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

STACH&LIU

STACH&LIU

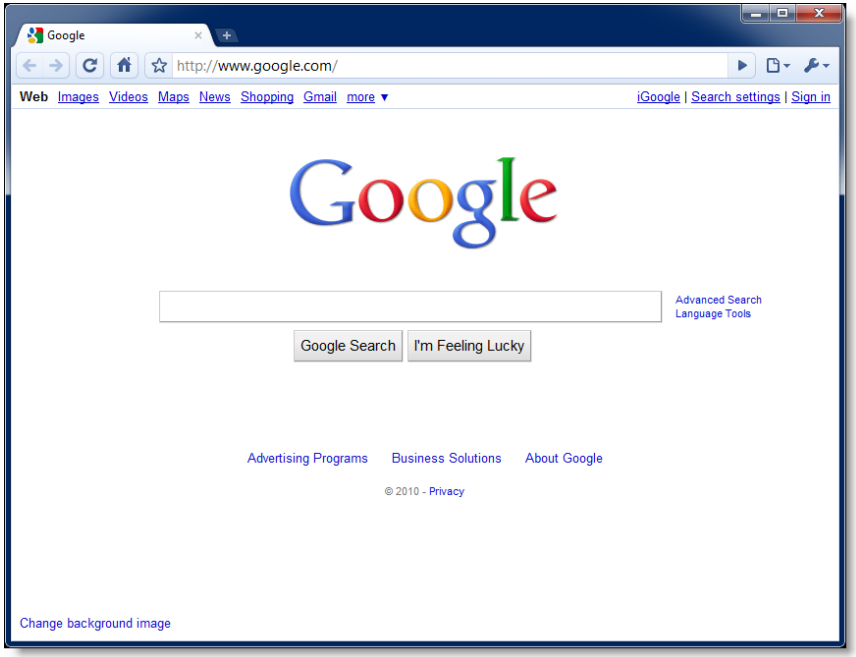
Goals

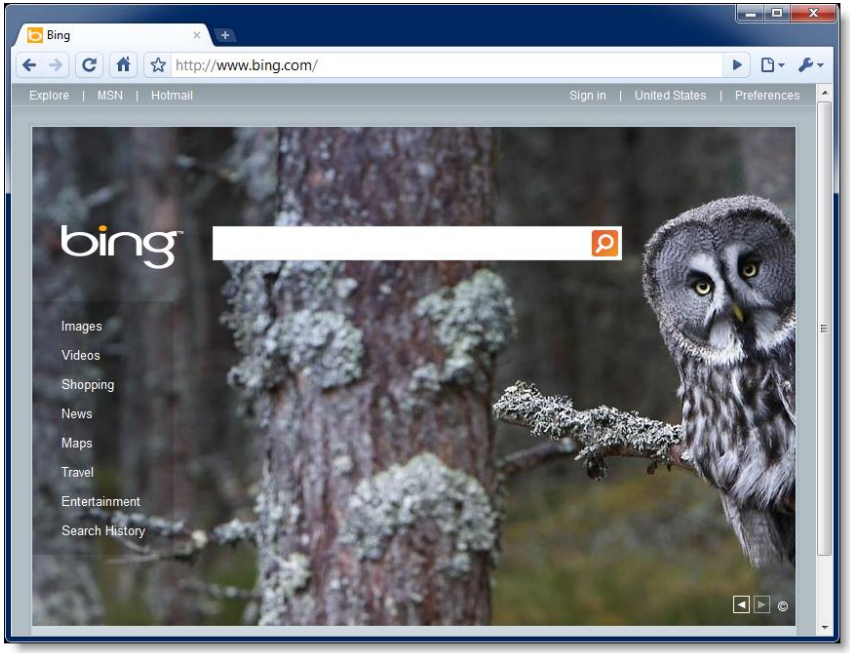
DROP KNOWLEDGE ON YOU

- *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
- NEW • Can leverage Google custom search

Bing Diggity

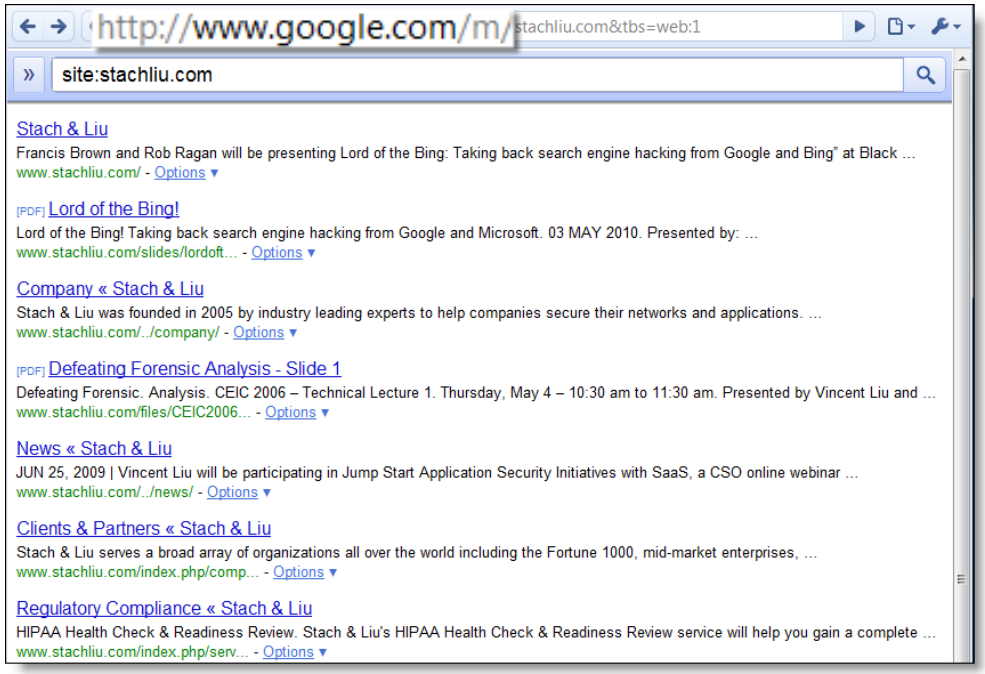
- Uses Bing 2.0 SOAP API
- Company/Webapp Profiling
  - Enumerate: URLs, IP-to-virtual hosts, etc.
- NEW • Bing Hacking Database (BHDB)
  - Vulnerability search queries in Bing format

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"`

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:sql "insert into" (pass|passwd|password)`
- `!Host=*.* intext:enc_UserPassword=* ext:pcf`
- `"your password is" filetype:log`

NEW GOOGLE HACKING TOOLS

DEMO

Traditional Defenses

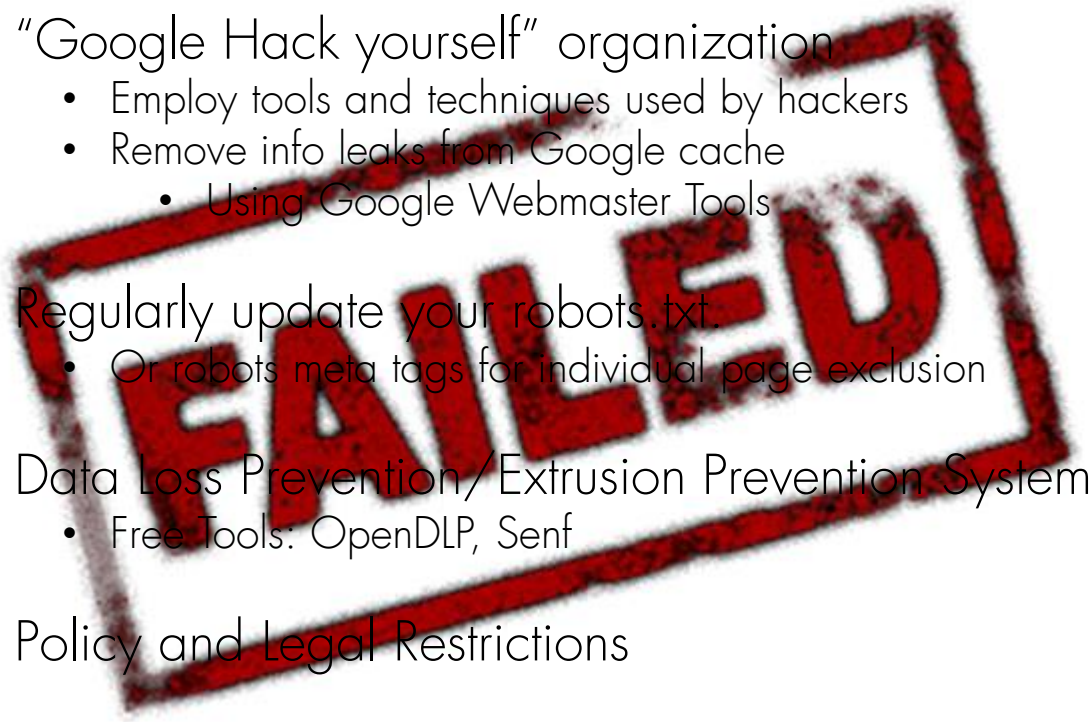
GOOGLE HACKING DEFENSES

- "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:

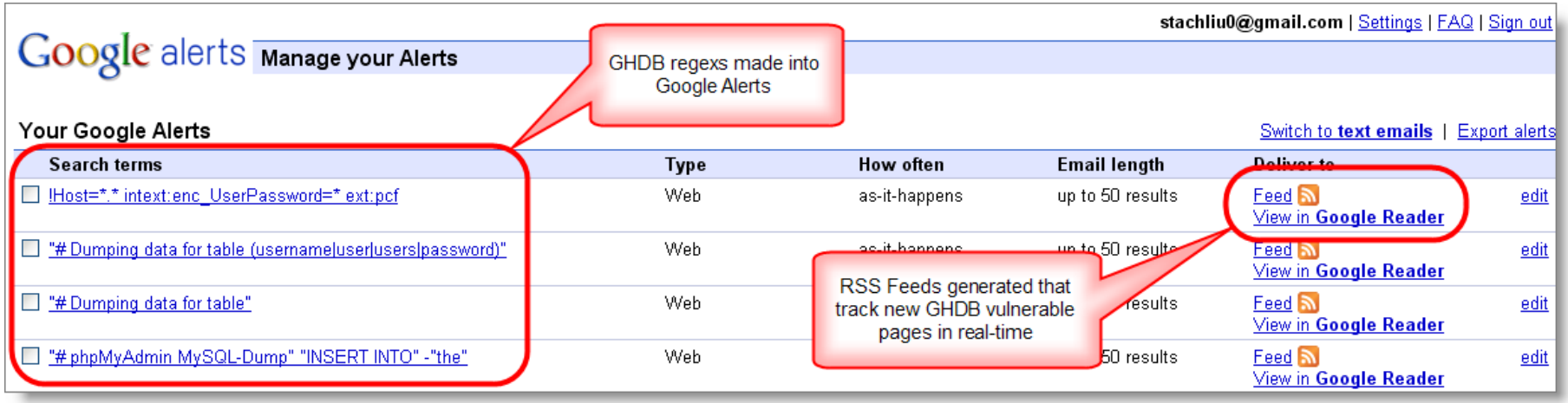
- Google Hacking Alerts
- Bing Hacking Alerts

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



Google Hacking Alerts

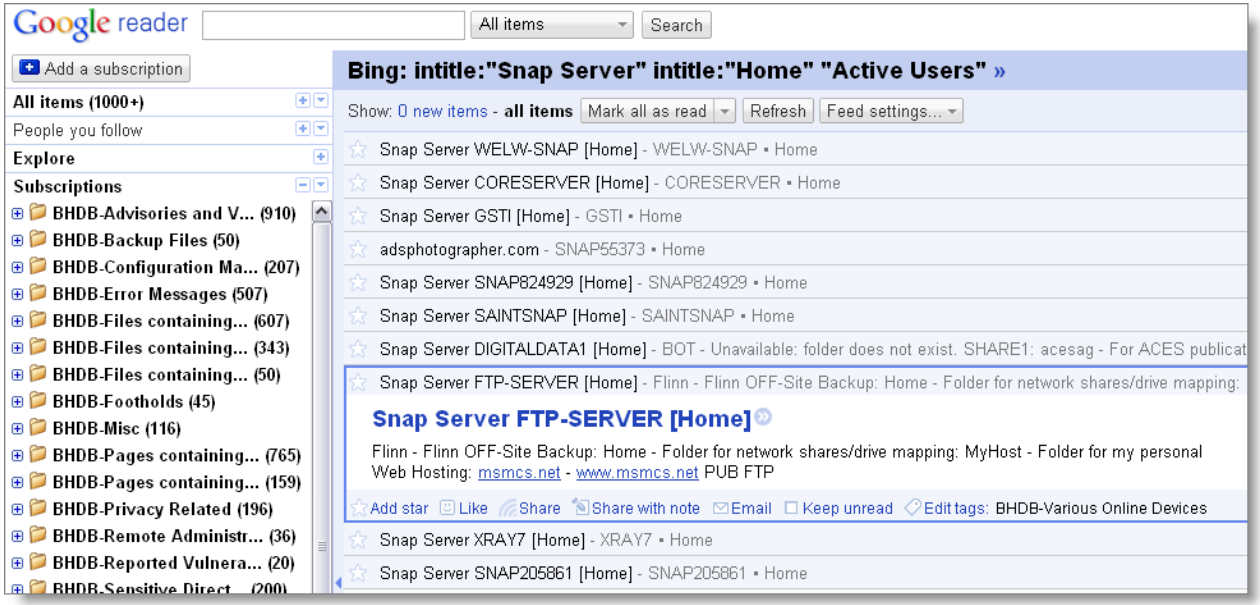
ADVANCED DEFENSES

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



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

phonebook: schmidt, eric | Search PhoneBook | Search the Web | Preferences

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

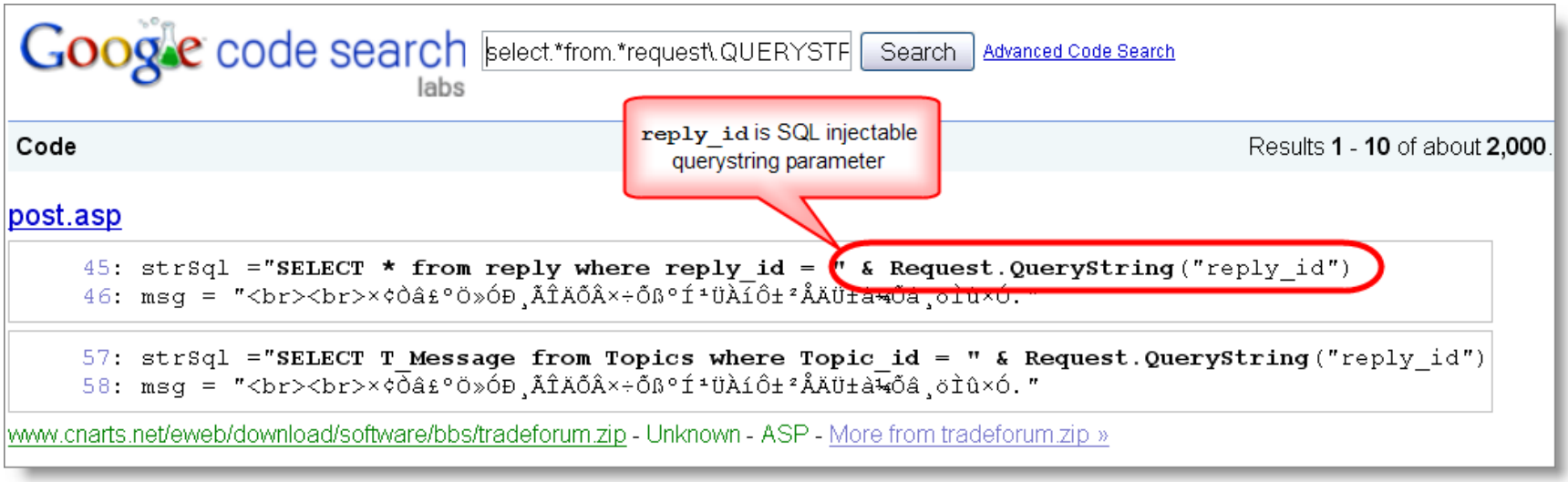
Eric Schmidt	(952) 403-9689	1761 Countryside Dr,Shakopee, MN 55379-4451	Map
Eric Schmidt	(815) 522-6299	413 Prairie St,Kirkland, IL 60146-0000	Map
Eric Schmidt	(636) 942-3494	6404 Lipizzaner Dr,Imperial, MO 63052-4142	Map
Eric Schmidt	(618) 644-9277	2260 Steinkoenig School R,Highland, IL 62249-4006	Map
Eric Schmidt	(715) 324-5232	N17082 Roth Ln,Pembine, WI 54156-0000	Map
Eric Schmidt	(360) 854-0973	24400 Mckendree Ln,Sedro Woolley, WA 98284-7814	Map
Eric Schmidt	(650) 964-4017	Mountain View, CA 94043-0000	Map
Eric Schmidt	(207) 848-2221	41 Hardwood Dr,Hermon, ME 04401-0253	Map

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

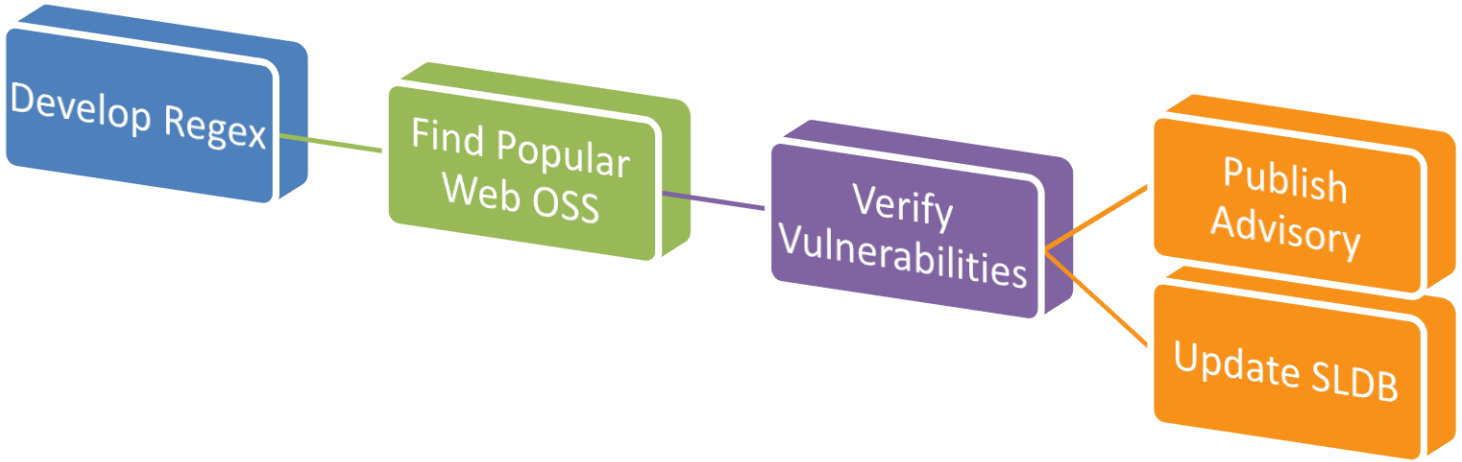


GOOGLE CODE SEARCH HACKING

DEMO

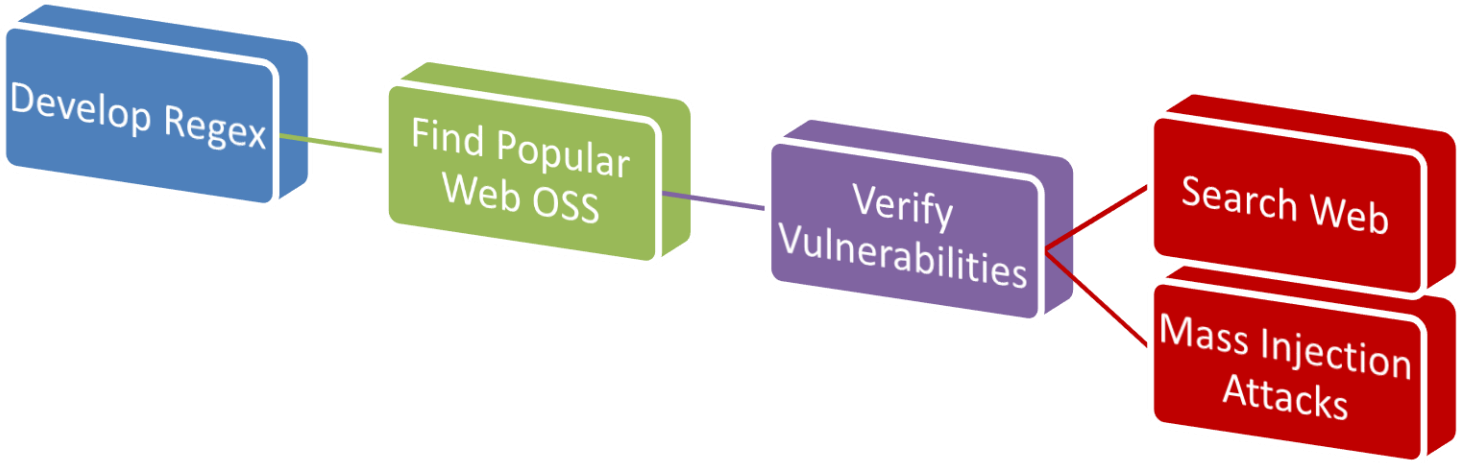
Google Code Search

VULNS IN OPEN SOURCE CODE



Google Code Search

VULNS IN OPEN SOURCE CODE



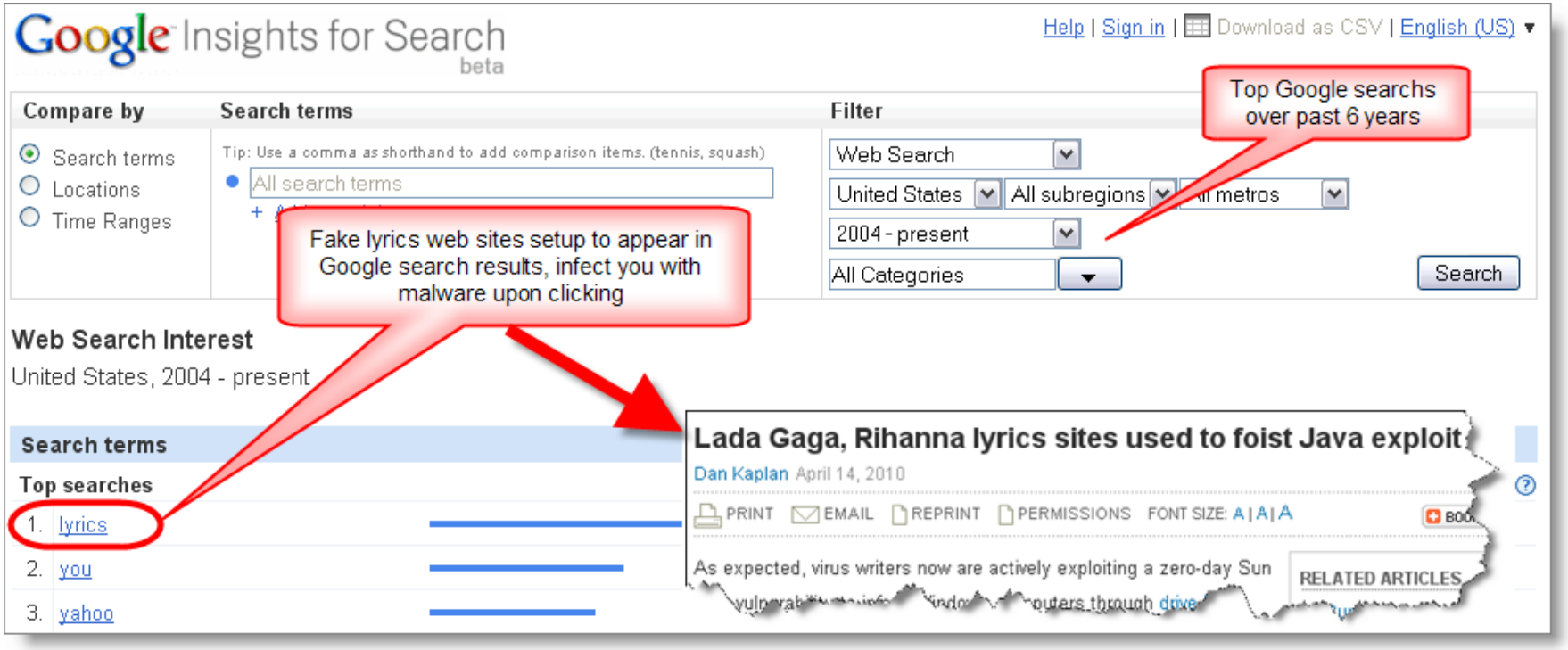
Black Hat SEO

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



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
  - 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/stor

"Every time I load Jpost site, I get na
on Tuesday, referring to the Jerusale

Sure enough, the Web sites of the *Je*
and the Association of Christian Sch
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 Intljobs.org.

Malware Browser Filters

URL BLACK LIST

Protecting users from known threats

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

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

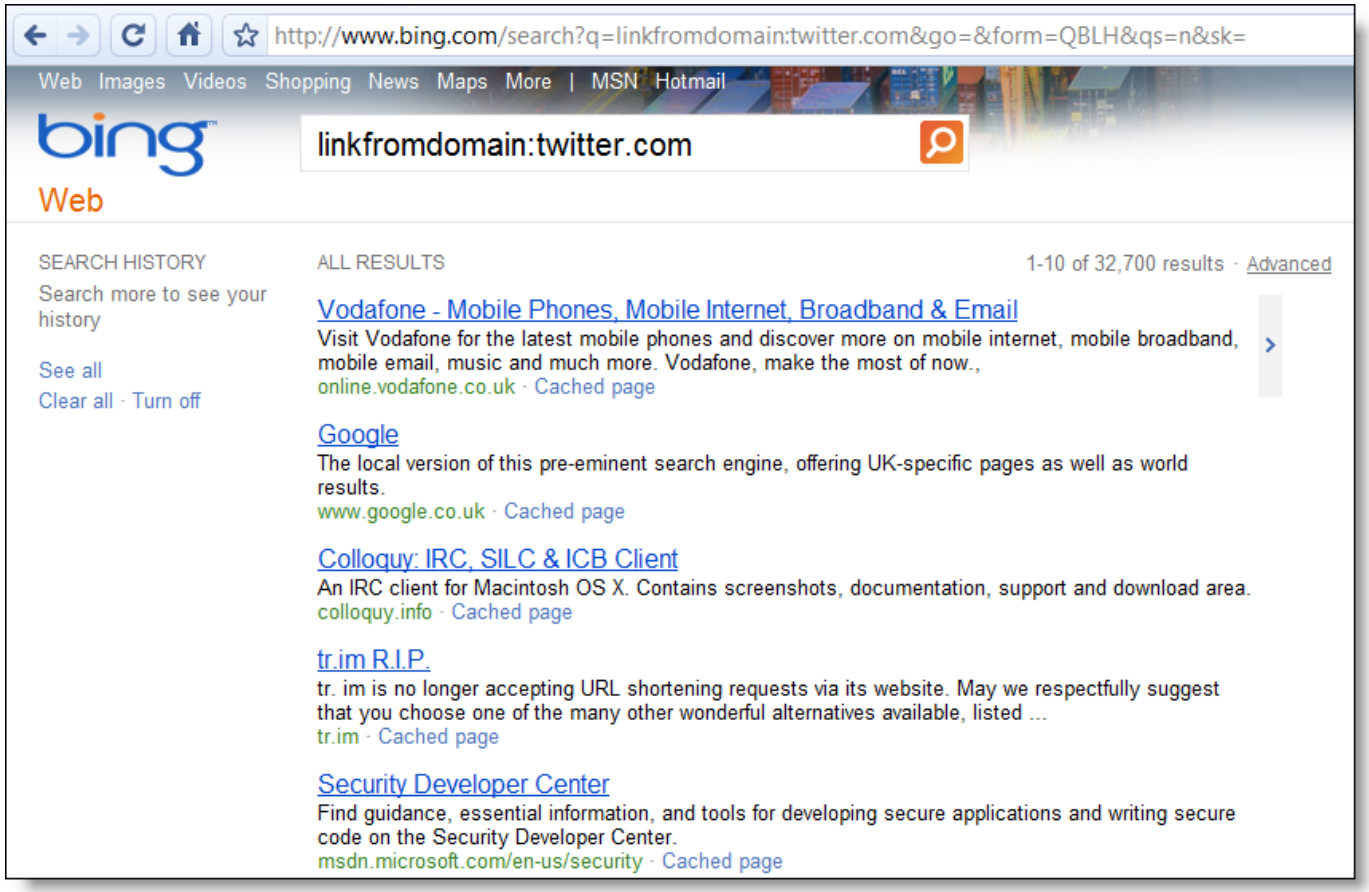
- Uses Bing's linkfromdomain: directive to *identify off-site links* of the domain(s) you wish to monitor
- Compares to *known malware sites/domains*
  - Alerts if site is compromised and now distributing malware

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

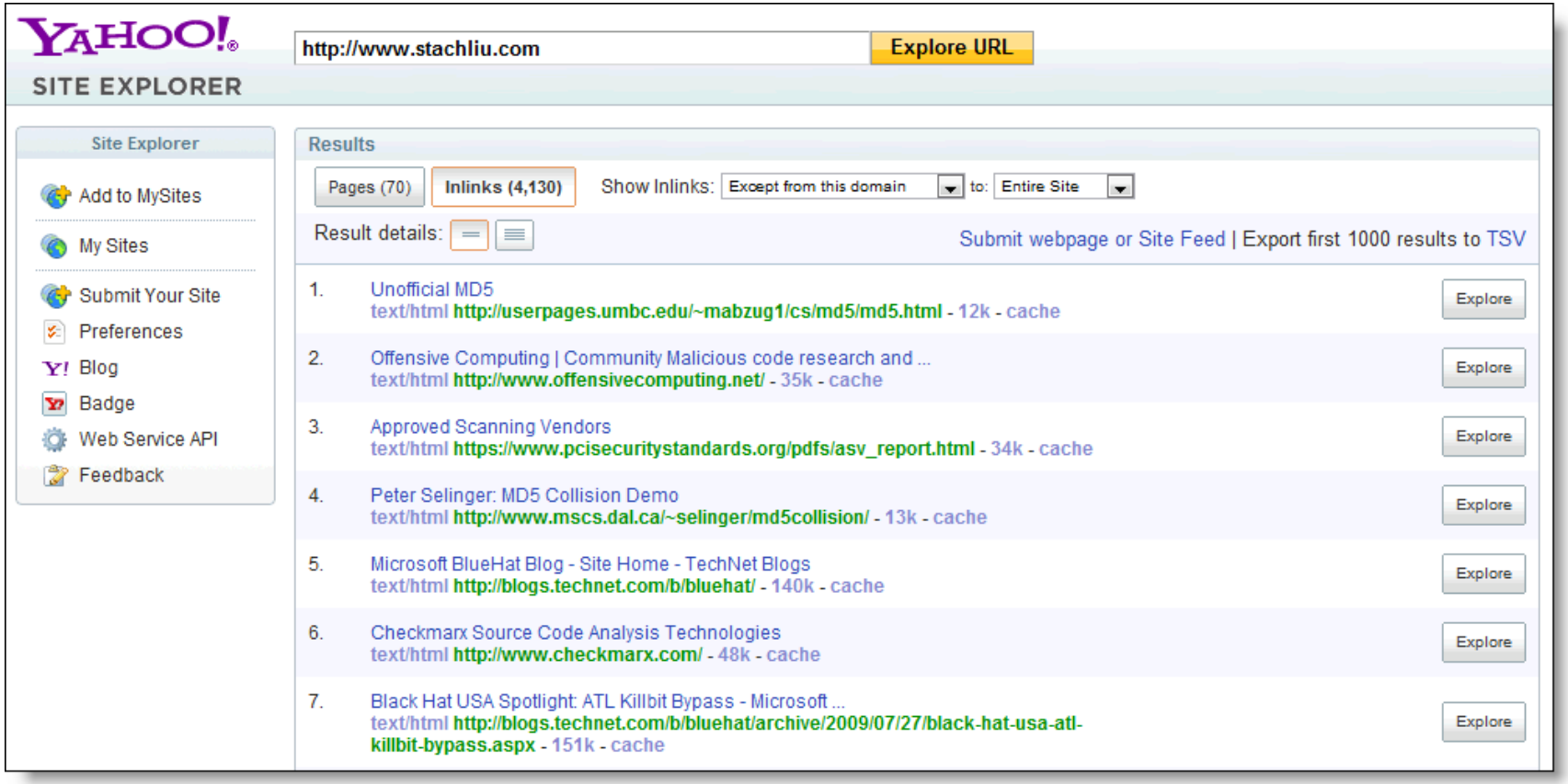
Malware Diggity

ADVANCED DEFENSES



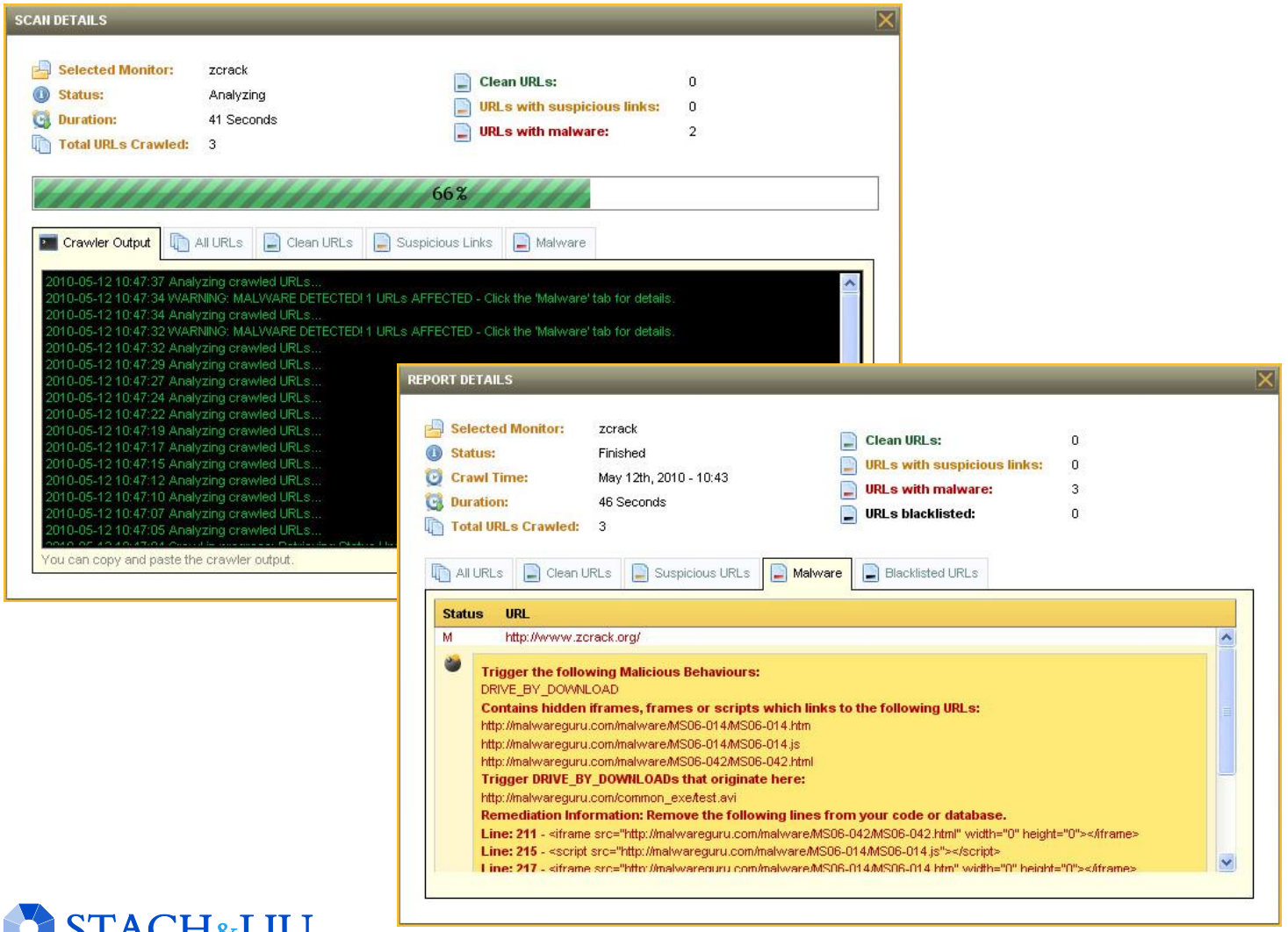
Malware Diggity

ADVANCED DEFENSES



armorize
Secure Your Web Applications

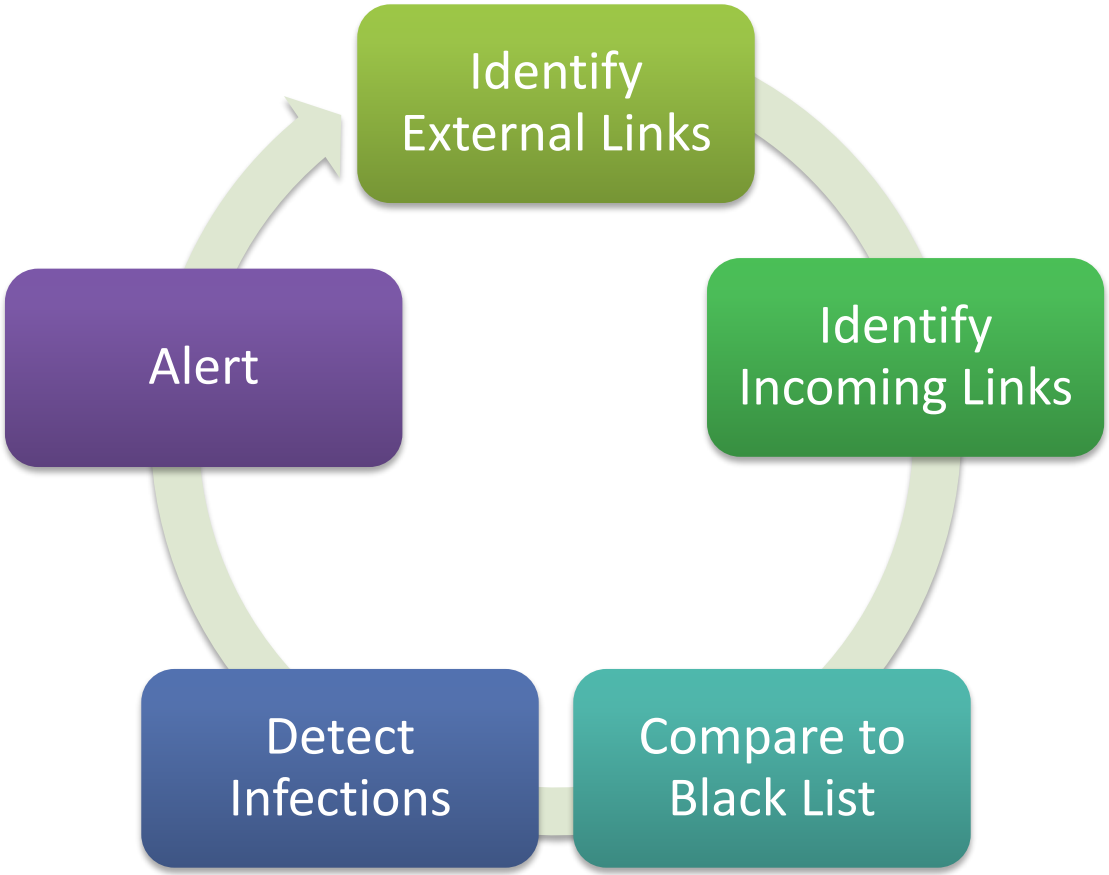
HackAlert™



STACH&LIU

Malware Monitoring

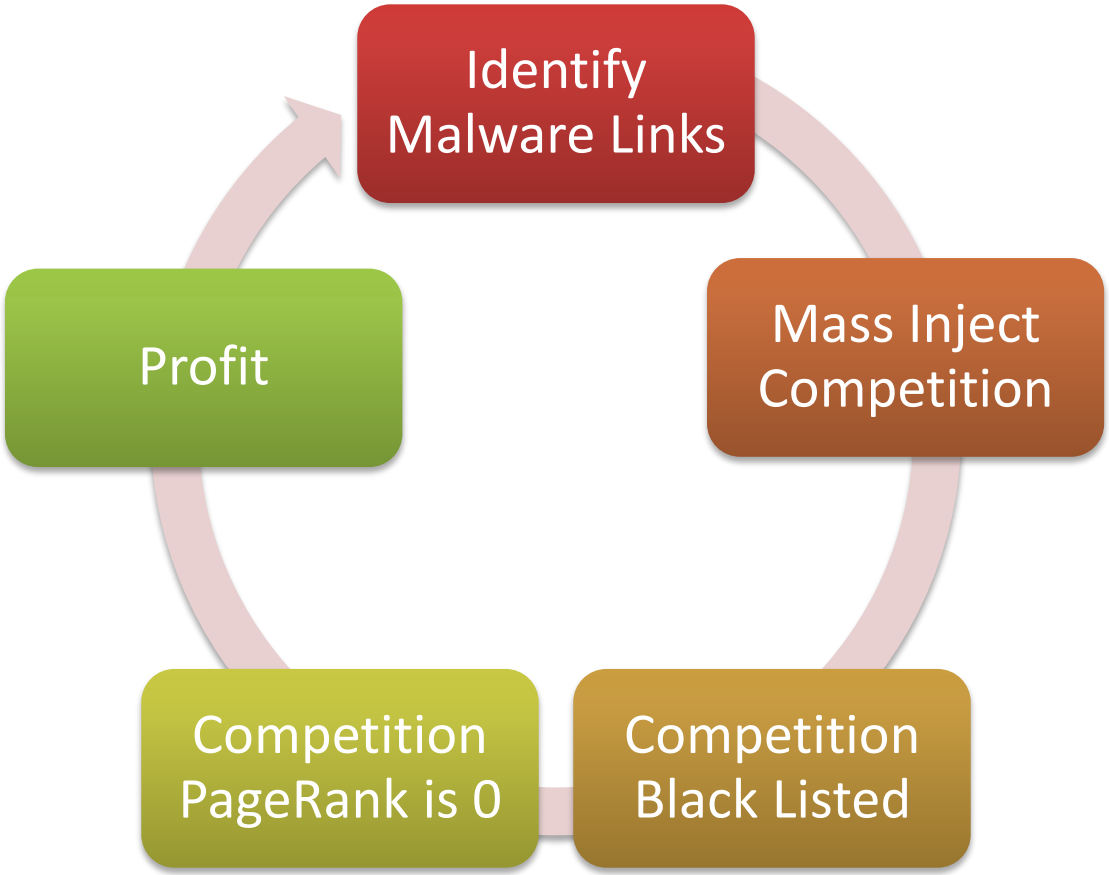
INFECTION DETECTION



STACH&LIU

Search Engine deOptimization

BLACK LIST YOUR FOES



STACH&LIU

Future Direction

PREDICTIONS

Predictions

FUTURE DIRECTIONS

Data Explosion

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

Google Involvement

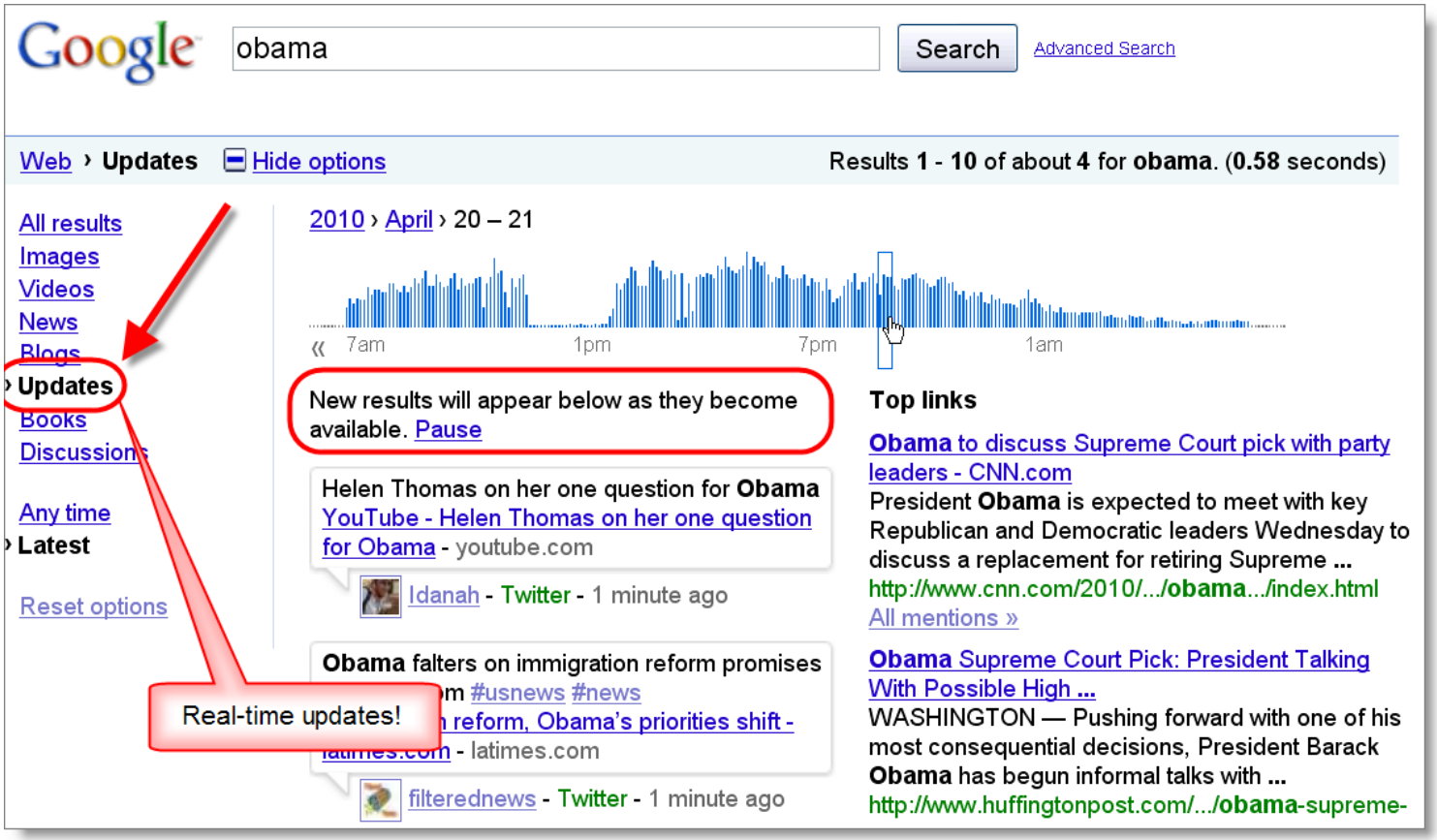
- Filtering of search results
- Better GH detection and tool blocking

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



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

STACH&LIU

Thank You

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