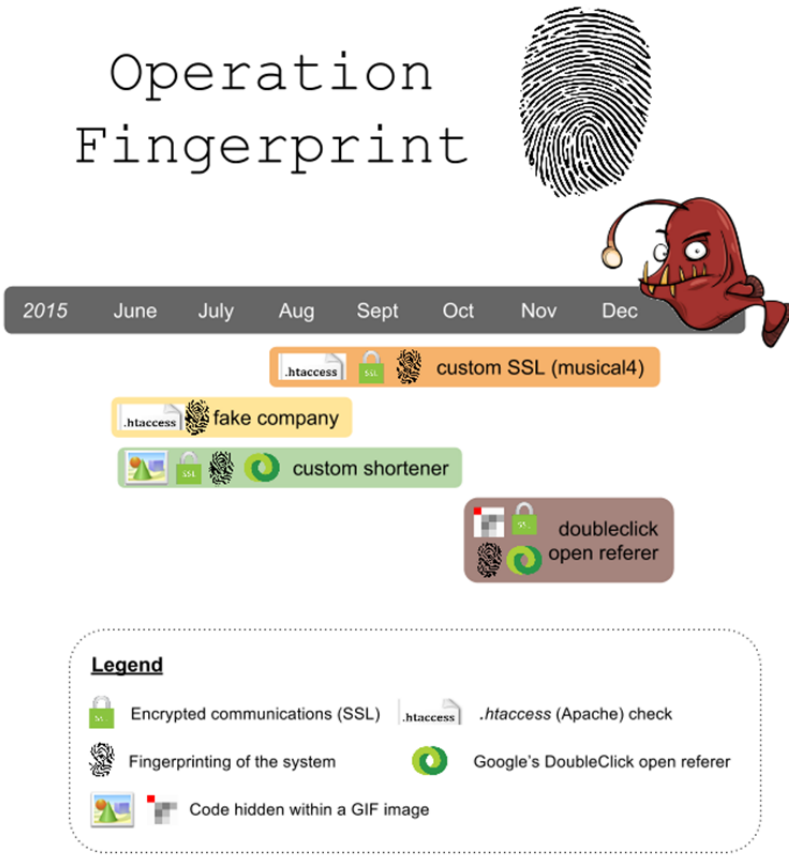
Operation Fingerprint

A look into several Angler Exploit Kit malvertising campaigns

Jérôme Segura, Malwarebytes | Eugene Aseev, GeoEdge

Overview

This paper is the result of several months of researching and monitoring malvertising campaigns that we have observed affect thousands of publishers and dozens of ad networks. The goal of this research is to summarize some of the malvertising campaigns we have seen and give numbers to quantify their impact. While some of those incidents have ceased, others are still ongoing and the threat actors responsible for them are very successful at bypassing most ad quality and security checks.



Fingerprinting: From Exploit Kit to (rogue) advertiser

One of the newest evasion techniques being used by cybercriminals is fingerprinting, a way to check potential victims' computers with snippets of code injected directly into the ad banner. This code can quickly rule out non-viable targets, such as honeypots set up by malware researchers to detect malware or security companies performing ad check validation. Fingerprinting joins a growing arsenal of tactics developed by cybercriminals to avoid discovery by security researchers.

The notion of fingerprinting is not new. But what this research has uncovered is that fingerprinting has moved up the chain, no longer simply at the exploit kit (EK) level, but also at the malvertising phase, thanks to online ads.

With some rare exceptions (including the mimetype check[1]), fingerprinting techniques have been employed by exploit kits[2] like Angler for some time, thanks in part to a vulnerability in Internet Explorer's XMLDOM ActiveX control (CVE-2013-7331).

This flaw allows attackers to enumerate the local file system and look for the presence of certain clues that might identify a machine belonging to a security researcher or acting as a honeypot.

The fingerprinting techniques (coupled with geolocation and IP checks) are effective but happen low down the infection chain. It only made sense to add them at the traffic redirection phase to ensure only "qualified" users were being redirected to exploit kits.

Fingerprinting represents the next step in malvertising attacks, where bogus advertisers are analyzing potential victims and either showing a benign ad or an ad laced with malicious code that ultimately redirects to an exploit kit.

The campaigns

Fake company campaign

This campaign used stolen websites that were slightly rebranded to appear like legitimate companies. Although it did not appear to use the traditional fingerprinting method via the XMLDOM flaw, it had custom filters for those who see the malicious code and those who only see a benign advert.

The redirection mechanism was made possible by a core Apache server component called the .htaccess file, which allows criminals to specify who received the malicious redirection in addition to having their IP logged to a blacklist.

Specifically, certain IP addresses belonging to VPN providers can easily be added to prevent security researchers from replaying the attack.

1 - Jérôme Segura, Malwarebytes, https://blog.malwarebytes.org/wp-content/uploads/2014/11/sourcecode2.png
2 - Kafeine, "CVE-2013-7331 and Exploit Kits" http://malware.dontneedcoffee.com/2014/10/cve-2013-7331-and-exploit-kits.html

Custom SSL (musical4) campaign

This campaign leveraged the CloudFlare infrastructure to hide the malicious server's IP in addition to connection via SSL, which encrypts communications. The server performed a check to ensure visitors were genuine before launching a redirection to Angler EK landing pages.

Fingerprinting code was hidden within the fake advertiser's JavaScript. The code was checking for the presence of security products by trying to identify if the Virtual Keyboard Plugin, used in many Kaspersky products, was installed. If one was found, the malicious redirection would not happen.

Custom URL shortener campaign

This campaign is one of the first attacks that hid the fingerprinting payload within a GIF image served over HTTPS. This was intended to throw off security researchers and users who might be looking for a specific type of file that indicates malicious content.

In addition to the use of GIFs, this campaign also employed shortened URLs to add an extra layer of complexity to the infection chain.

DoubleClick Open Referer campaign

This is the latest and most advanced fingerprinting campaign. While the code is still hidden within a GIF image, it is now encoded with a special key, only provided once per IP address, and embedded in a JavaScript sequence. New fake advertiser domains (nginx servers) are created on a regular basis, many of them using CloudFlare and employing proxies for domain registration.

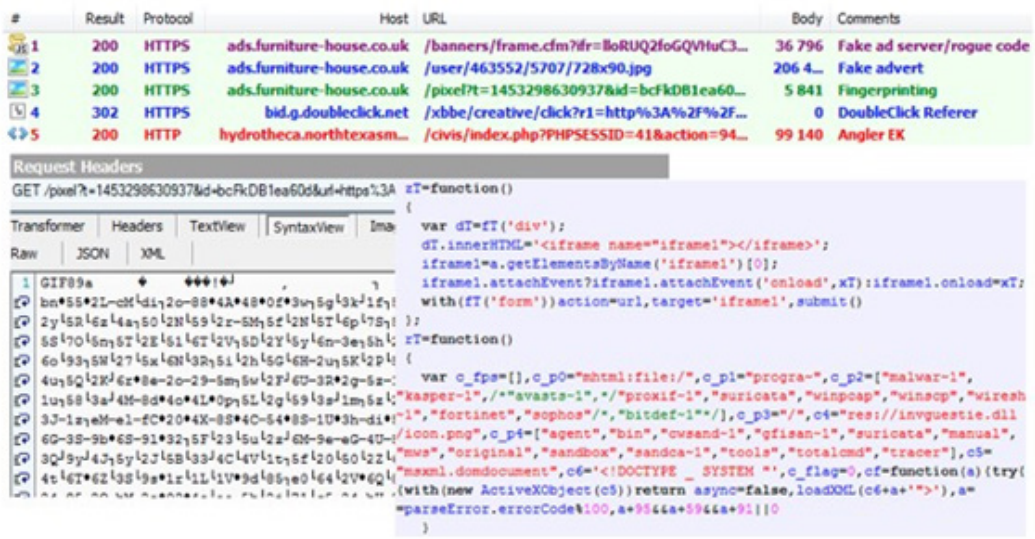
Connecting the dots

All the campaigns share the same basic methodology. They:

- used advertisement-related domain names and URL paths;
- used an intermediate redirector;
- had a once-per-IP delivery;
- served Angler EK in the end.

Stealth techniques

On the top of the feature stack already mentioned, some campaigns included additional layers to prevent detection by security researchers. Let's take the DoubleClick campaign as an example:



If a user's browser passed the initial IP and HTTP header-based checks, a GIF file was loaded. In the request URL for the GIF file, we could see the visitor's system details, for example, their OS, browser type, and preferred language. This information was probably used by attackers to accumulate statistics.

Fingerprinting code checked for the presence of security products from Malwarebytes, Kaspersky, TrendMicro, and Invincea using the Internet Explorer information disclosure vulnerability found in versions of Internet Explorer 10 and below. If no security products were found, a redirect to an Angler EK landing page occurred.

To summarize, the following requirements needed to be fulfilled in order to encounter the actual exploits versus the non-malicious banner:

1. Unique IP address
2. Internet Explorer browser, version 10 and below
3. No security products from the list above installed

The choice of security products to check was most likely based on detection quality. It seemed that most other security vendors were incapable of catching exploit attempts as proactively. This allowed criminals using malvertising to stay under the radar for long periods of time.

We constantly monitor ongoing malvertising campaigns and see how their tricks evolve. They are becoming more complex, and we will be covering this evolution in future publications.

Protecting your end users

At Malwarebytes, our primary goal is to protect and inform users about the latest threats. It is obvious that malvertising has become a major issue that no one has a clear answer for. However, there are steps you can take to mitigate the problem and protect your end users.

Perhaps the greatest protection against malvertising is addressing what it ultimately redirects to: exploit kits. Malwarebytes Endpoint Security employs anti-exploit technology that blocks unknown and known exploits before they can deliver malicious code and compromise your network.

In addition to exploits, some cases of malvertising lead to scams. For example, users are socially engineered into installing bogus video players or plugins. These programs are typically bundled with toolbars, adware and, countless other unwanted pieces that end up slowing down computers. Malwarebytes Endpoint Security employs a very aggressive approach to detecting these kinds of potentially unwanted programs (PUPs) and, in doing so, allow users to regain control of their systems.

About Malwarebytes

Malwarebytes provides software designed to protect businesses and consumers against malicious threats that escape detection by traditional antivirus solutions. Founded in 2008, Malwarebytes is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts. For more information, please visit us at www.malwarebytes.com.

About GeoEdge

GeoEdge's holistic security solution protects your brand and your users from much more than malware. With advanced safeguards in place, you can finally eliminate dynamic security threats from third-party demand partners. GeoEdge keeps your users protected and prevents malicious activities from jeopardizing your immediate ad revenues.