



Let’s Encrypt Now Being Abused By Malvertisers

- Posted on:January 6, 2016 at 9:49 am
- Posted in:Bad Sites, Malware, Social
- Author:
  Joseph C Chen (Fraud Researcher)

11

Encrypting all HTTP traffic has long been considered a key security goal, but there have been two key obstacles to this. First, certificates are not free and many owners are unwilling to pay; secondly the certificates themselves are not always something that could be set up by a site owner.

The Let’s Encrypt project was founded with the goal of eliminating these obstacles. The project’s goal is to provide free certificates to all site owners; in addition, software could be set up on a web server to make the process as automated as possible. It is backed by many major Internet companies and non-profit organizations – Akamai, Cisco, the Electronic Frontier Foundation (EFF), Facebook, and Mozilla to name a few. Let’s Encrypt only issues domain-validated certificates and not extended validation (EV) certificates, which include additional checks regarding the identity of the site owner.

Unfortunately, the potential for Let’s Encrypt being abused has always been present. Because of this, we have kept an eye out for malicious sites that would use a Let’s Encrypt certificate. Starting on December 21, we saw

activity going to a malvertising server, with traffic coming from users in Japan. This campaign led to sites hosting the Angler Exploit Kit, which would download a banking Trojan (BKDR_VAWTRAK.AAAFV) onto the affected machine.

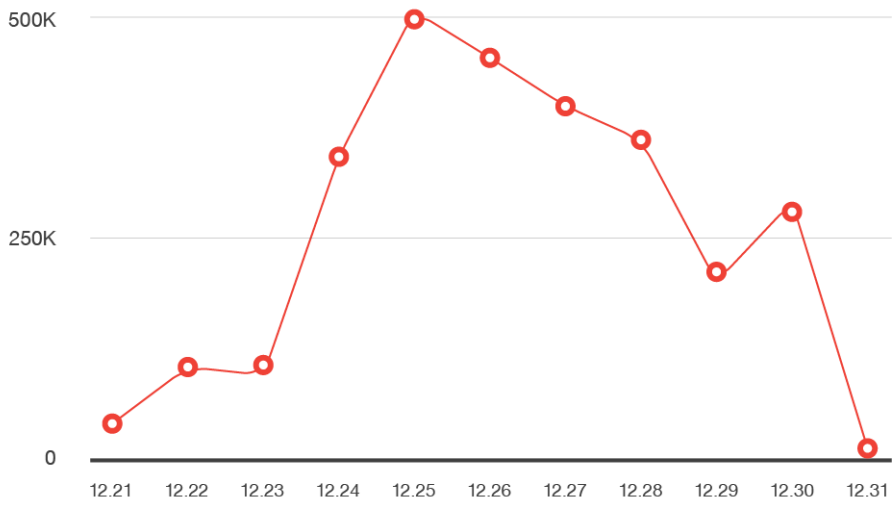

Figure 1. Daily hits to malvertising server

We believe that this attack is a continuation of the same malvertising campaign we first identified in September that also targeted Japanese users.

How was this attack carried out? The malvertisers used a technique called "domain shadowing". Attackers who have gained the ability to create subdomains under a legitimate domain do so, but the created subdomain leads to a server under the control of the attackers. In this particular case, the attackers created *ad.{legitimate domain}.com* under the legitimate site. Note that we are disguising the name of this site until its webmasters are able to fix this problem appropriately

Traffic to this created subdomain was protected with HTTPS and a Let's Encrypt certificate, as shown below:

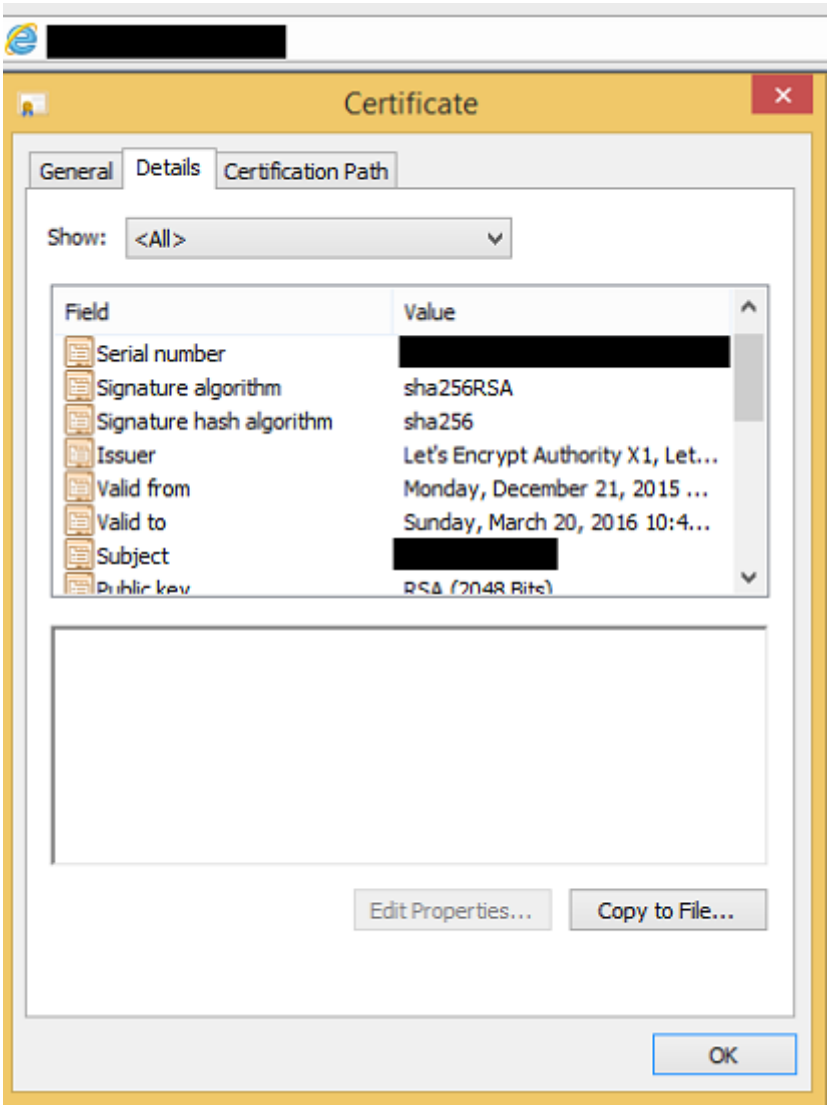

Figure 2. Let's Encrypt SSL certificate

The domain hosted an ad which appeared to be related to the legitimate domain to disguise its traffic. Parts of its redirection script have also been moved from a JavaScript file into a .GIF file to make identifying the payload more difficult. Anti-AV code similar to what we found in the September attack is still present. In addition, it uses an open DoubleClick redirect – a tactic previously discussed by Kafeine of Malware don't need Coffee.

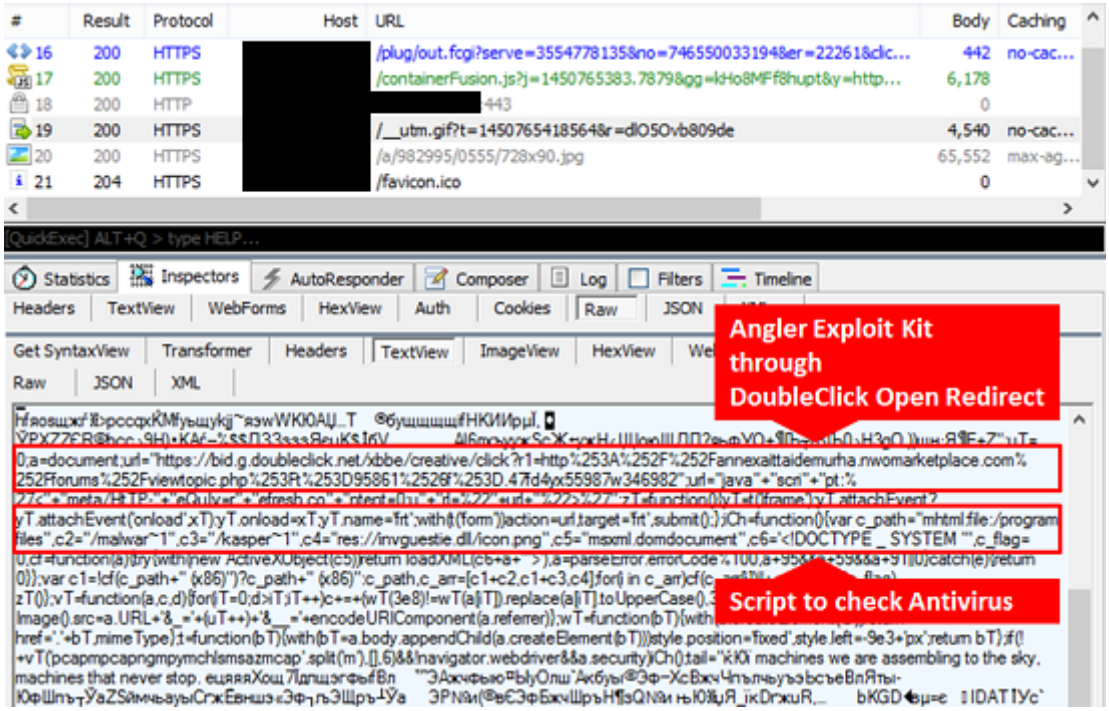

Figure 3. Code used by malvertising

Any technology that is meant for good can be abused by cybercriminals, and digital certificates like those of Let's Encrypt's is no exception. As a certificate authority ourselves we are aware of how the SSL system of trust can be abused. Cases like this one where an attacker is able to create subdomains under a legitimate domain name demonstrate a problem. A certificate authority that automatically issues certificates specific to these subdomains may inadvertently help cybercriminals, all with the domain owner being unaware of the problem and unable to prevent it.

Domain-validation certificates only confirm that the relevant domain is under the control of the site recipient. In theory, this should not validate the identity of the recipient. However, end users less aware of the nuances of certificates may miss the differences, and as a result, these DV certificates can help the hacker gain legitimacy with the public.

While Let's Encrypt has stated that they do not believe CAs should act as a content filter, they do check domains that it issues against the Google safe browsing API.

Ideally, CAs should be willing to cancel certificates issued to illicit parties that have been abused by various threat actors. However, security on the infrastructure is only possible when all critical players – browsers, CAs, and anti-virus companies – play an active role in weeding out bad actors. A key takeaway from the malvertising incident is that website owners should ensure that they secure their own website control panels, to ensure that new subdomains beyond their control are not created without their knowledge.

At the same time, users should also be aware that a "secure" site is not necessarily a safe site, and we also note that the best defense against exploit kits is still keeping software up-to-date to minimize the number of vulnerabilities that may be exploited.

We have notified Let's Encrypt about this particular certificate being abused.

Indicators of compromise

The payload of the Angler Exploit Kit has the following SHA1 hash:

- 63c88467a0f67e2f3125fd7d3d15cad0b213a5cb

With additional insights by Kirk Hall and Stephen Hillier

Updated on January 7, 2016, 3:20 AM PST (UTC -8): *We have updated this entry to clarify our mention of Let's Encrypt in relation to the reported malvertising incident and in response to the points raised by security researcher Ryan Hurst about CAs. Let's Encrypt was the CA used in this case, but other CAs may be abused by other threat actors to launch similar attacks. We also clarified our positions regarding DV certificates, and reworded the last paragraph to emphasize the value of holistic solution and security posture in all aspects of an infrastructure.*

Related Posts:

- **Extended Validation Certificates: Warning Against MITM Attacks**
- **TROJ_WERDLOD: New Banking Trojan Targets Japan**
- **Digital Certificates: Who Can You Trust?**
- **OpenSSL CVE-2015-1793: Separating Fact from Hype**

Tags: Let's Encryptmalvertising

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

- A Case of Too Much Information: Ransomware Code Shared Publicly for "Educational Purposes", Used Maliciously Anyway
- January Patch Tuesday: Support Ends for Windows 8, Limited for Older IE Versions; 17 Adobe Flaws Resolved
- Think, Learn, Act – Training for Aspiring Cyber Criminals in the Brazilian Underground

- Android-based Smart TVs Hit By Backdoor Spread Via Malicious App
- Let's Encrypt Now Being Abused By Malvertisers

2016 Security Predictions

- From new extortion schemes and IoT threats to improved cybercrime legislation, Trend Micro predicts how the security landscape is going to look like in 2016.
  Read more

Popular Posts

Let's Encrypt Now Being Abused By Malvertisers
Hacking Team Flash Zero-Day Integrated Into Exploit Kits
Android-based Smart TVs Hit By Backdoor Spread Via Malicious App
Cybercriminals Improve Android Malware Stealth Routines with OBAD
Operation Black Atlas, Part 2: Tools and Malware Used and How to Detect Them

Latest Tweets

- Here are some #fastfacts about the recent Hyatt #databreach: bit.ly/1RpkS08

about 4 hours ago

- Surprisingly, #ransomware isn't a common threat in Canada: bit.ly/1OJNNd2
  about 5 hours ago
- What is business email compromise? bit.ly/111WinS #infosec
  about 10 hours ago

Stay Updated

Email Subscription

Your email here

Subscribe