SIGN IN

RISK ASSESSMENT —

Millions exposed to malvertising that hid attack code in banner pixels

Manipulated images are almost impossible to detect by the untrained eye.

DAN GOODIN - 12/6/2016, 2:16 PM

Millions of people visiting mainstream websites over the past two months have been exposed to a novel form of malicious ads that embed attack code in individual pixels of the banners.

FURTHER READING
Steganography: how al-Qaeda hid secret documents in a porn video

Researchers from antivirus provider Eset said "Stegano," as they've dubbed the campaign, dates back to 2014. Beginning in early October, its unusually stealthy operators scored a major coup by getting the ads displayed on a variety of unnamed reputable news sites, each with millions of daily visitors. Borrowing from the word steganography—the practice of concealing secret messages inside a larger document that dates back to at least 440 BC—Stegano hides parts of its malicious code in parameters controlling the transparency of pixels used to display banner ads. While the attack code alters the tone or color of the images, the changes are almost invisible to the untrained eye.

Enlarge / Left: Clean picture; middle: picture with malicious content; right: malicious version enhanced for illustrative purposes.

The malicious script is concealed in the alpha channel that defines the transparency of pixels, making it extremely difficult for even sharp-eyed ad networks to detect. After verifying that the targeted browser isn't running in a virtual machine or connected to other types of security software often used to detect attacks, the script redirects the browser to a site that hosts three exploits for now-patched Adobe Flash vulnerabilities.

"We can say that even some of the other major exploit kits, like Angler and Neutrino, are outclassed by the Stegano kit in terms of referrals—the websites onto which they managed to get the malicious banners installed," Eset researchers wrote in a report published Tuesday. "We have observed major domains, including news websites visited by millions of people every day, acting as 'referrers' hosting these advertisements. Upon hitting the advertising slot, the browser will display an ordinary-looking banner to the observer. There is, however, a lot more to it than advertising."

The ads promote applications calling themselves "Browser Defence" and "Broxu" and targeted people who visited the news sites using Internet Explorer browsers. The script concealed in the pixels exploited a now-patched IE vulnerability indexed as CVE-2016-0162 to obtain details about the visitors' computers. Among other things, the script checked for the presence of packet capture, sandboxing, and virtualization software and a variety of security products. Machines that didn't exhibit signs of the software and contained a vulnerable version of Flash were then redirected to the exploit site, which would serve one of two families of malware. The Ursnif family is made up mainly of modules for stealing e-mail credentials, logging keystrokes, taking screenshots and videos, and acting as a backdoor. The Ramnit variety of malware offers most of the same capabilities and mainly targets the banking industry.

The attackers took extra pains to ensure the machines being infected didn't belong to security-savvy people who might detect what was happening. In addition to a check carried out by the script embedded in the ad, a separate check was carried out by the exploit server before going through with the attack. The Eset report didn't identify any of the sites that delivered the malicious ads. It did say that the people exposed were concentrated in Canada, the UK, Australia, Spain, and Italy, which are the countries served by the affected ad networks. Earlier versions of the campaign from 2014 and 2015 targeted people in the Netherlands and the Czech Republic. The Flash vulnerabilities exploited included CVE-2015-8641, CVE-2016-1019, and CVE-2016-4117.

Update: To execute the hidden payload, the malicious ads load a heavily modified version of Countly, an open-source package for measuring website traffic. That JavaScript extracts the hidden code out of the image and executes it. Because there's nothing per se malicious in the JavaScript, ad networks fail to detect what's happening. Referring to an ad located at hxxps://browser-defence.com/ads/s/index.html?w=160&h=600, Eset researchers described it this way:

> The index.html loads countly.min.js and feeds the initial parameters to the script. This countly, however, is not the stock library of the open source mobile & web analytics platform you would download from github. It is a heavily modified and obfuscated version, with some parts deleted and interlaced with custom code. This custom code is responsible for an initial environment check. Information about the environment is reported back to the server as XOR-encrypted parameters of the 1x1gif file, as captured in the image above.
>
> The following information about the environment is sent:
> `systemLocale^screenResolution^GMT offset^Date^userAgent^pixelRatio`
>
> After that, the script will request the advertising banner. The server will reply with either a clean or a malicious version, most likely also depending on the previous environment check.
>
> The script will then attempt to load the banner and read the RGBA structure. If a malicious version of the image was received, it will decode some Javascript and variables from the alpha channel
>
> The steganography is implemented in the following way: Two consecutive alpha values represent the tens and ones of a character code, encoded as a difference from 255 (the full alpha). Moreover, in order to make the change more difficult to spot by naked eye, the difference is minimized using an offset of 32.

Researchers from Eset competitor Malwarebytes have published their own write-up of the campaign, which they are calling AdGholas.

Despite targeting only people using IE and unpatched versions of Flash, Stegano is noteworthy for its concealment of exploit code in the pixels of the banner ads. There's no reason future campaigns—or possibly ongoing ones that have yet to be discovered—couldn't exploit zero-day vulnerabilities that infected a much larger base of people. Until ad networks get much better at detecting malvertising campaigns, the scourge is likely to continue.

FURTHER READING
Big-name sites hit by rash of malicious ads spreading crypto ransomware [Updated]

Promoted Comments

The God on Kobol / Wise, Aged Ars Veteran

JUMP TO POST

> adamsc wrote:
> The article didn't make that point clear, probably because the linked blog post had a confusing intro as well, but the browser isn't executing images: rather, the first stage exploit reads the pixel values from the image and executes code if it contains a payload. The server decides whether to serve the clean images or an exploit based on things like the reported browser and OS.

Which is pretty sneaky. I wonder how much of that lent this to being undetected for so long.

234 posts | registered 10/7/2016

---

mrsifter / Smack-Fu Master, in training

JUMP TO POST

> Coriolanus wrote:
>
> > show nested quotes
>
> I mean, I understand that this is a bug, but aren't alpha channels for a pixel just a number defining how transparent that pixel is, when it's above another pixel? I'm genuinely baffled how someone was able to trick a browser to run a script that is either entirely within the alpha channel itself, or run a script that was able to use the numerical values of the alpha channels within a picture to run the exploit.

In the actual report http://www.welivesecurity.com/2016/12/0 ... cious-ads/, it mentions that the initial ad loads some javascript disguised as countly.js (which is a metrics tracking app for advertisers). This javascript is what the browser executes, and this javascript is what pulls the hidden code out of the image. The javascript itself doesn't contain any exploits, so it is much harder for ad networks to detect there is an issue.

2 posts | registered 4/28/2014

Andy Haveland-Robinson / Smack-Fu Master, in training

JUMP TO POST

Javascript is anything but a simple scripting language!
It can be as complex as the warped imagination of the programmer.

I spend a lot of time reverse engineering malicious js code to extract and report payload urls distributing ransomware and other nasties.

The level to which they can take the complexity of code can be breathtaking and take hours to dissect manually.
However, all their genius amounts to nothing when I run the code on my js vm, and the urls just appear by magic in milliseconds.
Every other day they'll throw a curveball, and some tweaking to the script or deobfuscator needs doing.
Some people like crosswords, I like doing this for the intellectual challenge, helping to keep our net clean and helping to stop people from getting stiffed, whether they realize it or not.

I run exclusively on Linux Fedora and have never worried about malware personally for over a decade. I humbly suggest that people consider using an operating system that is completely immune to the vast majority of Windows-based attacks, and it is free.

If most of what you do on your computer is browsing the net, then using Linux is the safest.
Keep a separate Linux machine specifically for shopping/banking etc, and regularly updated, and you should almost never have to worry about being compromised, ever.

57 posts | registered 12/18/2008

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 149

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

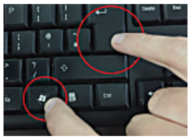
Related Stories

Sponsored Stories

Powered by

Son dismembers parents, dissolved bodies in acid
Washington Post Video

39 Mob Photos That Will Make Your Skin Crawl
historicalpast



Do This Every Time You Turn On Your Computer...
Web Life Advice

The Glorious Dell 43-inch Monitor: Living with Monitor Lust
Techspective

A Mind-Blowing 10% Cash Back Card Has Arrived (See Terms)
Credit Cards

20 Worst Dog Foods of 2016
Puppy Toob

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS