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
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

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

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"

STACH&LIU
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 YOUR NECK
Existing Defenses

“HACK YOURSELF”

✔ Tools exist
✖ Convenient
✖ Real-time updates
✖ Multi-engine results
✖ Historical archived data
✖ Multi-domain searching
Advanced Defenses

Stach & Liu now proudly presents:

• Google Hacking Alerts
• Bing Hacking Alerts
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
Google Hacking Alerts
ADVANCED DEFENSES

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

James Bond 007 :: MI6 - The Home Of James Bond
via Google Alerts "mySQL error with query"

Several thousand GHDB/FSDB vuln alerts generated each day

STACH&LIU
Bing Hacking Alerts

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

Google reader

Navigation: Bing: "mySQL error with query" »

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

- www.kloosterman.be - mySQL error with query SELECT p pfie as pfie, 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
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 Voice

PARTY LINE

http://www.google.com/m/search?q=site:https://www.google.com/voice/fm/*&start=10&

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...

Google Voice
Google Voice Home. New Message From. Blue_ghost. +881631562579 +881631562579...
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...

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...

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...
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

VULNS IN OPEN SOURCE CODE

Develop Regex → Find Popular Web OSS → Verify Vulnerabilities

Publish Advisory

Update SLDB
Google Code Search

VULNS IN OPEN SOURCE CODE

Develop Regex → Find Popular Web OSS → Verify Vulnerabilities → Search Web

Mass Injection Attacks
Black Hat SEO

- 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

- Top Google searches over past 6 years
- Fake lyrics websites setup to appear in Google search results, infect you with malware upon clicking

Web Search Interest
- United States, 2004 - present

Search terms
1. lyrics
2. you
3. yahoo

Lada Gaga, Rihanna lyrics sites used to foist Java exploit

As expected, virus writers now are actively exploiting a zero-day Sun vulnerability that enters through drive

STACH&LIU
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)
  • Dell KACE - Secure Browser
  • Adobe Reader Sandbox (Protected Mode)

• No-script and Ad-block browser plugins
Mass Injection Attacks

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/stories/hits-media-web-sites-

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

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

From: 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 Ingubs.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

Malware Black List Woes
- Average web administrator has no idea when their site gets blacklisted
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
  - 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
Malware Diggity
ADVANCED DEFENSES

http://www.stachliu.com

1. Unofficial MD5
   http://userpages.umbc.edu/~mebzaug1/cs/md5/md5.html - 12k - cache

2. Offensive Computing | Community Malicious code research and...
   http://www.offensivocomputing.net - 35k - cache

3. Approved Scanning Vendors
   https://www.pcisecuritystandards.org/pts/asv_report.html - 34k - cache

4. Peter Selinger MD5 Collision Demo
   http://www.mscs-dal.ca/~selinger/md5collision/ - 13k - cache

5. Microsoft BlueHat Blog - Site Home - TechNet Blogs
   http://blogs.technet.com/b/bluehat/ - 140k - cache

6. Checkmarx Source Code Analysis Technologies
   http://www.checkmarx.com/ - 48k - cache

7. Black Hat USA Spotlight: ATL Killbit Bypass - Microsoft
Malware Monitoring

Identify External Links

Alert

Detect Infected Links

Compare to Black List

Identify Incoming Links
Search Engine deOptimization

BLACK LIST YOUR FOES

Identify Malware Links

Profit

Mass Inject Competition

Competition PageRank is 0

Competition Black Listed
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

P R E D I C T I O N S
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
Project: diggity@stachliu.com
Stach & Liu, LLC
www.stachliu.com
Thank You

Stach & Liu Project info:
http://www.stachliu.com/index.php/resources/tools/google-hacking-diggity-project/