1300 - Game of Chromes: Owning the Web with Zombie Chrome Extensions

Sunday at 13:00 in 101 Track
45 minutes | Demo

Tomer Cohen*R&D Security Team Leader, Wix.com*

On April 16 2016, an army of bots stormed upon Wix servers, creating new accounts and publishing shady websites in mass. The attack was carried by a malicious Chrome extension, installed on tens of thousands of devices, sending HTTP requests simultaneously. This "Extension Bot" has used Wix websites platform and Facebook messaging service, to distribute itself among users. Two months later, same attackers strike again. This time they used infectious notifications, popping up on Facebook and leading to a malicious Windows-runnable JSE file. Upon clicking, the file ran and installed a Chrome extension on the victim's browser. Then the extension used Facebook messaging once again to pass itself on to more victims.

Analyzing these attacks, we were amazed by the highly elusive nature of these bots, especially when it comes to bypassing web-based bot-detection systems. This shouldn't be surprising, since legit browser extensions are supposed to send Facebook messages, create Wix websites, or in fact perform any action on behalf of the user.

On the other hand, smuggling a malicious extension into Google Web Store and distributing it among victims efficiently, like these attackers did, is let's say - not a stroll in the park. But don't worry, there are other options.

Recently, several popular Chrome extensions were found to be vulnerable to XSS. Yep, the same old XSS every rookie finds in so many web applications. So browser extensions suffer from it too, and sadly, in their case it can be much deadlier than in regular websites. One noticeable example is the Adobe Acrobat Chrome extension, which was silently installed on January 10 by Adobe, on an insane number of 30 million devices. A DOM-based XSS vulnerability in the extension (found by Google Project Zero) allowed an attacker to craft a content that would run Javascript as the extension.

In this talk I will show how such a flaw leads to full and permanent control over the victim's browser, turning the extension into zombie. Additionally, Shedding more light on the 2016 attacks on Wix and Facebook described in the beginning, I will demonstrate how an attacker can use similar techniques to distribute her malicious payload efficiently on to new victims, through popular social platforms - creating the web's most powerful botnet ever.

Tomer Cohen

Tomer Cohen leads the team at Wix.com responsible for all R&D and production systems security. Previous to that, Tomer has worked as an application security expert in several firms. Tomer was also one of the founders of "Magshimim" cyber training program, which teaches development and cyber security among high-school students in the periphery of Israel.

#defcon25/by_track/101/Sunday #defcon25/By_Day/_Sunday