BIZCOMMUNITY

Mobile malvertising skyrockets

By Lutz Blaeser

9 Feb 2015

As the use of mobile devices continues to skyrocket, so do the number of threats aimed at the platform. Due to their rise in popularity, and the fact that they are almost always carried around wherever we go, mobile devices have also become a target for malicious advertising or 'malvertising'.

Malvertising utilises online advertising channels to infect users and websites with malicious code. He says there are several ways that advertising can be manipulated to serve up malware.

False sense of security

Malvertising usually happens in one of several ways. Firstly, cyber criminals could pay for and place malware-free ads on trusted, legitimate sites that run third-party adverts and leave them for a time, until they are trusted and both the site and viewers have been lulled into a false sense of security. After this time has passed, the criminals could inject malware into the ads, and quickly infect as many as possible before removing the malware or the ad itself.

Another way, is through ad exchanges. Threat actors position their malicious ad within an ad network or exchange that automatically distributes ad space on websites. Due to the complexity of the ad ecosystem, involving several entities and exchanges, it is virtually impossible to pinpoint the actual source of the ad, as well as where it has appeared.

Thirdly, attackers can exploit technical vulnerabilities, piggy-backing on existing vulnerabilities within the ad servers and other infrastructures in the ad ecosystem, to compromise networks, and replace legitimate ads with nefarious counterparts which are then sent to a variety of destinations.

It was always assumed that sites hosting pornography and other adult content, as well as online gambling sites, were the main culprits when it comes to infecting mobile devices, but this is not the case. In fact, malvertising is the primary source of infection, and usually via trusted websites, which cyber criminals rely on to carry out their evil ends.

Anti-malware solution

There are several ways to avoid falling foul of malvertising, and none so effective as having a good mobile anti-malware solution, such as Bitdefender Mobile Security, which is able to offer complete protection from malicious websites and will prevent any malware from being installed, and will also warn the user of websites that could potentially contain some form of malware, or notifying when an application displays anomalous behaviour such as trying to access personal data.

Research from security vendor, Blue Coat, revealed that every one in five times a user visits a website from their smartphone and is directed to a malicious webpage, it is because of malvertising. Moreover, the same research showed that malvertising is skyrocketing, showing a threefold jump from the end of 2013. Malvertising is so successful, because people are still unaware of what it is, and the danger it represents.

ABOUT LUTZ BLAESER

In 2011, Blaeser founded Intact Security, building on his knowledge and experience of the reseller market. His main focus at Intact Security is to continue building the Avira Antivirus market but also provide additional solutions into the offering. Since the company's inception, he has added additional antivirus and content security products such as Bitdefender, AVAST, G Data and Kaspersky as well as leading backup and disaster recovery solution StorageCraft.

- How to understand bad user behaviour - 12 Nov 2015
- The dangers of a connected world - 8 May 2015
- Mobile malvertising skyrockets - 9 Feb 2015
- Security is no longer a catch-up game - 30 May 2014

View my profile and articles...