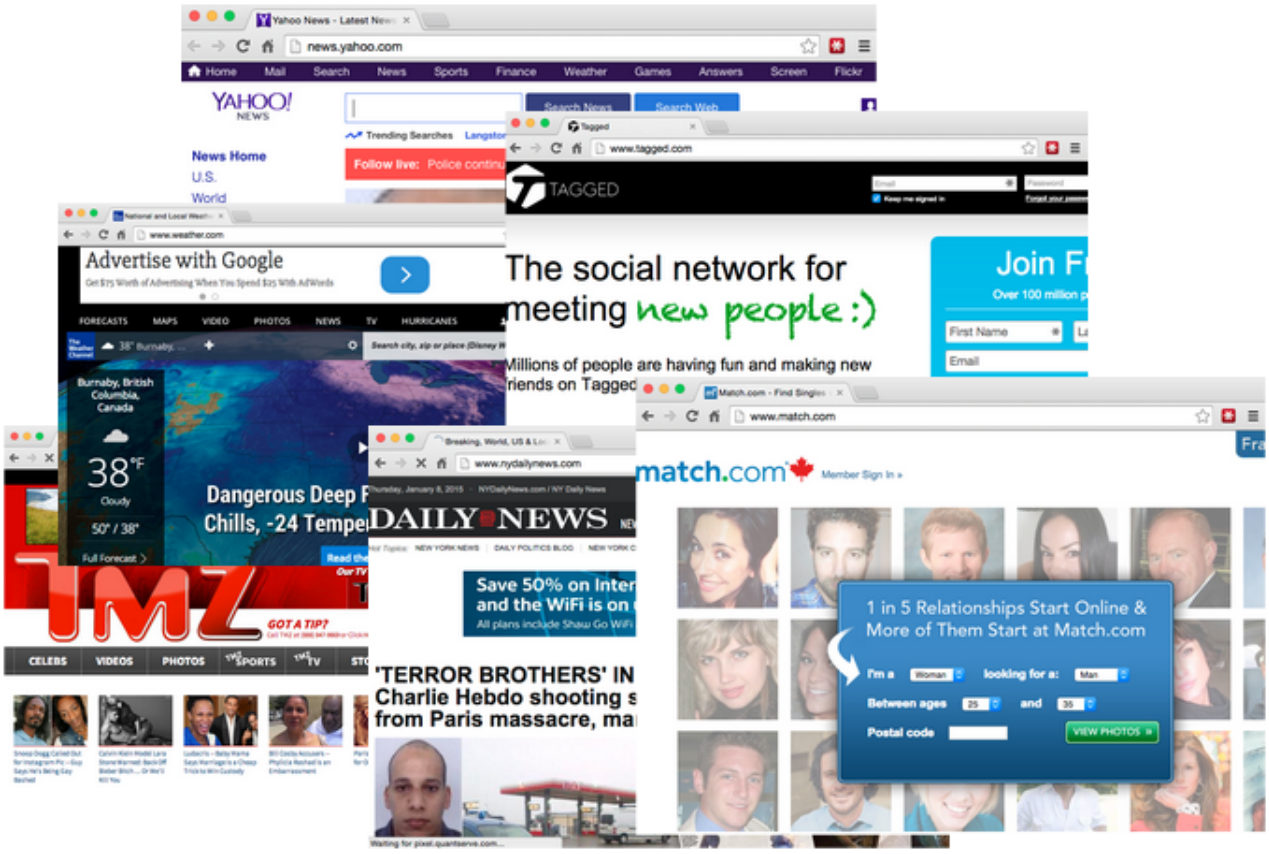
Major malvertising campaign spreads Kovter Ad Fraud malware

blog.malwarebytes.com/threat-analysis/2015/01/major-malvertising-campaign-hits-sites-with-combined-total-monthly-traffic-of-1-5bn-visitors/

Jérôme Segura January 8, 2015



Last year was a busy year for malvertising with top rank ad networks such as Google's DoubleClick caught in large scale attacks, and popular sites unwillingly infecting their visitors because of malicious advertisements.

And 2015 is getting off to a rough start as well.

As Nick Bilogorskiy from Cyphort reported earlier this week, a campaign has been wreaking havoc on sites generating much Internet traffic.

These attacks are the work of the Kovter gang which has been busy hitting major other players (ie. YouTube) during the past year. We tracked this particular campaign as well and have observed several high level domains being victim of malvertising with a combined monthly traffic of 1.5 billion visitors.

People surfing with outdated plugins or browser get infected through a ‘drive-by download’ attack that turns their PCs into bots participating in Ad Fraud.

Affected sites

Domain name	Alexa rank*	Monthly traffic**
news.yahoo.com	65	527
huffingtonpost.com	88	248
aol.com	156	218
weather.com	159	138
sports.yahoo.com	187	188
tmz.com	454	43
nydailynews.com	609	46
tagged.com	611	58
chron.com	736	31
match.com	826	35
legacy.com	1537	22
startribune.com	3648	5
123greetings.com	3854	12
gaiaonline.com	4462	2
beforeitsnews.com	4553	7
intellicast.com	4681	13
mom.me	6515	4
centurylink.net	6580	8
rent.com	12582	2
entertainment.verizon.com	12667	3
windstream.net	12802	3
twincities.com	17457	2

webmail.comcast.net	N/A	N/A
webmaila.juno.com	N/A	3

** Alexa rank based on Alexa.com data. Subdomains' rank checked against SimilarWeb.com*
*** Estimated monthly traffic in millions according to data from SimilarWeb.com*

Ad networks

- **advertising.com**
- **adtech.de**
- **googlesyndication.com**

Intermediate site

foxbusness.com

```
"domain"=>"foxbusness.com", "resolv"=>["176.9.251.252"], "port"=>"443", "uri"=>"/?
serve&id=1347&log=235", "md5"=>"", "header"=>"
 ---- Referer: http://tpc.googlesyndication.com/safeframe/1-0-
1/html/container.html\r\nAccept-Language: en-us\r\nUser-Agent: Mozilla/5.0
(compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)\r\nAccept-Encoding: gzip, deflate
```

Referrers

Examples of direct referrers (IP address: 162.247.13.70 – Canada)

```
uhupa.econsumerproductexposed.swidnica.pl/1141843503/c5893070b1e9a472d191ceb6b65e2d472

choim.vjutakujoho.mazowsze.pl/1144037683/46cab3acbf9a045526dca7c288a3b051064fd23b
keywo.mbaang.olsztyn.pl/1809008432/8eb85bf31fa1e087bd8165bbe8876e32a137fd07
etern.xbkblogueurpro.nysa.pl/849637756/8d75a79e1ee7a789ba8c26ef163fab9a2b81d81d
omais.uacademics.miasta.pl/1111073264/0b457ead38ceaed7d086cea48e2b21a7d264f863
```

```
<html><body><iframe src=
"http://mommy.hmadonnatribe.babia-gora.pl:8080/support/page.php?email=190228&smiles=18&rssscss=2463
73&staff=198517&cityprice=159083&radio=193209"></iframe></body></html>
```

Exploit Kit (Sweet Orange)

Examples of Exploit Kit landing pages (IP address:195.138.246.17 – Germany)

```
forex.dsantanderbillpayment.pruszkow.pl/download/page.php?
vendor=228376&products=105122&smiles=18&back=150083&linktous=3314
vivaw.hloupfute.sanok.pl/link/counter/page.php?
time=254228&cityprice=160825&aboutus=88234&smiles=18&community=158990
georg.tgrupoeroski.ostrowwlkp.pl/server_admin_small/template/dcontent/page.php?
flash=296895&personal=312161&english=311124&downloads=241026&smiles=18&contests=234771

jazzp.yv102.limanowa.pl/notebook/gp/page.php?
events=156334&browse=278551&documents=60024&smiles=18&contests=9009
blaze.vnoeuf.podlasie.pl/cadmins/page.php?
classes=163726&virus=195712&customer=197770&top_left=95496&smiles=18&proxy=198597
```

Sweet Orange landing page source code

The vulnerability exploited was CVE-2014-6332 and Internet Explorer was the target.

Malwarebytes Anti-Exploit blocks this attack:

Payload

The payload, Kovter, gets dropped in the Temp folder:

“C:\Users\{username}\AppData\Local\Temp\repfix.exe”

The payload is VM aware and also looks for debugging and other security tools. One way to know if the sample properly ran is whether it deletes itself after execution or not.

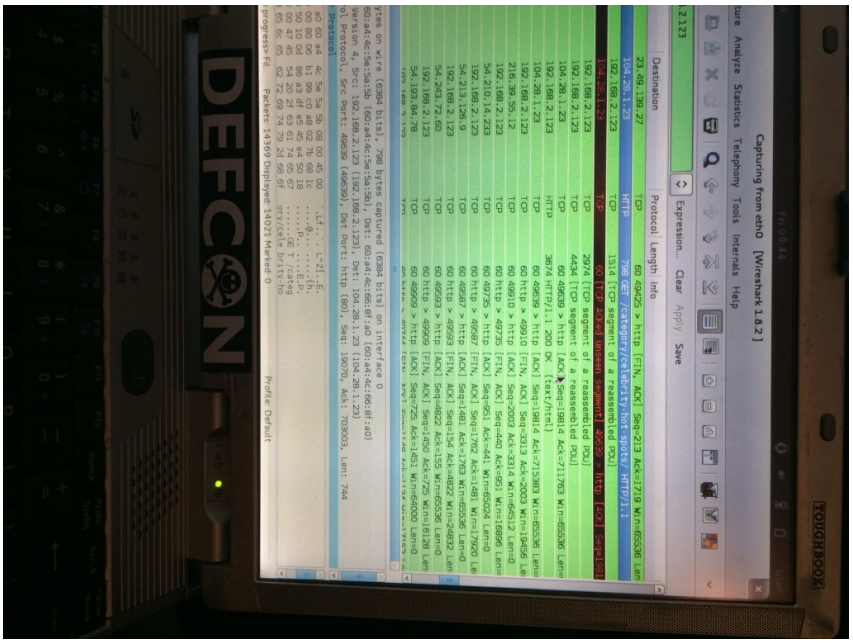
VM or security tools on a real PC:

- Sample does not delete itself
- POST request (domain may change) in this format: (*a16-kite.pw/form2.php*):

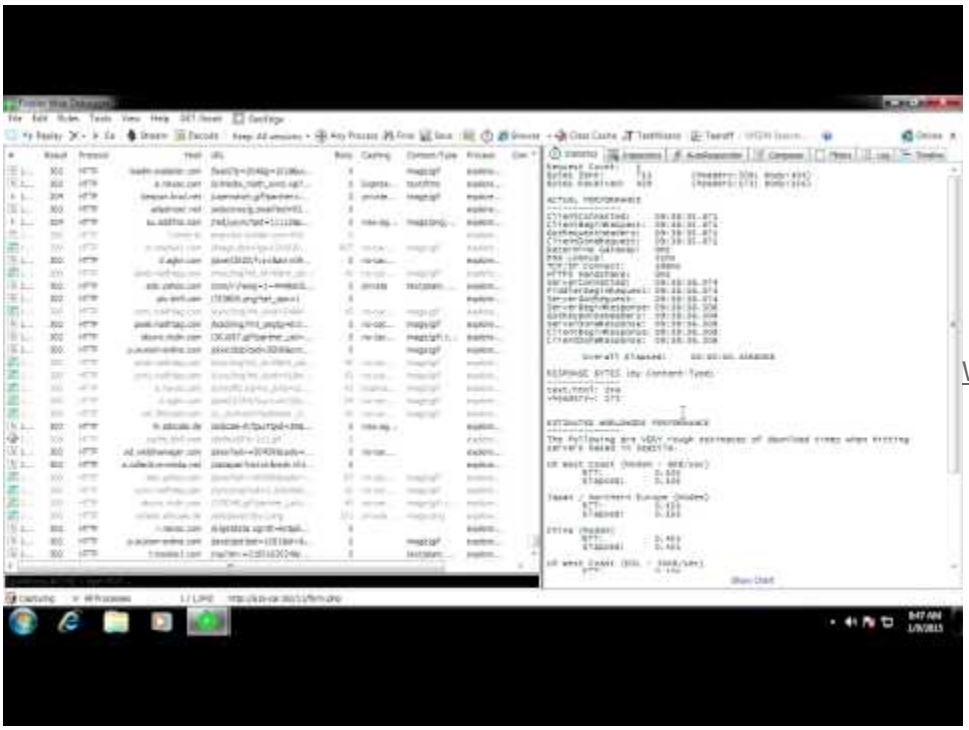
Real machine, no security tools:

- Sample deletes itself
- POST request (domain may change) in this format: *a16.car.biz/11/form.php*

We analyzed this in a real environment using Wireshark on an external laptop to make this completely transparent to the malware. That allowed us to see what it really is: **Ad Fraud** (and not ransomware as reported earlier by other sites)



Shortly after, the flood of ad fraud requests begins:



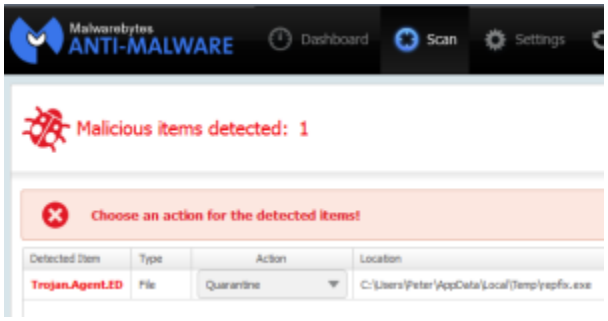
Watch Video At:

https://youtu.be/LIOZyyEumg4

Ad fraud, or also click fraud, account for a large part of the billion dollar ad industry. Ad fraud malware essentially simulates the user visiting pages with adverts as if they were legitimate views.

All these requests are made in the background and game the system while the victim is none the wiser.

Malwarebytes Anti-Malware already detects and blocks this threat:



Malvertising to remain one of the top threats in 2015

As we had said it in our end of year report, malvertising is a huge issue that affects a wide range of people. End users, of course, but also advertisers and publishers who have to fight to defend their legitimacy.

Cyber criminals will likely continue to hijack ad networks with malicious code and pocket the dividends from hundreds of thousands of successful infections.

This particular campaign is likely to migrate to other controllers or evolve into something else since it is now in the public domain and affected parties are cleaning up and securing their systems.

Malwarebytes Labs will continue to monitor the situation and update you on any new developments.

Special thanks to JP Taggart for providing the external recording system.