geoedge
Add Integrity

# AUTO-REDIRECTS

## A Security Paper by GeoEdge

January 2018

# THE BATTLE AGAINST AUTO-REDIRECTS - SAVING PUBLISHERS AND ADVERTISERS $1.13 BILLION ANNUALLY

GeoEdge has uncovered multiple hacker networks involved in large-scale auto-redirect attacks with payloads of mobile click fraud, tech support scams, and malicious installations.

# SUMMARY

Auto-redirects are a growing pestilence for publishers: a vehicle for malvertising that seizes users and reroutes them, or a protocol that remains hidden and enables click fraud. Auto-redirects alone cost the industry an estimated $210 million annually, and they also cost it another $920 million by facilitating ads with click fraud.

The auto-redirect problem particularly festers in the mobile space and until recently, attacks managed to elude detection by publishers and security experts alike.

GeoEdge ran an in-depth research and has discovered distinct classes of redirect attacks and their underlying mechanisms, making it possible to thwart many of the auto-redirects' countermeasures. What long seemed like an impossible magician's trick is now anything but.

This report will cover:

- The emergence of redirects
- Their evasive tactics,
- The discovery of redirect code
- Best practices for frontline defense

# REVENUE IMPACT

### $210M Loss for Publishers

With hundreds of millions of impressions impacted by auto-redirect attacks, publishers' revenues are significantly affected. For publishers who are unable to identify those auto-redirect attacks, the impact is even greater. Hackers continue to target their sites and users. The GeoEdge team estimates that auto-redirect activities cost $210 million annually, including identification, documentation, and remediation.

### $920M Damages from Mobile Click Fraud

Every click means money. GeoEdge determined that click fraud is a part of the underlying mechanism of the attacks discovered. The trouble with hidden redirects is that they are even harder to identify, as they do not obviously affect the user experience. This causes a drain on the publishers' resources. In a general sense, hidden mobile redirects resulting in click fraud are estimated to cost the industry $920 million dollars.

# A SNAPSHOT OF AUTO-REDIRECTS

## STATISTICS

### Tactics for Malvertising Distribution

Auto-redirects make up 48% of all malvertising events, with malicious URL pre-click far behind at 18%.

### Redirect Geographic Breakdown

The US accounts for 48% of auto-redirects, nearly five times as many Canada (the second most targeted) and Australia (the third most targeted).

### Auto-Redirect Device Breakdown

A total of 27% occur on desktops and 72% on mobile devices, with 57% on iOS and 15% on Android.

### Hidden Redirects Coupled with Click Fraud

Hidden redirects are programmed with an underlying mechanism to run click-fraud campaigns. GeoEdge research shows that the US and Great Britain have more than 20% of hidden auto-redirect campaigns enabling mobile click fraud.

## METHODOLOGY

This report features research that uses internal data approximating 650 million impressions. The GeoEdge's Security team analyzed the data and herein lies the results.

# TABLE OF CONTENTS

# INTRODUCTION

For publishers and users alike, auto-redirects have become a bane nearly unrivaled by other types of attacks. Traditional malvertising vehicles often appear as a tasteless banner ad sitting atop a webpage, beckoning users with the promise of free lotto money or phony security alerts. They're dangerous, and they still bedevil publishers. But even in their most obnoxious, scroll-across-the-screen forms, they can be ignored. Typical auto-redirects, when they appear, are difficult to elude.

They arrest the entire user experience and send the user spinning into bizarre territories that can feel impossible to escape because hackers have designed the process of getting back to the original site to be almost extremely confusing. Users often accidentally install malware in desperate, disoriented attempts to leave the malicious page. And since few methods of malvertising are as intrusive, publishers risk having malicious third parties alienate their readers after a single bad experience. With each redirect, the pact between publisher and user fizzles.

There is another type of redirect – the hidden one. As the name implies, this type of redirect does not affect the user experience and remains under the radar. The redirect operates from within an invisible iframe or image, and unbeknownst to the user, goes on its own delivery path. It is most often a vehicle for click fraud and at other times attribution fraud and cookie stuffing. However, some networks assert that it is a needed tracking tactic.

Redirects have earned a reputation for being stubbornly hydra-like: every time the source of one redirect attack has been identified, another emerges to take its place, making them particularly elusive for publishers and conventional ad verification tools. But GeoEdge has recently discovered seven different families of redirect attack, increasing identification and prevention by 30%. The discovery makes incursions into critical terrain of the redirects' perpetrators. This report presents an example of one such attack and dives into the source, playing field, and future expectations of auto-redirects.

# MALVERTISING'S NEW ATTACK VEHICLE

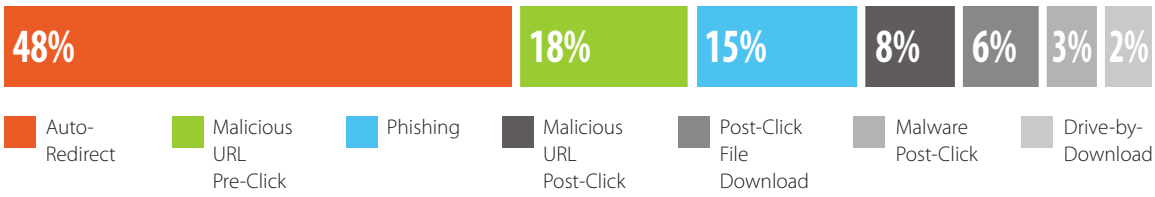
The problem, it seems, took off in 2013: Mobile website visitors who just wanted to browse some news headlines were suddenly whisked to the app store. Many thought they'd accidentally clicked an ad for an app. But it kept happening, over and over, and no publisher was immune. Properties belonging to NBC, Hearst, and the Associated Press all kept bouncing their readers and driving them mad.

Unfortunately, the early wave of auto-redirects wasn't a one-off attack, to be quickly identified and controlled. Instead, it was the beginning of malvertising's new normal, and the app store is hardly the only place redirects lead.

Today, four years after auto-redirects emerged in force, they account for 48% of malvertising events, according to GeoEdge security research. The next-largest security issue, malicious URL pre-clicks, comes in at a distant 18% (see Picture 1 for complete breakdown).

The high probability that users will react is precisely why auto-redirects have taken the place of exploit kits as the most dominant web-based threat. In spite of high-profile ransomware attacks, software vendors have mostly risen to the challenges that exploit kits pose. Operating system vendors, browser makers, anti-virus systems and ad verification tools have worked in concert to close critical vulnerabilities that allowed hackers to simply run an executable on a user's machine and directly install malware. Even just the removal of Flash from Google Chrome and the nearly complete obsolescence of Internet Explorer went a long way to barricading easy avenues for malvertisers. Computers are still hacked, money is still lost, and panics still ensue – but far less than in the past. Every day, the number of computers vulnerable to traditional exploit kits shrinks.

Not so with redirects. Because the attack doesn't directly install files on a user's computer, it can't simply commandeer the machine, and so the attacker has to hope that users sabotage themselves. Instead of targeting computers in the fashion of exploit kits, auto-redirects hack the user – and the susceptibilities of the human brain, unlike browsers, have yet to be patched.

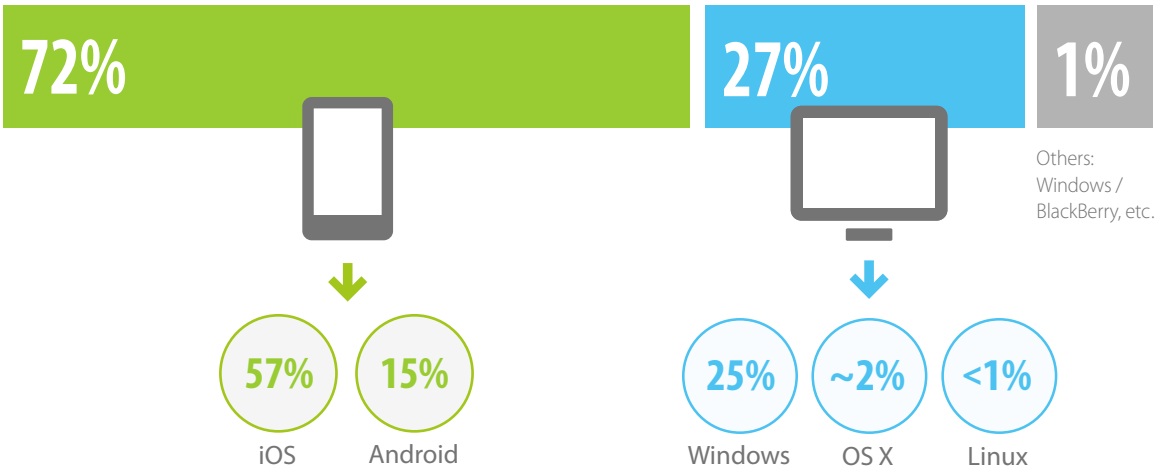



***Picture 1: Distribution of Malvertising Issues***

# THE FERTILE GROUND OF SMARTPHONES

The combination of fear and confusion sown by redirects is particularly pronounced on mobile platforms, and it's why the technique has such an affinity for phones. While a non-trivial 27 percent of auto-redirects occur on desktops, 72 percent occur on mobile devices, with 57 percent on iOS and 15 on Android (see Picture 2). For malvertisers, the advantages of auto-redirects generally, and mobile redirects specifically, are legion. Ads can redirect to pages, fashioned after Google or Apple, that falsely alert users that their devices are infected or that a free iPhone awaits, in turn pushing them to download malware or dial a scam number. In other words, the schemes are the same as those used for non-redirecting attacks. But by taking users to an entirely separate window – rather than simply an irksome banner ad – the scam can appear more legitimate than it otherwise would. For example, a webpage wholly constructed to look like Microsoft's site can feel more real than a simple banner ad. Attacking banks is hard, while replicating a bank's web page and getting users to hand over their info is comparatively easy. And to mobile users, a "System Warning!" in the style of a popup notification they regularly see on their phones can seem too real to ignore.

This makes mobile redirects particularly effective for click fraud and for phishing and mining personal data. While scammers can lure users to call a fake number, the distance between a scammy webpage and dialing numbers on the phone involves several steps, each one reducing the chance that the target will fall prey to the trap.




***Picture 2: Auto-Redirect Attack Breakdown***

With mobile redirects, the number of steps can be reduced to one: scare users into enabling permissions on their phone. In a sense, it's a technique straight from Silicon Valley's playbook, the principle of reducing friction between users and a product. Each successive step involved in making a purchase online is reduced to increase the chance that the purchase will occur – and it's just as effective for increasing Amazon sales as it is for enriching con artists.

# EVASIVE AUTO-REDIRECT MANEUVERS

The sheer diversity of the redirects – their sources, behaviors, and motivations – makes dispatching them a slippery challenge. Hackers can inject malicious code into the ad creative itself, at the ad request level, or by post-click. These perfectly innocent ads get infected, unbeknownst to anyone in the advertising chain, and a benign ad hosted by a perfectly responsible network now takes the user directly to a tech support scam without passing go.

From the perspective of the operating systems' creators, the problem is difficult to solve. Apple seemed to have addressed auto-redirects to the App Store with iOS 8, but the problem reared its

head shortly after, with the release of iOS 10.3. Rinse and repeat. And regrettably for those on Android, mobile redirects have long been a reliable mainstay of their mobile experience.

That's because it's difficult for the app store operators to determine whether it was a human or a script that opened the app store to begin with. The mechanism allowing app stores to automatically open without actually clicking the store's icon is part of what makes the mobile experience seamless. That mechanism is called a deep link, and it's why clicking a link to a Twitter handle on a web page will open the Twitter app instead of twitter.com. When it works as intended, it's convenient. But the same mechanism can be embedded into a web frame by dubious networks.

Many redirects execute dynamic, targeted attacks, sending the user to another domain only if certain conditions are met. Examples of such conditions are whether the website is being visited on a mobile device or from a specific country. Redirect attacks can track who has already been redirected to the malicious site or the app store. Scripts often redirect users once and no more; after that, as far as that user is concerned, the malicious script vanishes. The redirect stops redirecting, thwarting efforts to replicate the problem. Users complain to publishers about being bounced from their site, publishers can't seem to recreate the problem the users complained about, and redirects live another day.

Identifying and locating a redirect script that is here today and gone tomorrow is just as challenging using typical security measures, which rely on recreating malvertising in mobile emulators. This adaptability is what often makes redirects so peculiarly vexing. Unlike many other forms of attack, redirects can be maddeningly chameleonic, never holding on to a steady form and shifting the moment they seem to have been identified.

While security solutions emulate user experiences to detect typical malvertising attacks, the creators of redirect attacks have anticipated such a solution and placed emulators high on the list of a redirect's array of conditions to avoid. This means that ultimately, it is easier for the attacker to avoid the solutions than for security systems to spot them. Demand partners are spending lots of time, money, and resources to track these redirects but often fail.

# ARRESTING THE AUTO-REDIRECT ATTACKS

What did GeoEdge uncover? Seven distinct classes of redirect attacks as well as major hacker networks. These families of attacks, and the hacker networks that use them, are responsible for hundreds of millions of monthly impressions and for publishers, scores of irritated users.

In a few of the attacks discovered, the auto-redirect was taking the user out of the browser and into app stores. The redirect method in mobile devices, by and large, redirects to the App Store or Google Play store, rather than simply mimicking the usual desktop tricks.

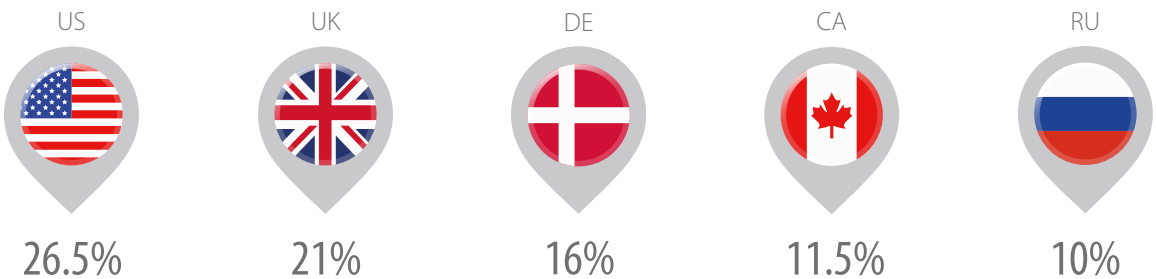
However, GeoEdge also found "hidden" redirect attacks, meaning one thing: click fraud. The mobile browser opens multiple invisible iframes and calls multiple URLs, until ultimately executing fraudulent clicks.

In this particular attack, GeoEdge found what made these attackers so elusive for publishers and security experts: a whitelist of hundreds of domains where the attack would actually occur (see Picture 3). The ad loads a script from Amazon AWS S3 and checks the domain to see if it should execute. If the specific domain is on the whitelist, the code will embed hidden iframes in the browser and click on the ads.


***Picture 3: Snippet of Malvertisement Script***

In other words, if the attack appeared on Reuters, Ars Technica, Forbes, or Alternet, for example, it executed multiple clicks on the malicious ad. If the ad appeared on any other domain not on the whitelist, it didn't trigger a hidden redirect.

When the malvertisement runs on the whitelisted sites, it opens numerous invisible frames and executes clicks. Click fraud abounds – and while in this case the primary target was the US, on a global scale, click fraud is an underlying mechanism programmed into auto-redirect behavior in many geos (see Picture 4).




***Picture 4: Percentage of Hidden Redirects Coupled with Mobile Click Fraud in Several Countries***

The click-fraud scam is highly attractive to hackers, as they can slip into the convoluted labyrinth of the ad tech ecosystem without detection and get a payday. The hacker in this particular attack redirected users to nearly a dozen different apps in the App Store and Google Play store, including the Star Wars: Galaxy of Heroes game made by Electronic Arts. In general, the redirects are to the highest-paying advertisers.

Electronic Arts isn't the culprit. Bad actors provide traffic to legitimate advertisers through malicious means, and this attack is no different. The GeoEdge Security Lab analyzed the script and found the malicious code in the ad creative itself. The hacker created this campaign for legitimate advertisers, is only running it on legitimate websites, and is reaping the rewards.

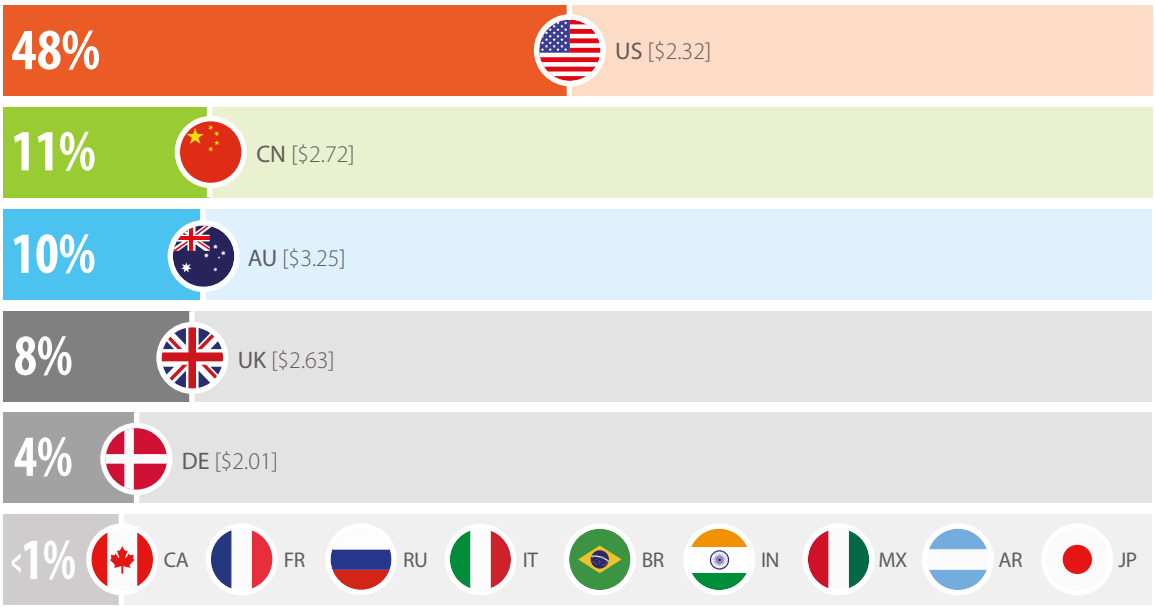
# IT'S NOT JUST HACKERS DRIVING AUTO-REDIRECTS

It's within the app economy that the connections between malvertisers, ad networks and app developers become a kind of toxic mix. App designers give their ads to ad networks that are charged with the sole task of increasing downloads. Unfortunately, different networks, behave with different degrees of integrity, and app makers are dismayingly likely to look the other way at whatever underhanded tactics the networks employ to make downloads happen. And because networks are paid on the basis of cost-per-install, or CPI, incentives between networks and users can become wildly misaligned.

CPIs don't come cheap – globally, as of last year, the average CPI was $1.24 for iPhone apps and $0.53 for those on Android. That's probably why redirects, whether to app stores or to phishing scams, occur on iOS nearly four times as often as they do on Android: By nearly every metric – including personal income, money spent on apps and time spent on their phones – iOS users are more valuable. That makes them equally valuable to malvertisers. [chartboost.com/insights, November 12, 2017]

So the networks follow a simple, shortsighted math: swamp users with redirects to the app, expect that most of them will be so furious at having been shooed out of their webpage that they'll forever consider the app a nuisance, and at the same time plan for a tiny fraction which, out of confusion or a spontaneous impulse to download the app, will actually install it. The number of installs could be far below even single-digit percentages, but given sufficient volume, that's enough. The more users who are annoyed, the more money is made.

This helps explain why redirect events break down geographically as they do (see Picture 5). A CPI in the United States costs on average $2.32, slightly less than an install in Australia at $3.25 or one in Canada at $2.72. But according to GeoEdge data, the United States accounts for 50 percent of auto-redirects, nearly five times as after much Canada (the second most targeted) and Australia (the third most targeted). The United States provides the sweet spot between numbers and value-per-install, and accordingly, its citizens wind up the most harassed.




***Picture 5: Redirect Geographic Breakdown with Average CPI***

# HOW TO FIGHT AUTO-REDIRECTS

GeoEdge has uncovered these classes of redirect attacks by identifying specific codes and networks. With this intel, GeoEdge can pinpoint ads that contain redirect scripts and that have the potential for auto-redirect behavior. It doesn't matter whether the conditions that execute the redirect are triggered or not.

Often, finding a malvertisement relies on emulation, but auto-redirects are programmed to evade emulators. While GeoEdge does include emulation as one of the "scan-and-detect" techniques, it is just that: one of the techniques. The GeoEdge Security Lab has a multi-layered approach to malvertising detection and remediation.

It's like ad tech precognition. For publishers who spent years frustrated that they couldn't see what made their users so upset, GeoEdge's auto-redirect protection means that there's no need to vainly try to make lightning strike twice. Instead, it's like catching it in a bottle, then throwing the bottle in the garbage.

# 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, and 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.


geedge
Add Integrity