Sponsored Links Jacking

Researcher & Author: Yaniv Miron

Thanks to Yuri Gushin for his part in the research

Test Case: Google

Google SLJ attack

Version 1.0 - October 2008

Disclaimer:

This document was created for educational purposes only.

The author of this document is not and will not hold any responsibility for any illegal or unauthorized use of the information contained within this document, or that is implied from it.

The author of this document does not encourage in any way whatsoever using SLJ attacks, attacking Google, attacking any SL service or any illegal use of credit card information.

Certain parts of the SLJ attack are proven theoretically due to lack of time and resources while conducting this research.

What are Sponsored Links Jacking attacks?

Sponsored Links Jacking attacks or SLJ attacks are a way of attacking a specific target with the "kind" assistance of sponsored links that anyone over the internet can pay for and use for legal purposes.

Test case scenario: Google

Google search engine have a sponsored links system named: Google AdWords Ads.

> Google secures its sponsored links by testing them with automatic bots, spiders and crawlers alongside manually human checks. When Google finds a malicious website it removes it and takes actions against the malicious attacker and his account.

A malicious attacker that wants to create a "Spear Attack" on “Target corp.” company System Administrator that usually purchases software for the “Target corp.” company,

can advertise a sponsored link with Google with the sponsored keywords “Software, Operation Systems, Office” etc.

After entering those keywords for the advertising campaign (possibly using a stolen credit card, as malicious attackers often do) the malicious attacker creates two parts in his website, the first one looks like a valid software website and the second one is a malicious site that would install a Trojan horse on the “Target corp.” company's System Administrator computer. Both of these two different sites are actually stored under the same URL.

Reminder: Google tests would find the malicious website in no time and remove it but:

Here the new thing about Sponsored Links Jacking. The malicious attacker would gather information about Google. The information that needs to be gathered is:

1. Google’s automatic bots, spiders and crawlers headers.
2. Google’s IP ranges all over the world (From which Google manually test the sponsored links).
3. Optional: To create a better accurate spear attack the attacker needs to gather the IP address or IP range of the "Target corp." company.

This kind of information gathering is a very simple task to perform, especially for a malicious attacker that intends to gain profit from this "Spear Attack". The malicious attacker does not have to be extremely skilled hacker nor does he need relatively big amount of time for this kind of information gathering.

After the information is gathered, the malicious attacker would create a website with a mechanism that checks the information of the visitor. If it’s one of Google automatic bots, spiders and crawlers or the access is identified as being from one of the gathered Google IPs, the website would show a nice legitimate software selling website. If the access is identified as different from Google, the site will show a malicious page that would affect the user in a malicious way such as installing a Trojan horse on his computer.

The ”Target corp.” company System Administrator will probably search Google for software as he usually does and will probably encounter the sponsored link. Because it’s a Google sponsored link it should be relatively safe so there is probable that the System Administrator will enter this sponsored link to inquire about some software he needs.

At this point the game is over and the “Target corp.” company System Administrator's computer is infected.

There is an improved way to use this attack if the malicious attacker could get the optional information (the IP address or IP range of the Target). The malicious attacker can create the same mechanism as described above but limit it specifically for the Target's IP or IP range. That way Google or any other user that will enter this website will see a harmless software selling website. Only the users from the specific IP address or IP range will see the malicious page. This improved method will also prevent from link scanners to report this website as malicious because it will not show in their malicious websites repository.

Why Sponsored Links Jacking attacks are a security issue?

Sponsored Links Jacking attacks can be a “good” replacement to phishing attacks in general and to spear phishing attacks in particular. These days it’s easier than ever to identify phishing attack and stop them. Sponsored Links Jacking attacks overpower phishing attacks. SLJ is the real thing – while phishing attacks are just a disguise and are relatively easy to identify.

What are the differences between Sponsored Links Jacking attacks and any other Google adware attacks?

There are many Google, Google Adware, spear phishing and spear attacks out there. The Sponsored Links Jacking attack is another clever way of creating spear attacks. It does not replace any other form of attack, there are similar ways that can be used just like using the Sponsored Links Jacking attack.

Will the Sponsored Links Jacking attacks be used only to attack Google?

No.

This attack can be used to compromise any Sponsored Links service, services similar to Google, or any similar services in general. I used Google only as a Test Case.

Will the Sponsored Links Jacking attacks work perfectly every time?

No.

The Sponsored Links Jacking attack needs to have the proper environment and preparation in order for it to work as described in this document. However, if we compare it to any other spear attack it is not too complicated to implement.

Sponsored Links Jacking – Yaniv Miron - October 2008.

[#] E0F [#]