

# Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

8 October 2010



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

# Goals

## DESIRED OUTCOME

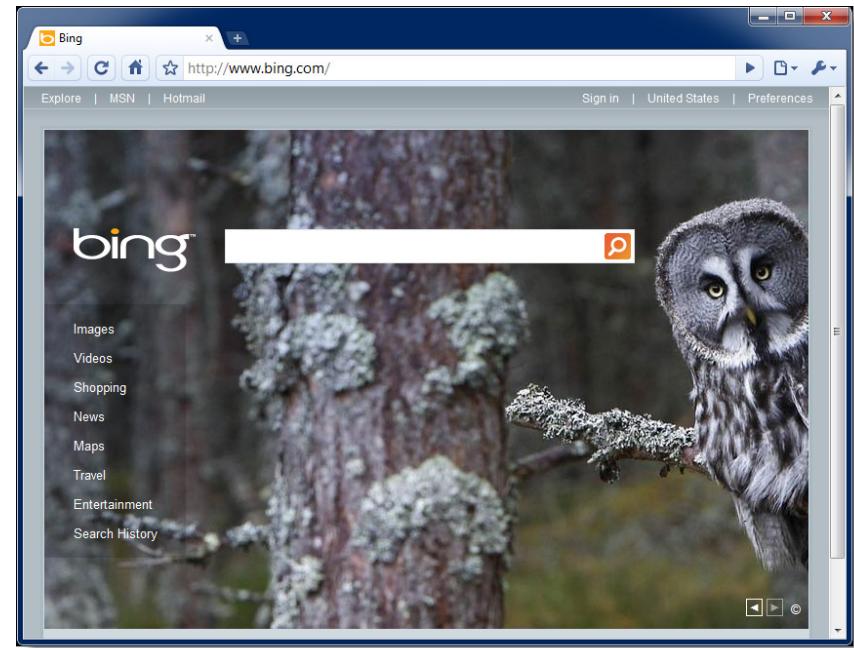
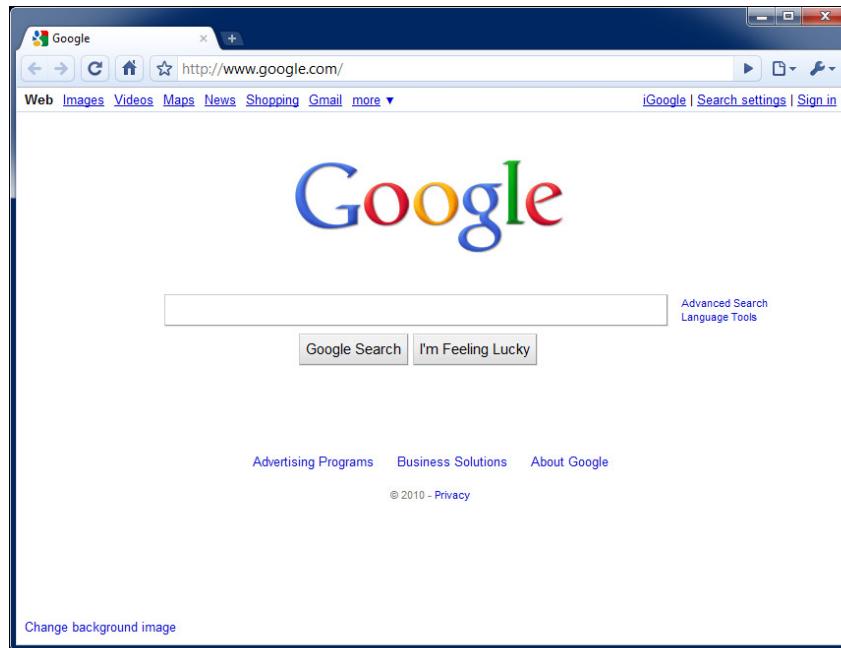
- *To improve* Google Hacking
  - Attacks and defenses
  - Advanced tools and techniques
- *To think differently* about exposures in publicly available sources
- To blow your mind!



# 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

http://www.google.com/m/stachliu.com&tbs=web:1

site:stachliu.com

[Stach & Liu](#)  
Francis Brown and Rob Ragan will be presenting Lord of the Bing: Taking back search engine hacking from Google and Bing" at Black ...  
[www.stachliu.com/](#) - Options ▾

[\[PDF\] Lord of the Bing!](#)  
Lord of the Bing! Taking back search engine hacking from Google and Microsoft. 03 MAY 2010. Presented by: ...  
[www.stachliu.com/slides/lordof...](#) - Options ▾

[Company « Stach & Liu](#)  
Stach & Liu was founded in 2005 by industry leading experts to help companies secure their networks and applications. ...  
[www.stachliu.com/..company/](#) - Options ▾

[\[PDF\] Defeating Forensic Analysis - Slide 1](#)  
Defeating Forensic Analysis. CEIC 2006 – Technical Lecture 1. Thursday, May 4 – 10:30 am to 11:30 am. Presented by Vincent Liu and ...  
[www.stachliu.com/files/CEIC2006...](#) - Options ▾

[News « Stach & Liu](#)  
JUN 25, 2009 | Vincent Liu will be participating in Jump Start Application Security Initiatives with SaaS, a CSO online webinar ...  
[www.stachliu.com/..news/](#) - Options ▾

[Clients & Partners « Stach & Liu](#)  
Stach & Liu serves a broad array of organizations all over the world including the Fortune 1000, mid-market enterprises, ...  
[www.stachliu.com/index.php/comp...](#) - Options ▾

[Regulatory Compliance « Stach & Liu](#)  
HIPAA Health Check & Readiness Review. Stach & Liu's HIPAA Health Check & Readiness Review service will help you gain a complete ...  
[www.stachliu.com/index.php/serv...](#) - Options ▾

# 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. The search query is "inanchor:pl inanchor:cgi intitle:"FormMail"" with a wildcard at the end. The results are filtered to show 1-10 of 13 results. The first result is "FormMail.com :: HTML Form Processor", which is described as a web service for processing and emailing form results. The second result is "Matt's Script Archive: FormMail", which is a generic HTML form to email gateway. The third result is "Bin Cgi Formmail.pl", which is a script for handling form submissions. The fourth result is "FormMail v1.92", which is a free product from Matt Wright's Script Archive. The fifth result is "FormMail v1", which is another version of the script.

Result	Description
1. FormMail.com :: HTML Form Processor	Web Service to process and email the results of web forms. No programming or installation is needed.
2. Matt's Script Archive: FormMail	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 ...
3. Bin Cgi Formmail.pl	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
4. FormMail v1.92	Copyright 1995 - 2002 Matt Wright Version 1.92 - Released April 21, 2002 A Free Product of Matt's Script Archive, Inc.
5. FormMail v1	FormMail

# 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](#)

**Your Google Alerts**

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

**GHDB regexes made into Google Alerts**

**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 - "mySQ... (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 Mark all as read Refresh Feed settings...

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

東京都文京区の不動産仲介・管理会社です。文京区・豊島区を中心に、駅 ... - mySQL error with query CREATE TEMPORARY TABLE p

期間延長 - わかの奇妙な日常 - mySQL error with query SELECT COUNT(\*) AS result FROM nucleus\_actionlog: Can't open file: 'nucleus\_actio

James Bond 007 :: MI6 - The Home Of James Bond - mySQL error with query SELECT c.itemid, c.cnumber as commentid, c.cbody as

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

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

mySQL error with query SELECT c.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...t...](http://www.mi6.co.uk/mi6.php3//news/index.php?itemid...)

Add star Like Share Share with note Email Add tags

等価交換 » ジェノベソース - mySQL error with query INSERT INTO nucleus\_plugin\_captcha (ckey, time, solution, active) VALUES ('890c8be4819...  
埼玉県上尾市 駅 土地情報 | 売 ... - mySQL error with query INSERT INTO nucleus\_plugin\_option (ova...  
mysql macosx collate character set latin1 - Broadway Rings Jewelry ... - mysql error with query creating standalone applications with mysql, mysql o

Several thousand GHDB/FSDB vuln alerts generated each day

# Bing Hacking Alerts



ADVANCED DEFENSES

## Bing Hacking Alerts

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

Google reader

All items Search

Navigation ▾ Bing: "mySQL error with query" » Show: Expanded - List

Show: 5 new items - all items Mark all as read Refresh Feed settings... show details

☆ <a href="#">www.kloosterman.be</a> - mySQL error with query SELECT p.pfile as pfile, e.event as event FROM	Apr 13, 2010	»
☆ <a href="#">The Shadow Project - Blog</a> - mySQL error with query SELECT COUNT(*) FROM nucleus_comment as c WHERE	Apr 13, 2010	»
☆ <a href="#">Hou-Hou Blog : tunisie blogs</a> - mySQL error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody	Apr 13, 2010	»
☆ <a href="#">Hou-Hou Blog : tunisie</a> - mySQL error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody as	Apr 13, 2010	»
☆ <a href="#">www.radiosonic.it</a> - mySQL error with query SELECT * FROM nucleus_config: Table 'Sql99301_1.nucleus_config'	Apr 13, 2010	»
☆ <a href="#">Hou-Hou Blog : george bush</a> - mySQL error with query SELECT i.inumber as itemid, i.iblog as blog, i.ititle as title, i.ibody as	Apr 7, 2010	»
☆ <a href="#">PHP /MYSQL - Error with query - ClanTemplates</a> - PHP /MYSQL - Error with query Programming ... Programming Got	Apr 5, 2010	»
☆ <a href="#">www.tutje.nl</a> - 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 buzz

Google™  
trends

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&

Google

site:<https://www.google.com> 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...](https://www.google.com/voice/fm/01377638746...)

[Google Voice](#)  
Google Voice Home. New Message From. Blue\_ghost. +881631562579 +881631562  
[www.google.com/voice/fm/11063046644...](https://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...](https://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...](https://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...](https://www.google.com/voice/fm/13418109598...)

**Google Voice messages  
publicly accessible**

# 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`

Google code search labs

select.\*from.\*request\QUERYSTF  Advanced Code Search

Code Results 1 - 10 of about 2,000.

post.asp

reply\_id is SQL injectable  
querystring parameter

```
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br><?<?>Ó»ÓÐ,ÃÍÄÖÅ×÷ÓÑ°Í¹ÜÀíÔ±²ÅÄÜràçÙá,öìû×ó."
57: strSql = "SELECT T_Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br><?<?>Ó»ÓÐ,ÃÍÄÖÅ×÷ÓÑ°Í¹ÜÀíÔ±²ÅÄÜàçÙá,öìû×ó."
```

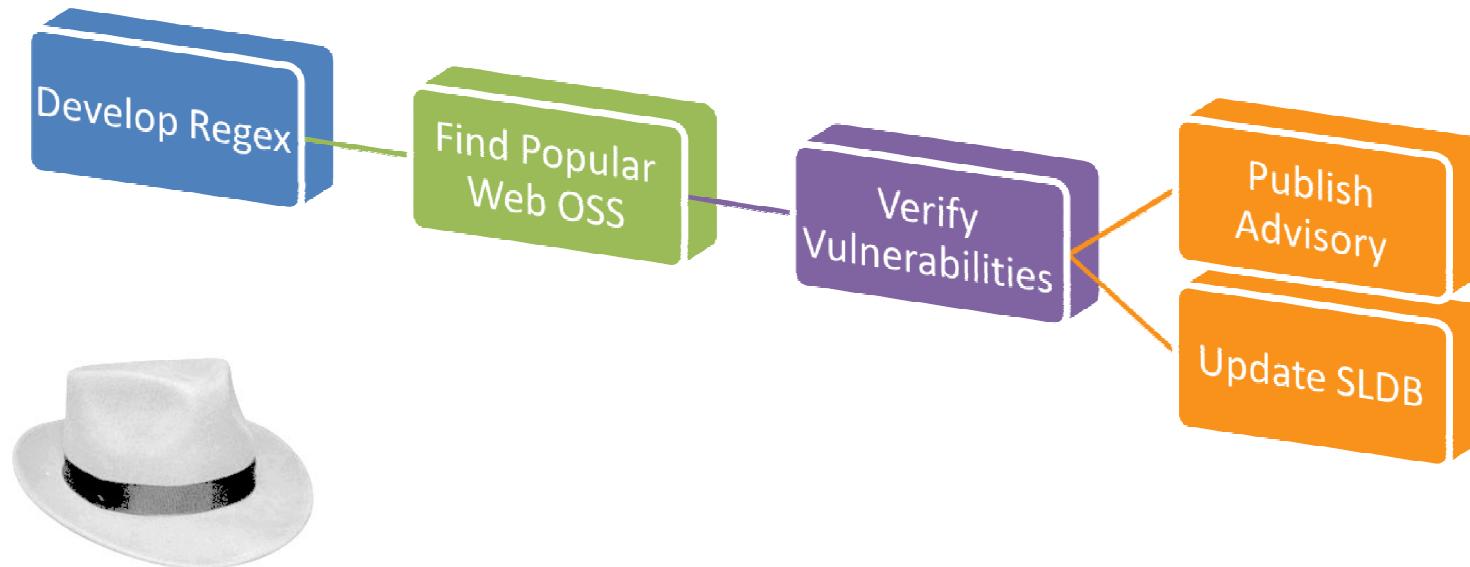
[www.cnarts.net/eweb/download/software/bbs/tradeforum.zip](http://www.cnarts.net/eweb/download/software/bbs/tradeforum.zip) - Unknown - ASP - [More from tradeforum.zip »](#)

GOOGLE CODE SEARCH HACKING

# DEMO

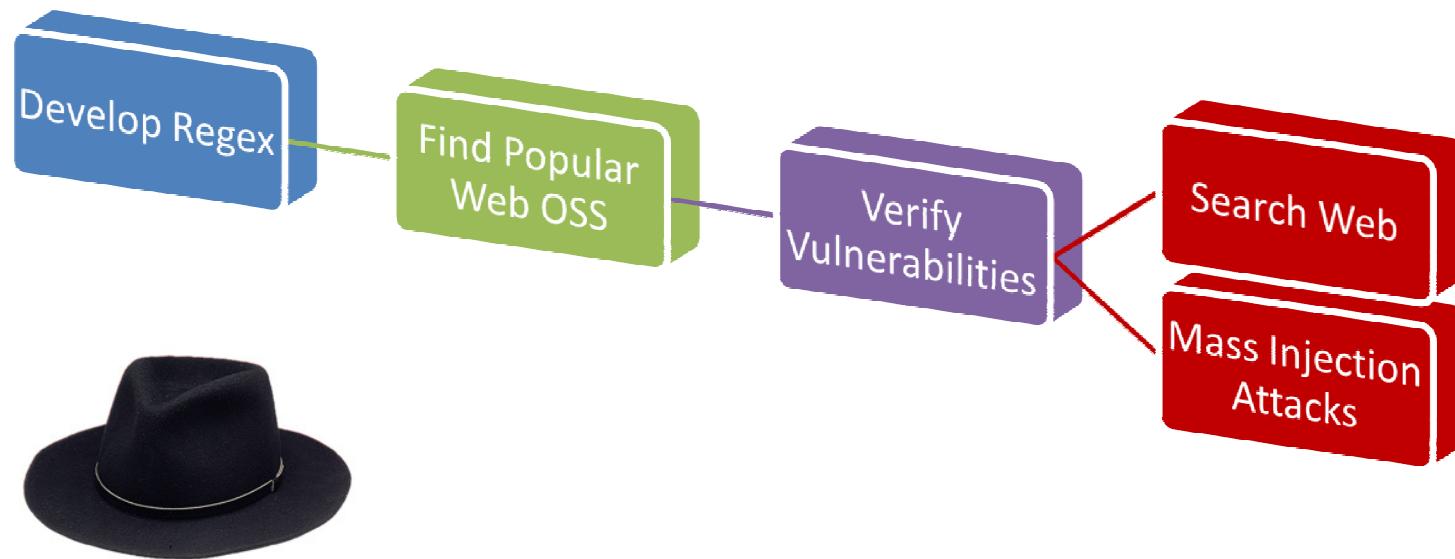
# Google Code Search

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



Google Insights for Search beta

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

Compare by: Search terms (radio button selected)

Search terms: All search terms

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

Filter: Web Search, United States, All subregions, All metros, 2004 - present, All Categories

Top Google searches over past 6 years

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

Web Search Interest: United States, 2004 - present

Search terms: Top searches

1. lyrics (circled in red)

2. you

3. 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 vulnerability to indo... cutters through drive... RELATED ARTICLES

A screenshot of the Google Insights for Search interface. The top navigation bar includes links for Help, Sign in, Download as CSV, and English (US). The main search term is set to 'All search terms'. The filter dropdowns show 'Web Search', 'United States', 'All subregions', 'All metros', '2004 - present', and 'All Categories'. A red callout box points to the 'Top Google searches over past 6 years' section, which contains the text: 'Fake lyrics web sites setup to appear in Google search results, infect you with malware upon clicking'. Another red callout box points to the 'lyrics' entry in the 'Top searches' list. A large red arrow points from the 'lyrics' entry to a news article titled 'Lada Gaga, Rihanna lyrics sites used to foist Java exploit' by Dan Kaplan from April 14, 2010. The news article discusses a Java exploit found in lyrics websites.



I've Become A  
Wet Dream Tomato

There's Nothing You Can't Dew

# 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/11550007>

"Every time I load Jpost site, I get nasty ads on Tuesday, referring to the Jerusalem Post."

Sure enough, the Web sites of the *Jerusalem Post* and the Association of Christian Schools International are 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](#) and [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](#)

# Inconvenient Truth



## DICKHEAD ALERTS

### Malware Black List Woes

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

Haha!

reddit

NETSEC comments related

reddit is a source for what's new and popular online. vote on links that you like or dislike and help decide what's popular, or submit your own!

↑ Chrome has labelled one of my websites as "dangerous" and hosting  
11 malware. How did this happen and how can I get this undone? (self.netsec)  
↓ submitted 2 days ago by neofrom3

Some dickhead emailed me weeks ago claiming my site has malware on it, it's a completely bogus claim, but now I've noticed that chrome is flagging my site as hosting malware.. :| How did he do that?

Site is nakidness.com (NSFW obviously). I don't even have any 3rd party ads on the site. I just have the reddit badge, disqus commenting and stumble badge...

26 comments share

# Advanced Defenses

PROTECT YO NECK



# Malware Diggity

ADVANCED DEFENSES



## Malware Diggity

- Uses Bing's `linkfromdomain:` directive to *identify offsite 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 offsite 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 search bar contains the query, and the results page displays several links:

- 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](#) · 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](#) · Cached page
- Colloquy: IRC, SILC & ICB Client**  
An IRC client for Macintosh OS X. Contains screenshots, documentation, support and download area.  
[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](#) · 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](#) · Cached page

# Malware Diggity



## ADVANCED DEFENSES

**YAHOO!** SITE EXPLORER

http://www.stachliu.com **Explore URL**

**Site Explorer**

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

**Results**

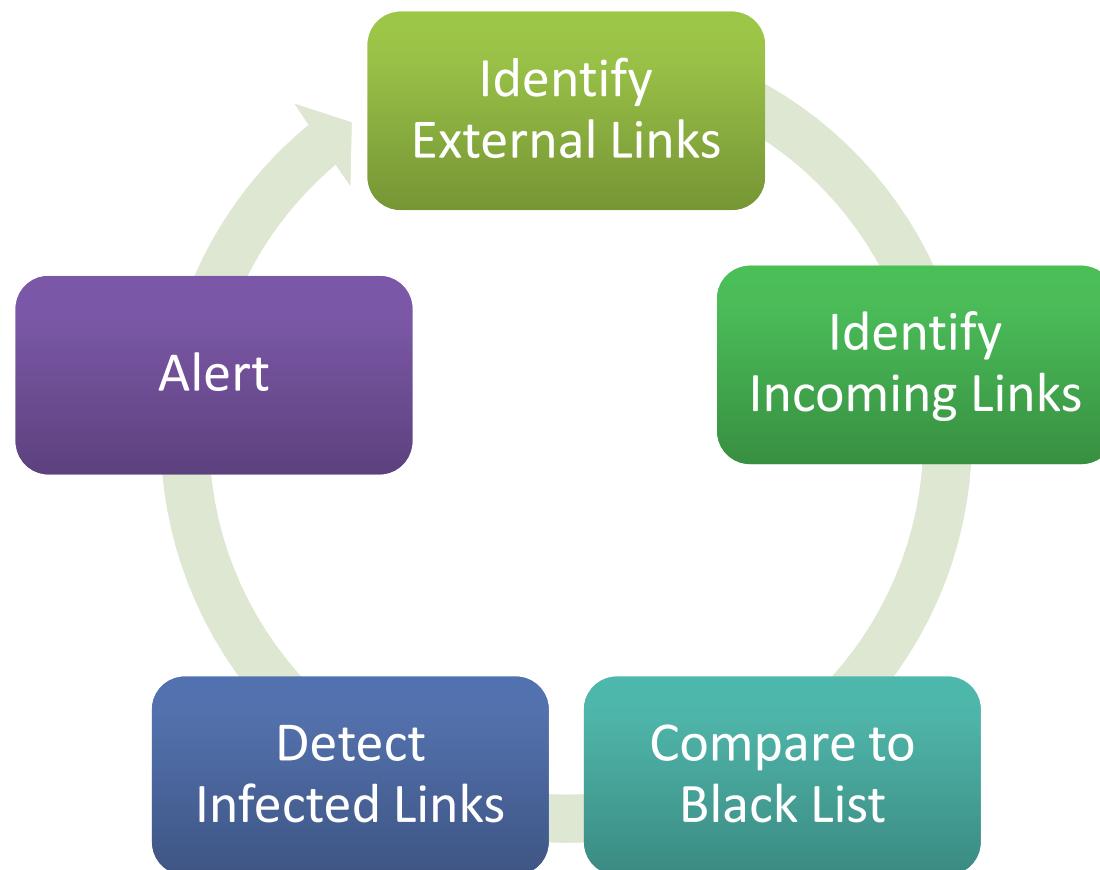
Pages (70) Inlinks (4,130) Show Inlinks: Except from this domain to: Entire Site

Result details:   Submit webpage or Site Feed | Export first 1000 results to TSV

1.	Unofficial MD5 text/html <a href="http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html">http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html</a> - 12k - cache	<input type="button" value="Explore"/>
2.	Offensive Computing   Community Malicious code research and ... text/html <a href="http://www.offensivecomputing.net/">http://www.offensivecomputing.net/</a> - 35k - cache	<input type="button" value="Explore"/>
3.	Approved Scanning Vendors text/html <a href="https://www.pcisecuritystandards.org/pdfs/asv_report.html">https://www.pcisecuritystandards.org/pdfs/asv_report.html</a> - 34k - cache	<input type="button" value="Explore"/>
4.	Peter Selinger: MD5 Collision Demo text/html <a href="http://www.mscs.dal.ca/~selinger/md5collision/">http://www.mscs.dal.ca/~selinger/md5collision/</a> - 13k - cache	<input type="button" value="Explore"/>
5.	Microsoft BlueHat Blog - Site Home - TechNet Blogs text/html <a href="http://blogs.technet.com/b/bluehat/">http://blogs.technet.com/b/bluehat/</a> - 140k - cache	<input type="button" value="Explore"/>
6.	Checkmarx Source Code Analysis Technologies text/html <a href="http://www.checkmarx.com/">http://www.checkmarx.com/</a> - 48k - cache	<input type="button" value="Explore"/>
7.	Black Hat USA Spotlight: ATL Killbit Bypass - Microsoft... text/html <a href="http://blogs.technet.com/b/bluehat/archive/2009/07/27/black-hat-usa-atl-killbit-bypass.aspx">http://blogs.technet.com/b/bluehat/archive/2009/07/27/black-hat-usa-atl-killbit-bypass.aspx</a> - 151k - cache	<input type="button" value="Explore"/>

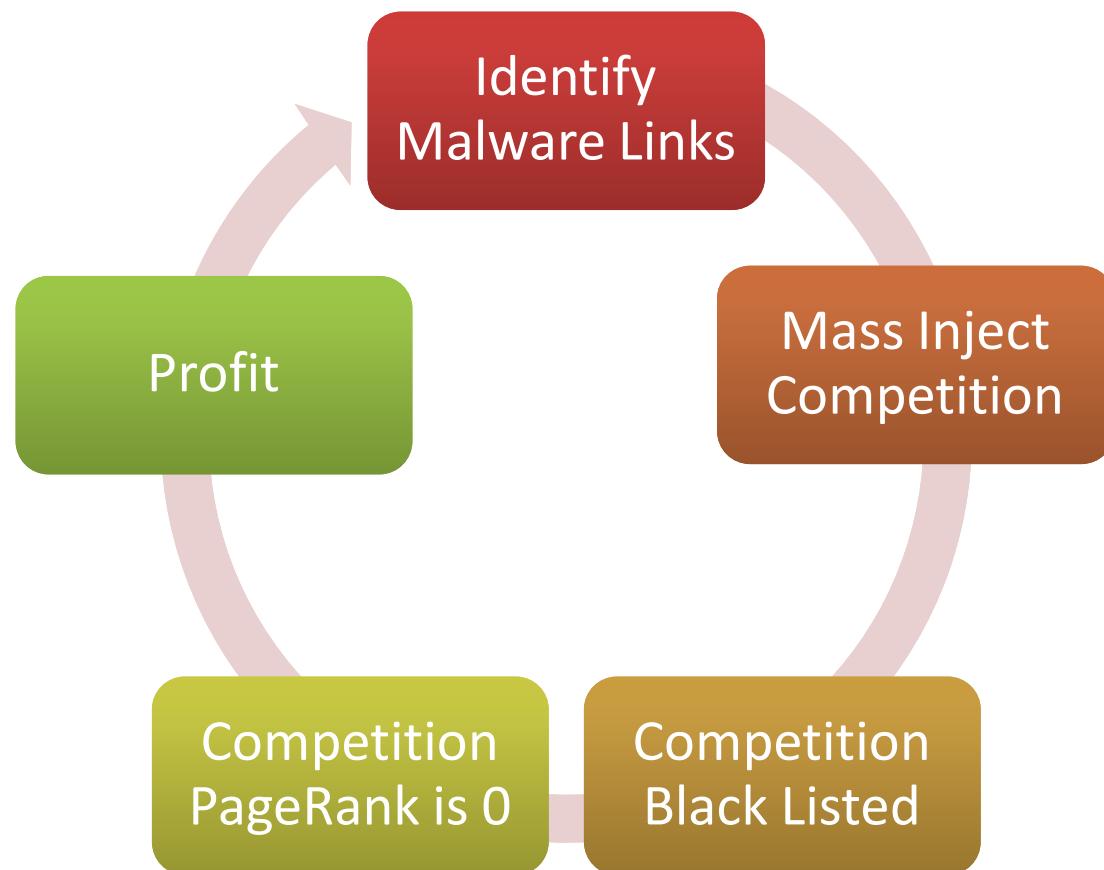
# Malware Monitoring

## INFECTION DETECTION



# Search Engine deOptimization

BLACK LIST YOUR FOES



# Safe Browsing Alerts



## ADVANCED DEFENSES

**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

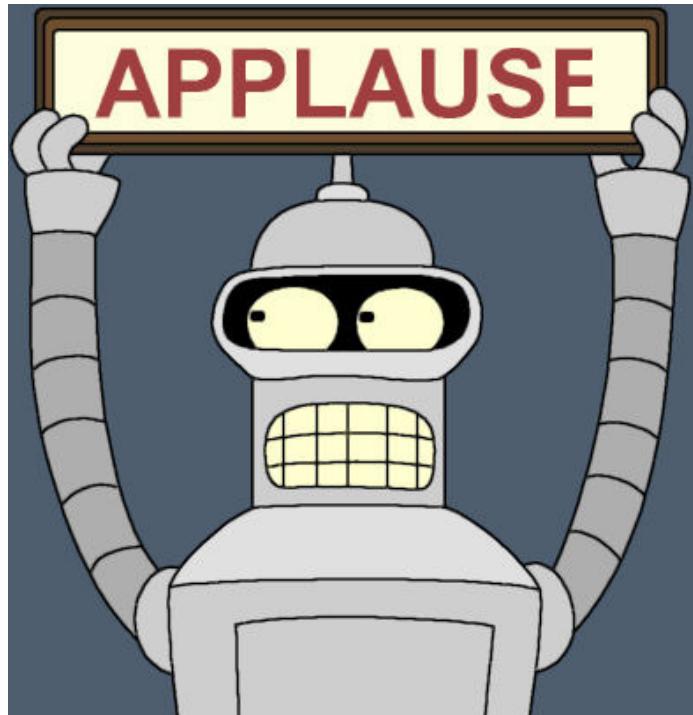
- Google Ajax API based
- Bing/Yahoo/other engines
  - Search engine aggregators
  - Customized search engines
- Google Code and Other Open Source Repositories
  - MS CodePlex, SourceForge, ...
- More automation in tools
  - Real-time detection and exploitation
  - Google worms

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/>