RISKIQ

TOP FIVE MALVERTISING THREATS

December 2014

Top Five Malvertising Threats

Malvertising is arguably the fastest growing and least well understood online threat vector today. Malicious advertising, or malvertising for short, is a technique used to distribute malware on popular websites via online advertising networks. RiskIQ has observed an exponential increase in the number and ferocity of malvertising campaigns in 2014. This report summarizes the top five malvertising threats we've observed on the web over the past 12 months: brand impersonating fake software, generic Trojan software, fake antivirus software, Angler exploit kit and RIG exploit kit.

Key Facts and Findings

In 2014, most news reports on malvertising have centered on sophisticated attacks and complex malware. However, the highest frequency attacks that RiskIQ has observed are relatively simple and highly effective. They're based on convincing victims to install malicious applications. These applications in turn are programmed to steal user credentials, money, PII, or raw data.

The Danger

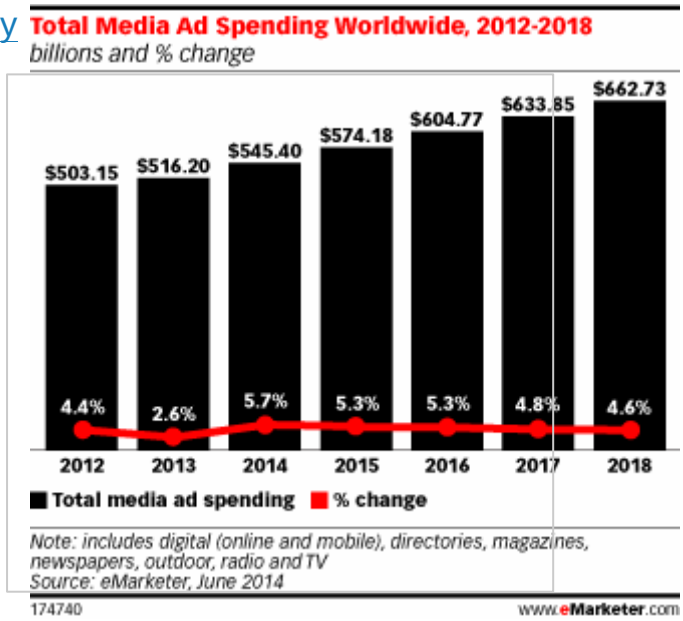
Malvertisements can appear on any website at any given time, and there is little that the website owner can do to prevent them. That's because third-party providers known as ad delivery networks plant malvertisements on web pages. These networks auction website placements to advertisers using a high-bid, free-market system. There is currently very little oversight in this industry.

Why Should We Be Concerned?

1. Attackers have gotten away with substantial amounts of money and data
2. Most organizations lack tools to measure and manage this problem
3. There still isn't any consensus on who is responsible for mitigating these threats. With no formal processes in place, the problem is increasing in size and velocity.
4. The scope of the problem is so large that the United States Senate Committee on Homeland Security and Government Affairs convened a Subcommittee on investigations into threats in online advertising and hidden hazards.

The problem is this system was built for efficiency, not security, and the marketplace has very little regulation to force better security practices. To make matters worse, malvertisers can use various techniques to disguise the true purpose of their advertisements. For example, they build entire infrastructures designed to redirect users between URLs—some hosting malware, some completely benign. Pinpointing offenders that are serving up malware in this marketplace is extremely difficult.

Sizing the Digital Media Marketing Industry

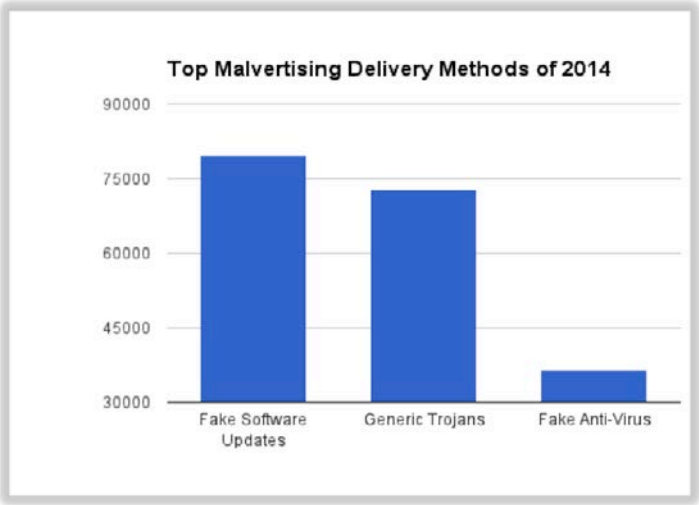


Digital media marketing is a $500 billion industry, and malvertising is a major threat to its continued success and expansion. In a report compiled by eMarketer, it was determined that the worldwide paid media market is at $545 billion and will increase by around 5% annually for the foreseeable future. Digital media marketing is what funds all the "free" websites we know and enjoy online. The success of the entire Internet and all the people that rely on it is inextricably linked to digital media marketing.

The more aggressive forms of digital media marketing such as pop-up ads and spam have already tested consumers' patience. If malvertising continues to cause harm to Internet users, the entire industry could be at risk.

The Data

In order to better understand the risks to brands and their consumers, RiskIQ examined the top five malvertising threats by frequency and ferocity. The data is a summary of findings collected on behalf of RiskIQ customers and tracks back to the beginning of Q3 2014. In total, we detected almost 200,000 malvertising examples on live websites. Below is a chart measuring frequency of malvertising delivery methods within the sample:

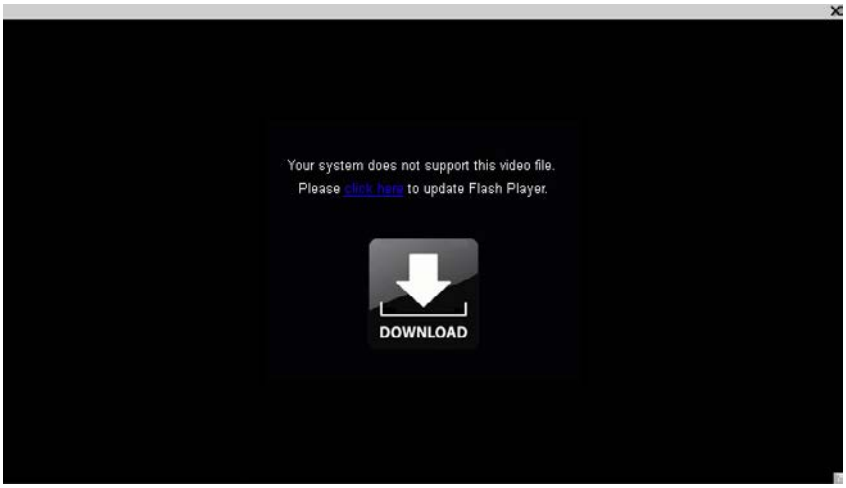


Top Five Malvertising Threats Examined Individually

Delivery Methods

1. Brand Impersonating Fake Software

As the name implies, this form of attack exploits the online trust users have established with brand-name companies. The most common technique observed in the study was to present victims with a fake software update, usually from a well-known software vendor. Instead of downloading a software update, victims are tricked into installing malware.



2. Generic Trojan Software

In this form of attack, a pop-up appears on the victim's machine, which prompts him or her to click on an executable file. It would look something like this:

This technique exploits victims who have been conditioned to execute programs when prompted and lack the security knowledge to recognize they are downloading malware.

3. Fake Antivirus Software

Much like the fake software update technique, this attack attempts to trick victims into installing malware by prompting them to update their antivirus software program.

Exploit Kits

4. Angler Exploit Kit

Angler was one of the first exploit kits to integrate Silverlight into its arsenal. Reports suggest that Angler first looks for Silverlight vulnerabilities, then Flash and Java flaws in order to infect a victim's device. This is possibly due to the fact that plugins for the two later platforms are often missing or out of date. Angler uses landing page scripts, which can check for the presence of specific kernel driver files on a system. If these are found, it aborts the exploit session and redirects the potential victim to a benign website.

Sophisticated Malvertising Attacks using RIG and Angler

RiskIQ researchers have observed a particularly devious way of distributing these sophisticated exploit packs. Web serving infrastructures are put in place that can pop on one-day registered URLs. A malvertising campaign will fire off. Using the demographic targeting configurations that come standard with ad delivery services, attackers can direct their attack at pre-built lists of preferred targets. Upon clicking on a malicious ad a user's browser will be sent a series of redirects to mostly innocuous sites and somewhere along this chain the infection will occur in a drive-by download style infection. These types of attacks, though less common to date, are largely invisible to most security solutions.

5. RIG Exploit Kit

RIG is believed to be a rip or similar evolution of the *Infinity/RedKitv2* exploit kit. It is currently offered as a hosted/rented crimeware as a service. RIG is known to support at least the following software: Java, Flash, MSIE and Silverlight. Also notable, the kit includes logic in the landing page script to check for the presence of at least the kernel driver *kl1.sys*, installed by Kaspersky antivirus, and abort the infection attempt if it is found. This behavior is observed with other exploit deliveries as well.

Conclusion

What makes malvertising insidious is its ability to hide and deliver malware using an internet-wide infrastructure that can target specific types of users. Since malicious ads do not persist once a user session is terminated, they're extremely difficult to detect and track. Worst of all, there is still a lot of grey area regarding who exactly should be solving this problem. Meanwhile, consumers and their personal data are being put at risk.

Remediation

It all starts with better detection. Malvertising has grown unencumbered because it's incredibly difficult to detect. Brands have a difficult time identifying and tracking campaigns targeting their customers. However, once an event is witnessed it's much easier to discover the attack source. That is why continued monitoring with advanced detection tools is critical.

RiskIQ has been detecting malvertising campaigns large and small for several years. Our sophisticated web crawling infrastructure observes brand-name web landscapes from the perspective of the end user and can capture examples of malvertisements as they occur. All the data is captured and stored in a searchable database, while alerts are simultaneously sent out to incident responders. This allows IT to incorporate malvertisement management programs into their security operations and limit customer exposure to harm.

About RiskIQ

RiskIQ is a cloud-based, SaaS platform for the security and IT teams of widely recognized brands that interact with the public over web and mobile platforms.

The RiskIQ brand security platform is a web, mobile and social asset discovery, indexing and threat detection solution that provides a dynamic-real-time digital footprint including official assets, shadow IT assets and rogue sites and apps with malicious intent.

Unlike solutions that rely on manual searching or brand monitoring to uncover potential threats to brand, customers and company, our product experiences millions of sites and mobile apps as a real user to quickly find defacement, impersonation, fraud and malware at scale and alert security teams for fast incident response.

Our customer base includes eight of the 10 largest financial institutions in the U.S. and five of the nine leading Internet companies in the world. These and more than 100 additional brands rely on RiskIQ to continuously monitor web and mobile assets for malware, malicious apps and brand infringements.