

Bad Sites Botnets CTO Insights Exploits Internet of Things Mac Malware Mobile Social Spam Targeted Attacks Vulnerabilities

blog.trendmicro.com Sites > TrendLabs Security Intelligence Blog > Bad Sites > Ad Network Compromised, Users Victimized by Nuclear Exploit Kit

May7 Ad Network Compromised, Users Victimized by Nuclear Exploit Kit

11:35 am (UTC-7) | by Joseph C Chen (Fraud Researcher)



MadAdsMedia, a US-based web advertising network, was compromised by cybercriminals to lead the visitors of sites that use their advertising platform to Adobe Flash exploits delivered by the **Nuclear Exploit Kit**. Up to 12,500 users per day may have been affected by this threat; three countries account for more than half of the hits: Japan, the United States, and Australia.

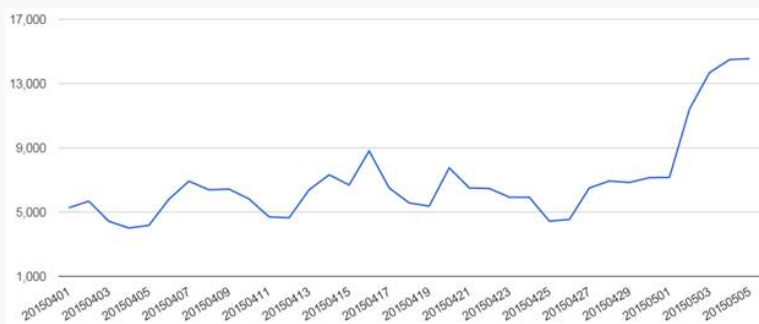


Figure 1. This attack was first seen in April, although at relatively low traffic levels. The number of users at risk grew significantly as May started, with the peak of 12,500 daily affected users reached on May 2.

We initially thought that this was another case of malvertising, but later found evidence that said otherwise. Normal malvertising attacks involve the redirect being triggered from the advertisement payload registered by the attacker. This was not evident in the MadAdsMedia case. What we saw was an anomaly in the URL of their JavaScript library—originally intended to assign what advertisement will be displayed in the client site:

```
GET http://ads-by.madadsmedia.com/tags/25628/10217/async/160x600.js HTTP/1.1
Accept: */*
Referer: http://ads-by.madadsmedia.com/tags/25628/10217/iframe/160x600.html
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident
Accept-Encoding: gzip, deflate
Host: ads-by.madadsmedia.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/0.8.55
Date: Wed, 06 May 2015 08:26:37 GMT
Content-Type: application/x-javascript
Content-Length: 3972
X-Varnish: 256383207 242242650
Age: 46954
Via: 1.1 varnish
X-Cache: HIT

if (!window.ActiveXObject){ document.write("<div style='text-align: center;");
```

Figure 2. The JavaScript library URL serving the JavaScript, as intended

We found in our investigation that the URL didn't always serve JavaScript code, and instead would sometimes redirect to the **Nuclear Exploit Kit** server:



Search our blog:

 Go

## Targeted Attacks



- Identifying and Dividing Networks and Users
- Messaging Application LINE Used as a Decoy for Targeted Attack
- CTO Insights: Defending Your Organization From Insider Attacks

Bookmark the [Threat Intelligence Resources](#) site to stay updated on valuable information you can use in your APT defense strategy

## Recent Posts

- Identifying and Dividing Networks and Users
- Ad Network Compromised, Users Victimized by Nuclear Exploit Kit
- Macro Malware: When Old Tricks Still Work, Part 2

## Calendar

May 2015						
S	M	T	W	T	F	S
3	4	5	6	7	8	2
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

« Apr

## Email Subscription

### Email Subscription

Your email here

Subscribe

## About us



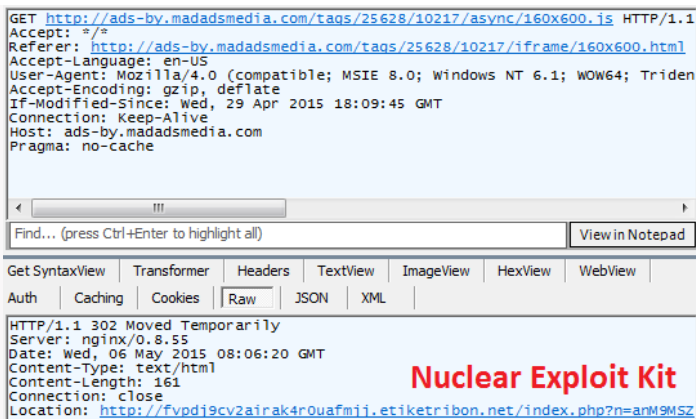


Figure 3. The JavaScript library URL leading to the Nuclear Exploit Kit server

This led us to the conclusion that the server used by the ad network to save the JavaScript library was compromised to redirect website visitors to the exploit kit. MadAdsMedia serves a variety of websites globally, and several of the affected sites appear to be related to anime and manga.

The Flash exploits in use are targeting [CVE-2015-0359](#), a vulnerability that was patched only in [April of this year](#). Some users may still be running older versions of Flash and thus be at risk. The Flash exploits are being delivered by the Nuclear Exploit Kit, a kit that has been [constantly updated](#) to add new Flash exploits and has been tied to [crypto-ransomware](#).

In this case, the final payload of the infection chain we were able to analyze is TROJ\_CARBERP.YVA. [CARBERP](#) malware variants are known for stealing information, specifically for those related to [Russian banks](#). Note however that cybercriminals can choose to change the final payload at any time. We have reached out to MadAdsMedia and fortunately they were quick to investigate and take action on the issue.

#### Solutions and best practices

Attacks like these highlight the importance for ad networks to keep their infrastructure secure from attacks. Making sure that [web servers and applications are secure](#) will help ensure the protection of the business and their customers.

End users, on the other hand, are advised to keep popular web plugins up to date. Users with the latest versions of Adobe Flash would not have been at risk. Monthly Adobe updates are released at approximately the same time as Patch Tuesday (the second Tuesday of each month); this would be a good time for users to perform what is, in effect, preventive maintenance on their machines.

[Trend Micro Deep Security and Vulnerability Protection](#) protect user systems from threats that may leverage this vulnerability. [Trend Micro endpoint solutions](#) additionally protect systems against malware and related attacks.

#### Additional analysis by Brooks Li

**Update as of May 8, 2015, 11:45 PM PDT**

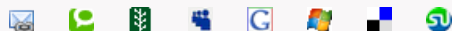
As of this writing, the affected URL is no longer connecting to the Nuclear Exploit Kit.

**Update as of May 8, 2015, 12:15 PM PDT:**

A representative from MadAdsMedia shared their official comment with us regarding this report:

*We launched an investigation shortly after noticing suspicious activity in our network. Soon after, we were contacted by Trend Micro; the details from their research played a crucial role in our efforts to eliminate this threat. We provided Trend Micro's information to our hosting company, GigeNET.com, and they swiftly took action. Within hours, GigeNET identified the breach and simultaneously secured the network. We thank both Trend Micro and GigeNET for their efforts in protecting our users.*

#### Share this article



Get the latest on malware protection from **TrendLabs**



This entry was posted on Thursday, May 7th, 2015 at 11:35 am and is filed under [Bad Sites](#), [Vulnerabilities](#). You can [leave a response](#), or [trackback](#) from your own site.












Disqus seems to be taking longer than usual. [Reload?](#)

[Identifying and Dividing Networks and Users](#)

[Macro Malware: When Old Tricks Still Work, Part 2](#)

#### Other Trend Micro blogs

-  [CTO Insights](#)
-  [CounterMeasures Blog](#)
-  [Cloud Security Blog](#)
-  [Consumerization Blog](#)
-  [Fearless Web](#)
-  [Internet Safety for Kids & Families](#)
-  [Simply Security News](#)
-  [Trend Micro Blog \[German\]](#)
-  [TrendLabs Security Blog \[Japan\]](#)
-  [Cloud Security APAC](#)



Do you have a product-related question? [Visit our eSupport website.](#)