Sponsored Links Jacking

Yaniv Miron aka Lament

/ About Me

- Yaniv Miron aka Lament
- Security Researcher and Consultant
- CISO Certified from the Technion (Israel Institute of Technology)
- Certified Locksmith

Disclaimer

- This presentation was created for educational purposes only
- Certain parts of the SLJ attack are proven theoretically due to lack of time and resources while conducting this research
- No illegal actions were made during this research

Agenda

- Glossary
- What are SLJ Attacks?
- SLJ Test Case
- SLJ attack example

Glossary

- PPC - Pay Per Click
  - Internet advertising model, advertisers pay their host only when their ad is clicked.
- AdWords
  - Google's flagship advertising product, offers PPC advertising.

Glossary Cont.

- Phishing
  - …
- Spear Phishing
  - Targeted versions of phishing.

Glossary Cont.

- Sponsored Links
  - When a user searches Google's search engine, ads for relevant words are shown

    as "sponsored links" on the right side of the screen, and sometimes above the main search results.

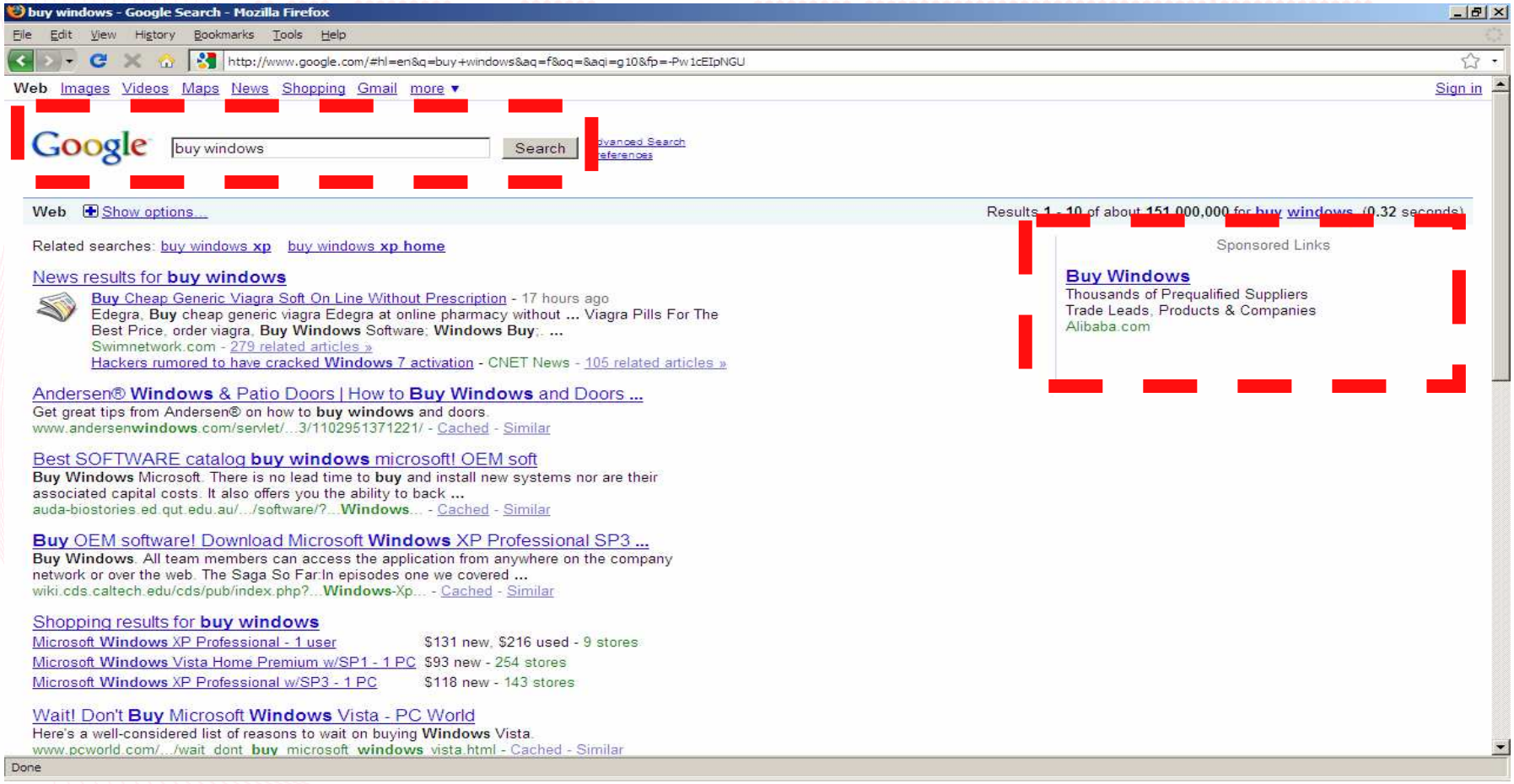
SLJ Attacks

- SLJ - Sponsored Links Jacking
- 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

- Test case scenario: Google
- Google search engine have a sponsored links system named Google AdWords Ads.
- Google is just an example, you can apply the attack on different search engines and websites.

Google SL


buy windows - Google Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.com/#hl=en&q=buy+windows&aq=f&oq=&aqi=g10&fp=-Pw1cEIpNGU
Web Images Videos Maps News Shopping Gmail more ▾
Sign in
Google
buy windows
Search
Advanced Search
Preferences
Web
Show options...
Results 1 - 10 of about 151,000,000 for buy windows. (0.32 seconds)
Related searches: buy windows xp buy windows xp home
Sponsored Links
Buy Windows
Thousands of Prequalified Suppliers
Trade Leads, Products & Companies
Alibaba.com
News results for buy windows
Buy Cheap Generic Viagra Soft On Line Without Prescription - 17 hours ago
Edegra, Buy cheap generic viagra Edegra at online pharmacy without ... Viagra Pills For The Best Price, order viagra, Buy Windows Software; Windows Buy;. ...
Swimnetwork.com - 279 related articles »
Hackers rumored to have cracked Windows 7 activation - CNET News - 105 related articles »
Andersen® Windows & Patio Doors | How to Buy Windows and Doors ...
Get great tips from Andersen® on how to buy windows and doors.
www.andersenwindows.com/servlet/...3/1102951371221/ - Cached - Similar
Best SOFTWARE catalog buy windows microsoft! OEM soft
Buy Windows Microsoft. There is no lead time to buy and install new systems nor are their associated capital costs. It also offers you the ability to back ...
auda-biostories.ed.qut.edu.au/.../software/?...Windows... - Cached - Similar
Buy OEM software! Download Microsoft Windows XP Professional SP3 ...
Buy Windows. All team members can access the application from anywhere on the company network or over the web. The Saga So Far:In episodes one we covered ...
wiki.cds.caltech.edu/cds/pub/index.php?...Windows-Xp... - Cached - Similar
Shopping results for buy windows
Microsoft Windows XP Professional - 1 user $131 new, $216 used - 9 stores
Microsoft Windows Vista Home Premium w/SP1 - 1 PC $93 new - 254 stores
Microsoft Windows XP Professional w/SP3 - 1 PC $118 new - 143 stores
Wait! Don't Buy Microsoft Windows Vista - PC World
Here's a well-considered list of reasons to wait on buying Windows Vista.
www.pcworld.com/.../wait_dont_buy_microsoft_windows_vista.html - Cached - Similar
Done

Google SL Security

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

The Victim

- 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.

SLJ Attack Base

- An attacker would advertise a sponsored link with Google with the sponsored keywords “Software, Operation Systems, Office” etc.

SLJ Attack Base Cont.

- 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.

SLJ Attack Base Cont.

- The first one looks like a valid software website.
- 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.

SLJ Attack Base Cont.

- **Reminder:** Google tests would find the malicious website in no time and remove it.
- That's where SLJ should be used.

SLJ Attack Base Cont.

- Here the new thing about Sponsored Links Jacking. The malicious attacker would gather information about Google.

SLJ Attack Base Cont.

- The information that needs to be gathered:
  - Google's automatic bots, spiders and crawlers headers / User-Agents.
  - Google's IP ranges all over the world (From which Google manually test the sponsored links).
  - Optional: To create a better accurate spear attack the attacker needs to gather the IP address or IP range of the "Target corp." company.

SLJ Attack Base Cont.

- Google's automatic bots, spiders and crawlers headers / User-Agents.
- From Google.com
  - http://www.google.com/support/webmasters/bin/answer.py?hl=en&answer=40364

SLJ Attack Base Cont.

Home
Help topics
Webmaster essentials
My site and Google
Using Webmaster Tools
Sitemaps
Help forum

Get started
Webmaster Guidelines
Webmaster checklist
Webmaster Central blog

Explore Google
About Google search results
Services and tools
Business solutions
Advertising

Blocking Googlebot and other Google robots with robots.txt

Print

Blocking Googlebot

Google uses several user-agents. You can block access to any of them by including the bot name on the User-agent line of an entry. Blocking Googlebot blocks all bots that begin with "Googlebot".

- **Googlebot:** crawl pages from our web index and our news index
- **Googlebot-Mobile:** crawls pages for our mobile index
- **Googlebot-Image:** crawls pages for our image index
- **Mediapartners-Google:** crawls pages to determine AdSense content. We only use this bot to crawl your site if AdSense ads are displayed on your site.
- **Adsbot-Google:** crawls pages to measure AdWords landing page quality. We only use this bot if you use Google AdWords to advertise your site.

For instance, to block Googlebot entirely, you can use the following syntax:

```
User-agent: Googlebot
Disallow: /
```

Allowing Googlebot

If you want to block access to all but a single robot, you can use the following syntax (note: we don't recommend doing this if you want your site to appear in the search results for other search engines such as MSN and Yahoo!):

```
User-agent: *
Disallow: /

User-agent: Googlebot
Disallow:
```

Googlebot follows the line directed at it, rather than the line directed at everyone.

The Allow extension

Googlebot recognises an extension to the robots.txt standard called Allow. This extension may not be recognized by all other search engine bots, so check with other search engines in which you are interested to find out. The Allow line works exactly like the Disallow

SLJ Attack Base Cont.

- Googlebot: crawl pages from our web index and our news index
- Googlebot-Mobile: crawls pages for our mobile index
- Googlebot-Image: crawls pages for our image index

SLJ Attack Base Cont.

- Mediapartners-Google: crawls pages to determine AdSense content. We only use this bot to crawl your site if AdSense ads are displayed on your site.
- Adsbot-Google: crawls pages to measure AdWords landing page quality. We only use this bot if you use Google AdWords to advertise your site.

SLJ Attack Base Cont.

- 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.

SLJ Attack Base Cont.

- After the information is gathered, the malicious attacker would create a website with a mechanism that checks the information of the visitor.

SLJ Attack Base Cont.

- 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.

SLJ Attack Base Cont.

- 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.

SLJ Attack Source Code Example

ConTEXT - [C:\sljgoogle.php *]

File Edit View Format Project Tools Options Window Help

```php
<?php
ob_start(); /* Fixing the 'header' error */

$useragent=$_SERVER['HTTP_USER_AGENT']; /* Getting the UserAgent */
$ipaddress=$_SERVER['REMOTE_ADDR']; /* Getting the IP Address */
$hostname=$_SERVER['REMOTE_HOST']; /* Getting the Host name */

$useragent=strtolower($useragent); /* Change to lowercase for old PHP versions */

/* Start echo some information */
echo "UserAgent is: $useragent";
echo "<br>";
echo "IP Address is: $ipaddress";
echo "<br>";
echo "Host name is: $hostname";
/* End echo some information */

/* Start Check for Google */
if ((strpos($ipaddress, "74.125.53") !== false) or (strpos($useragent, "google") !== false))
   /* If the 3 first octets equal to Google IP and the useragent contains the word google do */
   {
     echo "Hi Google!, How are you today?";
     header("Location:good.html"); /* Redirect to a good website */
   }
else
   {
     echo "Hi Victim!, Welcome!";
     header("Location:bad.html"); /* Redirect to a good website */
   }
/* End Check for Google */

ob_flush(); /* Fixing the 'header' error */
?>
```

Ln 35, Col 1 | Insert | Sel: Normal | Modified | DOS | File size: 1093

SLJ Attack Base Cont.

- The ”Target corp.” company system administrator will probably search Google for software as he usually does and will probably encounter the sponsored link.

SLJ Attack Base Cont.

- 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.

SLJ Attack Base Cont.

- At this point the game is over and the “Target corp.” company system administrator's computer is infected.

SLJ Attack Base Cont.

- 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.

SLJ Attack Base Cont.

- 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.

SLJ Attack Base Cont.

- 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.

SLJ as Security Issue

- Sponsored Links Jacking attacks can be a "good" replacement to phishing attacks in general and to spear phishing attacks in particular.

SLJ as Security Issue Cont.

- 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.

SLJ and 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.

SLJ and AdWare Attacks Cont.

- SLJ does not replace any other form of attack, there are similar ways that can be used just like using the Sponsored Links Jacking attack.

SLJ and Google

- Q: Will the Sponsored Links Jacking attacks be used only to attack Google?
- A: 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.

SLJ Success Rate

- Q: Will the Sponsored Links Jacking attacks work perfectly every time?
- A: 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.

/ Credits

- Milw0rm
  - www.milw0rm.com/papers/248
- Hacker Halted 2009
  - www.hackerhalted.com
- Wikipedia
  - www.wikipedia.org
- Google
  - www.google.com

#EOF#

Thank You!

Questions ?

>>

lament@ilhack.org