

# Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

26 October 2010



**October 26-28th 2010 Singapore**

Presented by:  
Rob Ragan  
Stach & Liu, LLC  
[www.stachliu.com](http://www.stachliu.com)

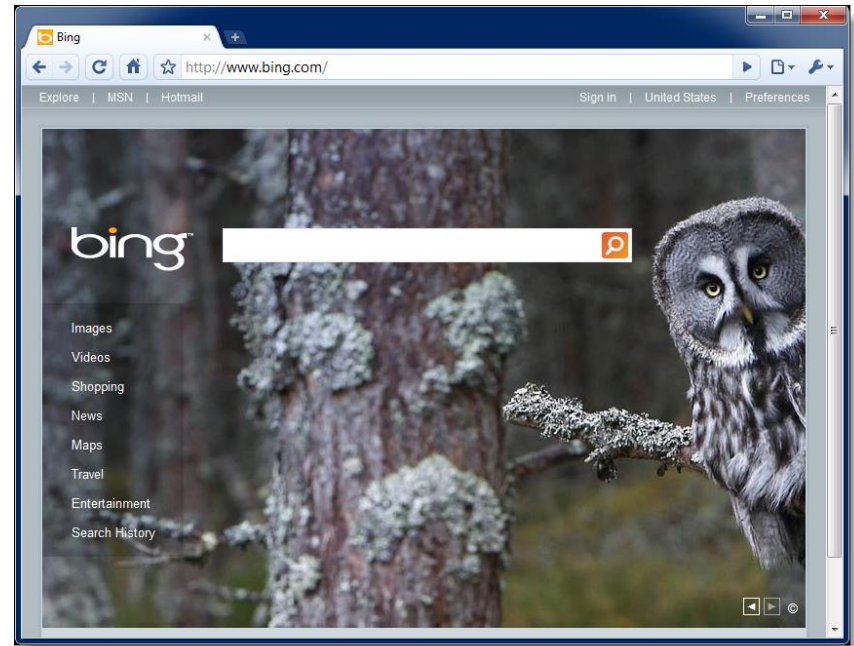
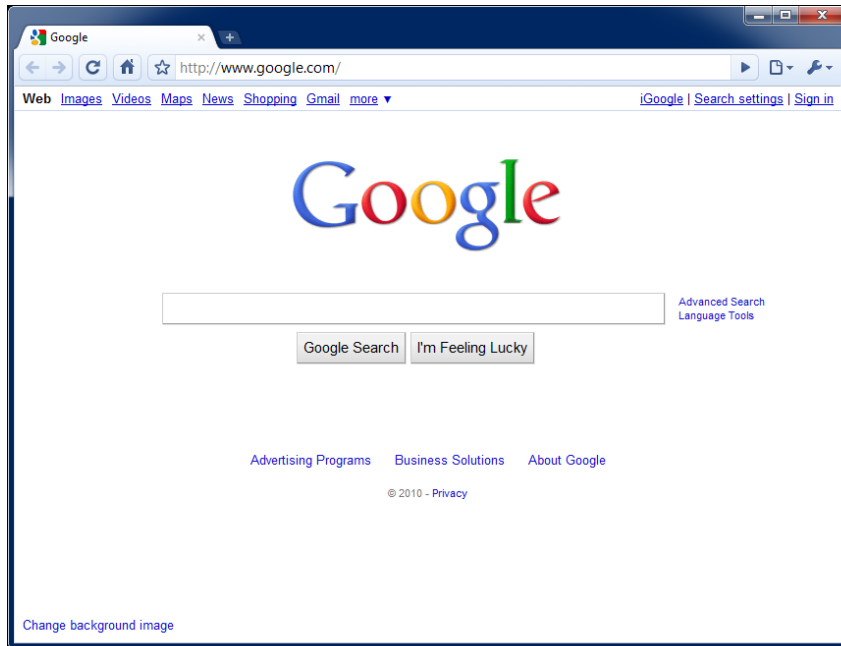
# Goals

## DESIRED OUTCOME

- *To improve* Google Hacking
  - Attacks and defenses
  - Advanced tools and techniques
- *To think differently* about exposures in publicly available sources
- To blow your mind!

# Google/Bing Hacking

## SEARCH ENGINE ATTACKS



# Attack Targets

## GOOGLE HACKING DATABASE

- Advisories and Vulnerabilities (215)
- Error Messages (58)
- Files containing juicy info (230)
- Files containing passwords (135)
- Files containing usernames (15)
- Footholds (21)
- Pages containing login portals (232)
- Pages containing network or vulnerability data (59)
- Sensitive Directories (61)
- Sensitive Online Shopping Info (9)
- Various Online Devices (201)
- Vulnerable Files (57)
- Vulnerable Servers (48)
- Web Server Detection (72)

# Attack Targets

GOOGLE HACKING DATABASE

## Old School Examples

- Error Messages
  - `filetype:asp + "[ODBC SQL"`
  - `"Warning: mysql_query()" "invalid query"`
- Files containing passwords
  - `inurl:passlist.txt`

# New Toolkit

STACH & LIU TOOLS

## Google Diggity

- Uses Google AJAX API
  - Not blocked by Google bot detection
  - Does not violate Terms of Service
- Can leverage [Google custom search](#)

## Bing Diggity

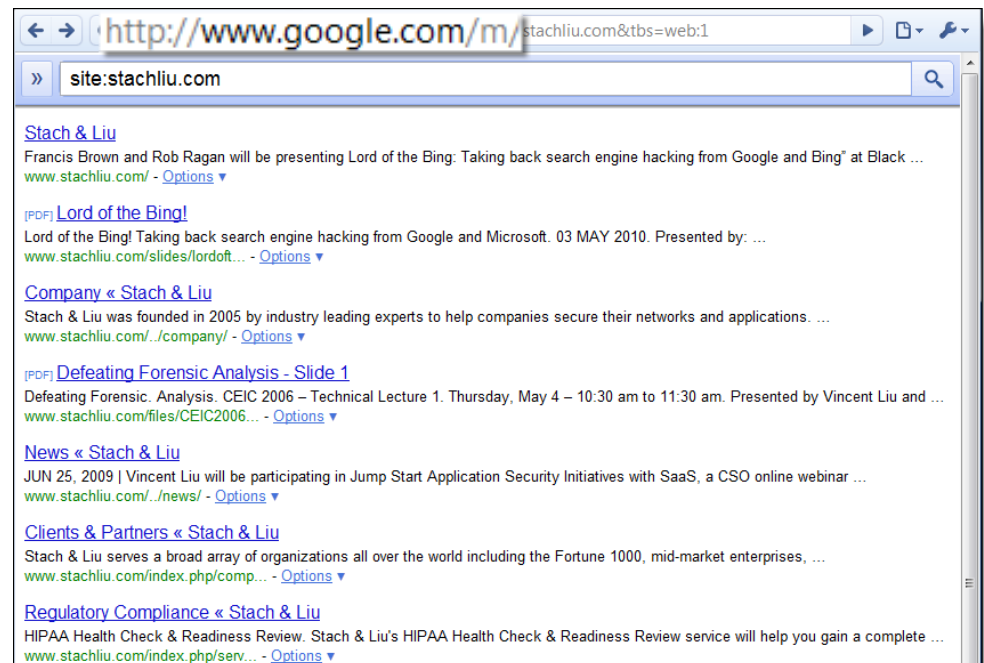
- Uses Bing SOAP API
- Company/Webapp Profiling
  - Enumerate: URLs, IP-to-virtual hosts, etc.
- Bing Hacking Database (BHDB)
  - Vulnerability search queries in Bing format

# New Toolkit

## STACH & LIU TOOLS

### GoogleScrape Diggity

- Uses Google mobile interface
  - Light-weight, no advertisements or extras
  - *Violates* Terms of Service
- Automatically leverages valid open proxies
- Spoofs User-agent and Referer headers
- Random `&userip=` value



# New Hack Databases

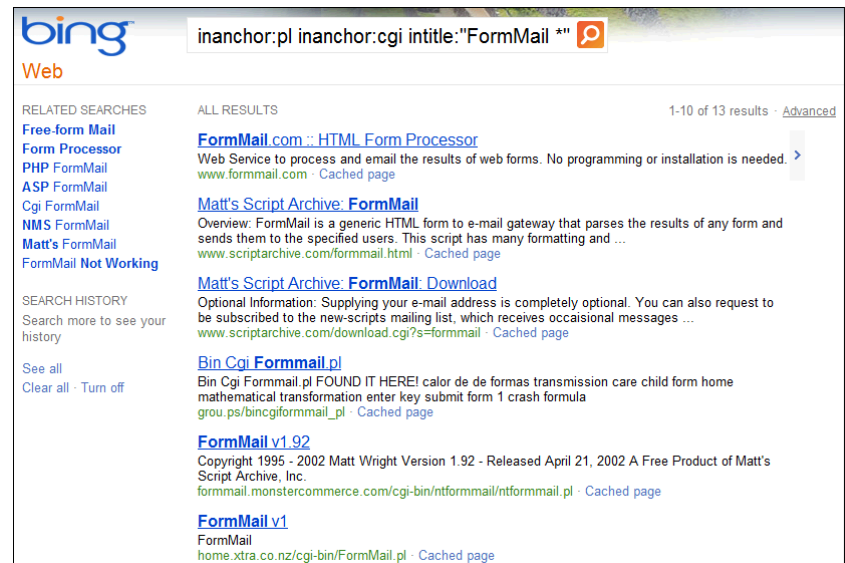
## ATTACK QUERIES

### BHDB – Bing Hacking Data Base

- First ever Bing Hacking database
- Bing has limitations that make it difficult to create vuln search queries
  - Bing disabled the **link:** and **linkdomain:** directives to combat abuse in March 2007
  - Does not support **ext:** or **inurl:**
  - The **filetype:** functionality is limited

### Example - Bing vulnerability search:

- GHDB query
  - "allintitle:Netscape FastTrack Server Home Page"
- BHDB version
  - "intitle:Netscape FastTrack Server Home Page"



The screenshot shows a Bing search results page for the query "inanchor:pl inanchor:cgi intitle:"FormMail \*"". The search results are displayed in a grid format. The top result is "FormMail.com :: HTML Form Processor" with a description: "Web Service to process and email the results of web forms. No programming or installation is needed." Below this is "Matt's Script Archive: FormMail" with a description: "Overview: FormMail is a generic HTML form to e-mail gateway that parses the results of any form and sends them to the specified users. This script has many formatting and ...". Other results include "FormMail v1.92" and "FormMail v1".



# New Hack Databases

## ATTACK QUERIES

### SLDB - Stach & Liu Data Base

- New Google/Bing hacking searches in active development by the S&L team

### SLDB Examples

- `ext:(doc | pdf | xls | txt | ps | rtf | odt | sxw | psw | ppt | pps | xml) (intext:confidential salary | intext:"budget approved") inurl:confidential`
- `( filetype:mail | filetype:eml | filetype:mbox | filetype:mbx ) intext:password|subject`
- `filetype:sql "insert into" (pass|passwd|password)`
- `!Host=*. * intext:enc_UserPassword=* ext:pcf`
- `"your password is" filetype:log`

NEW GOOGLE HACKING TOOLS

**DEMO**

# Traditional Defenses

## GOOGLE HACKING DEFENSES

- “Google Hack yourself” organization
  - Employ tools and techniques used by hackers
  - Remove info leaks from Google cache
    - Using Google Webmaster Tools
- Regularly update your robots.txt.
  - Or robots meta tags for individual page exclusion
- Data Loss Prevention/Extrusion Prevention Systems
  - Free Tools: OpenDLP, Senf
- Policy and Legal Restrictions

# Traditional Defenses

## GOOGLE HACKING DEFENSES

- “Google Hack yourself” organization
  - Employ tools and techniques used by hackers
  - Remove info leaks from Google cache
    - Using Google Webmaster Tools
- Regularly update your robots.txt
  - Or robots meta tags for individual page exclusion
- Data Loss Prevention/Extrusion Prevention Systems
  - Free Tools: OpenDLP, Senf
- Policy and Legal Restrictions



# Advanced Defenses

PROTECT YO NECK

# Existing Defenses

"HACK YOURSELF"

- ✓ Tools exist
- ✗ Convenient
- ✗ Real-time updates
- ✗ Multi-engine results
- ✗ Historical archived data
- ✗ Multi-domain searching

# Advanced Defenses

NEW HOT SIZZLE

Stach & Liu now proudly presents:

- Google Hacking Alerts
- Bing Hacking Alerts

# Google Hacking Alerts

## ADVANCED DEFENSES

### Google Hacking Alerts

- All hacking database queries using **Google alerts**
- Real-time vuln updates to >2400 hack queries via RSS
- Organized and available via **Google reader** importable file

stachliu0@gmail.com | [Settings](#) | [FAQ](#) | [Sign out](#)

**Google alerts** Manage your Alerts

GHDB regexes made into Google Alerts

Your Google Alerts [Switch to text emails](#) | [Export alerts](#)

Search terms	Type	How often	Email length	Deliver to
<input type="checkbox"/> <a href="#">!Host=*.*.intext:enc_UserPassword=* ext:pcf</a>	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a> <a href="#">edit</a>
<input type="checkbox"/> <a href="#">"# Dumping data for table (username user users password)"</a>	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a> <a href="#">edit</a>
<input type="checkbox"/> <a href="#">"# Dumping data for table"</a>	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a> <a href="#">edit</a>
<input type="checkbox"/> <a href="#">"# phpMyAdmin MySQL-Dump" "INSERT INTO" -"the"</a>	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a> <a href="#">edit</a>

RSS Feeds generated that track new GHDB vulnerable pages in real-time



# Google Hacking Alerts

## ADVANCED DEFENSES

Google reader

All items (1000+)

People you follow

Explore

Subscriptions

- FSDB-Backup Files (195)
- FSDB-Configuration Ma... (371)
- FSDB-Error Messages (654)
- FSDB-Privacy Related (501)
- FSDB-Remote Administr... (102)
- FSDB-Reported Vulnera... (90)
- FSDB-Technology Profile (652)
- GHDB-Advisories and V... (1000+)
- GHDB-Error Messages (1000+)
- Google Alerts - "mysql..." (11)**
- Google Alerts - "A sv..." (10)
- Google Alerts - "acce..." (45)
- Google Alerts - "An i..." (1)
- Google Alerts - "ASP..." (5)

Google Alerts - "mysql error with query"

Show: 11 new items - all items

James Bond 007 :: MI6 - The Home Of James Bond

via [Google Alerts - "mysql error with query"](#)

mysql error with query SELECT c.citem as itemid, c.cnumber as commentid, c.cbody as body, c.cuser as user, c.cmail as userid, c.cemail as email, ...  
[www.mi6.co.uk/mi6.php3/news/index.php?itemid...](http://www.mi6.co.uk/mi6.php3/news/index.php?itemid...)

James Bond needs help!  
mysql error page snippet conveniently provided in RSS summary

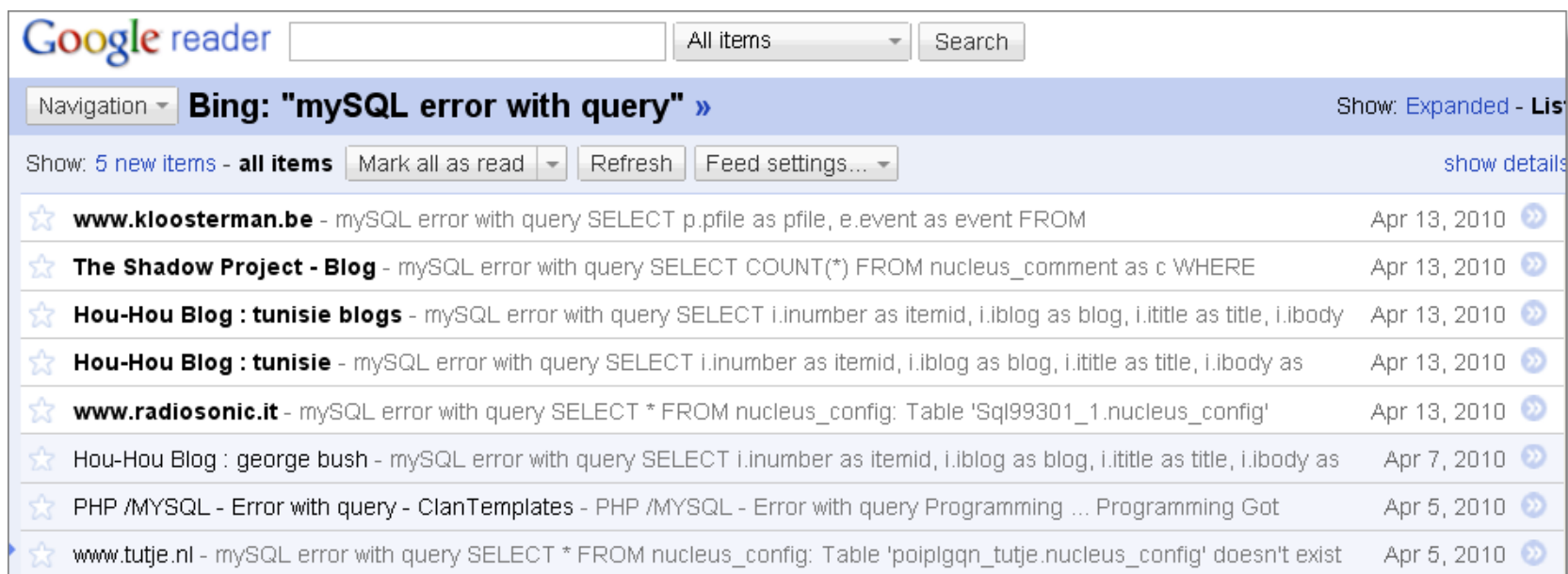
Several thousand GHDB/FSDB vuln alerts generated each day

# Bing Hacking Alerts

## ADVANCED DEFENSES

### Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Leverage `&format=rss` directive to turn into update feeds



The screenshot shows a Google Reader interface. At the top, there is a search bar with the text "Google reader" and a search button. Below the search bar, there is a navigation bar with a dropdown menu set to "All items" and a "Search" button. The main content area displays a feed titled "Bing: 'mysql error with query' »". The feed shows a list of items with their titles, descriptions, and dates. The items are:

Item	Date
www.kloosterman.be - mysql error with query SELECT p.pfile as pfile, e.event as event FROM	Apr 13, 2010
The Shadow Project - Blog - mysql error with query SELECT COUNT(*) FROM nucleus_comment as c WHERE	Apr 13, 2010
Hou-Hou Blog : tunisie blogs - mysql error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody	Apr 13, 2010
Hou-Hou Blog : tunisie - mysql error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody as	Apr 13, 2010
www.radiosonic.it - mysql error with query SELECT * FROM nucleus_config: Table 'Sql99301_1.nucleus_config'	Apr 13, 2010
Hou-Hou Blog : george bush - mysql error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody as	Apr 7, 2010
PHP /MYSQL - Error with query - ClanTemplates - PHP /MYSQL - Error with query Programming ... Programming Got	Apr 5, 2010
www.tutje.nl - mysql error with query SELECT * FROM nucleus_config: Table 'poiplgqn_tutje.nucleus_config' doesn't exist	Apr 5, 2010

ADVANCED DEFENSE TOOLS

DEMO

# New Defenses

"GOOGLE/BING HACK ALERTS"

- ✓ Tools exist
- ✓ Convenient
- ✓ Real-time updates
- ✓ Multi-engine results
- ✓ Historical archived data
- ✓ Multi-domain searching

# Google Apps Explosion

SO MANY APPLICATIONS TO ABUSE

Google alerts

Google reader

Google™  
PhoneBook

Google custom search

Google™  
trends

Google buzz 

Google™  
code search labs 

Google code

Google health

Google calendar

Google news

Google™  
public data explorer  
labs 

Google docs

Google Insights for Search  
beta

Google™ wave   
preview

Google blogs

Google maps

Google groups

# Google Voice



## PARTY LINE

← → ↻ ↑ ☆ [http://www.google.com/m/search?q=site:https://www.google.com/voice/fm/\\*&start=10&](http://www.google.com/m/search?q=site:https://www.google.com/voice/fm/*&start=10&)

Google

site:https://www.goog Search

Web Images Local News

[Google Voice](#)  
hi andy this is mom i just wanted you to know that i just got out of the eye doctor and he says he lives in it is ...  
[www.google.com/voice/fm/01377638746...](http://www.google.com/voice/fm/01377638746...)

[Google Voice](#)  
Google Voice Home. New Message From. Blue\_ghost. +881631562579 +881631562...  
[www.google.com/voice/fm/11063046644...](http://www.google.com/voice/fm/11063046644...)

[Google Voice](#)  
hello this is lauren john reporting from the village instead of the in molly this is a little the because it was but ...  
[www.google.com/voice/fm/11063046644...](http://www.google.com/voice/fm/11063046644...)

[Google Voice](#)  
Hey, good morning. If it's David, calling from box. Dot Net just want to get touch. It looks like you were trying to ...  
[www.google.com/voice/fm/03548537891...](http://www.google.com/voice/fm/03548537891...)

[Google Voice](#)  
New Message From. Thach Nguyen (206) 321-2080. 7/14/09 9:02 AM (104 minutes ago) . Play.  
[www.google.com/voice/fm/13418109598...](http://www.google.com/voice/fm/13418109598...)

# Google Code Search



## VULNS IN OPEN SOURCE CODE

- Regex search for vulnerabilities in public code
- Example: SQL Injection in ASP querystring
  - `select.*from.*request\..QUERYSTRING`

The screenshot shows a Google Code Search result for the query `select.*from.*request\..QUERYSTRING`. The search results are for a file named `post.asp`. A red callout box points to the `reply_id` parameter in the SQL query, stating that it is an SQL injectable querystring parameter. The search results show two instances of the vulnerability, both with the `reply_id` parameter highlighted in red.

Code

Results 1 - 10 of about 2,000.

[post.asp](#)

```
45: strSql ="SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br>×çðâ±°ö»óð,ÃîÃðÃ×-ðß°í²ùÀíô±²ÅÄÜ±±±öâ,øìú×ó."

57: strSql ="SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çðâ±°ö»óð,ÃîÃðÃ×-ðß°í²ùÀíô±²ÅÄÜ±±±öâ,øìú×ó."
```

[www.cnarts.net/eweb/download/software/bbs/tradeforum.zip](http://www.cnarts.net/eweb/download/software/bbs/tradeforum.zip) - Unknown - ASP - [More from tradeforum.zip](#) »

GOOGLE CODE SEARCH HACKING

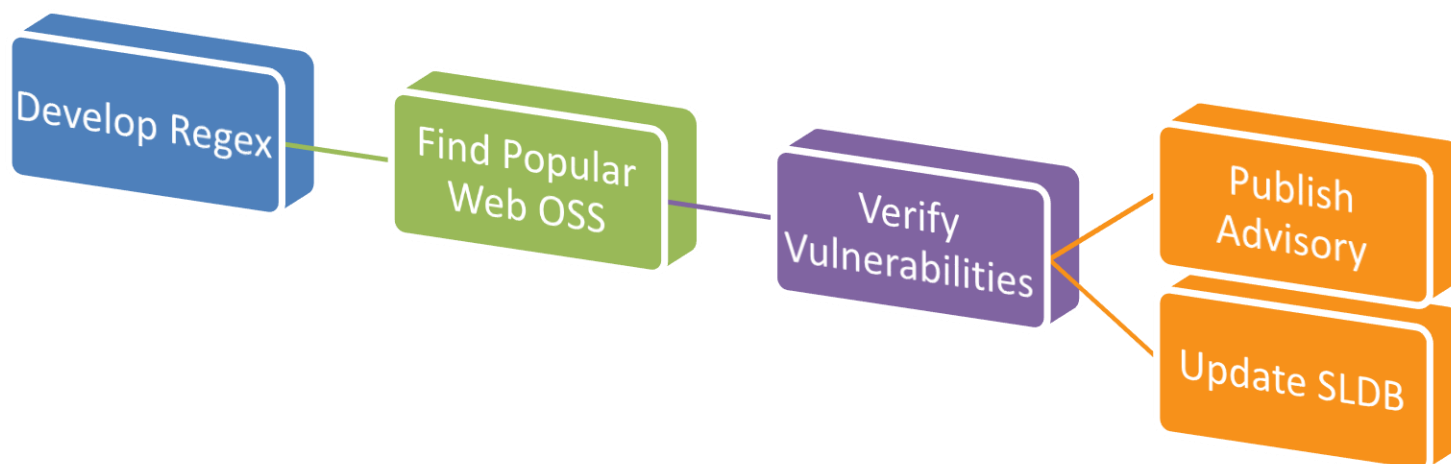
**DEMO**



# Google Code Search



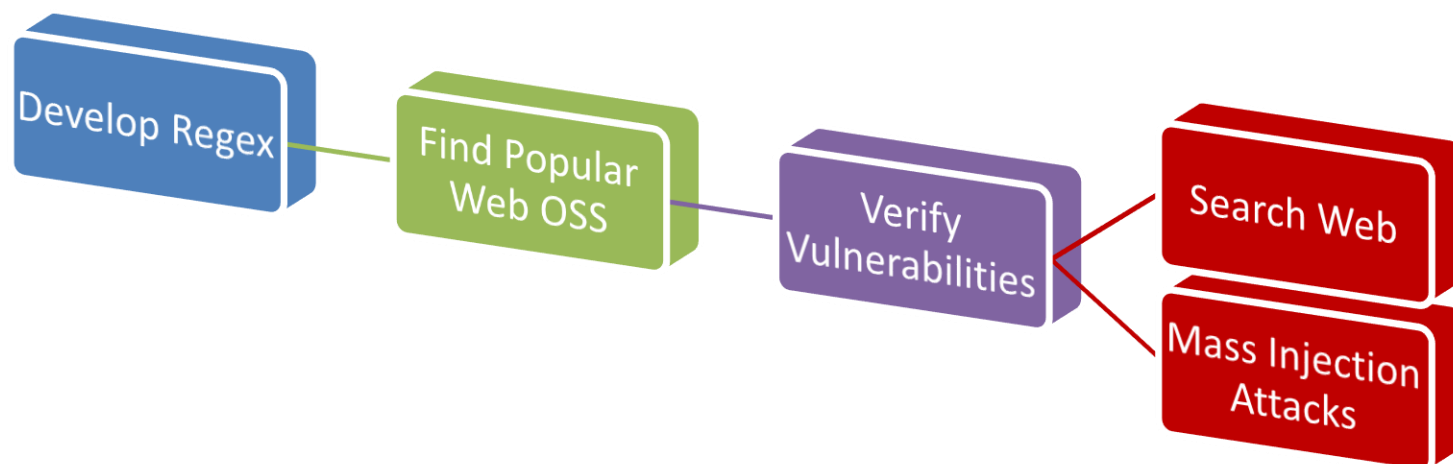
VULNS IN OPEN SOURCE CODE



# Google Code Search



VULNS IN OPEN SOURCE CODE



# Black Hat SEO

## SEARCH ENGINE OPTIMIZATION

- Use popular search topics du jour
- Pollute results with links to badware
- Increase chances of a successful attack



# Google Trends



## BLACK HAT SEO RECON

The screenshot shows the Google Insights for Search interface. The 'Compare by' section has 'Search terms' selected. The 'Search terms' input field contains 'All search terms'. The 'Filter' section is set to 'Web Search', 'United States', 'All subregions', 'All metros', '2004 - present', and 'All Categories'. A red callout box points to the filter settings with the text 'Top Google searches over past 6 years'. Below the filters, the 'Web Search Interest' section shows 'United States, 2004 - present'. The 'Search terms' table lists 'lyrics' as the top search, circled in red. A red callout box points to this entry with the text 'Fake lyrics web sites setup to appear in Google search results, infect you with malware upon clicking'. To the right, a news article snippet is visible with the headline 'Lada Gaga, Rihanna lyrics sites used to foist Java exploit'.

Google Insights for Search beta

Help | Sign in | Download as CSV | English (US)

**Compare by**

- Search terms
- Locations
- Time Ranges

**Search terms**

Tip: Use a comma as shorthand to add comparison items. (tennis, squash)

All search terms

**Filter**

Web Search

United States | All subregions | All metros

2004 - present

All Categories

Search

**Web Search Interest**

United States, 2004 - present

**Search terms**

**Top searches**

- lyrics
- you
- yahoo

**Lada Gaga, Rihanna lyrics sites used to foist Java exploit**

Dan Kaplan April 14, 2010

PRINT | EMAIL | REPRINT | PERMISSIONS | FONT SIZE: A | A | A

As expected, virus writers now are actively exploiting a zero-day Sun

RELATED ARTICLES

# Defenses

## BLACKHAT SEO DEFENSES

- Malware Warning Filters
  - Google Safe Browsing
  - Microsoft SmartScreen Filter
  - Yahoo Search Scan
- Sandbox Software
  - Sandboxie ([sandboxie.com](http://sandboxie.com))
  - Dell KACE - Secure Browser
  - Adobe Reader Sandbox (Protected Mode)
- No-script and Ad-block browser plugins

# Mass Injection Attacks

## MALWARE GONE WILD

### Malware Distribution Woes

- Popular websites victimized, become malware distribution sites to their own customers

#### Massive Malware Hits Media Web Sites

Security researchers estimate that roughly 7,000 Web pages were compromised in a SQL injection attack this week, including *The Wall Street Journal* and *Jerusalem Post*.

By Mathew J. Schwartz, [InformationWeek](#)

June 10, 2010

URL: <http://www.informationweek.com/story/showArticle.jstpl?articleID=225600247>

"Every time I load Jpost site, I get nas on Tuesday, referring to the Jerusalem

Sure enough, the Web sites of the *Jerusalem Post* and the Association of Christian Scholars sites serving malware to viewers.

From: [www.itworld.com](http://www.itworld.com)

#### Mass Web attack hits Wall Street Journal, Jerusalem Post

by Robert McMillan

**June 9, 2010** —Internet users have been hit by a widespread Web attack that has compromised thousands of Web sites, including Web pages belonging to the Wall Street Journal and the Jerusalem Post.

Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include [servicewomen.org](http://servicewomen.org) and [intjobs.org](http://intjobs.org).

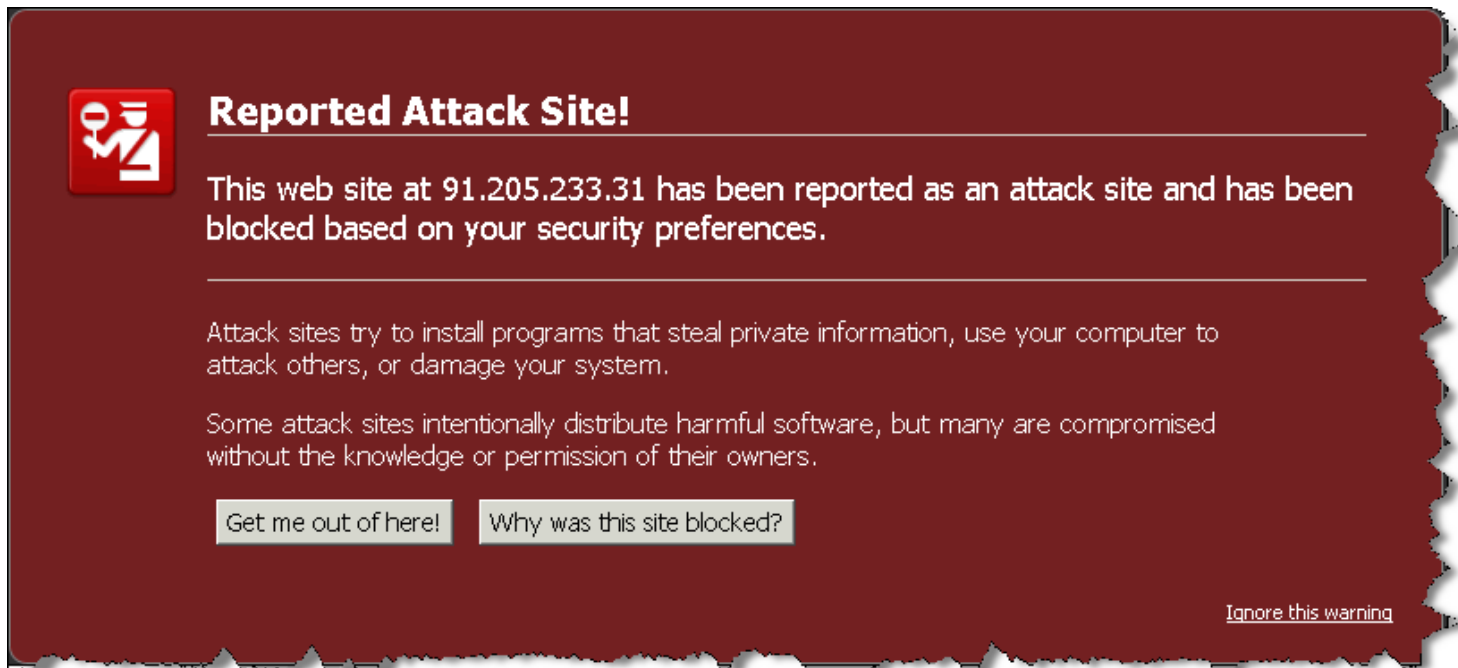



# Malware Browser Filters

## URL BLACK LIST

Protecting users from known threats

- Joint effort to protect customers from known malware and phishing links



 **Reported Attack Site!**

This web site at 91.205.233.31 has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#) [Why was this site blocked?](#)

[Ignore this warning](#)

# Malware Ads

## BLACK HAT ADS

The image shows a Bing search results page for the query "adobe reader". The search bar at the top contains "adobe reader" and the Bing logo is on the left. Below the search bar, there are tabs for "Web" and "News". The search results are displayed in a grid format. On the left side, there are "RELATED SEARCHES" and "SEARCH HISTORY" sections. The main search results are listed in the center, with a red box highlighting the top three sponsored results and a green box highlighting the bottom result. The top three results are for "Reader 9.0 -Official Site", "Adobe Acrobat 9 Download", and "Adobe Reader Download". The bottom result is for "Adobe - Adobe Reader".

**bing**™

adobe reader

Web News

RELATED SEARCHES

- Adobe Reader 0Day
- Adobe Reader Free Download
- Adobe Reader 7 Free Download
- Adobe Acrobat Reader 8.1
- Adobe Reader Plugin
- Adobe Reader 10
- Free Adobe Reader for XP
- Java

SEARCH HISTORY

adobe reader

See all

Clear all · Turn off

ALL RESULTS 1-10 of 54,900,000 results · [Advanced](#)

**Reader 9.0 -Official Site** Sponsored sites  
[www.PDF-Format.com](http://www.PDF-Format.com) · Open, Create & Edit PDF Files! Official Site (Recommended Download)

**Adobe Acrobat 9 Download**  
[AdobeAcrobat.PDF-Software.com](http://AdobeAcrobat.PDF-Software.com) · Ultra Fast Acrobat Download - Latest Version 100% Guaranteed

**Adobe Reader Download**  
[AdobeProReader10.com/Free](http://AdobeProReader10.com/Free) · New **Adobe Reader** Official Version. 100% Support. Free Download!

**Adobe Acrobat 9.3 Version**  
[www.PDF-9-D0wnload.com](http://www.PDF-9-D0wnload.com) · Download **Adobe** PDF Latest Version Ultra Fast 100% Guaranteed!

**Adobe - Adobe Reader**  
Download **Adobe Reader** to view, print and collaborate on PDF files.  
[get.adobe.com/reader](http://get.adobe.com/reader) · Cached page

- Get Flash Player
- Adobe - Adobe Reader
- Show more results from [get.adobe.com](http://get.adobe.com)
- Adobe - Adobe Air
- Accessibility

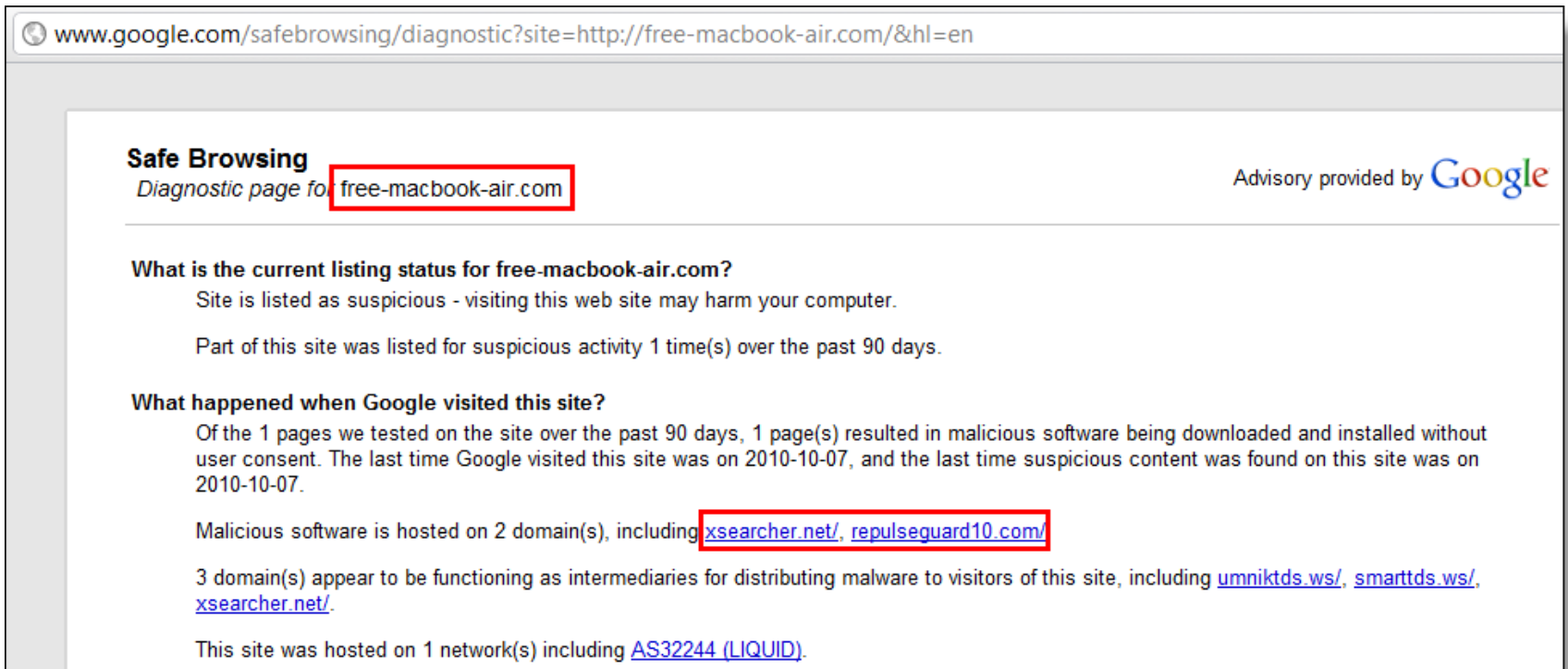


# Advanced Defenses

PROTECT YO NECK

# SafeBrowsing Diagnostic

## ADVANCED DEFENSES



The screenshot shows a web browser window with the address bar containing the URL: [www.google.com/safebrowsing/diagnostic?site=http://free-macbook-air.com/&hl=en](http://www.google.com/safebrowsing/diagnostic?site=http://free-macbook-air.com/&hl=en). The page content includes:

- Safe Browsing** header with the text "Diagnostic page for [free-macbook-air.com](http://free-macbook-air.com)".
- Advisory provided by Google logo.
- What is the current listing status for free-macbook-air.com?**
  - Site is listed as suspicious - visiting this web site may harm your computer.
  - Part of this site was listed for suspicious activity 1 time(s) over the past 90 days.
- What happened when Google visited this site?**
  - Of the 1 pages we tested on the site over the past 90 days, 1 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2010-10-07, and the last time suspicious content was found on this site was on 2010-10-07.
  - Malicious software is hosted on 2 domain(s), including [xsearcher.net/](http://xsearcher.net/), [repulseguard10.com/](http://repulseguard10.com/).
  - 3 domain(s) appear to be functioning as intermediaries for distributing malware to visitors of this site, including [umniktds.ws/](http://umniktds.ws/), [smarttds.ws/](http://smarttds.ws/), [xsearcher.net/](http://xsearcher.net/).
  - This site was hosted on 1 network(s) including [AS32244 \(LIQUID\)](#).

# Malware Diggity

## ADVANCED DEFENSES

### Malware Diggity

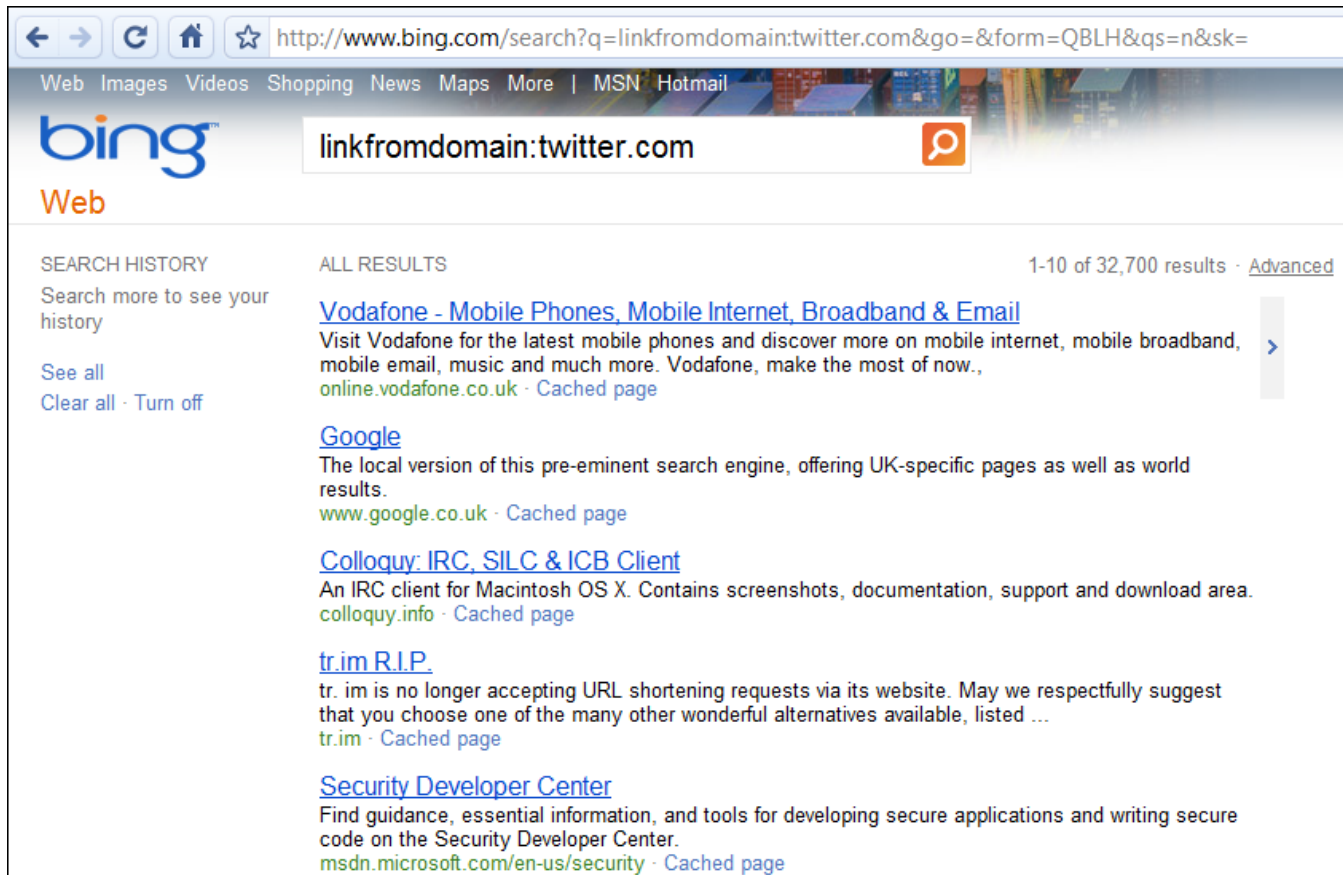
- Uses Bing's **linkfromdomain:** directive to *identify off-site links* of the domain(s) you wish to monitor
- Compares to *known malware sites/domains*
  - Alerts if site is compromised and now distributing malware
  - Monitors new Google Trends links

### Malware Diggity Alerts

- Leverages the Bing **'&format=rss'** directive, to *actively monitor new off-site links* of your site as they appear
- Immediately lets you know if you have been compromised by one of these mass injection attacks or if your site has been black listed

# Malware Diggity

## ADVANCED DEFENSES



The screenshot shows a Bing search results page for the query "linkfromdomain:twitter.com". The browser address bar displays the URL "http://www.bing.com/search?q=linkfromdomain:twitter.com&go=&form=QBLH&qsn=n&sk=".

The search results are categorized under "Web" and show "ALL RESULTS" for "1-10 of 32,700 results". The results list includes:

- Vodafone - Mobile Phones, Mobile Internet, Broadband & Email**  
Visit Vodafone for the latest mobile phones and discover more on mobile internet, mobile broadband, mobile email, music and much more. Vodafone, make the most of now.,  
[online.vodafone.co.uk](http://online.vodafone.co.uk) - Cached page
- Google**  
The local version of this pre-eminent search engine, offering UK-specific pages as well as world results.  
[www.google.co.uk](http://www.google.co.uk) - Cached page
- Colloquy: IRC, SILC & ICB Client**  
An IRC client for Macintosh OS X. Contains screenshots, documentation, support and download area.  
[colloquy.info](http://colloquy.info) - Cached page
- tr.im R.I.P.**  
tr. im is no longer accepting URL shortening requests via its website. May we respectfully suggest that you choose one of the many other wonderful alternatives available, listed ...  
[tr.im](http://tr.im) - Cached page
- Security Developer Center**  
Find guidance, essential information, and tools for developing secure applications and writing secure code on the Security Developer Center.  
[msdn.microsoft.com/en-us/security](http://msdn.microsoft.com/en-us/security) - Cached page

# Malware Diggity

ADVANCED DEFENSES

**YAHOO!**

**SITE EXPLORER**

Site Explorer

- Add to MySites
- My Sites
- Submit Your Site
- Preferences
- Blog
- Badge
- Web Service API
- Feedback

**Results**

Pages (70) **Inlinks (4,130)** Show Inlinks:  to:

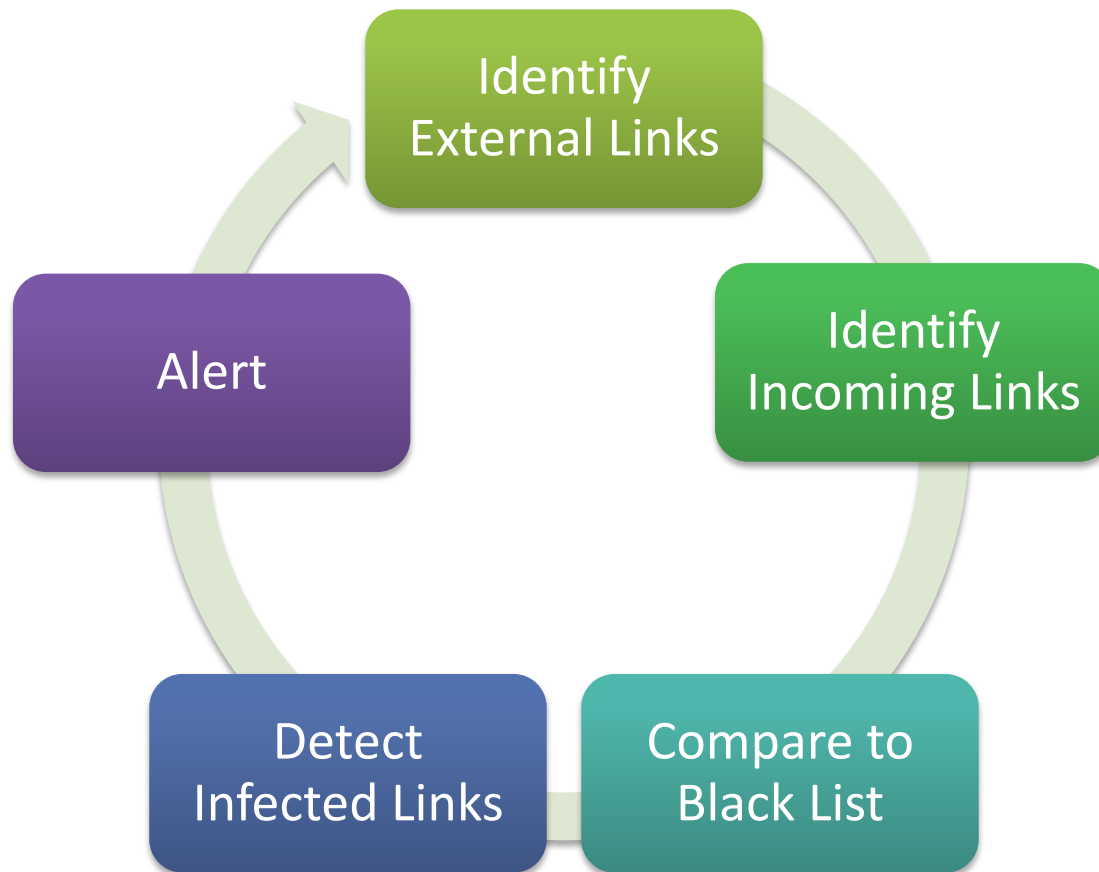
Result details:

[Submit webpage or Site Feed](#) | [Export first 1000 results to TSV](#)

- Unofficial MD5**  
text/html <http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html> - 12k - cache
- Offensive Computing | Community Malicious code research and ...**  
text/html <http://www.offensivecomputing.net/> - 35k - cache
- Approved Scanning Vendors**  
text/html [https://www.pcisecuritystandards.org/pdfs/asv\\_report.html](https://www.pcisecuritystandards.org/pdfs/asv_report.html) - 34k - cache
- Peter Selinger: MD5 Collision Demo**  
text/html <http://www.mscs.dal.ca/~selinger/md5collision/> - 13k - cache
- Microsoft BlueHat Blog - Site Home - TechNet Blogs**  
text/html <http://blogs.technet.com/b/bluehat/> - 140k - cache
- Checkmarx Source Code Analysis Technologies**  
text/html <http://www.checkmarx.com/> - 48k - cache
- Black Hat USA Spotlight: ATL Killbit Bypass - Microsoft ...**  
text/html <http://blogs.technet.com/b/bluehat/archive/2009/07/27/black-hat-usa-atl-killbit-bypass.aspx> - 151k - cache

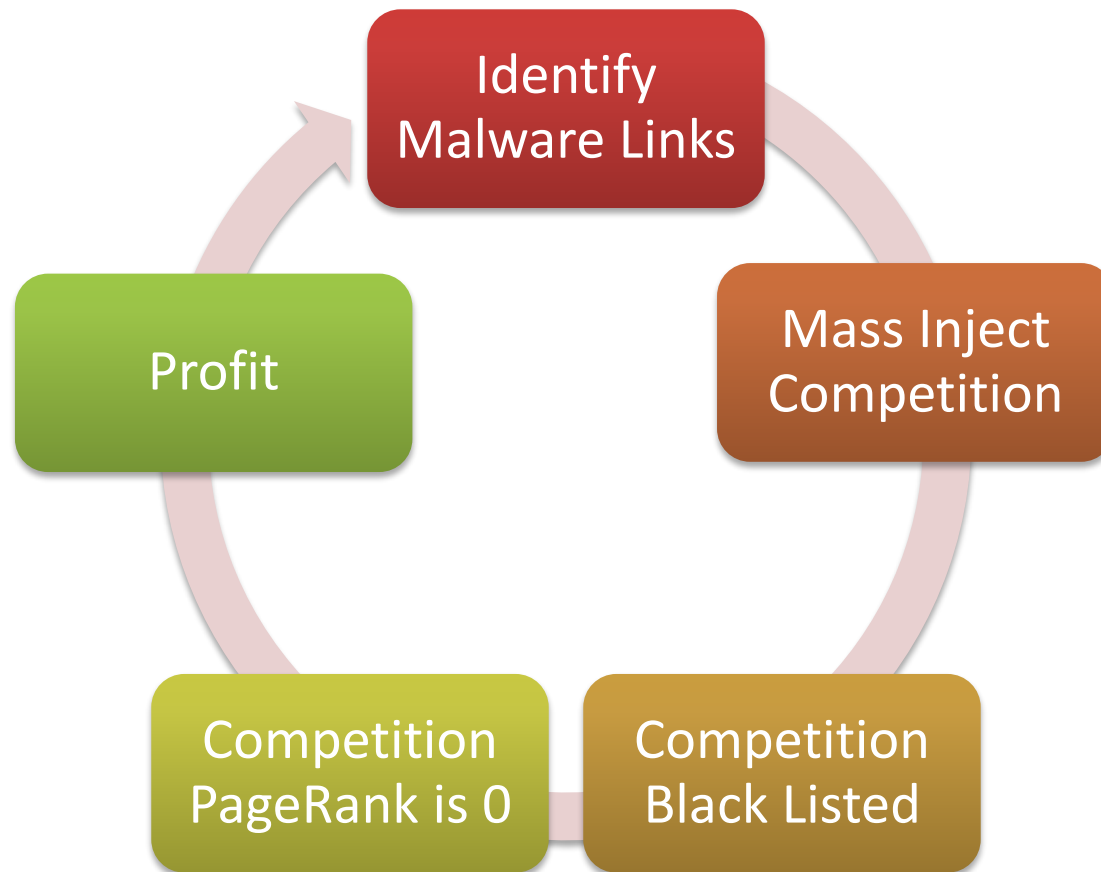
# Malware Monitoring

## INFECTION DETECTION



# Search Engine deOptimization

BLACK LIST YOUR FOES



# Safe Browsing Alerts

## ADVANCED DEFENSES

The screenshot shows the Google Safe Browsing Alerts for Network Administrators interface. The page title is "Google Safe Browsing Alerts for Network Administrators". The main content area is titled "Home" and contains a "Messages" section. A message states: "You have no recent notification emails. Once you add and verify an AS,". Below this message is a text input field with the placeholder text "Enter the AS you'd like to manage." and a "Continue" button. On the left side, there is a navigation menu with "Home" and "Messages" links. Below the navigation menu, there is a paragraph of text explaining the service: "Safe Browsing Alerts for Network Administrators allows autonomous system (AS) administrators to register to receive Google Safe Browsing notifications. The goal is to provide network administrators with information of malicious content that is being hosted on their networks." At the bottom of the left sidebar, there is a yellow box containing a link to "Malware Forum".

Google Safe Browsing Alerts for Network Administrators

Home

Messages

Safe Browsing Alerts for Network Administrators allows autonomous system (AS) administrators to register to receive Google Safe Browsing notifications. The goal is to provide network administrators with information of malicious content that is being hosted on their networks.

Malware Forum

Home

Messages

You have no recent notification emails. Once you add and verify an AS,

Enter the AS you'd like to manage.

Continue



# Future Direction

## PREDICTIONS

Google policy is to get right up to the creepy line and **not** cross it.

– Eric Schmidt  
Google CEO

# Predictions

## FUTURE DIRECTIONS

### Data Explosion

- More data indexed, searchable
- Real-time, streaming updates
- Faster, more robust search interfaces

### Google Involvement

- Filtering of search results
- Better GH detection and tool blocking

### Renewed Tool Dev

- Google Ajax API based
- Bing/Yahoo/other engines
  - Search engine aggregators
  - Customized search engines
- Google Code and Other Open Source Repositories
  - MS CodePlex, SourceForge, ...
- More automation in tools
  - Real-time detection and exploitation
  - Google worms

Questions?  
Ask us something  
We'll try to answer it.

For more info:  
Email: [contact@stachliu.com](mailto:contact@stachliu.com)  
Project: [diggity@stachliu.com](mailto:diggity@stachliu.com)  
Stach & Liu, LLC  
[www.stachliu.com](http://www.stachliu.com)

# Thank You

Stach & Liu Project info:

<http://www.stachliu.com/index.php/resources/tools/google-hacking-diggity-project/>