April 15, 2016

comScore Labs Discovers Placement Laundering Attack in SafeFrame

RESTON, Va., April 15, 2016 /PRNewswire/ -- Today, comScore (NASDAQ: SCOR) announced that comScore Labs has discovered a sophisticated new form of placement laundering that that has been used to generate considerable amounts of invalid traffic to take advantage of advertisers over the past year. Like other placement laundering attacks (a form of ad fraud originally identified by comScore Labs' Jeff Kline in 2014), this exploit enables ad requests to appear to originate from high quality publishers, thereby enabling requesting entities to derive significantly higher ad prices for low quality placements.

comScore discovered the attack using its own diverse data assets. Forensic analysis revealed two key features: the use of an API-enabled iframe called "SafeFrame" and redefining global JavaScript functions within the SafeFrame environment. The redefined functions interfere with the normal functionality of JavaScript tags that are used to measure campaign placements.

SafeFrame, defined by the Interactive Advertising Bureau (IAB), is intended to allow information to pass between ad creatives and publishers in a secure and standardized manner. The goal of SafeFrame is to protect publishers from misbehaving or malicious advertisers, but it was not designed to protect advertisers against invalid traffic. Google has its own implementation of SafeFrame, which analysis indicates is used in an unintended way as part of the exploit.

The attack starts with an ad request to an account associated with a malicious party on an ad network. The response instructs the browser to create two iframes, one iframe displays an ad creative that is visible in the browser while the other iframe has its source parameter set to Google SafeFrame's URL. The SafeFrame API can be used to include malicious JavaScript hosted on a third-party server. The malicious JavaScript repeatedly creates and destroys iframes that request ads and have tainted global objects. Specifically, each iframe is created with its global URL-encoding functions (escape, encodeURI and encodeURIComponent) redefined. The redefined functions detect whether the passed-in argument matches SafeFrame's URL. If the argument matches, the returned value is chosen from a list of URLs that are loaded dynamically during the course of ad delivery. If the argument does not match, the original encoding function is called and the standard behavior occurs. The implications of this attack are significant. Specifically, any ad tag that does not verify the integrity of global JavaScript functions is at risk.

Since discovery and diagnosis of the attack, comScore Labs has worked closely with Google's Ad Traffic Quality team to understand the implications of the attack. Google has indicated that the use of SafeFrame is orthogonal to placement laundering via a tainted encodeURI function. This same exploit could be conducted without a SafeFrame environment. In general, any ad tech that relies on an overridable component is at some risk. Detailed analysis of Google's ad traffic shows no evidence that its systems are affected by this particular placement laundering attack. Indeed, Google's ad systems have significant placement laundering safeguards including automated infrastructure and review by operations teams to exclude traffic that is falsely represented as coming from a different website.

Similarly, comScore Labs has developed comprehensive capability to identify and remove placement laundering attacks from all of its reporting products.

About comScore

comScore, Inc. (NASDAQ: SCOR) is a leading cross-platform measurement company that precisely measures audiences, brands and consumer behavior everywhere. comScore completed its merger with Rentrak Corporation in January 2016, to create the new model for a dynamic, cross-platform world. Built on precision and innovation, our unmatched data footprint combines proprietary digital, TV and movie intelligence with vast demographic details to quantify consumers' multiscreen behavior at massive scale. This approach helps media companies monetize their complete audiences and allows marketers to reach these audiences more effectively. With more than 3,200 clients and global footprint in more than 75 countries, comScore is delivering the future of measurement. For more information on comScore, please visit comscore.com.

Logo - http://photos.prnewswire.com/prnh/20160131/327730LOGO

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/comscore-labs-discovers-placement-laundering-attack-in-safeframe-300252170.html

SOURCE comScore