The many tentacles of Magecart Group 8

blog.malwarebytes.com/threat-intelligence/2021/09/the-many-tentacles-of-magecart-group-8/

Threat Intelligence Team September 13, 2021

This blog post was authored by Jérôme Segura

During the past couple of years online shopping has continued to increase at a rapid pace. In a recent survey done by Qubit, 70.7% of shoppers said they increased their online shopping frequency compared to before COVID-19.

Criminals gravitate towards opportunities, and these trends have made digital skimming attacks such as Magecart all the more profitable.

To protect our customers, we need to constantly look out for novel attacks. Having said that, we sometimes need to check for past ones too. In fact, many threat actors will reuse certain patterns or resources which allows us to make connections with previous incidents.

One Magecart group that has left a substantial amount of bread crumbs from their skimming activity has been documented under various names (Group 8, CoffeMokko, Keeper, FBseo). It is believed to be one of the older threat actors in the digital skimming space.

In this blog post, we publish a number of connections within their infrastructure usage that we've been able to uncover by cross-referencing several data sources.

Reconnecting with Magecart Group 8

In a recent article, RiskIQ researchers unravelled a large part of the infrastructure used by Magecart Group 8 and how they migrated to different hosts in particular Flowspec and OVH over time.

We had been looking at Group 8 also, but starting from a different angle. Back in June we were checking skimmer code that looked somewhat different than anything we could categorize. We didn't think much of it until in July Eric Brandel tweeted about a skimmer he called 'checkcheck' that was using some interesting new features and was essentially the same thing we had found.

After some additional research we noticed that some parts of the code were unique but not new. In particular the exfiltration of credit card data was using a string swapping function identical to the one used by the 'CoffeMokko' family described by Group-IB. In their blog, they mention some overlap with the original Group 1 (RiskIQ) that was eventually merged into what is now Group 8.

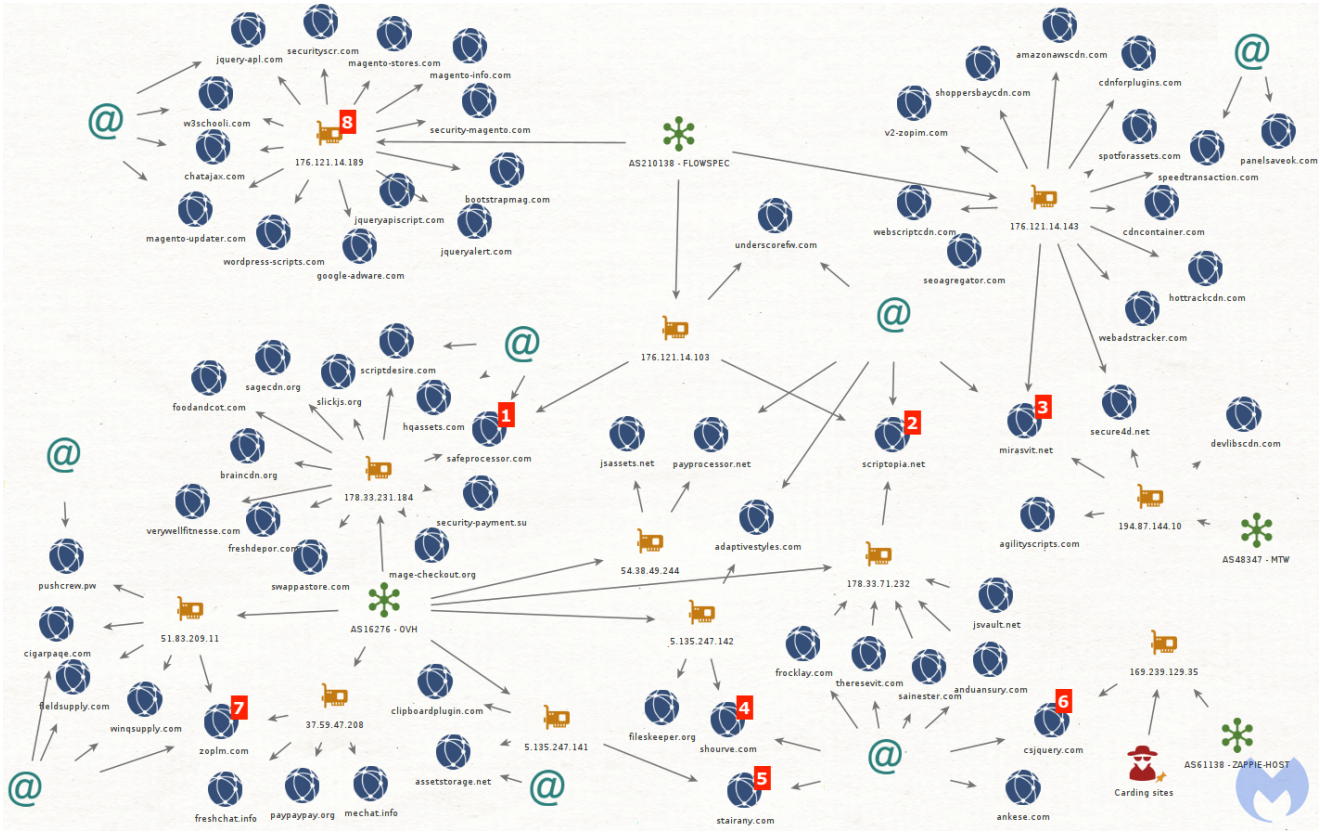
From there, we were reacquainted with a threat group that we had not seen in a while but that had been busy. There were a number of domain names that were new to us. We rapidly got down a rabbit hole and lost track of the big picture. However, the blog from RiskIQ helped to put some perspective on one part of the infrastructure that we referred to as Flowspec – OVH.

Most of the domains and IP addresses have already been covered by RiskIQ. However we were to create some mapping that showed some interesting historical connections between well-known past campaigns. In Part 1, we will explore those links.

We had also uncovered another large part of infrastructure while reporting our findings on 'checkcheck' to Eric Brandel. Then in August, Denis tweeted about some of those domains which interestingly are old but somehow managed to stay low for a long time. We will review those in Part 2.

Part 1: Flowspec and OVH

The RiskIQ article describes this part of the infrastructure in great details. We will review some connecting points that allowed us to rediscover older campaigns. Flowspec is a known bulletproof hosting service that has been used beyond just skimmers, but also for phishing, ransomware and other malware.



[1] The domain **safeprocessor[.]com** was hosted at **176.121.14[.]103** (Flowspec) and **178.33.231[.]184** (OVH). It was listed in the indicators of compromise (IOCs) from Gemini Advisory's "Keeper" Magecart Group Infects 570 Sites blog post. On the same OVH IP is the domain **foodandcot[.]com** listed in the IOCs section for Group-IB's Meet the JS-Sniffers 4: CoffeMokko Family.

[2] scriptopia[.]net was also on 176.121.14[.]103 (Flowspec) and **178.33.71[.]232** (OVH). The domain was spotted by Dmitry Bestuzhev on the website for a Chilean wine. Other domains on that IP were also caught by Rommel.

[3] mirasvit[.]net shares the same registrant as scriptopia[.]net. It was hosted at **194.87.144[.]10** and **176.121.14[.]143** (Flowspec). That IP address came across Denis' radar in a tweet and was largely covered by RiskIQ.

[4] shourve[.]com shares the same registrant as the other skimmer domains hosted at 178.33.71[.]232. It was hosted at **5.135.247[.]142**. On that same IP is **adaptivestyles[.]com** which shared the same registrant as scriptopia[.]net, and **fileskeeper[.]org** from which Gemini Advisory derived the name of their blog post.

[5] stairany[.]com hosted at **5.135.247[.]141** (OVH) appeared in a report by CSIS Group. Another domain on that IP address is clipboardplugin[.]com which was mentioned by Félix Aimé along with a screenshot of a carding website.

[6] csjquery[.]com shares the same registrant as stairany[.]com and is hosted at **169.239.129[.]35** (ZAPPIE-HOST). On that IP are hundreds of carding sites.

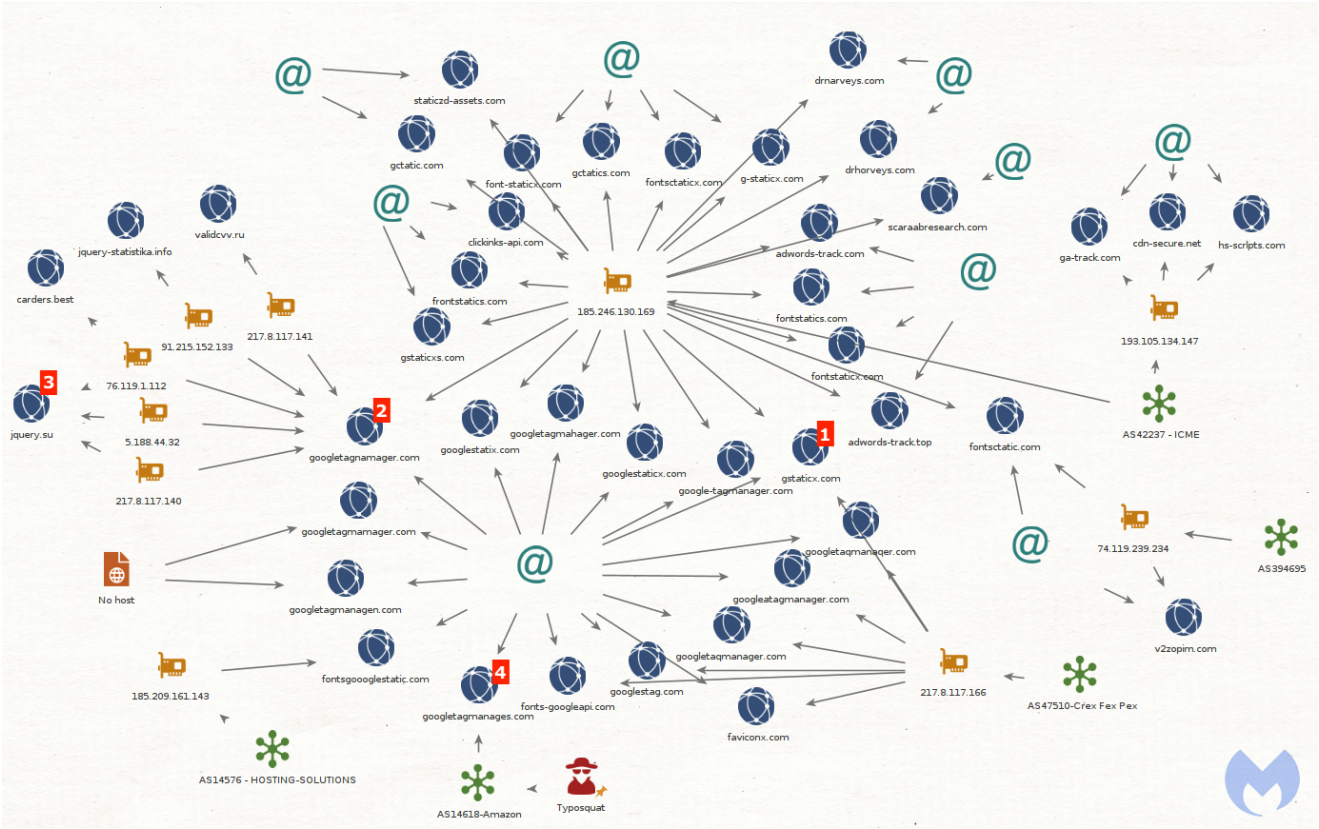
[7] zoplm[.]com hosted at **37.59.47[.]208** (OVH) and **51.83.209[.]11** (OVH) shares the same registrant as **cigarpaqe[.]com** and **fleldsupply[.]com** mentioned in our blog using Homoglyph domains.

[8] 176.121.14[.]189 (Flowspec) was covered by RiskIQ for its number of skimmer domains that later moved to Velia.net hosting.

Part 2: ICME and Crex Fex Pex

This bit of infrastructure was interesting because it tied back to activity we saw from domains like jquery[.]su. This was actually the starting point of our investigation, which eventually led to *Part 1: Flowspec and OVH* and back to Group 8.

Crex Fex Pex (Крекс-фекс-пекс) refers to a Russian play with a character that looks like Pinocchio. However in our case it is a bulletproof hoster that has seen significant skimmer activity.



[1] gstaticx[.]com was hosted at **217.8.117[.]166** (Crex Fex Pex) and **185.246.130[.]169** (ICME). We can see a recent compromise here, and the skimmer (which uses that character swapping function) in particular here.

[2] googletagnamager[.]com hosted at **217.8.117[.]141** (Crex Fex Pex) shared the same registrant as gstaticx[.]com. Interestingly, one version of this skimmer from googletagnamager[.]com/ki/x19.js loaded JavaScript from **jquery[.]su**.

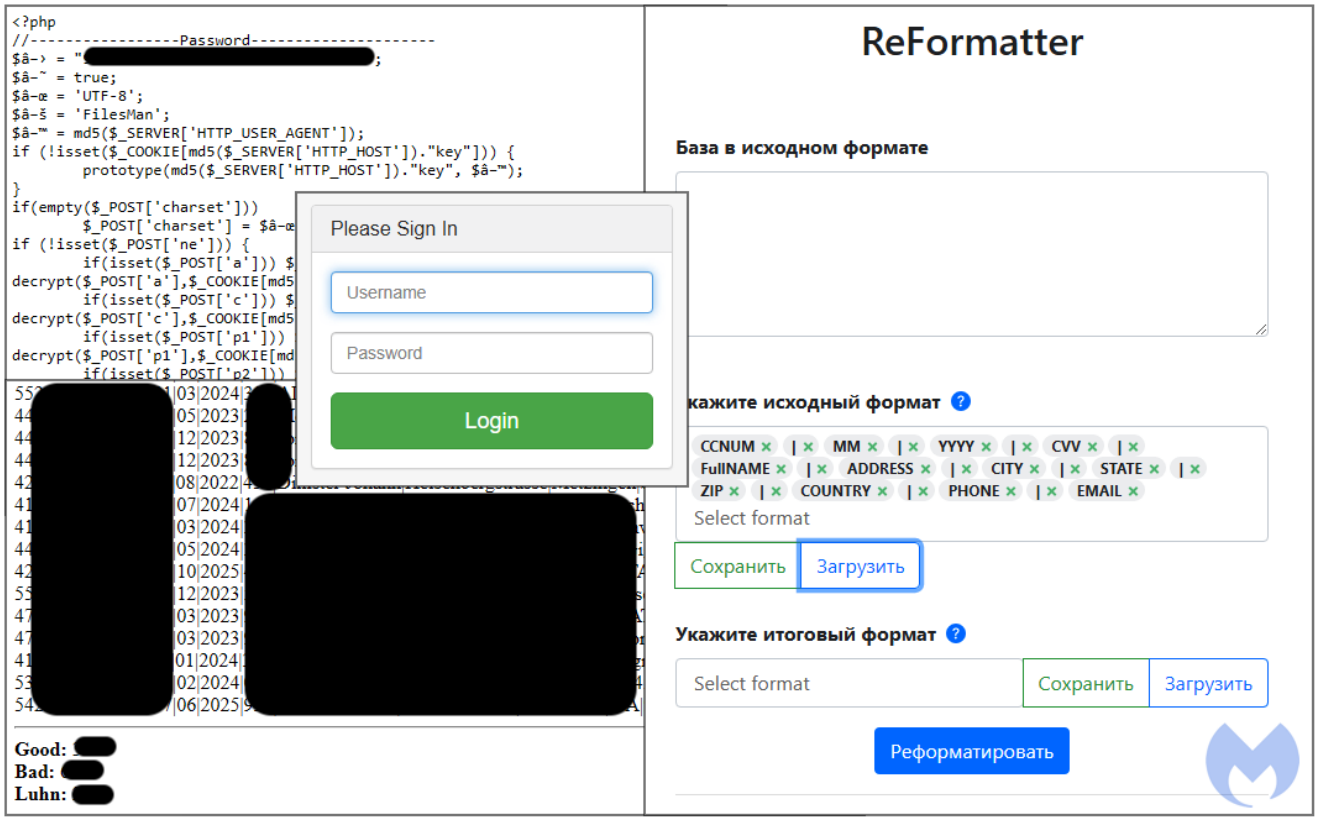
We can find a similar path structure at jquery[.]su/ki/x2.js which also references the same min-1.12.4.js script. A version of this script can be seen here (capture).

[3] The domain **jquery[.]su** was registered by **alexander.colmakov2017@yandex[.]ru**. The same email address was used to register **serversoftwarebase[.]com** which is connected to brute force attacks against various CMS. In that blog post, we mention googletagmanager[.]eu hosted at 185.68.93[.]22 which is associated with a campaign against MySQL/Adminer.

[4] googletagmanages[.]com has the same registrant as googletagnamager[.]com. contrary to the other domains we've seen so far, this one is on Amazon. Reviewing the IP addresses which hosted it (AS14618-Amazon), we find hundreds of typosquat domains for skimming (see IOCs section for list). It seems though that most were not used, perhaps just kept for a rainy day.

Digital skimming artifacts

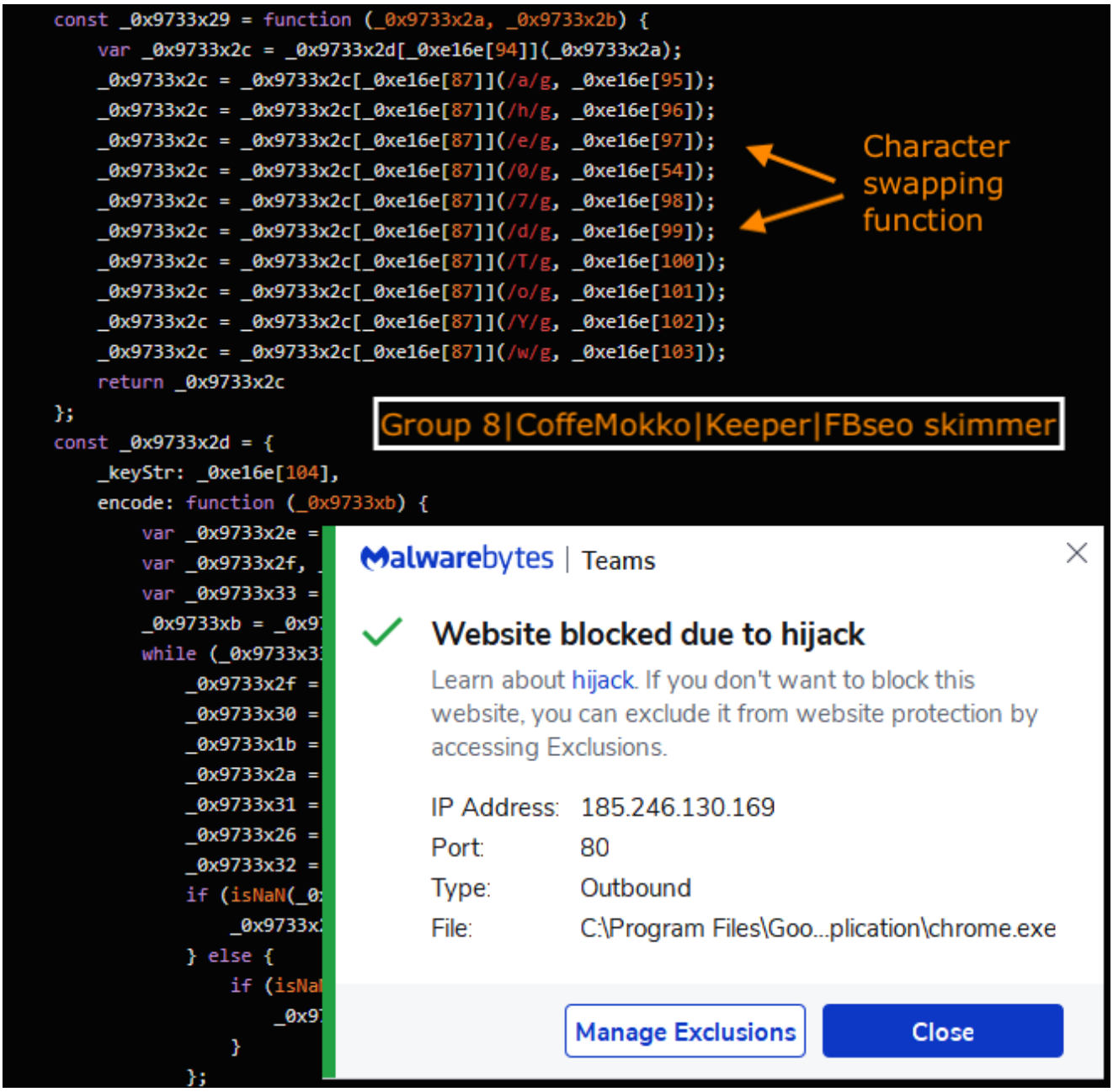
While checking this infrastructure we came across a number of artifacts related to web skimming activity including webshells, panels, and other tools. With such a sprawling network, it's not hard to imagine that the criminals themselves may have a tough time keeping track of everything they have.



Tracking digital skimmers is a time consuming effort where one might easily get lost in the noise. Criminals are constantly setting up new servers and moving things around. In addition, with the help of bulletproof services, they make it difficult to disrupt their infrastructure.

However we and many researchers regularly publish information that helps to identify and block new domains and IP addresses. We also work with law enforcement and have reported many of these artifacts, in particular the stolen customer data. Finally, we also notify merchants although too many are still unaware of this threat and lack the proper contact details.

Malwarebytes customers are protected against digital skimmers thanks to the web protection module available in our consumer and enterprise products.



Indicators of Compromise (IOCs)

Skimmer domains

adaptivestyles[.]com
agilityscripts[.]com
amazonawscdn[.]com
anduansury[.]com
ankese[.]com
assetstorage[.]net
bootstrapmag[.]com
braincdn[.]org
cdncontainer[.]com
cdnforplugins[.]com
chatajax[.]com
cigarpaqe[.]com
clipboardplugin[.]com
csjquery[.]com
devlibscdn[.]com
fileskeeper[.]org
fleldsupply[.]com
foodandcot[.]com
freshchat[.]info
freshdepor[.]com
frocklay[.]com
google-adware[.]com
hottrackcdn[.]com
hqassets[.]com
jquery-apl[.]com
jqueryalert[.]com
jqueryapiscript[.]com
jsassets[.]net
jsvault[.]net
mage-checkout[.]org
magento-info[.]com
magento-stores[.]com
magento-updater[.]com
mechat[.]info
mirasvit[.]net
panelsaveok[.]com
paypaypay[.]org

payprocessor[.]net
pushcrew[.]pw
safeprocessor[.]com
sagecdn[.]org
sainester[.]com

scriptdesire[.]com
scriptopia[.]net
secure4d[.]net
security-magento[.]com
security-payment[.]su
securityscr[.]com
seoagregator[.]com
shoppersbaycdn[.]com
shourve[.]com
slickjs[.]org
speedtransaction[.]com
spotforassets[.]com
stairany[.]com
swappastore[.]com
theresevit[.]com
underscorefw[.]com
v2-zopim[.]com
verywellfitnesse[.]com
w3schooli[.]com
webadstracker[.]com
webscriptcdn[.]com
winqsupply[.]com
wordpress-scripts[.]com
zoplm[.]com
adwords-track[.]com
adwords-track[.]top
carders[.]best
cdn-secure[.]net
clickinks-api[.]com
drhorveys[.]com
drnarveys[.]com
faviconx[.]com

font-staticx[.]com
fonts-googleapi[.]com
fontsctatic[.]com
fontsctaticx[.]com
fontsgoooglestatic[.]com
fontstatics[.]com
fontstaticx[.]com
frontstatics[.]com
g-staticx[.]com
ga-track[.]com

gctatic[.]com
gctatics[.]com
google-tagmanager[.]com
googleatagmanager[.]com
googlestag[.]com
googlestaticx[.]com
googlestatix[.]com
googletagmahager[.]com
googletagmamager[.]com
googletagmanagen[.]com
googletagmanages[.]com
googletagnamager[.]com
googletaqmanager[.]com
googletaqmanaqer[.]com
gstaticx[.]com
gstaticxs[.]com
hs-scrlpts[.]com
jquery-statistika[.]info
jquery[.]su
scaraabresearch[.]com
staticzd-assets[.]com
v2zopim[.]com
validcvv[.]ru

Related IP addresses

169[.]239[.]129[.]35
176[.]121[.]14[.]103
176[.]121[.]14[.]143
176[.]121[.]14[.]189
178[.]33[.]231[.]184
178[.]33[.]71[.]232
194[.]87[.]144[.]10
37[.]59[.]47[.]208

5[.]135[.]247[.]141
5[.]135[.]247[.]142
51[.]83[.]209[.]11
54[.]38[.]49[.]244
185[.]209[.]161[.]143
185[.]246[.]130[.]169
193[.]105[.]134[.]147
217[.]8[.]117[.]140

217[.]8[.]117[.]141
217[.]8[.]117[.]166
5[.]188[.]44[.]32
74[.]119[.]239[.]234
76[.]119[.]1[.]112
91[.]215[.]152[.]133

Typosquat

googheusercontent[.]com
googlatagmanager[.]com
googlausercontent[.]com
google5sercontent[.]com
googleafalytics[.]com
googleanadytics[.]com
googleanahytics[.]com
googleanal9tics[.]com
googleanalxtics[.]com
googleanaly4ics[.]com
googleanalydics[.]com
googleanalypics[.]com
googleanalytacs[.]com
googleanalytias[.]com
googleanalytibs[.]com
googleanalyticc[.]com
googleanalyticr[.]com
googleanalyticw[.]com
googleanalytigs[.]com
googleanalytiks[.]com
googleanalytkcs[.]com
googleanalytmcs[.]com
googleanalytycs[.]com
googleanalyuics[.]com
googleanalyvics[.]com
googleanamytics[.]com
googleananytics[.]com
googleanclytics[.]com
googleanelytics[.]com
googleanilytics[.]com
googleanqlytics[.]com
googleaoalytics[.]com
googlecnalytics[.]com
googledagmanager[.]com

googleenalytics[.]com
googleesercontent[.]com
googleinalytics[.]com
googlepagmanager[.]com
googleqnalytics[.]com
googleqsercontent[.]com
googletacmanager[.]com
googletaemanager[.]com

googletag-anager[.]com
googletageanager[.]com
googletagianager[.]com
googletaglanager[.]com
googletagmafager[.]com
googletagmajager[.]com
googletagmalager[.]com
googletagmanacer[.]com
googletagmanaeer[.]com
googletagmanafer[.]com
googletagmanagar[.]com
googletagmanagdr[.]com
googletagmanage2[.]com
googletagmanageb[.]com
googletagmanagep[.]com
googletagmanages[.]com
googletagmanagev[.]com
googletagmanagez[.]com
googletagmanaggr[.]com
googletagmanagmr[.]com
googletagmanagur[.]com
googletagmanaoer[.]com
googletagmanawer[.]com
googletagmancger[.]com
googletagmaneger[.]com
googletagmaniger[.]com
googletagmanqger[.]com
googletagmaoager[.]com
googletagmcnager[.]com
googletagminager[.]com
googletagmqnager[.]com
googletagoanager[.]com
googletaomanager[.]com
googletawmanager[.]com

googletcgmanager[.]com
googletigmanager[.]com
googletqgmanager[.]com
googletsercontent[.]com
googleu3ercontent[.]com
googleuagmanager[.]com
googleucercontent[.]com
googleuqercontent[.]com

googleurercontent[.]com
googleusarcontent[.]com
googleusdrcontent[.]com
googleuse2content[.]com
googleusebcontent[.]com
googleusepcontent[.]com
googleuseraontent[.]com
googleuserbontent[.]com
googleusercgntent[.]com
googleuserckntent[.]com
googleusercmntent[.]com
googleusercnntent[.]com
googleusercoftent[.]com
googleusercojtent[.]com
googleusercoltent[.]com
googleusercon4ent[.]com
googleusercondent[.]com
googleuserconpent[.]com
googleusercontant[.]com
googleusercontdnt[.]com
googleuserconteft[.]com
googleusercontejt[.]com
googleusercontelt[.]com
googleuserconten4[.]com
googleusercontend[.]com
googleusercontenp[.]com
googleusercontenu[.]com
googleusercontenv[.]com
googleuserconteot[.]com
googleusercontgnt[.]com
googleusercontmnt[.]com
googleusercontunt[.]com
googleuserconuent[.]com
googleusescontent[.]com

googleusgrcontent[.]com
googleusmrcontent[.]com
googlevagmanager[.]com
googlganalytics[.]com
googluanalytics[.]com
googlutagmanager[.]com
googmeanalytics[.]com