A Security Paper by GeoEdge

Security Aspects of Flash, HTML5, and Video in the Ad Tech Industry

About Us

GeoEdge is the premier provider of ad security and verification solutions for the online and mobile advertising ecosystem. The company ensures high ad quality and verifies that sites and apps offer a clean, safe, and engaging user experience. GeoEdge guards against malware (malvertising), non-compliance, inappropriate content, data leakage, operational, and performance issues.

Leading publishers, ad platforms, exchanges, and networks rely on GeoEdge's automated ad verification solutions to monitor and protect their ad inventory. To find out how GeoEdge can enhance your quality assurance and verify your online and mobile campaigns, head to **www.geoedge.com**

If you want to learn more, head over to www.geoedge.com.

With the Death of Flash, Are Video Ads Safe from Malvertising?

Introduction

For the last several years, Adobe Flash has been an enemy of the online community. In general, the position is well deserved: there were more than 300 vulnerabilities found in Flash Player during 2015 alone, making it the most vulnerable PC software of the year. In 2016, Flash continues to hold that privileged position, sharing it with its brother, Adobe AIR, a system created for cross-platform mobile and desktop applications. These vulnerabilities have been, and continue to be, heavily used by attackers in some of the most dangerous and prevalent web attacks today. The weapon of choice for such attacks is known as an exploit kit, which silently attacks users and attacks malicious software on their endpoints (the user's computer).

In direct contrast to Flash, the community has confidence in HTML5, which is being intensively pushed forward by major digital companies like Google, Amazon, and other big players. They consider HTML5 as the more secure and less resource-greedy alternative. Microsoft has also joined the movement recently by adding the Flash auto-pause in their Edge browser.

Since there are many proponents pushing for Flash to be prohibited from use in an ad creative, with HTML5 as it replacement, this begs the question: Will the use of HTML5, in place of Flash, prevent malvertising attacks?

HTML5 vs. Flash

Before we delve into the logistics of replacing one technology with another, let's review the reasons why developers prefer one technology over the other. Below is a feature comparison:

- **Size:** HTML5 ads are larger in file size than Flash-based ads. This is because HTML5 ads include the backup images, click tags/codes and other elements. Flash ad sizing, however, is based on the creative size only. Because of this, HTML5 ads are around 100Kb larger.
- **Cost:** Constructing Flash ads can be costly. You have to create a Flash ad for every possible size placement. Once you create an HTML5 ad, the ad is responsive to all possible sizes.
- **Convenience:** Unlike Flash, which requires a dedicated plug-in, HTML5 can render multimedia content easily without plugins or player applications. However, the downside to this is that some older browsers do not support HTML5.
- **Picture Clarity:** Flash has greater image clarity, as it can offer sub-pixel support. This results in crisper images. HTML5 can lead to inconsistency and unreliability in display.
- **Mobile Support:** HTML5 offers better support for mobile sites. Flash is PC-based only, giving HTML5 a large advantage over Flash as we move into an era of mobile-web accessibility. HTML5 offers much better cross-device support.
- **Development Resources:** Flash has a large resource pool and even larger community, whereas HTML5 is still a fairly new technology with a growing community and some still-prevalent inconsistencies and support issues.
- **Parent Company:** Flash is not an open standard; it is controlled by ADOBE systems. HTML5 is largely controlled by the Web Hypertext Application Technology Working Group (WHATWG), managed by Mozilla, Opera Software and Apple.

- **Optimization:** Flash provides automatic optimization and compiles everything into a single compact file. HTML5 currently offers no optimization. However, HTML5 ads can be packaged and delivered optimally as long as special attention is paid to their packaging.
- **Usability:** HTML5 requires considerably lower processing power than Flash. This is a great advantage to companies who want to be visible on mobile devices.
- **Semantic Elements:** In HTML5, semantic elements follow the HTML language's use of the semantic meaning of the information in webpages and web applications. This is an improvement over the use of non-semantic elements, i.e. , , etc, to define web presentation. This results in faster processing. Flash does not provide this level of semantic functionality, and so does not benefit from the resulting performance improvements.
- **Security:** Flash vulnerabilities allow for malicious software to install on a user's computer silently. Currently, HTML5 has no vulnerability that would allow malicious software to install on a user's computer silently. HTML5 alerts the user whenever an install attempt is made.

As you can see, there are some advantages to Flash-based ads. However, in terms of security, HTML5 is the more secure option.

Overview of a Malvertising Attack in a Video Ad

There are three stages for the video ad lifecycle in a malvertising attack:

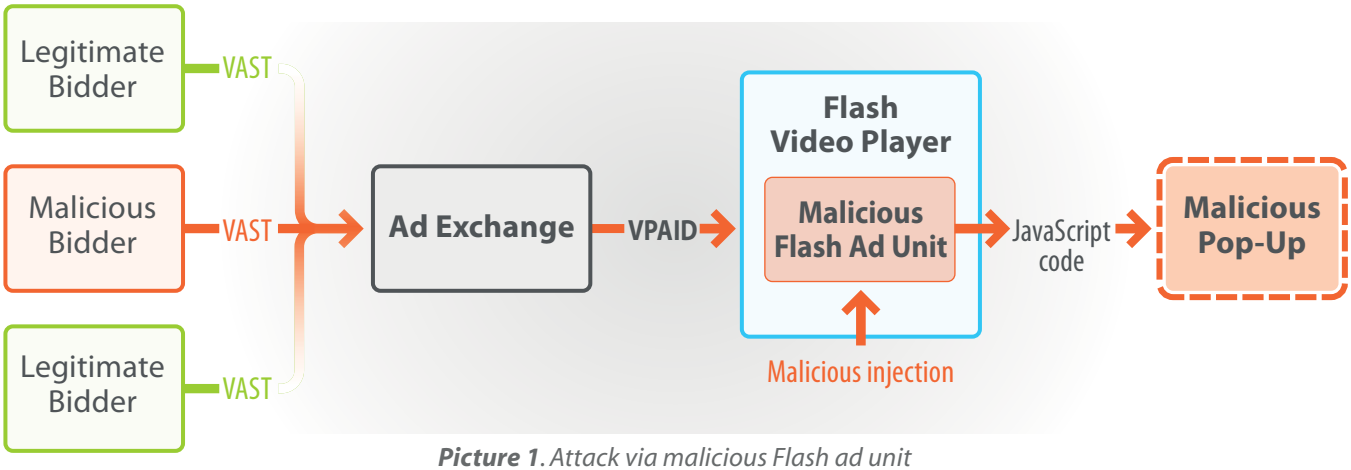
1. Ad Creation: Building the ad
2. Ad Delivery: Serving of the ad
3. Infection Procedure: Performing malvertising objectives, aka installing malware onto the user's computer

The proponents pushing for Flash to be prohibited from use in an ad creative are saying that HTML5 is the remedy that can handle security threats in the advertising industry. It stands to reason that if the ad unit itself is clean, then the user won't have any problems. Unfortunately, this is an inaccurate statement.

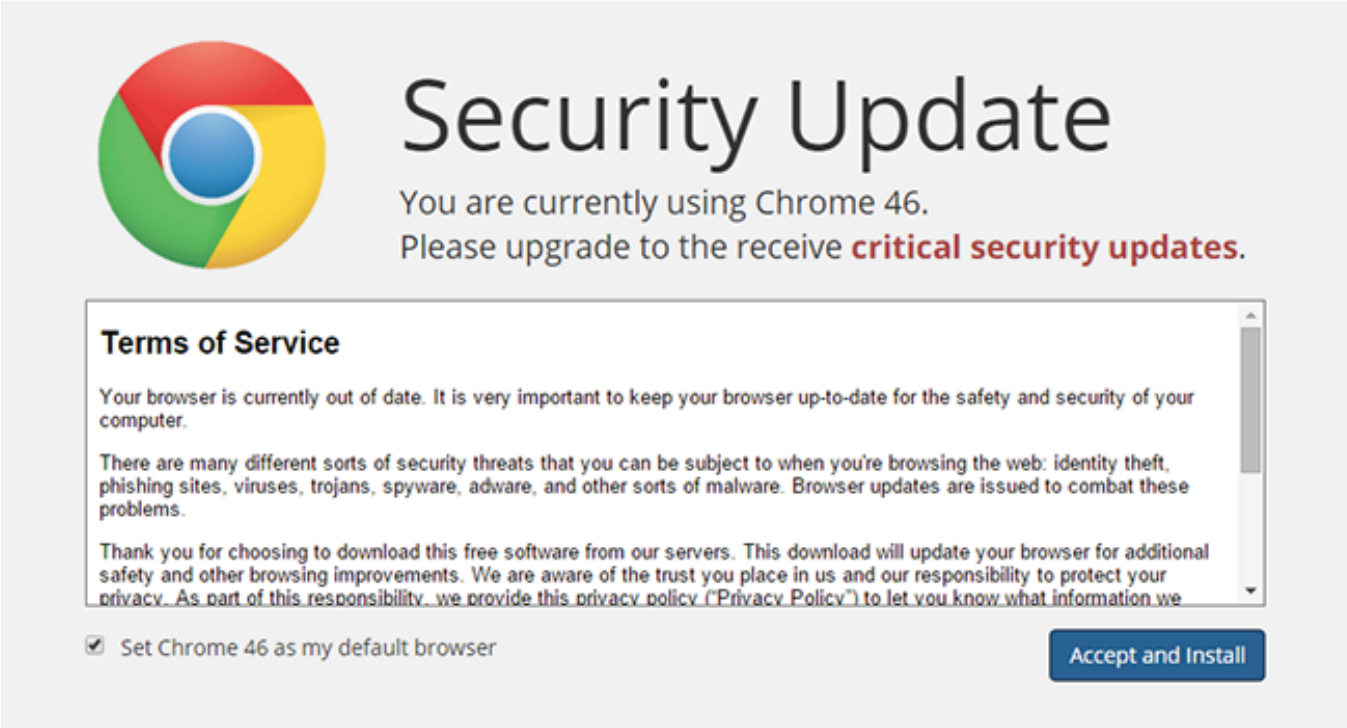
Malvertising attacks using video ads were already occurring in late 2015 and early 2016.
Let's take a look at a couple of examples:

In the first attack scenario (picture below), a malicious Flash ad unit was loaded into a legitimate Flash video player with VAST/VPAID support. The ad carried malicious JavaScript code inside, which was then executed by the ActionScript ExternalInterface.call function.

As a result, there was a malicious pop-up that tried to convince the user to update their Chrome browser. If the user clicked on "Accept and Install", then the malware was installed and infected the user's computer.



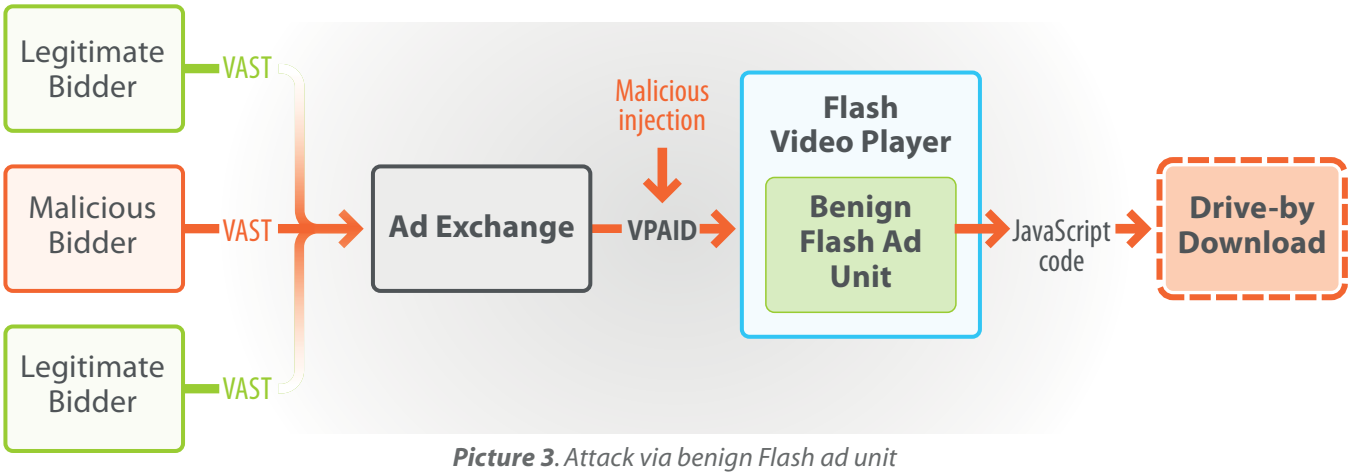
Picture 1. *Attack via malicious Flash ad unit*



Picture 2. *Pop-up from malvertisement*

In the second attack scenario there was no malicious code inserted into the main creative. In this case, the malicious URL was stored inside the VAST AdParameters tag as a tracking URL. The video player opened this URL using embedded JavaScript code and the same ExternalInterface.call function. The user was then navigated to a harmful resource as a result. The payload of this attack was Angler exploit kit — which is much worse than a pop-up, as users are infected automatically without any interaction with dangerous malware like ransomware.

The first scenario demonstrates the reason people are limiting use of Flash in their ads. However, the second scenario shows how the ad unit itself is not the only piece of the malvertising pie.



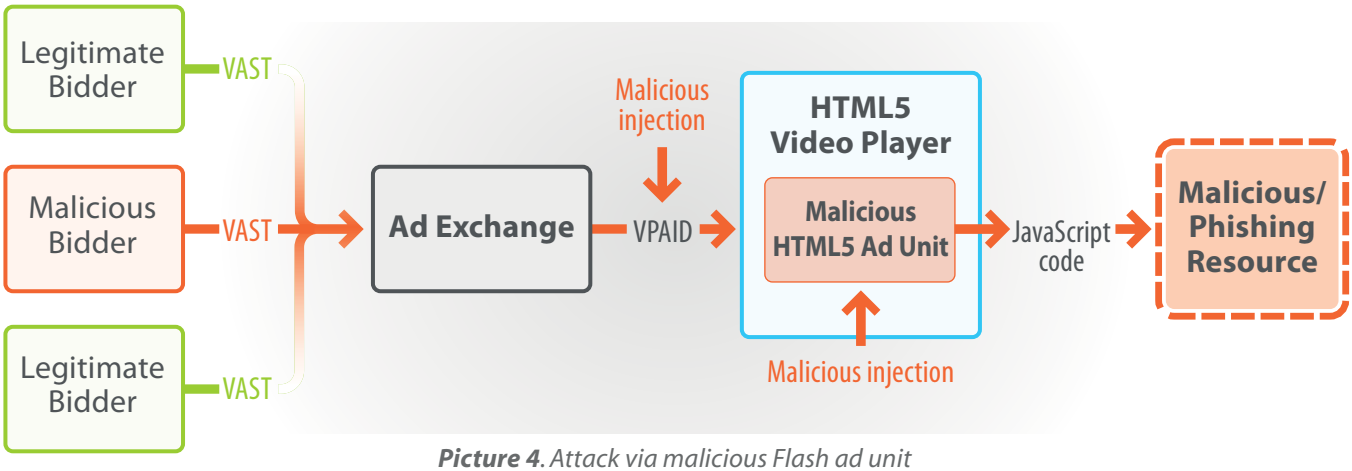
Picture 3. *Attack via benign Flash ad unit*

Is HTML5 the Security Remedy the Industry Needs?

Even if Flash is prohibited from use, malvertising can still be inserted in the first two stages of video ad delivery. Bad actors can insert malicious code because of the third-party code allowance. They can circumvent the clean build of the ad and insert a malicious tracking URL that redirects to a malicious web page, as well as other options which are just as effective. Users will then be affected in a myriad of ways: those who have Flash player or Silverlight (or any other vulnerable software) installed can be infected; users who click on a misleading button can be infected; users can also be redirected to a phishing page, etc. Clearly, there are many techniques for malvertising infection that don't require the use of Flash in the ad creative.

Moreover, one of the key features of the attacks was that an inserted JavaScript code was the source for the main malicious redirections. In fact, JavaScript is the base language for HTML5, so malicious code can be packaged in HTLM5 without much difficulty. One can easily see how other scenarios, similar to the ones shown above, could be performed with HTML5 instead of Flash. To elucidate this point further, please refer to picture 4 (below).

This diagram demonstrates what attacks could look like using HTML5. The malicious code could be inserted into the ad itself or VAST parameters, or a Flash-based malicious landing page could be inserted in the later stage – labeled malicious/phishing resource.



Picture 4. *Attack via malicious Flash ad unit*

The Vulnerability of Our Standards

The main root of the video ad malvertising problem is, unfortunately, fundamental. VAST/VPAID standards, developed in 2012, provide extensive abilities so that ad industry players can create a rich ad experience. As IAB writes, "The significance is that advertisers using VPAID ads can provide rich ad experiences for viewers and collect ad playback and interaction details that are just as rich as the ad experience."

Since these standards allow advertisers to receive data about the user, they allow for third-party codes to be inserted inside the ad. Once a third-party code is allowed, there is an open door for bad actors to perpetrate malicious activities, i.e. insert malicious code. Moreover, each ad industry player can develop its own player and ad unit, using standard guidelines. As there are no specific restrictions for impression counting using external ad servers or the contents of the AdParameters element, developers are not limited. This gives tremendous freedom to the video player. For example, it can access web pages, which then allows bad actors

to re-write advertising links or make other unauthorized changes to web pages on devices.

In an HTML5 implementation of rich ads, Flash video player is replaced with an HTML5 video player. The Flash ad unit is replaced with an HTML5 ad unit. However, there is nothing to prevent an attacker from injecting a malicious URL using third-party code into the VAST XML, or from direct injection of a malicious ad unit into the site's self-designed video player. That is why, whether the ad is created using HTML5 or Flash, (and it is easier to create ads in HTML5 than in any other technology), the user can still be infected.

VAST and VPAID are the standard format specifications used to build video ads – and they allow for insertions of malicious code. Even if the ad tech industry eliminates Flash in the creatives, malware can still come through. The threat level for malvertising is still extremely high.

Finding a Solution to Stop Malvertising Practices

Now that we have debunked the idea that malvertising would be eliminated if the industry prohibited the use of Flash in their ads, let's discuss solutions.

If the standard is enhanced to limit third-party code insertions, that would help alleviate the malvertising crisis. However, the amended standard needs to retain the ability for advertisers to collect data, as this data is extremely important to the success of their business.

When sites build their own video player, they should design it using secure coding practices and with security as a key design goal. However, even so, this is not a complete solution, just another level of defense.

The true way to defend your sites and apps from malvertising – in any stage of the lifecycle and from any technology or code – is with a third-party ad security and verification partner.

GeoEdge provides publishers, platforms, and networks with full-scale malware protection, specializing in comprehensive video ad scanning.

Sophisticated Malvertising Protection for HTML5 (& Flash) with GeoEdge

With the GeoEdge solution, companies get unprecedented visibility and control over the video ads served on their sites and inside their apps.

Capabilities include:

- **Full visibility** of the served video ad's VAST tree – Know all the VAST/VPAID requests that were made in order to deliver an ad (in addition to the final request chain). This way you will know if specific demand partners are making a lot of requests, which results in slowing down your site or app. In addition, you can see if there are any domains appearing for a bid that are problematic or on your "watch list".
- **Complete malvertising protection** with full pixel scan – Know all the possible responses of all the URLS involved in the delivery of the ad. Even if there was no malware in the final delivery of the ad, but there was a possibility of malicious activity in one of the possible responses, you will know and be able to exclude them from future bids.
- **Latency identification** – Know if there is an ad that is taking too long to load and slowing down your site or app.
- **Sound autoplay** – Know if there is a video ad that has automatic playback, distracting your users from your content and perhaps motivating them to exit the page.
- **Auto-scroll** – Know when the video player takes control of your page and automatically scrolls to the ad.

With real-time notifications, you will instantly know when aggressive or interruptive behavior takes place inside your video ad inventory, be able to quickly block the campaign, and allow your users' experiences to continue as expected. Your brand stays intact and your users are kept safe.