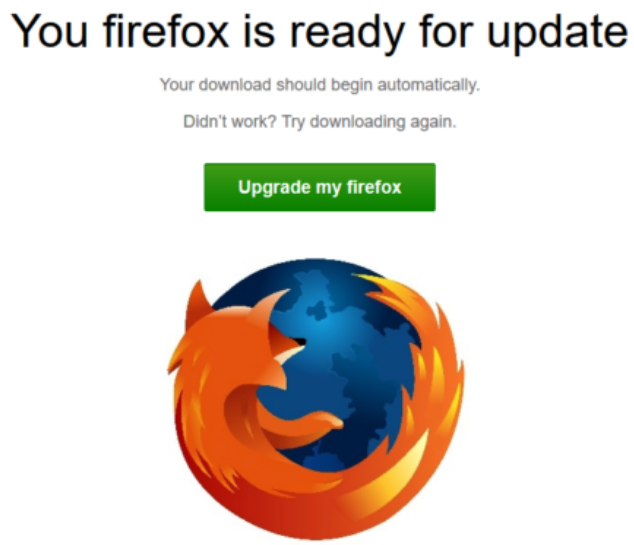
MakeMoney malvertising campaign adds fake update template

blog.malwarebytes.com/threat-intelligence/2022/06/makemoney-malvertising-campaign-adds-fake-update-template/

Threat Intelligence Team June 8, 2022

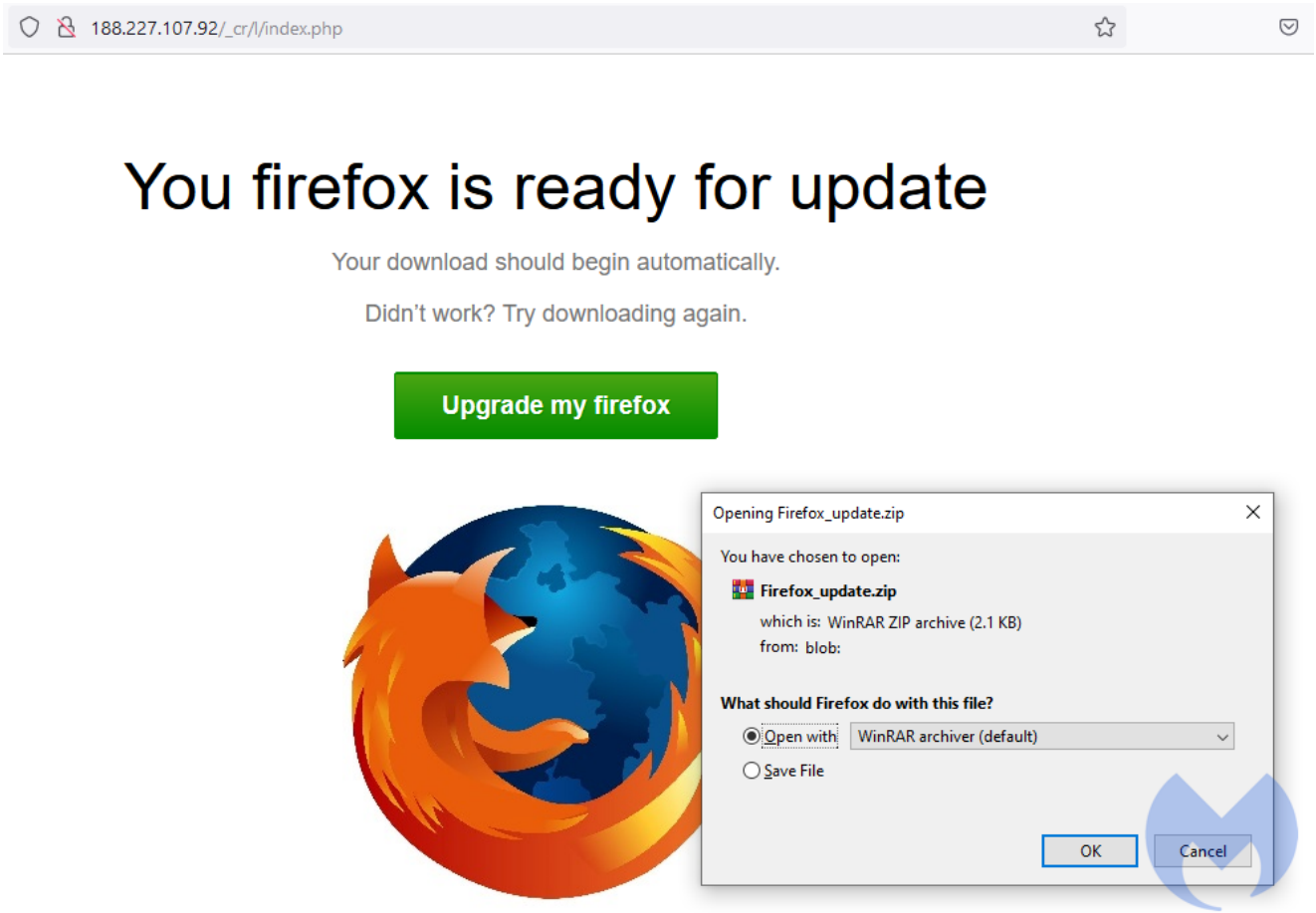


Malware authors and distributors are following the ebbs and flow of the threat landscape. One campaign we have tracked for a numbers of years recently introduced a new scheme to possibly completely move away from drive-by downloads via exploit kit.

In this quick blog post, we will look at this new attack chain and link it with previous activity from what we believe are the same threat actors.

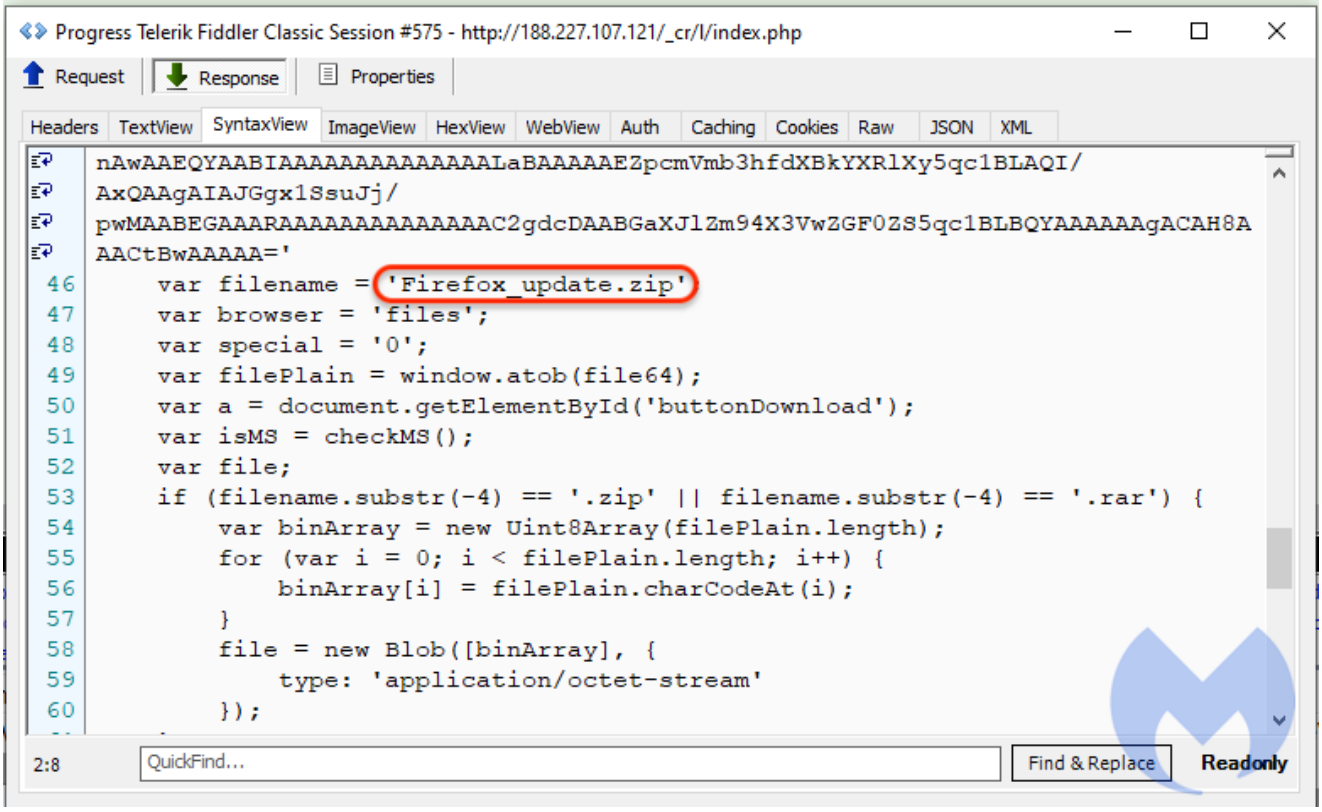
FakeUpdates (SocGholish) lookalike

Our researcher Fillip Mouliatis identified a malvertising campaign leading to a fake Firefox update. The template is strongly inspired from similar schemes and in particular the one distributed by the FakeUpdates (SocGholish) threat actors.



However distribution and implementation are very different. Unlike FakeUpdates which uses compromised websites to push their template, this one is driven via malvertising. Please note the IP addresses involved in the redirection infrastructure as we will come back to them in a moment.

Server IP	Host	URL	Comments
162.252.21.20	safebrowsdv.com	/?r[redacted]	Ad network
2607:fbe0:1:42::17	ladyphapty.com	/b[redacted]	Malvertising
2607:fbe0:1:42::17	ladyphapty.com	/d[redacted]	Malvertising
188.225.75.54	cryptosuite.pro	/cryptoland3	Malicious infrastructure
185.220.33.3	adsinside.xyz	/hilltoplands/	Malicious infrastructure
188.225.75.54	www.usemoney.life	/[redacted]	Malicious infrastructure
188.227.107.121	188.227.107.121	/_cr/l/index.php	Payload



The template itself is much more simplified and appears to be in development with a fake Firefox update that contains a couple of scripts that pull down an encrypted payload. The initial executable consists of a loader which retrieves a piece of Adware detected as BrowserAssistant. This payload was seen before and interestingly through a similar malvertising campaign involving the RIG exploit kit.

MakeMoney connection

The malvertising infrastructure is essentially the same one that was used in numerous drive-by campaigns with exploit kits since late 2019. For some reason the threat actors are reusing the same servers in Russia and naming their malvertising gates after different ad networks.

Security researcher @na0_sec saw the “MakeMoney gate”, named after the domain makemoneywithus[.]work (**188.225.75.54**), redirect to the Fallout exploit kit in October 2020, although it mostly used RIG EK for several years. Probably the earliest instance of this threat group was seen in December 2019 via the gate gettime[.]xyz (**185.220.35.26**).

> #MakeMoney -> #RigEK -> What is this malware?https://t.co/Fdl4PXNsFA pic.twitter.com/q2D4jwneKV
>
> — nao_sec (@nao_sec) November 26, 2020

Looking at this infrastructure shows that the group reused a few servers quite predictably during these years between AS59504 vpsville and AS9123 TimeWeb. For example, gettime[.]xyz was hosted on the same server (185.220.35.26) as makemoneyeazzywith[.]me. Staying with the MakeMoney theme, we see makemoneywith[.]us on 188.225.75[.]54. That server was likely hosting a Keitaro TDS given such hostnames as keitarotrafficdelivery[.]xyz.

There is also activity on **185.220.33.3**, **185.230.140.210** and **188.225.75.54** hosting a number of impersonation hostnames such as magicpropeller[.]xyz (PropellerAds), magicpopcash[.]xyz (PopCash).

> ℹ️ #RIGEK drops #Redline #stealer
>
> 🚨 IOCs 🚨
> Malvertising domains:
> adsterramagic[.]me
> magicadsterra[.]xyz
> 188.225.75[.]54
>
> RIG:
> 45.138.27[.]29
>
> Redline:
> 82dd6739ed808fd3231910c3aebf3ab9001c033cb7d28112174d5a19ab55a51f
> 185.215.113[.]121 pic.twitter.com/Pd6BWNeSfZ
>
> — Malwarebytes Threat Intelligence (@MBThreatIntel) January 18, 2022

We find it interesting that the same threat actors remained faithful to RIG EK for so long during a period where exploit kits were going out of business. They also seemed to poke fun at the same ad networks they were abusing, unless the choice for names associated with their gates was motivated by sorting out their upstream traffic.

We don't believe we have seen the last of this threat group. Having said that, their latest social engineering scheme could use some improvements to remove some blatant typos while their server-side infrastructure could be tidied up.

Indicators of Compromise

IP addresses (malvertising domains, gates)

185.220.35.26
188.225.75.54
185.220.33.3
185.230.140.210

IP addresses (fake template)

188.227.107.121
188.227.107.92

Domains (malvertising domains, gates)

adcashtds2[.]xyz
adcashtdssystem[.]site
adsinside[.]xyz
adsterramagic[.]me
adstexx[.]xyz
allmagnew[.]xyz
alltomag[.]xyz
an-era[.]shop
ankgomag[.]xyz
anklexit[.]online
ankltrafficexit[.]xyz
ankmagicgo[.]xyz
blackexit[.]xyz
ccgmaining[.]life
ccgmaining[.]live
ccgmaining[.]work
clickadusweep[.]vip
clickadusweeps[.]vip
clickadutds[.]xyz
clicksdeliveryserver[.]space
clicktds2[.]xyz
cryptomoneyinside[.]xyz
cryptomoneyinsider[.]biz
cryptomoneyinsider[.]link
cryptomoneyinsider[.]site
cryptomoneyinsider[.]work
cryptomoneyinsiders[.]com
cryptomoneyinsiders[.]site
cryptomoneyinsiders[.]work
cryptomoneytds[.]xyz
cryptopaycard[.]shop
cryptosuite[.]pro

cryptosuitetds[.]com
cryptotraffic[.]vip
cryptotraffictds[.]online
cryptotraffictdss[.]xyz
cryptozerotds[.]xyz
daiichisankyo-hc[.]live
earncryptomoney[.]info
exitmagall[.]xyz
extradeliverytraffic[.]com
extramoneymaker[.]vip
familylabs[.]xyz
fujimi[.]fun

gettime[.]xyz
hilldeliveryexit[.]xyz
hillex[.]xyz
hilllandings[.]xyz
hillmag[.]xyz
hillmagnew[.]xyz
hilltopmagic[.]xyz
hilltoptds[.]xyz
hilltoptdsserver[.]xyz
hilltoptdsservers[.]fun
hilltoptrafficdelivery[.]com
hilltoptrafficdelivery[.]xyz
jillstuart-floranotisjillstu[.]art
k-to-kd[.]me
keitarotrafficdelivery[.]com
keitarotrafficdelivery[.]xyz
lahsahal[.]site
magcheckall[.]me
magicadss[.]xyz
magicadsterra[.]xyz
magicclickadu[.]xyz
magickhill[.]xyz
magickpeoplenew[.]xyz
magicpopcash[.]xyz
magicpropeller[.]xyz
magicself[.]xyz
magiczero[.]xyz
makemoneyeazzywith[.]me
makemoneynowwith[.]me
makemoneywith[.]us

makemoneywithus[.]work
mizuno[.]casa
money365[.]xyz
myallexit[.]xyz
myjobsy[.]com
nawa-store[.]com
newallfrommag[.]xyz
newzamenaadc[.]xyz
newzamenaclick[.]xyz
newzamenaself[.]xyz
newzamenazero[.]xyz
nippon-mask[.]site
northfarmstock[.]xyz
offers[.]myjobsy[.]com

offersstudioex[.]live
openphoto[.]xyz
partners[.]usemoney[.]xyz
prelandingpages[.]xyz
promodigital[.]me
propellermagic[.]xyz
sberbank[.]hourscareer[.]com
sberjob[.]hourscareer[.]com
selfadtracker1[.]online
selfadtrackerexit[.]xyz
selftraffictds[.]xyz
selfyourads[.]xyz
shop[.]mizuno[.]casa
supersports[.]fun
surprise[.]yousweeps[.]vip
tracker[.]usemoney[.]xyz
traffic[.]selfadtracker1[.]online
traffic[.]usemoney[.]xyz
trafficdeliveryclick[.]xyz
trafficdeliveryoffers[.]com
trafficdeliverysystem[.]world
traffictrackerself[.]xyz
tryphoto[.]xyz
trytime[.]xyz
usehouse[.]xyz
usemoney[.]life
usemoney[.]xyz
ymalljp[.]com

yousweeps[.]vip
zamenaad[.]xyz
zamenaclick[.]xyz
zamenahil[.]xyz
zamenazer[.]xyz
zapasnoiadc[.]xyz
zapasnoiclick[.]xyz
zapasnoiself[.]xyz
zapasnoizero[.]xyz
zermag[.]xyz
zernewmagcheck[.]xyz
zerocryptocard[.]shop
zeroexit[.]xyz
zerok2exit[.]xyz
zeroparktraffic[.]xyz
zeroparktrakeroutside[.]shop
zerotdspark[.]space
zerotracker[.]shop

References

https://twitter.com/MBThreatIntel/status/1483235125827571715
https://twitter.com/MBThreatIntel/status/1361824286499950601
https://twitter.com/malware_traffic/status/1412128664721014785
https://twitter.com/malware_traffic/status/1357513424566124548
https://twitter.com/FaLconIntel/status/1351739449932083200
https://twitter.com/tkanalyst/status/1226125887256416256
https://twitter.com/david_jursa/status/1346562997305696262
https://twitter.com/nao_sec/status/1334289601125445633
https://twitter.com/FaLconIntel/status/1298661757943087105
https://twitter.com/nao_sec/status/1294871134001799168
https://twitter.com/david_jursa/status/1232996830520193024
https://twitter.com/david_jursa/status/1229354505583628288
https://twitter.com/nao_sec/status/1211975197219151876