Targeted SSL Stripping Attacks Are Real

By bferrite

Published: 2016-03-07 · Archived: 2026-04-06 03:17:25 UTC

Having access to the Internet is critical for on-the-go professionals. So the convenience of open Wi-Fi hotspots often outweighs the risk these connections may not be safe. Recently, a senior executive and Mobile Threat Prevention customer at a large financial company connected her iPad to a local hotspot while traveling for business. But when she tried to access sensitive company information she was blocked because her device was under a targeted SSL stripping attack.

SSL stripping attacks – defeating communication encryption

In order to understand what an SSL stripping attack is, we first need to understand what SSL really is. SSL (Secure Socket Layer) is a secure protocol used to communicate sensitive information. This protocol is used when exchanging sensitive data such as banking information and email correspondence for example. The protocol's security is established by creating an encrypted connection between two parties (usually a client application and a server).

Browsers and web servers regularly use this protocol when a secure connection is needed. In most scenarios the following events take place when establishing a secure connection:

1. The user sends an unsecured HTTP request.
2. The server answers via HTTP and redirects the user to a secure protocol (HTTPS).
3. The user sends a secure HTTPS request, and the secure session begins.

In order to "strip" the SSL, an attacker intervenes in the redirection of the HTTP (regular unsecured protocol) to the secure HTTPS protocol. The attacker will intercept a request from the user to the server. He will then continue to establish a HTTPS connection between himself and the server, and an unsecured HTTP connection with the user, acting as a "bridge" between them. This means all information transferred over the unsecured HTTP connection is exposed to EVERYONE in the network, including the attacker. Among the information at risk, one can find the user's credentials and sensitive business data.

Back to the attack

One of the ways an attacker can intercept the user's communications is by using hotspots. Many attackers establish fake hotspots with names similar to legitimate hotspot names, for example, "Starbucks Coffee" instead of "Starbucks". Unaware, the user connects to the malicious hotspot. Once the user tries to connect to the server, the attacker uses his control over the hotspot and attacks the user.

What's interesting in the attack on the executive mentioned earlier is that the attacker targeted a specific user and not all the users connected to the same hotspot. Two other company personnel who had the same protections were

connected to the same hotspot, yet they were not attacked. This is not a common course of action for cyber criminals and may suggest the attacker had preliminary intelligence regarding his target. An attacker could possibly acquire such information by scanning a network to obtain connected devices' details before initiating the attack.

In this case, the user was protected by the Check Point Mobile Threat Prevention solution and the attacker did not achieve his malicious intent. If he had succeeded he could have compromised web-based applications and apps which rely on web widgets when accessing personal and business information. Our protection prevented valuable business and personal information from being stolen. This case, like many others before it, emphasizes the reality of this type of threat and the need for protective security measures against it.

Oren Koriat is a Mobile Information Security Analyst in the Check Point Mobile Threat Prevention Research Group. He is a technology enthusiast and a polyglot, whose expertise is in the field of Asian mobile software markets. Koriat holds a degree in linguistics from Bar Ilan University.
