geedge
Add Integrity

Cookie Sync Malvertising

Fighting A New Form Of Obfuscated Attacks

As malvertising detection capabilities evolve, malware continues to slither its way through digital advertising channels onto users devices in various ways-- including cookie sync enabled campaigns. At the onset of 2021, GeoEdge's security research team uncovered the abuse of cookie syncing, a process used by AdTech players to exchange user data across platforms to better target online audiences. In this report, we'll guide you through the abuse of cookie syncing, and why more robust ad security solutions are required to mitigate this growing threat.

UNCOVERING THE MALICIOUS COOKIE-SYNC ATTACK

In late February 2021, GeoEdge's security researchers uncovered a widespread malvertising attack exploiting an AdTech cookie syncing code to serve malicious Bitcoin popups. The attack targeted users from the popular Bitcoin wallet, Electrum, which stores and sends cryptocurrency transactions. Unlike conventional malicious attempts which traffic the malicious payload through ad creatives, the attackers compromised a mid-size SSP's (supply-side platform) cookie syncing code—compromising every linking partner.

The syncing process works when two different systems map each other's unique IDs and share data gathered about the same user. Because cookies are domain-specific, a cookie created by one ad-tech partner cannot be read by another. Thus, cookie syncing was created to circumvent the domain limitation and share data about users across platforms and advertisers-- and has quickly become a standard industry practice. While a successful technique for audience targeting- cookie syncing is clearly not without its challenges or vulnerabilities. In this attack, the malicious payload is not tied to a single malicious creative or advertiser, but rather is served when an AdTech partner syncs with the breached SSP, resulting in mass exposure. In this campaign, the Electrum attackers implemented heavily obfuscated code to fingerprint user devices, redirecting users to popups, leading to a deceptive Electrum software update. By leveraging behavioral and code-based analysis expertise, GeoEdge was first to identify the anomalous code and trace the attack across networks back to it's source.

HOW COOKIE SYNC ENABLED MALVERTISING WORKS

It's common -- if not universal for AdTech players to practice cookie syncing. However, the nature of cookie syncing isn't entirely opaque, as the relationships of which players are cookie matching and how the sync is executed can vary. Rather than spreading malvertising through the ad server- but through user sync URLs, the malicious code was loaded by partners in order to sync user identifiers. As a result, any AdTech vendor using this SSP's cookie sync was impacted, infecting the AdTech ecosystem at large, within a few short hours.

According to GeoEdge's security researchers tracking this campaign, the abuse of cookie syncing is a new evasion tactic to avoid detection by ad verification solutions and target legitimate victims with maliciously rigged deceptive advertisements. While cookie syncing is an essential practice, it doesn't involve a publisher's ad server, making it difficult to identify and thwart. According to GeoEdge's security team, the primary goal of this cookie syncing campaign is to steal user funds from cryptocurrency wallets and scale attacks while simultaneously circumventing traditional RTB costs. This effectively means that cybercriminals can entirely detach attacks from the ad server to exploit the opaque nature of programmatic- including vulnerabilities in audience targeting transactions.

ANATOMY OF THE ATTACK

The Electrum attackers served unsuspecting users a fishing popup with a message indicating the latest wallet app software update should be installed, citing a vulnerability in the current version. This message convinced trusting Electrum users to install the malicious update, which in turn drained the user's Bitcoin wallet by initiating a direct transfer to the attacker's pre-defined addresses.

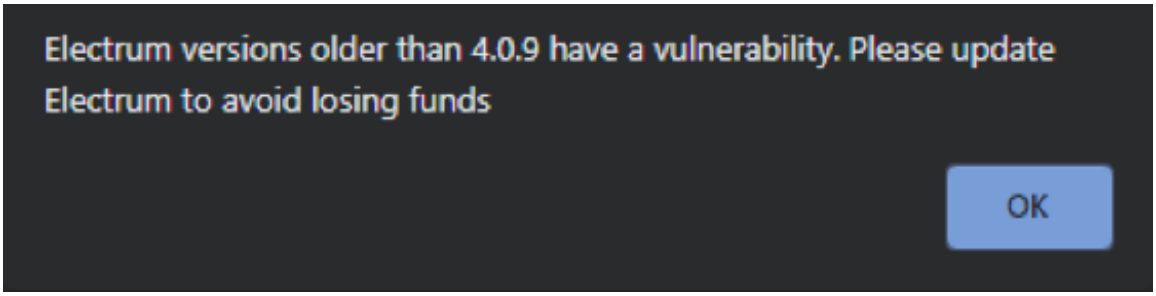

Figure 1: Example of popup message to users

Script deobfuscation reveals the malicious payload that was added into code loaded the following URL: https://ipfs-hosting[.]tk/redirect.php, which redirected the victim's browser to: https://electrum-4.github[.]io/electrum.html. (This page is taken down by Github now). The page displayed the malicious JS alert and initiated a request to the following URL: microsoft-edge:https://electrum-4.github[.]io/, which automatically opens Microsoft Edge browser with the malicious download page.

Figure 2: An example of different SSP calls to the compromised SSP cookie syncing code

Through this attack vector, the Electrum attacker successfully avoided wasting ad dollars traditionally spent on obtaining winning bids to push malicious code within RTB auctions, creating a challenge for blocking solutions as the attack was uniquely integrated within an integral part of the ad serving process.

FIGHTING COOKIE SYNC ENABLED MALVERTISING

Between the DSP and the publisher sit any number of SSPs, ad exchanges and ad networks — presenting a web of supply paths where malicious activity can stow away. And in the ongoing cat-and-mouse game between attackers and security experts, the cookie sync abuse provides just another method for attackers to execute malicious activity at a broad scale. Its worthwhile to emphasize, because cookie syncing is a legitimate element of the ad serving process, it's difficult to mitigate the attack. And this-- says Liran Lavi, GeoEdge's Head of Security Research, should be a warning to today's digital publishers and ad platforms. Malvertising tactics are evolving-- requiring dedicated ad security professionals to go toe to toe with cybercriminals.

Regardless of what cybercriminals dream up to harm users, user experience and cheat digital businesses out of revenue, GeoEdge provides the solution to the complex situation of an obfuscated attack. GeoEdge's Security Research team will continue to track this trend closely, to ensure the quality of the advertising experience.

ABOUT GEOEDGE

GeoEdge's mission is to protect the integrity of the digital advertising ecosystem and to preserve a quality experience for users. GeoEdge's advanced security solutions ensure high ad quality and verify that sites offer a clean, safe and engaging user experience, so publishers can focus on their business success. Publishers around the world rely on GeoEdge to stop malicious and low-quality ads from reaching their audience.

GeoEdge allows publishers to maximize their ad revenue without quality concerns, protect their brand reputation and increase their user loyalty. GeoEdge guards digital businesses against unwanted, malicious, offensive and inappropriate ads – without sacrificing revenue.

Test drive GeoEdge's ad quality solution and gain the freedom to maximize your ad revenue without quality concerns.

To Start Your Free 30-Day Trial, visit: **www.geoedge.com**

Contact us: **info@geoedge.com**


geedge
Add Integrity