30:443 -> jinoso.com,/d_config -> 1
-> jinoso.com,/eso -> 1
23.108.57.186:443 -> kuyeguh.com,/ba.css -> 1
-> kuyeguh.com,/Content.css -> 1
23.106.160.95:443 -> zedoxuf.com,/links.html -> 2
103.195.100.2:443 -> yeyidun.com,/an -> 2
64.187.238.138:443 -> showmod.com,/an -> 8
-> showmod.com,/as -> 8
104.194.10.22:443 -> koxiga.com,/xmlconnect -> 2
209.222.101.221:443 -> ganobaz.com,/styles -> 1
-> ganobaz.com,/RELEASES -> 1
23.106.160.77:443 -> yawero.com,/skin.js,sazoya.com,/skin.js,192.198.86.130,/skin.js
-> 2
23.106.160.143:443 -> dihata.com,/search.js -> 2
172.241.27.22:443 -> pigaji.com,/favicon.css -> 1
192.254.65.202:443 -> hireja.com,/Content -> 2
23.106.160.231:443 -> hoguyum.com,/rw -> 1
-> hoguyum.com,/da -> 1
209.222.104.194:443 -> bulozeb.com,/ak.html -> 16
-> bulozeb.com,/mg.html -> 16
192.198.93.86:443 -> yisimen.com,/link -> 1
-> yisimen.com,/es -> 1
23.108.57.50:443 -> kelowuh.com,/FAQ.js -> 1
-> kelowuh.com,/remove.js -> 1
209.222.98.33:443 -> dapapev.com,/br.js -> 1
-> dapapev.com,/fam_cart.js -> 1
173.234.155.86:443 -> xivuli.com,/nd.js -> 2
108.62.12.114:443 -> gimazic.com,/ur,fipoleb.com,/ur -> 2
23.82.140.156:443 -> tifiru.com,/btn_bg -> 2
206.221.176.171:443 -> nokuje.com,/tab_home -> 2

206.221.184.130:443 -> gohaduw.com,/us.html -> 2
204.16.247.104:443 -> wezaju.com,/nv -> 1
-> wezaju.com,/skin -> 1
199.191.56.170:443 -> tucosu.com,/ur.html -> 21
-> tucosu.com,/Content.html -> 21
185.150.190.54:443 -> raniyev.com,/styles.html,movufa.com,/styles.html -> 1
-> raniyev.com,/RELEASE.html,movufa.com,/styles.html -> 1
23.106.160.136:443 -> riolist.com,/av -> 6
104.243.34.210:443 -> wudepen.com,/template -> 2
104.243.42.31:443 -> wideri.com,/language.css -> 6
-> wideri.com,/tab_shop.css -> 6
209.222.101.21:443 -> lajipil.com,/lt.js -> 2
23.106.215.71:443 -> wukeyos.com,/modules -> 2
45.58.112.202:443 -> tepiwo.com,/ur.html -> 1
-> tepiwo.com,/be.html -> 1
23.108.57.145:443 -> hakakor.com,/logo.js -> 1
89.163.140.101:443 -> waceko.com,/FAQ.html -> 2
199.127.61.223:443 -> pofafu.com,/avatars -> 2
23.106.215.151:443 -> raniyev.com,/styles.html,movufa.com,/styles.html -> 1
-> raniyev.com,/RELEASE.html,movufa.com,/styles.html -> 1
23.82.140.186:443 -> yazorac.com,/us.css -> 18
-> yazorac.com,/ms.css -> 18
209.222.98.75:443 -> wuluxo.com,/as.css -> 2
209.222.98.168:443 -> lozobo.com,/posting -> 2
172.93.201.14:443 -> nihahi.com,/modcp.css,yedawu.com,/modcp.css -> 9
-> nihahi.com,/html.css,yedawu.com,/modcp.css -> 9
199.127.61.167:443 -> winohak.com,/common -> 104
108.62.118.51:443 -> barovur.com,/eo.html -> 2
23.106.160.144:443 -> raniyev.com,/styles.html,movufa.com,/styles.html -> 1
-> raniyev.com,/RELEASE.html,movufa.com,/styles.html -> 1
108.177.235.115:443 -> buremih.com,/styles.html -> 2
172.93.105.2:443 -> hetamuf.com,/mobile-home.js,hepide.com,/link.js -> 1
-> hetamuf.com,/link.js,hepide.com,/link.js -> 1
103.195.101.98:443 -> jafiha.com,/FAQ -> 1
-> jafiha.com,/skin -> 1
23.106.160.141:443 -> hejalij.com,/panel.js -> 2

104.194.11.248:443 -> hakakor.com,/logo.js -> 2
104.238.205.32:443 -> luherih.com,/lt -> 2
199.191.57.246:443 -> rivuha.com,/styles.html -> 1
-> rivuha.com,/link.html -> 1
104.243.33.221:443 -> xoxalab.com,/d_config.js,bucejay.com,/d_config.js -> 1
-> xoxalab.com,/link.js,bucejay.com,/link.js -> 1
104.243.34.58:443 -> hakenu.com,/eso.js -> 1
-> hakenu.com,/en.js -> 1
192.111.146.22:443 -> dahefu.com,/Content.html -> 1
-> dahefu.com,/posting.html -> 1
23.106.215.64:443 -> rivuha.com,/styles.html -> 1
-> rivuha.com,/link.html -> 1
23.108.57.15:443 -> pipipub.com,/admin -> 2
23.82.140.227:443 -> scalewa.com,/sm.html -> 34
23.106.215.141:443 -> maloxob.com,/admin.css -> 2
104.238.222.148:443 -> mebonux.com,/modcp.html -> 2
104.171.117.58:443 -> barovur.com,/eo.html -> 2
108.62.118.63:443 -> dirupun.com,/RELEASE_NOTES -> 2
209.222.98.14:443 -> xivuli.com,/nd.js -> 2
108.62.141.174:443 -> keholus.com,/ee -> 1
-> keholus.com,/Content -> 1
152.89.247.37:443 -> pobosa.com,/mk.js,racijo.com,/mk.js -> 2
142.234.157.105:443 -> zokotej.com,/mobile-android -> 1
-> zokotej.com,/tab_home_active -> 1
23.106.160.163:443 -> hexihan.com,/panel.html,vojefe.com,/btn_bg.html -> 2
192.254.76.78:443 -> capuxix.com,/media.css -> 96
104.194.11.107:443 -> zuveye.com,/default -> 2
103.195.103.171:443 -> zedoxuf.com,/links.html -> 2
104.171.125.14:443 -> moduwoj.com,/panel -> 1
-> moduwoj.com,/btn_bg -> 1
199.127.61.113:443 -> dirupun.com,/RELEASE_NOTES -> 2
173.234.155.101:443 -> hakenu.com,/eso.js -> 1
-> hakenu.com,/en.js -> 1
104.194.9.236:443 -> zosohev.com,/cr -> 2
23.92.222.170:443 -> roxiya.com,/FAQ -> 2
23.82.128.16:443 -> jesage.com,/profile,nefida.com,/profile -> 1

-> jesage.com,/profile,nefida.com,/ur -> 1
23.83.134.44:443 -> roxiya.com,/FAQ -> 2
152.89.247.172:443 -> fonazax.com,/kj -> 2
108.62.141.155:443 -> damacat.com,/styles -> 1
-> damacat.com,/logo -> 1
206.221.176.220:443 -> sidevot.com,/nd.html -> 2
23.82.19.204:443 -> comecal.com,/ml.js,rexagi.com,/ml.js -> 2
104.194.9.51:443 -> nemupim.com,/FAQ.html,sulezo.com,/r_config.html -> 1
-> nemupim.com,/r_config.html,sulezo.com,/r_config.html -> 1
104.194.10.21:443 -> dodefoh.com,/tab_shop_active,joxinu.com,/tab_shop_active -> 1
-> dodefoh.com,/tab_shop_active,joxinu.com,/ce -> 1
108.62.141.82:443 -> pobosa.com,/mk.js,racijo.com,/mk.js -> 2
108.62.118.29:443 -> derotin.com,/Content.html -> 2
142.234.157.125:443 -> lajipil.com,/lt.js -> 2
104.194.9.228:443 -> cuyuzah.com,/tab_home_active.css -> 1
104.194.9.101:443 -> xesoxaf.com,/remove.js -> 1
23.106.215.61:443 -> gojihu.com,/fam_cart.js,yuxicu.com,/fam_cart.js -> 2
104.171.122.198:443 -> hesovaw.com,/tab_shop_active.js -> 2
23.82.19.133:443 -> pazovet.com,/dhl.js -> 1
108.62.118.185:443 -> wuluxo.com,/as.css -> 2
45.126.211.2:443 -> bideluw.com,/af,hubojo.com,/af -> 2
172.96.143.218:443 -> jenupe.com,/templates.js -> 2
45.138.172.37:443 -> rasokuc.com,/bn.js -> 2
23.82.19.187:443 -> buloxo.com,/modcp.js -> 2
185.150.189.202:443 -> pofifa.com,/ki -> 1
-> pofifa.com,/Content -> 1
192.254.65.154:443 -> refebi.com,/bg -> 1
-> refebi.com,/faq -> 1
74.118.138.162:443 -> pavateg.com,/btn_bg -> 1
23.106.215.46:443 -> hexihan.com,/panel.html,vojefe.com,/btn_bg.html -> 2
173.234.155.82:443 -> lozobo.com,/posting -> 2
45.147.229.242:443 -> dodefoh.com,/hr.html,joxinu.com,/ml.html -> 1
-> dodefoh.com,/ml.html,joxinu.com,/hr.html -> 1
199.127.62.132:443 -> keholus.com,/ee -> 1
-> keholus.com,/Content -> 1
185.150.190.244:443 -> paxobuy.com,/eso -> 2

108.62.12.246:443 -> xisiyi.com,/gv -> 2
104.194.10.26:443 -> hiwiko.com,/r_config.html -> 1
-> hiwiko.com,/styles.html -> 1
23.82.140.102:443 -> badiwaw.com,/btn_bg -> 1
23.82.19.173:443 -> gojihu.com,/fam_cart.js,yuxicu.com,/fam_cart.js -> 2
199.127.61.201:443 -> yiyuro.com,/nl.js -> 2
192.198.88.110:443 -> dihata.com,/search.js -> 2
185.150.190.45:443 -> tamunar.com,/boxes -> 1
-> tamunar.com,/links -> 1
108.62.141.200:443 -> nemupim.com,/FAQ.html,sulezo.com,/r_config.html -> 1
104.243.32.108:443 -> hulixo.com,/ky -> 1
-> hulixo.com,/rn -> 1
104.194.10.3:443 -> bucudiy.com,/profile -> 1
199.127.60.15:443 -> fepaza.com,/sq.css -> 1
-> fepaza.com,/rw.css -> 1
104.243.34.57:443 -> yeruje.com,/es -> 2
23.106.160.78:443 -> sidevot.com,/nd.html -> 2
45.153.241.250:443 -> cubigif.com,/jp.html -> 1
-> cubigif.com,/fam_newspaper.html -> 1
104.243.40.170:443 -> kidukes.com,/as -> 1
-> kidukes.com,/br -> 1
23.106.223.116:443 -> koxiga.com,/xmlconnect -> 2
185.150.190.154:443 -> badiwaw.com,/link -> 1
-> badiwaw.com,/btn_bg -> 1
23.106.223.182:443 -> hulixo.com,/ky -> 1
-> hulixo.com,/rn -> 1
108.62.118.121:443 -> zuveye.com,/default -> 2
45.58.127.226:443 -> mezugen.com,/remove,zuwevex.com,/remove -> 2
23.81.246.189:443 -> nemupim.com,/FAQ.html,sulezo.com,/r_config.html -> 1
-> nemupim.com,/r_config.html,sulezo.com,/r_config.html -> 1
23.83.133.29:443 -> wiwege.com,/tab_home -> 2
54.158.194.151:443 -> yeyidun.com,/an -> 1
23.81.246.20:443 -> yipeyic.com,/adminhtml.css -> 2
23.108.57.130:443 -> hesovaw.com,/tab_shop_active.js -> 2
74.118.138.209:443 -> cuyuzah.com,/tab_home_active.css -> 2
104.243.43.207:443 -> fonazax.com,/kj -> 1

> *173.234.155.146:443 -> nagiwo.com,/ny,howeyoh.com,/ky -> 2*
> *108.62.118.236:443 -> paxobuy.com,/eso -> 2*
> *104.243.33.7:443 -> wiwege.com,/tab_home -> 2*
> *23.106.215.44:443 -> xesoxaf.com,/remove.js -> 1*
> *-> xesoxaf.com,/sitemap.js -> 1*
> *185.150.191.44:443 -> hacoyay.com,/be -> 2*
> *142.234.157.160:443 -> wigeco.com,/cs -> 1*
> *-> wigeco.com,/groupcp -> 1*
> *23.82.128.104:443 -> zikojut.com,/ee.css -> 1*
> *23.83.133.226:443 -> sexefo.com,/styles.html -> 2*
> *23.81.246.131:443 -> bideluw.com,/af,hubojo.com,/af -> 2*
> *192.111.144.150:443 -> damacat.com,/styles -> 1*
> *-> damacat.com,/logo -> 1*
> *104.194.11.148:443 -> rasokuc.com,/bn.js -> 2*
> *45.147.229.161:443 -> rucajit.com,/language.html -> 2*
> *45.147.229.93:443 -> tamunar.com,/boxes -> 1*
> *-> tamunar.com,/links -> 1*
> *209.222.98.111:443 -> sexefo.com,/styles.html -> 2*
> *104.194.10.57:443 -> cubigif.com,/jp.html -> 1*
> *-> cubigif.com,/fam_newspaper.html -> 1*
> *45.153.241.251:443 -> luherih.com,/lt -> 2*
> *185.150.191.35:443 -> zikojut.com,/ee.css -> 2*

The Spawnto_x86 path list in the CobaltStrike Beacon configuration information:

> *%windir%\syswow64\WUAUCLT.exe -> 2*
> *%windir%\syswow64\mstsc.exe -> 34*
> *%windir%\syswow64\rundll32.exe -> 18*
> *%windir%\syswow64\runonce.exe -> 2*
> *%windir%\syswow64\wusa.exe -> 104*

Next, we queried all the IP addresses and domain names that were collected on multiple internal platforms including virustotal.com, and finally found only one target that was marked by a relevant malicious organization:

waceko.com → TA551 (2021–07–28T)

Two IPs can be found by searching waceko.com through ZoomEye:

> *45.147.231.12*
> *89.163.140.101*

They are located in Frankfurt, Germany, The Operator: combahton.net, and the Spawnto_x86: %windir%\syswow64\wusa.exe , This is consistent with the IP corresponding to dodefoh.com and joxinu.com used by the attacker, but the Spawnto_x86 path is different.

IOCs：

All C2 IP/Domain from ZoomEye

> *23.106.215.137*
> *104.238.205.63*
> *45.147.230.64*
> *199.127.61.95*
> *74.118.138.125*
> *74.118.138.123*
> *192.198.86.130*
> *23.19.227.178*
> *23.82.140.162*
> *23.82.19.130*
> *104.238.221.50*
> *172.241.27.70*
> *23.106.223.184*
> *23.92.210.210*
> *206.221.185.106*
> *192.254.79.154*
> *23.106.160.218*
> *23.108.57.230*
> *199.101.185.62*
> *192.169.6.73*
> *172.98.201.38*
> *108.62.141.121*
> *192.198.89.242*
> *23.82.19.219*

45.147.231.12
213.227.155.7
172.241.29.110
23.83.133.14
23.106.160.151
199.241.187.138
74.118.138.254
23.108.57.39
108.62.141.7
74.118.138.160
204.16.247.171
23.81.246.18
108.177.235.13
209.222.98.79
104.171.121.174
192.198.92.246
74.118.138.139
23.106.160.40
199.191.57.222
45.128.156.177
23.92.212.54
209.222.98.225
104.243.33.123
108.62.141.5
23.92.216.30
172.241.27.145
206.221.176.103
172.93.105.162
172.98.197.30
192.198.85.182
23.81.246.247
23.108.57.186
192.198.89.58
104.243.37.143
23.106.160.95
103.195.100.2

104.254.62.100
64.187.238.138
173.234.155.124
104.194.10.22
209.222.101.221
199.101.185.58
23.82.140.223
23.106.160.77
74.118.138.249
23.81.246.113
23.106.215.209
23.106.160.143
45.147.230.71
23.81.246.102
172.241.27.22
192.254.65.202
23.82.185.104
185.150.190.153
23.106.215.45
199.241.184.2
160.202.65.114
23.106.160.231
209.222.104.194
74.118.138.207
104.244.156.18
209.222.101.242
104.194.9.113
209.222.104.194
64.187.238.58
192.111.144.6
108.62.118.193
108.62.12.190
23.83.133.187
192.254.76.214
23.83.134.212
192.198.93.86

23.108.57.50
192.254.78.106
209.222.98.33
104.194.11.92
199.101.184.190
173.234.155.86
104.194.8.13
23.106.160.22
23.19.227.247
104.194.8.13
108.62.12.114
45.147.231.98
172.97.71.156
23.82.140.156
23.82.185.122
104.194.10.206
45.147.230.84
172.96.172.218
23.108.57.23
107.161.114.226
74.118.138.237
206.221.176.171
192.198.81.46
108.62.141.55
206.221.184.130
204.16.247.104
23.19.227.8
199.191.56.170
108.177.235.212
23.81.246.177
173.234.155.98
104.194.11.118
192.111.149.58
107.161.114.226
185.150.190.54
104.254.57.126

23.106.160.51
160.202.116.42
45.147.230.80
23.106.160.136
104.243.34.210
74.118.138.253
23.106.223.49
104.243.42.31
104.238.221.213
209.222.101.21
23.106.215.71
104.194.10.22
23.106.223.110
104.194.10.33
172.96.143.178
108.62.12.100
108.62.118.15
23.81.246.206
45.58.112.202
45.147.229.51
23.108.57.145
199.127.61.194
108.62.118.149
45.153.240.234
89.163.140.101
199.127.61.223
23.81.246.222
104.243.37.30
192.254.68.130
108.62.118.218
23.106.215.151
23.82.140.186
209.222.98.75
23.81.246.167
209.222.98.168
172.93.201.14

199.127.61.167
199.241.187.126
74.118.138.134
108.62.118.51
104.194.10.181
23.106.160.144
23.106.223.150
108.177.235.214
108.177.235.115
172.93.105.2
103.195.101.98
23.106.160.141
45.58.117.178
104.194.11.248
104.238.205.32
108.62.12.80
199.191.57.246
185.150.189.186
104.243.33.221
204.16.247.190
104.243.34.58
192.111.146.22
192.111.153.186
104.194.10.201
45.58.123.178
173.234.155.26
108.62.141.184
23.106.215.64
18.222.162.20
74.118.138.159
23.108.57.15
23.82.140.227
104.244.156.179
172.93.201.161
104.152.186.14
23.106.215.141

104.238.222.148
192.111.146.58
104.171.117.58
108.62.118.63
104.243.35.115
209.222.98.14
89.163.210.85
23.81.246.123
108.62.141.174
152.89.247.37
192.111.154.86
104.194.9.47
142.234.157.105
192.198.86.130
23.106.160.163
192.254.76.78
172.93.110.138
104.194.11.107
103.195.103.171
45.147.229.185
104.171.125.14
199.127.61.113
173.234.155.101
104.194.9.236
23.92.222.170
172.93.102.164
23.82.128.16
23.83.134.44
152.89.247.172
108.62.141.155
206.221.176.220
204.16.247.94
104.243.33.100
23.82.19.204
104.194.9.51
104.194.10.21

108.62.141.82
108.62.118.29
172.96.160.214
142.234.157.125
23.106.223.246
104.194.9.228
104.194.9.101
23.106.215.61
204.16.247.176
104.238.221.42
104.171.122.198
23.82.19.133
108.62.118.185
45.126.211.2
172.96.143.218
45.138.172.37
172.82.179.58
23.82.19.187
185.150.189.202
192.254.65.154
23.106.223.11
74.118.138.162
23.106.215.46
173.234.155.82
45.147.229.242
199.127.62.132
192.111.146.58
185.150.190.244
108.62.12.246
104.194.10.26
23.82.140.102
74.118.138.246
23.82.19.173
199.127.61.201
192.198.88.110
185.150.190.45

108.62.141.200
104.243.32.108
104.194.10.3
199.127.60.15
104.243.34.57
23.106.160.78
45.153.241.250
108.62.118.232
104.243.40.170
23.106.223.116
152.89.247.26
185.150.190.154
23.106.223.182
108.62.118.121
45.147.230.236
45.58.127.226
23.81.246.189
23.83.133.29
54.158.194.151
23.81.246.20
23.108.57.130
74.118.138.209
104.243.43.207
108.62.12.186
173.234.155.146
108.62.118.236
104.243.33.7
23.106.215.44
185.150.191.44
142.234.157.160
23.82.128.104
23.83.133.226
23.81.246.131
104.194.11.148
45.147.229.161
216.126.193.126

45.147.229.93
209.222.98.111
192.111.144.150
104.194.10.57
209.222.101.96
45.153.241.251
185.150.191.35
laputo.com
gohaduw.com
kidukes.com
scalewa.com
hacoyay.com
riolist.com
pilagop.com
zeheza.com
waceko.com
showero.com
koviluk.com
gerepa.com
pazovet.com
touchroof.com
mevepu.com
jinoso.com
kuyeguh.com
zedoxuf.com
yeyidun.com
showmod.com
koxiga.com
ganobaz.com
yawero.com
dihata.com
pigaji.com
hireja.com
hoguyum.com
bulozeb.com
yisimen.com

kelowuh.com
dapapev.com
xivuli.com
gimazic.com
tifiru.com
nokuje.com
wezaju.com
tucosu.com
raniyev.com
wudepen.com
wideri.com
lajipil.com
wukeyos.com
tepiwo.com
hakakor.com
pofafu.com
yazorac.com
wuluxo.com
lozobo.com
nihahi.com
winohak.com
barovur.com
buremih.com
hetamuf.com
jafiha.com
hejalij.com
luherih.com
rivuha.com
xoxalab.com
hakenu.com
dahefu.com
pipipub.com
maloxob.com
mebonux.com
dirupun.com
keholus.com

pobosa.com
zokotej.com
hexihan.com
capuxix.com
zuveye.com
moduwoj.com
zosohev.com
roxiya.com
jesage.com
fonazax.com
damacat.com
sidevot.com
comecal.com
nemupim.com
dodefoh.com
derotin.com
cuyuzah.com
xesoxaf.com
gojihu.com
hesovaw.com
bideluw.com
jenupe.com
rasokuc.com
buloxo.com
pofifa.com
refebi.com
pavateg.com
paxobuy.com
xisiyi.com
hiwiko.com
badiwaw.com
yiyuro.com
tamunar.com
hulixo.com
bucudiy.com
fepaza.com

> *yeruje.com*
> *cubigif.com*
> *mezugen.com*
> *wiwege.com*
> *yipeyic.com*
> *nagiwo.com*
> *wigeco.com*
> *zikojut.com*
> *sexefo.com*
> *rucajit.com*

Zoomeye Shodan Apt Botnet