

Malvertising campaigns come back in full swing

blog.malwarebytes.com/social-engineering/2020/09/malvertising-campaigns-come-back-in-full-swing/

Threat Intelligence Team

September 9, 2020



Malvertising campaigns leading to exploit kits are nowhere near as common these days. Indeed, a number of threat actors have moved on to other delivery methods instead of relying on drive-by downloads.

However, occasionally we see spikes in activity that are noticeable enough that they highlight a successful run. In late August, we started seeing a Fallout exploit kit campaign distributing the Raccoon Stealer via high-traffic adult sites. Shortly after we reported it to the ad network, the same threat actor came back again using the RIG exploit kit instead.

Then we saw possibly the largest campaign to date on top site xhamster[.]com from a malvertiser we have tracked for well over a year. This threat actor has managed to abuse practically all adult ad networks but this may be the first time they hit a top publisher.

Malvertising on popular ad network

The first malicious advertiser we observed was able to bid for ads on a number of adult sites by targeting users running Internet Explorer without any particular geolocation restriction, although the majority of victims were in the US.

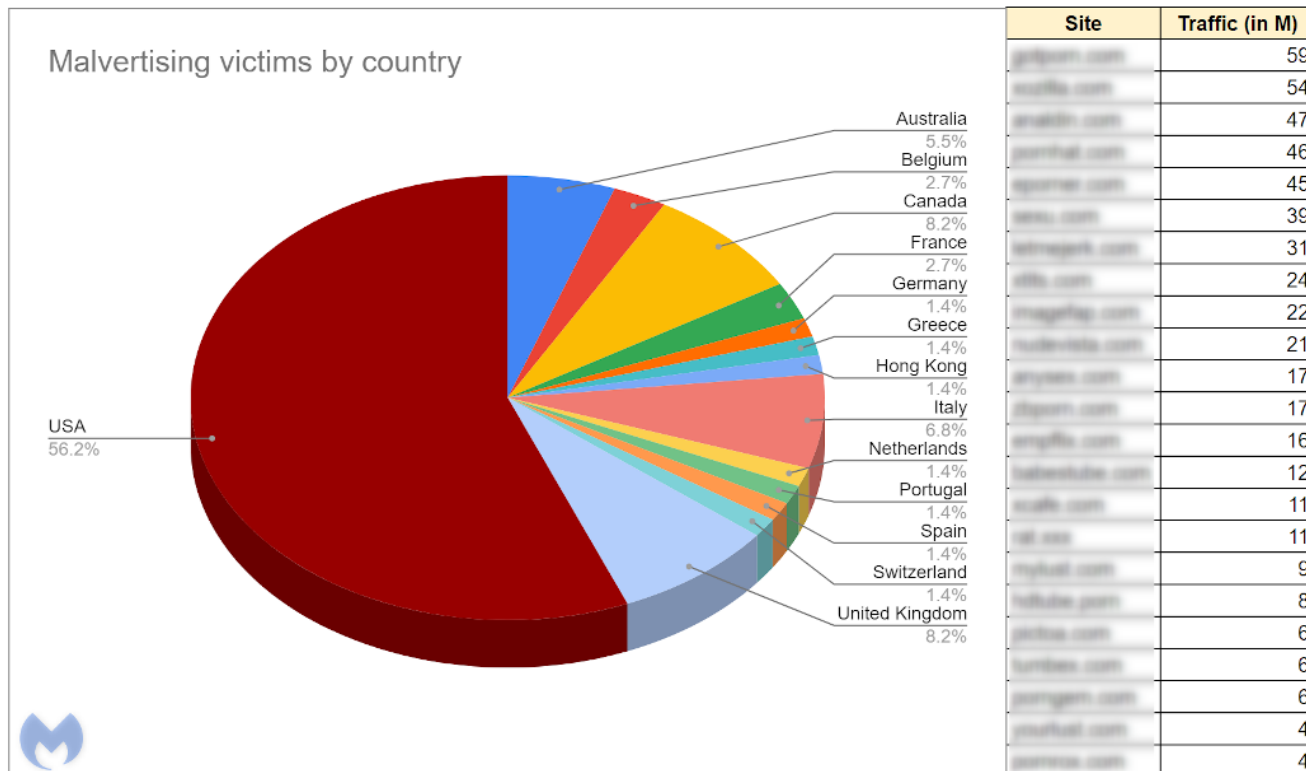


Figure 1: Victims by country on the left, adult sites traffic on the right

In this campaign, the crooks abused the popular ad network ExoClick by using different redirection pages. However, each time we were able to notify the ad network and get them shut down quickly.

The first domain they used was inteca-deco[.]com, which was setup as a web design agency but visibly a decoy page to the trained eye.

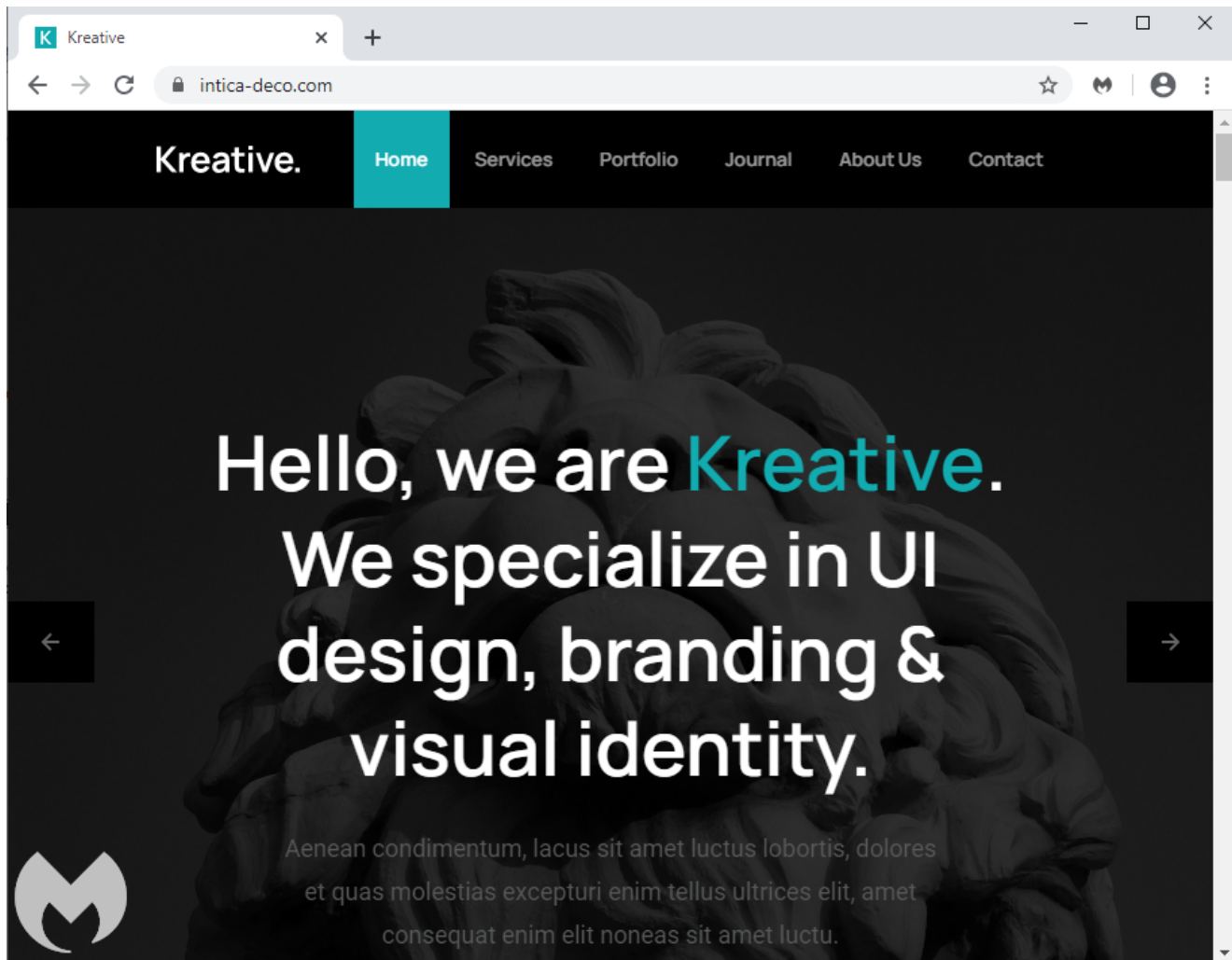


Figure 2: Decoy page used as a gate to exploit kit

Simple server-side cloaking performs the redirect to a Fallout exploit kit landing page which attempts to exploit [CVE-2019-0752](#) (Internet Explorer) and [CVE-2018-15982](#) (Flash Player) before dropping the Raccoon Stealer.

Host	URL	Body	Comments
████████.com	/zps/?zone=45	911	Adult site
syndication.realsrv.com	/splash.php?cat=&idzone=+████████&type=8&...	0	ExoClick malvertising
nutsells-dounerous.icu	/voluum/e6f88310-d545-46ab-9052-64574b00...	0	Redirect
intica-deco.com	/	43,712	Gate to EK
intica-deco.com	/redirect.php	84	Gate to EK
colorado4u.club	/13565/EzYF/wailment/Camions.cfm	4,986	Fallout EK [HTML/JS] (Landing)
colorado4u.club	/24-09-1982/F0sMs?e6e3X=yXcT&iqi=Tiniest	29,044	Fallout EK [HTML/JS] (Landing)
colorado4u.club	/12023/14_10_1944/04_06_1910/pKVHB	7,512	Fallout EK [URI]
colorado4u.club	/chorizos/Cleavage_Frustum	28,544	Fallout EK [URI]
colorado4u.club	/Blastoff-10001/Thinkably-bunsen/bnmZX/hSM...	35,153	Fallout EK [URI] (Flash Exploit)
colorado4u.club	/grandads_Stopwatch_Bittering/pEQM/OuV.as...	5,785	Fallout EK [URI]
colorado4u.club	/13565/EzYF/wailment/Camions.cfm	0	Fallout EK [URI]
colorado4u.club	/Tearier-10943/posited/ovNul/8642?misquote=...	508,416	Fallout EK [Headers] (Payload)
telete.in	/jjJunxShop	4,579	Telegram channel
telete.in	/jjJunxShop	4,579	Telegram channel
telete.in	/jjJunxShop	4,579	Telegram channel
telete.in	/jjJunxShop	4,944	Telegram channel
34.105.147.92	/gate/log.php	571	RaccoonStealer C2 [URI]

Figure 3: Traffic for Fallout exploit kit

About 10 days later, another domain, websolvent[.]me, became active but used a different redirection technique, a 302 redirect, also known as 302 cushioning. This time we see the RIG exploit kit which also delivers Raccoon Stealer.

Host	URL	Body	Comments
████████.com	/	145,245	Adult site
████████.com	/d/exonative1	500	Ad banner
ads.exosrv.com	/ads.js	2,315	ExoClick malvertising
ads.exosrv.com	/nativeads.js	44,978	ExoClick malvertising
syndication.exosrv.com	/splash.php?cat=&idzone=████████&type=8&p...	1,504	ExoClick malvertising
syndication.exosrv.com	/splash.php?cat=&idzone=████████&type=8&p...	0	ExoClick malvertising
websolvent.me	/8bZQWK	0	Gate to EK
91.210.171.116	?NjI1MzAw&thiJri&hKBiG=abettor&bwxiSw=di...	101,633	RIG EK [URI] (Landing Page)
91.210.171.116	?MzIyMjEz&quslwEv&jPLu=callous&wmPhJo=...	483,328	RIG EK [URI] (Payload)
telete.in	/jjJunxShop	4,578	Telegram channel
telete.in	/jjJunxShop	4,579	Telegram channel
telete.in	/jjJunxShop	4,579	Telegram channel
chinadevmonster.top	/gate/log.php	602	RaccoonStealer C2 [URI]

Figure 4: Traffic for RIG exploit kit

Beyond a common payload, those two domains are also related. A [RiskIQ crawl](#) confirms a relationship between these 2 domains where the parent host was caught doing a meta refresh redirect to the child:

HOST PAIRS ⓘ

1 - 2 of 2 Sort : First Seen Ascending 25 / Page

Parent Hostname	Child Hostname
<input type="checkbox"/> intica-deco.com	websolvent.me

Figure 5: Passive Total's host

pairs

Malvertising on top adult site gets maximum reach

The second malvertiser ('malsmoke') is one that we have tracked diligently over the past several months and whose end payload is often the Smoke Loader malware. It is by far the most daring and successful one in that it goes after larger publishers and a variety of ad networks. However, up until now we had only seen them on publishers from the adult industry that are still relatively small in scale.

In this instance, the threat actor was able to abuse the Traffic Stars ad network and place their malicious ad on xhamster[.]com, a site with just over 1.06 billion monthly visits according to SimilarWeb.com.

The gates used by this group also use a decoy site and over time they have registered domains mocking ad networks and cloud providers.

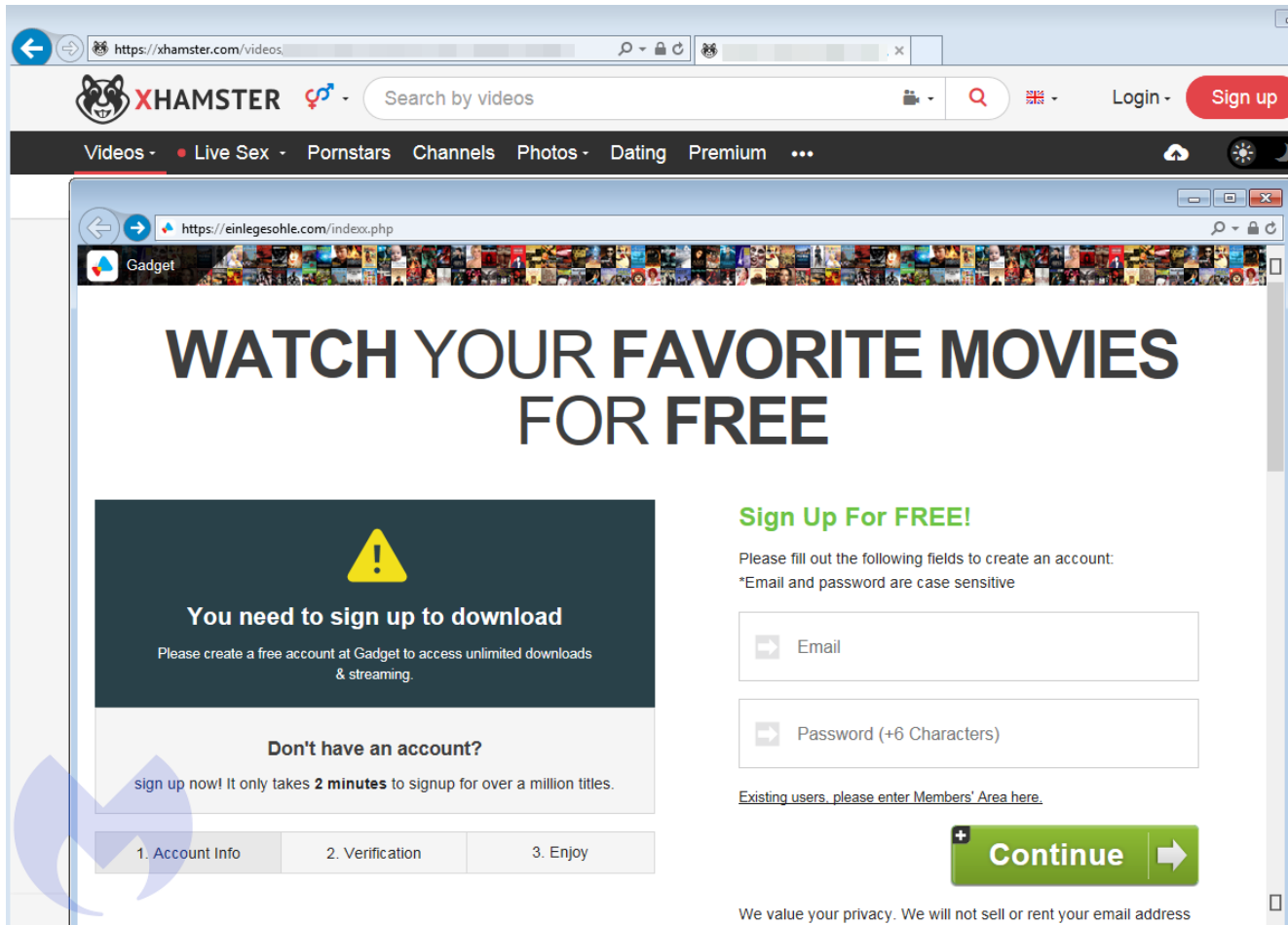


Figure 6: Malicious Popunder on xhamster (brought to the forefront)

The redirection mechanism is more sophisticated than those used in other malvertising campaigns. There is some client-side fingerprinting and connectivity checks to avoid VPNs and proxies, only targeting legitimate IP addresses.

Server IP	Host	URL	Body	Comments
104.18.156.3	xhamster.com	/categories/mature	195,522	(01)
213.174.157.82	tsyndicate.com	/api/v1/direct/...?domain=xhamster.com...	0	(02)
31.31.198.165	einlegesohle.com	/	256	(03)
31.31.198.165	einlegesohle.com	/indexx.php	0	(04)
13.52.20.229	avitquay.com	/click?trvid=10001&extid=[tracking]&campid=[campaignid]&creaid=[adid]&d...	1,190	(05)
13.52.20.229	avitquay.com	/double?t=2&d=...	675	(06)
31.31.198.96	adexhangetomatto.space	?sxid=er8p3s963a9v	2,732	(07)
31.31.198.96	adexhangetomatto.space	/api.php	719	(08)
31.31.198.96	adexhangetomatto.space	/api.php	90	(09)
216.171.233.6	corbenbaby.press	/1982-12-01/OQb/obZZa.jsp?Resought=3978-Whipworm-5531&Tah=Nuthatch	4,924	(10) Fallout EK
216.171.233.6	corbenbaby.press	/Jointless-Massoy/Nabathean-13630/sthenias_asphodel_xiphistna	28,998	(11) Fallout EK
216.171.233.6	corbenbaby.press	/UwdtBz/12-01-1933	7,424	(12) Fallout EK
216.171.233.6	corbenbaby.press	/Deadlier_sperms_Carried/28_04_1992/Louping_myopathy.phtml	28,460	(13) Fallout EK
216.171.233.6	corbenbaby.press	/xzTy/furnage	35,125	(14) Fallout EK
216.171.233.6	corbenbaby.press	/5045_Diagonal_6596/y2bPs.aspx?b95=prealter-10268-13730&cleanlier=900...	5,771	(15) Fallout EK
216.171.233.6	corbenbaby.press	/1982-12-01/OQb/obZZa.jsp?Resought=3978-Whipworm-5531&Tah=Nuthatch	0	(16) Fallout EK
216.171.233.6	corbenbaby.press	/tc497/1946_11_09.cfm	158,208	(17) Fallout EK

Figure 7: Traffic for xhamster malvertising

Interestingly, this Smoke Loader instance also downloads Raccoon Stealer and ZLoader.

Malsmoke is probably the most persistent malvertising campaigns we have seen this year. Unlike other threat actors, this group has shown that it can rapidly switch ad networks to keep their business uninterrupted.

Host	URL	Body	Comments
ps.popcash.net	/go/...	524	(01)
ps.popcash.net	/ad/ad?p=...	80	(02)
clk.rtpdn11.com	/click?i=...	0	(03)
Other malsmoke campaigns			
owymbngzu.com	/click?trvid=10004		
uneaskie.site	/jpexo.php?sxid=...		
uneaskie.site	/jpexo.php?d=...		
uneaskie.site	/caflexactive.php		
uneaskie.site	/caflexactive.php		
korben4u.com	/4ywTX/13_01_1941.jspx		
korben4u.com	/2790_Outscour/Rakely/5410-4216.		
korben4u.com	/2011_06_24/echoed_duckwing/JH		
korben4u.com	/17_02_1925/1998_09_05/10350/c		
korben4u.com	/12493/1962-04-02/galoisian-vamb		
korben4u.com	/QToV/loiterer_prorating_lealty		
korben4u.com	/4ywTX/13_01_1941.jspx		
korben4u.com	/alheit-neening/1966-10-11287Kz-		
korben4u.com	/1914-12-25/9023/13138/10331.cfm	7,488	(08)
korben4u.com	/Waiting/7021/17238_Jovial_earringed.shtml	4,699	(06) Fallout EK
korben4u.com	/1595/Engineery-Disbosoms/avanti-Hadjee/7035?Marigraph=p...	28,979	(07) Fallout EK
korben4u.com	/1914-12-25/9023/13138/10331.cfm	7,488	(08)
korben4u.com	/spence-Humorize/02-02-1929.dhtml?Dm...	28,608	(09)
korben4u.com	/serinette/5A6E?gJW=5208&tuebor=317...	5,877	(10)
korben4u.com	/newrayers-8513/4292_undereate_fostere...	35,152	(11)
korben4u.com	/8_Jovial_earringed.shtml	0	(12)
korben4u.com	/=tFY&NIMY=17_08_1983&gumptions=1...	802,816	(13) Fallout EK
hilltopads.net	/bz3AVB0CPD2EIFj...	4,346	
hilltopads.net	/cFGGFHzIcJzK9Lfi...	0	
clk.rtpdn11.com	/click?i=l8UwOwEOAGU_0	0	
owymbngzu.com	/click?trvid=10004		
uneaskie.site	/offerjp.php		
villandoping.site	/?tid=...&red=1		
clk.rtpdn11.com	/click?seat=1875786...		
owymbngzu.com	/click?trvid=10004		
uneaskie.site	/offerjp.php		
js.juicyads.com	/jp.php?c=...	104,680	
xapi.juicyads.com	/service_ao.php?c=...	4	
xapi.juicyads.com	/...?juicy_cod...	0	
redir.jads.co	/pu_uu.php?cb=...	0	
encelava.com	/usjuicy.php	87,333	
encelava.com	/js/main.js	250	
xnpxtith.com	/click?trvid=10002&extid={conversions_tracking}&cost={cost}...	1,224	(01)
xnpxtith.com	/double?t=2&d=eyJVUkwiOjodHRwcovL2NhbmFKYXZlcnNhG...	697	(02)
canadaversaliska.info	/usflexo.php?sxid=gv0wdfkt7smd	658	(03)
canadaversaliska.info	/usflexexo.php	713	(04)
canadaversaliska.info	/usflexexo.php	64	(05)
korben4u.com	/Waiting/7021/17238_Jovial_earringed.shtml	4,699	(06) Fallout EK
korben4u.com	/1595/Engineery-Disbosoms/avanti-Hadjee/7035?Marigraph=p...	28,979	(07) Fallout EK
korben4u.com	/1914-12-25/9023/13138/10331.cfm	7,488	(08)
korben4u.com	/spence-Humorize/02-02-1929.dhtml?Dm...	28,608	(09)
korben4u.com	/serinette/5A6E?gJW=5208&tuebor=317...	5,877	(10)
korben4u.com	/newrayers-8513/4292_undereate_fostere...	35,152	(11)
korben4u.com	/8_Jovial_earringed.shtml	0	(12)
korben4u.com	/=tFY&NIMY=17_08_1983&gumptions=1...	802,816	(13) Fallout EK
c1.popads.net	/pop.js	31,739	
serve.popads.net	/c?_E...	1,917	
serve.popads.net	/e.js	1	
serve.popads.net	/s?cid=...&uid=...&ts=...&ps=...	187	
www.predictionexchange.com	/jump/next.php?r=3001435&sub1=...	4,813	
www.predictionexchange.com	/jump/next.php?stamat=m%7C%2Cwo2IqY3KqB1dAJ0dEdHP3...	0	
surdised.site	/offerus.php?acsc=200137504	134,409	

Figure 8: Malvertising campaigns related to malsmoke

Still using Internet Explorer?

Threat actors still leveraging exploit kits to deliver malware is one thing, but end users browsing with Internet Explorer is another. Despite recommendations from Microsoft and security professionals, we can only witness that there are still a number of users (consumer and enterprise) worldwide that have yet to migrate to a modern and fully supported browser.

As a result, exploit kit authors are squeezing the last bit of juice from vulnerabilities in Internet Explorer and Flash Player (due to retire for good next year).

Malwarebytes customers have long been protected from malvertising and exploit kits. We continue to track and report the campaigns we run into to help do our part in keeping the Internet safer.

Indicators of compromise

Gates used in malvertising campaign pushing Raccoon Stealer

intica-deco[.]com
websolvent[.]me

Raccoon Stealer

b289155154642ba8e9b032490a20c4a2c09b925e5b85dda11fc85d377baa6a6c
f319264b36cdf0daeb6174a43aaf4a6684775e6f0fb69aaf2d7dc051a593de93

Raccoon Stealer C2s

34.105.147[.]92/gate/log.php
chinadevmonster[.]top/gate/log.php

Smoke Loader

23bef893e3af7cb49dc5ae0a14452ed781f841db7397dc3ebb689291fd701b6b

Smoke Loader C2s

dkajsdjiqwdwnfj[.]info
2831ujedkdajsdj[.]info
928eijdkksasnfss[.]info
dkajsdjiqwdwnfj[.]info
2831ujedkdajsdj[.]info
928eijdkksasnfss[.]info

Gates used in the malsmoke campaign

einlegesohle[.]com/indexx.php
adexhangetomatto[.]space
encelava[.]com/coexo.php
encelava[.]com/caac
uneaskie[.]com/ukexo.php
bumblizz[.]com/auexo.php
bumblizz[.]com/auflexexo.php
bumblizz[.]com/caexo.php
bumblizz[.]com/caflexexo.php
bumblizz[.]com/usexo.php
bumblizz[.]com/usflexexo.php
canadaversaliska[.]info/coflexexo.php
canadaversaliska[.]info/coflexo.php
canadaversaliska[.]info/ukflexexo.php
canadaversaliska[.]info/ukflexo.php
canadaversaliska[.]info/usflexexo.php
canadaversaliska[.]info/usflexo.php
krostaur[.]com/jpexo.php
krostaur[.]com/jpflexexo.php
krostaur[.]com/jpflexo.php

leiomity[.]com/ukexo.php
leiomity[.]com/ukflexexo.php
leiomity[.]com/usexo.php
leiomity[.]com/usflexexo.php
surdised[.]com/coexo.php
surdised[.]com/usexo.php

Tweets referencing the malsmoke campaign

[https://twitter\[.\]com/MBThreatIntel/status/1245791188281462784](https://twitter[.]com/MBThreatIntel/status/1245791188281462784)
[https://twitter\[.\]com/FaLconIntel/status/1232475345023987713](https://twitter[.]com/FaLconIntel/status/1232475345023987713)
[https://twitter\[.\]com/nao_sec/status/1231149711517634560](https://twitter[.]com/nao_sec/status/1231149711517634560)
[https://twitter\[.\]com/tkanalyst/status/1229794466816389120](https://twitter[.]com/tkanalyst/status/1229794466816389120)
[https://twitter\[.\]com/nao_sec/status/1209090544711815169](https://twitter[.]com/nao_sec/status/1209090544711815169)