Oct14 YouTube Ads Lead To Exploit Kits, Hit US Victims

4:10 am (UTC-7) | by Joseph C Chen (Fraud Researcher)

Malicious ads are a common method of sending users to sites that contain malicious code. Recently, however, these ads have showed up on a new attack platform: YouTube.

Over the past few months, we have been monitoring a malicious campaign that used malicious ads to direct users to various malicious sites. Users in the United States have been affected almost exclusively, with more than 113,000 victims in the United States alone over a 30-day period.

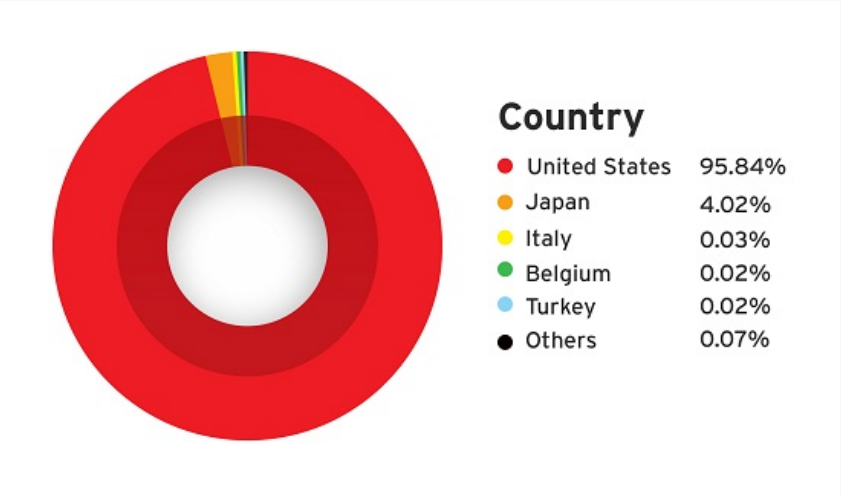


Figure 1. Countries affected by this malicious ad campaign

Recently, we saw that this campaign was showing up in ads via YouTube as well. This was a worrying development: not only were malicious ads showing up on YouTube, they were on videos with more than 11 million views – in particular, a music video uploaded by a high-profile record label.

The ads we've observed do not directly lead to malicious sites from YouTube. Instead, the traffic passes through two advertising sites, suggesting that the cybercriminals behind this campaign bought their traffic from legitimate ad providers.

In order to make their activity look legitimate, the attackers used the modified DNS information of a Polish government site. The attackers did not compromise the actual site; instead they were able to change the DNS information by adding subdomains that lead to their own servers. (How they were able to do this is unclear.)

The traffic passes through two redirection servers (located in the Netherlands) before ending up at the malicious server, located in the United States.

The exploit kit used in this attack was the Sweet Orange exploit kit. Sweet Orange is known for using four vulnerabilities, namely:

- CVE-2013-2460 – Java
- CVE-2013-2551 – Internet Explorer
- CVE-2014-0515 - Flash
- CVE-2014-0322 – Internet Explorer

Based on our analyses of the campaign, we were able to identify that this version of Sweet Orange uses vulnerabilities in Internet Explorer. The URL of the actual payload constantly changes, but they all use subdomains on the same Polish site mentioned earlier. However, the behavior of these payloads are identical.

The final payloads of this attack are variants of the KOVTER malware family, which are detected as TROJ_KOVTER.SM. This particular family is known for its use in various ransomware attacks, although they lack the encryption of more sophisticated attacks like Cryptolocker. The websites that TROJ_KOVTER.SM accesses in order to display the fake warning messages are no longer accessible.

Users who keep their systems up to date will not affected by this attack, as Microsoft released a patch for this particular vulnerability in May 2013. We recommend that read and apply the software security advisories by vendors like Microsoft, Java, and Adobe, as old vulnerabilities are still being exploited by attackers. Applying the necessary patches is essential part of keeping systems secure. Backing up files is also a good security practice to prevent data loss in the event of an attack like this.

In addition to blocking the files and malicious sites involved in this attack, our browser exploit prevention technology prevents attacks that target these vulnerabilities.

With additional insight from Rhena Inocencio

The following hashes are detected as part of this attack:

- 09BD2F32048273BD4A5B383824B9C3364B3F2575
- 0AEAD03C6956C4B0182A9AC079CA263CD851B122
- 1D35B49D92A6E41703F3A3011CA60BCEFB0F1025
- 32D104272EE93F55DFFD5A872FFA6099A3FBE4AA
- 395B603BAD6AFACA226A215F10A446110B4A2A9D
- 6D49793FE9EED12BD1FAA4CB7CBB81EEDA0F74B6
- 738C81B1F04C7BC59AD2AE3C9E09E305AE4FEE2D
- A1A5F8A789B19BE848B0F2A00AE1D0ECB35DCDB0
- A7F3217EC1998393CBCF2ED582503A1CE4777359
- C75C0942F7C5620932D1DE66A1CE60B7AB681C7F
- E61F76F96A60225BD9AF3AC2E207EA340302B523
- FF3C497770EB1ACB6295147358F199927C76AF21

We have already notified Google about this incident.

This entry was posted on Tuesday, October 14th, 2014 at 4:10 am and is filed under Malware . You can leave a response, or trackback from your own site.

MS Zero-Day Used in Attacks Against European Sectors, Industries

Spoofed Apps—a New iOS Concern?

Fake Viber Spam Changes Routines Based on Platform

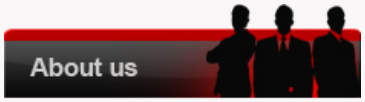
Tracking Activity in the Chinese Mobile Underground

Calendar

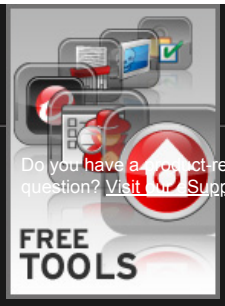
November 2014

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						

« Oct



- 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 Support website.