TrendLabs

SECURITY INTELLIGENCE BLOG
Threat News and Information Direct from the Experts

TREND MICRO

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

blog.trendmicro.com Sites > TrendLabs Security Intelligence Blog > Bad Sites > Website Add-on Targets Japanese Users, Leads To Exploit Kit

Aug21

Website Add-on Targets Japanese Users, Leads To Exploit Kit

5:25 pm (UTC-7) | by Joseph C Chen (Fraud Researcher)

Share | Recommend 30 | Tweet

In the past few weeks, an exploit kit known as FlashPack has been hitting users in Japan. In order to affect users, this particular exploit kit does not rely on spammed messages or compromised websites: instead, it uses a compromised website add-on.

This particular add-on is used by site owners who want to add social media sharing buttons on their sites. All the site owner would have to do is add several lines of JavaScript code to their site's design template. This code is freely available from the website of the add-on.

The added script adds an overlay like this to the site's pages:

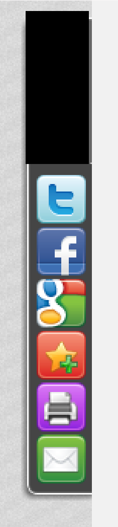

Figure 1. Added share buttons

To do this, a JavaScript file on the home page of the add-on is loaded. This *alone* should raise red flags: it means that the site owner is loading scripts from an *external* server not under their control. It's one thing if it loads scripts on trusted sites like Google, Facebook, or other well-known names; it's another thing to load scripts on little-known servers with no name to protect.

As it turns out, this script is being used for malicious purposes. On certain sites, instead of the original add-on script, the user is redirected to the script of FlashPack, like so:

```
GET http://{add-on domain}/s.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.13)
Gecko/20101203 Firefox/3.6.13
Accept: */*
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: {victimized website}
```

Search our blog:

Go

Targeted Attacks

- BIFROSE Now More Evasive Through Tor, Used for Targeted Attack
- Risks from Within: Learning from the Amtrak Data Breach
- 7 Places to Check for Signs of a Targeted Attack in Your Network

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

Popular Posts

- Netis Routers Leave Wide Open Backdoor
- 7 Places to Check for Signs of a Targeted Attack in Your Network
- New BlackPOS Malware Emerges in the Wild, Targets Retail Accounts

Recent Posts

- ShadowServer Scans Confirm Scale of Netis Threat
- PGP: Not Perfect, But Something To Build On
- Rebuilding Trust: Keeping Your Data Safe

Calendar

September 2014

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

« Aug

```
    Host: {add-on domain}
```

The text above is the HTTP request for the script of the add-on, with the URLs partially obfuscated. Below is the reply from the server:

```
    HTTP/1.1 302 Found
    Date: Thu, 14 Aug 2014 02:39:45 GMT
    Server: Apache/2.2.26 (Unix) mod_ssl/2.2.26 OpenSSL/0.9.8e-fips-rhel5
    mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635
    Location: {exploit kit URL}
    Content-Length: 386
    Connection: close
    Content-Type: text/html; charset=iso-8859-1
```

Note that loading the *s.js* file directly will simply load the "correct" script for the add-on. One site which, if found in the *Referer* header, will trigger the exploit kit is a well-known free blogging site in Japan. The exploit kit delivers various Flash exploits to targeted users; in at least one of these cases a Flash vulnerability (CVE-2014-0497) which was patched in February was used in the attack. We have seen that TROJ_CARBERP.YUG is downloaded onto the affected system.

The attack itself is aimed heavily at Japanese users. At least approximately 66,000 users have been affected by this attack, with more than 87% of these coming from Japan. The landing pages of the exploit kit are hosted in servers in the Czech Republic, the Netherlands, and Russia.

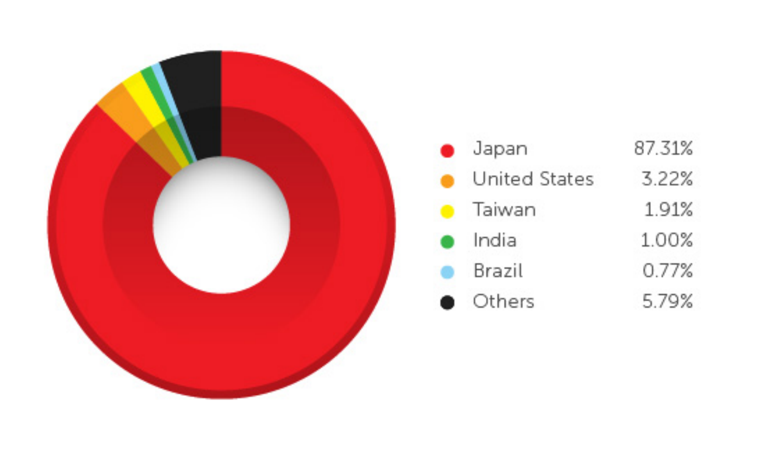

Figure 2. Number of hits by country from August 1 to 17

How can users and site owners prevent these attacks? Site owners should be very cautious about adding add-ons to their site that rely on externally hosted scripts. As shown in this attack, they are trivial to use in malicious activities. In addition, they can slow the site down as well. Alternatives that host the script on the same server as the site itself are preferable.

This incident illustrates for end users the importance of keeping software patched. The vulnerability we mentioned above has been fixed for half a year. Various auto-update mechanisms exist which can keep Flash up to date.

Trend Micro products and solutions block the sites and detect the malicious files that are part of this attack. In addition, the browser exploit prevention technology that is a part of our endpoint solutions is capable of preventing this attack from taking place in the first place.

With additional insights from Walter Liu

Update as of 7:30 PM, August 24, 2014

We updated the total number of affected users by this attack.

Share this article

This entry was posted on Thursday, August 21st, 2014 at 5:25 pm and is filed under Bad Sites, Malware, Vulnerabilities . You can leave a response, or trackback from your own site.

About us

Disqus seems to be taking longer than usual. Reload?

Netis Routers Leave Wide Open Backdoor

Vulnerability in In-App Payment SDKs May Lead to Phishing

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.