Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

ToorCon 12 - 24 October 2010

Presented by:
Francis Brown
Stach & Liu, LLC
www.stachliu.com

STACH&LIU

Agenda

OVERVIEW

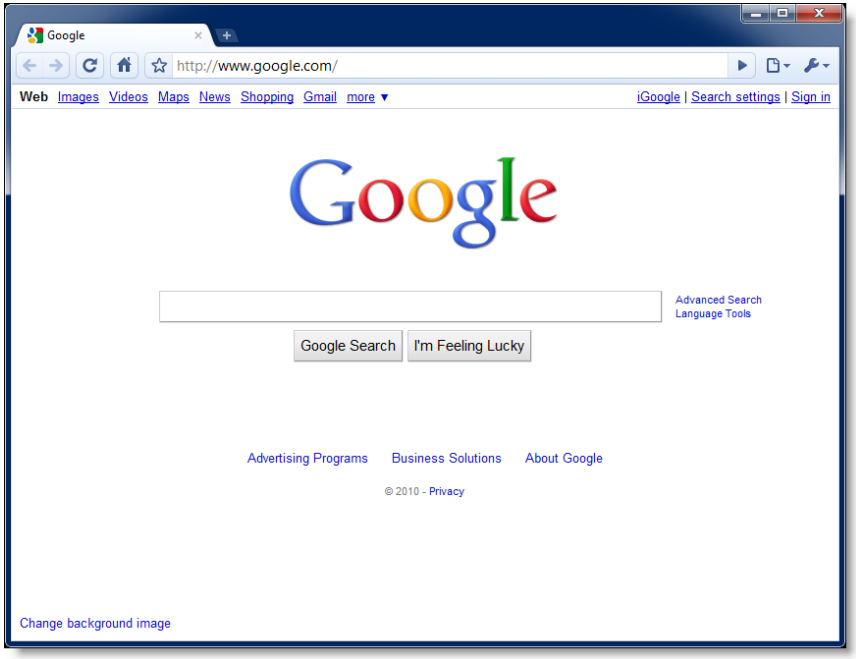
- Introduction/Background
- Advanced Attacks
  - Google/Bing Hacking
- Advanced Defenses
  - Google/Bing Hacking Alerts
- Demos (time permitting)

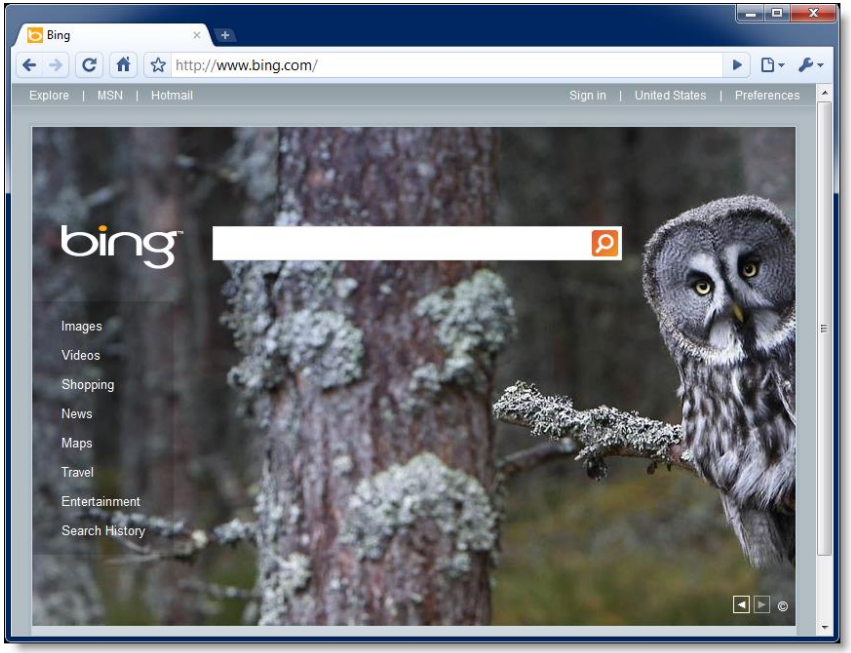
Introduction/ Background

GETTING UP TO SPEED

Google/Bing Hacking

SEARCH ENGINE ATTACKS





STACH&LIU

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`

Quick History

GOOGLE HACKING RECAP

Dates	Event
2004	Google Hacking Database (GHDB) begins
May 2004	Foundstone SiteDigger v1 released
2005	Google Hacking v1 released by Johnny Long
Jan. 2005	Foundstone SiteDigger v2 released
Feb. 13, 2005	Google Hack Honeypot first release
Jan. 10, 2005	MSNPawn v1.0 released
Dec. 5, 2006	Google stops issuing Google SOAP API keys
…	…

Quick History

GOOGLE HACKING RECAP

Dates	Event
Mar. 2007	Bing disables inurl: link: and linkdomain:
Nov. 2, 2007	Google Hacking v2 released
Mar. 2008	cDc Goolag - gui tool released
June 3, 2009	Bing goes online
Sept. 7, 2009	Google shuts down SOAP Search API
Nov. 2009	Binging tool released
Dec. 1, 2009	FoundStone SiteDigger v 3.0 released
2010	Googlag.org disappears

Google Apps Explosion

SO MANY APPLICATIONS TO ABUSE

Advanced Attacks

WHAT YOU SHOULD KNOW

New Toolkit

STACH & LIU TOOLS

Google Diggity

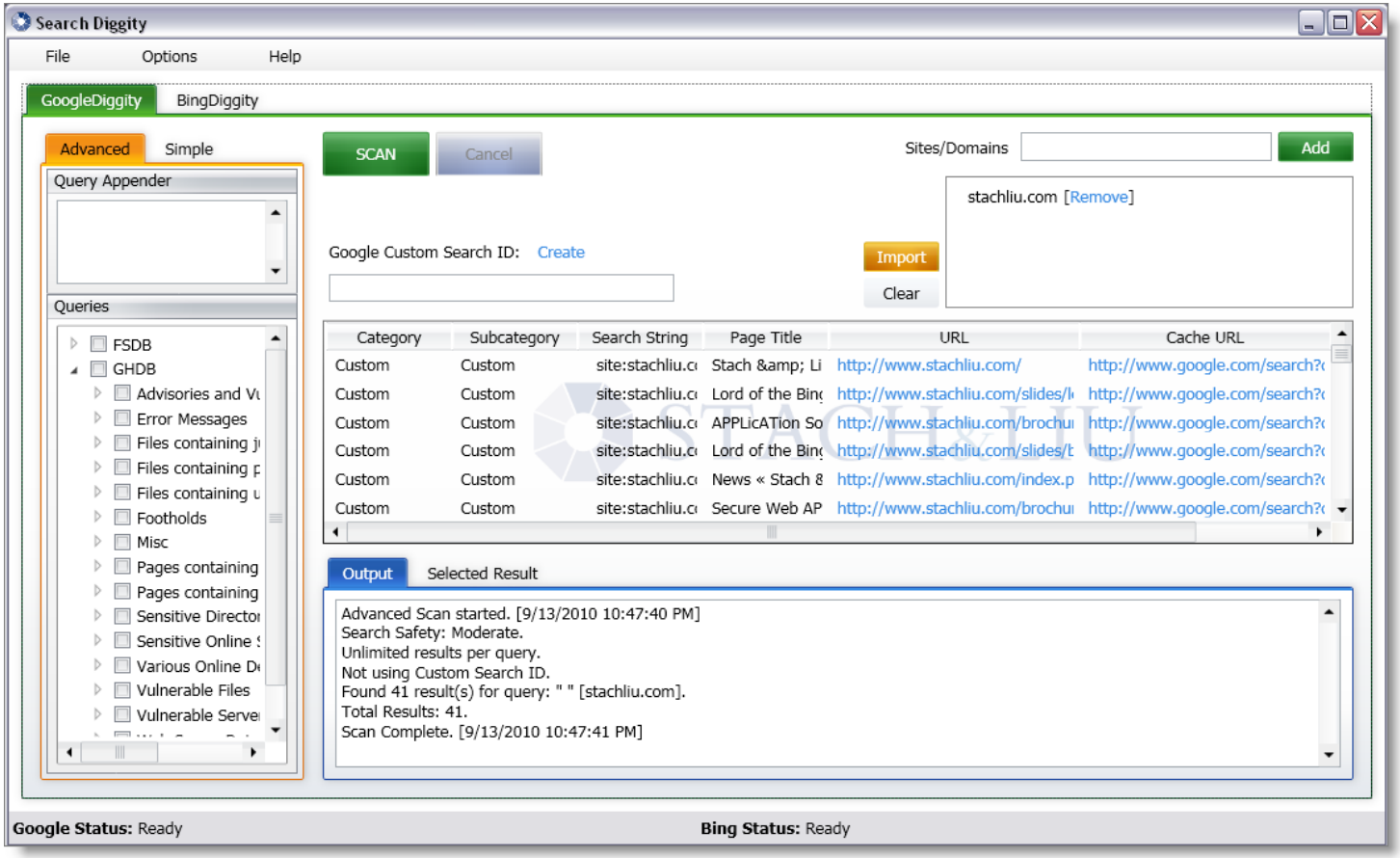
- Uses Google AJAX API
  - Not blocked by Google bot detection
  - Does not violate Terms of Service
- NEW Can leverage Google custom search

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

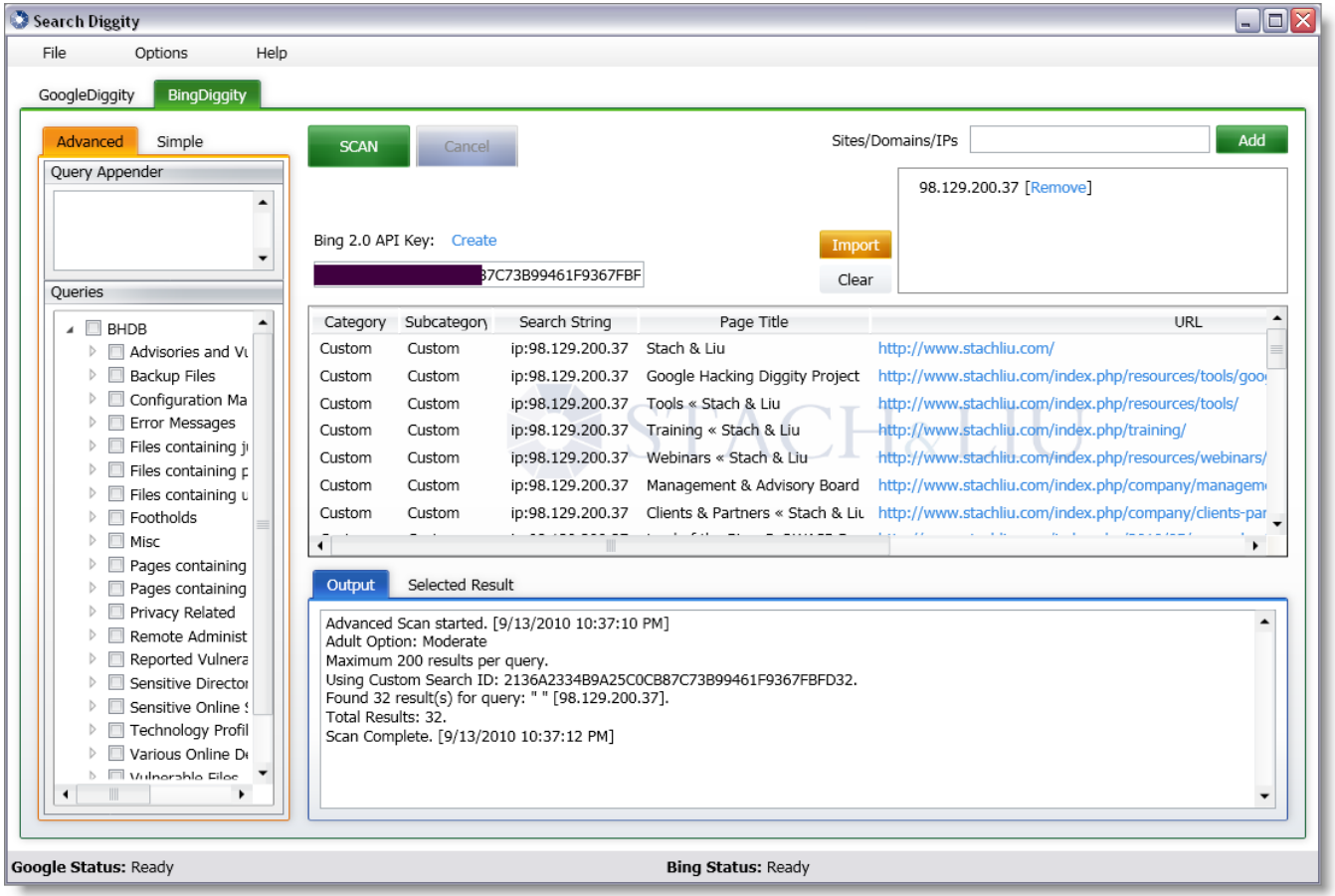
New Toolkit

GOOGLEDIGGITY



New Toolkit

BINGDIGGITY



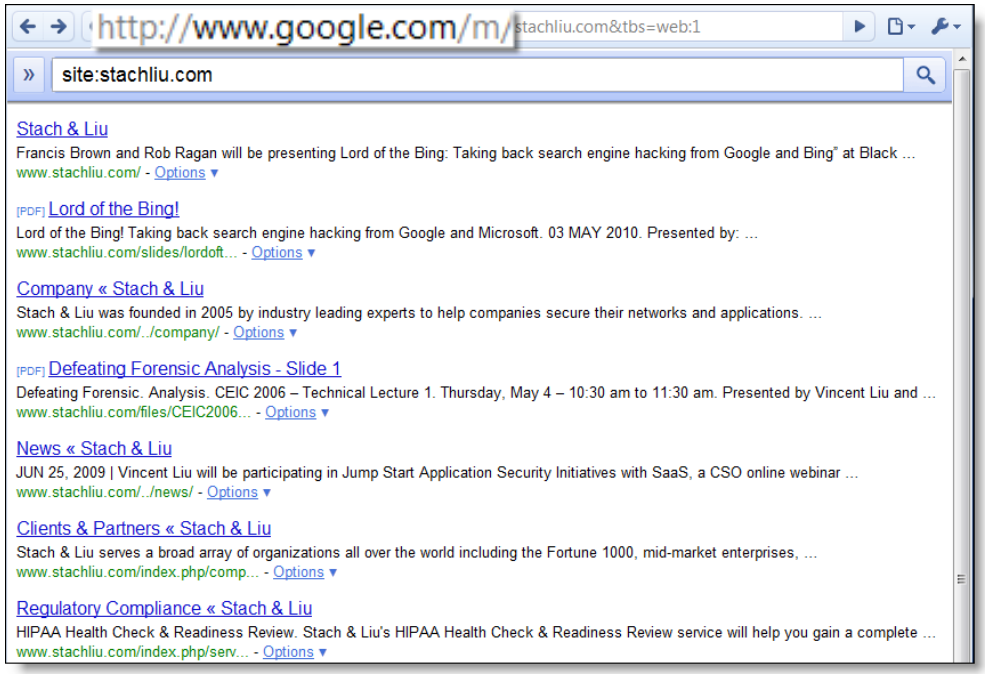
New Toolkit

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

COMING SOON



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 GOOGLE HACKING TOOLS

DEMO

Traditional Defenses

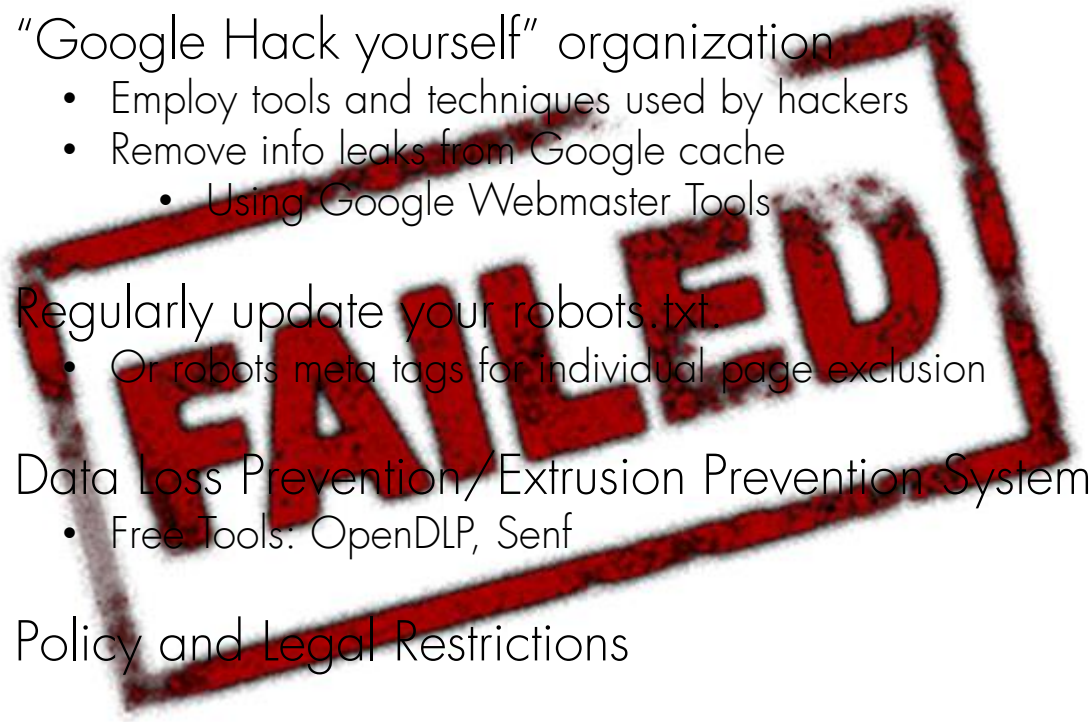
GOOGLE HACKING DEFENSES

- "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"

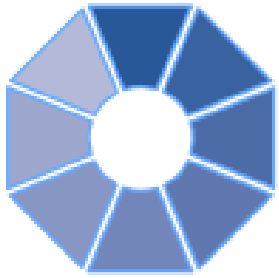
- ✓ Tools exist
- ✘ Convenient
- ✘ Real-time updates
- ✘ Multi-engine results
- ✘ Historical archived data
- ✘ Multi-domain searching

Advanced Defenses

NEW HOT SIZZLE

Stach & Liu now proudly presents:

- Google Hacking Alerts
- Bing Hacking Alerts

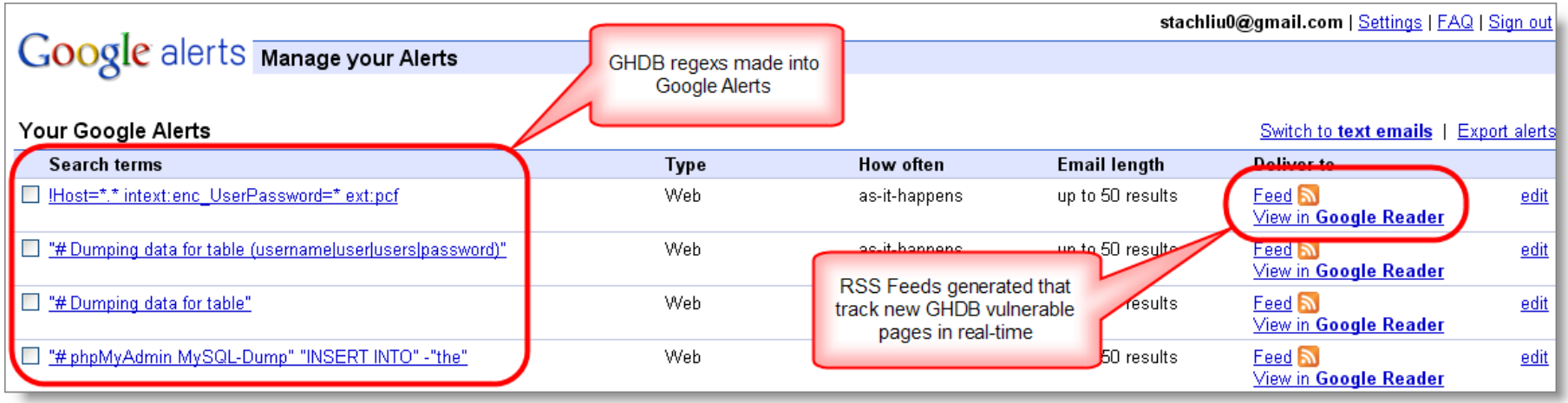


Google Hacking Alerts

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

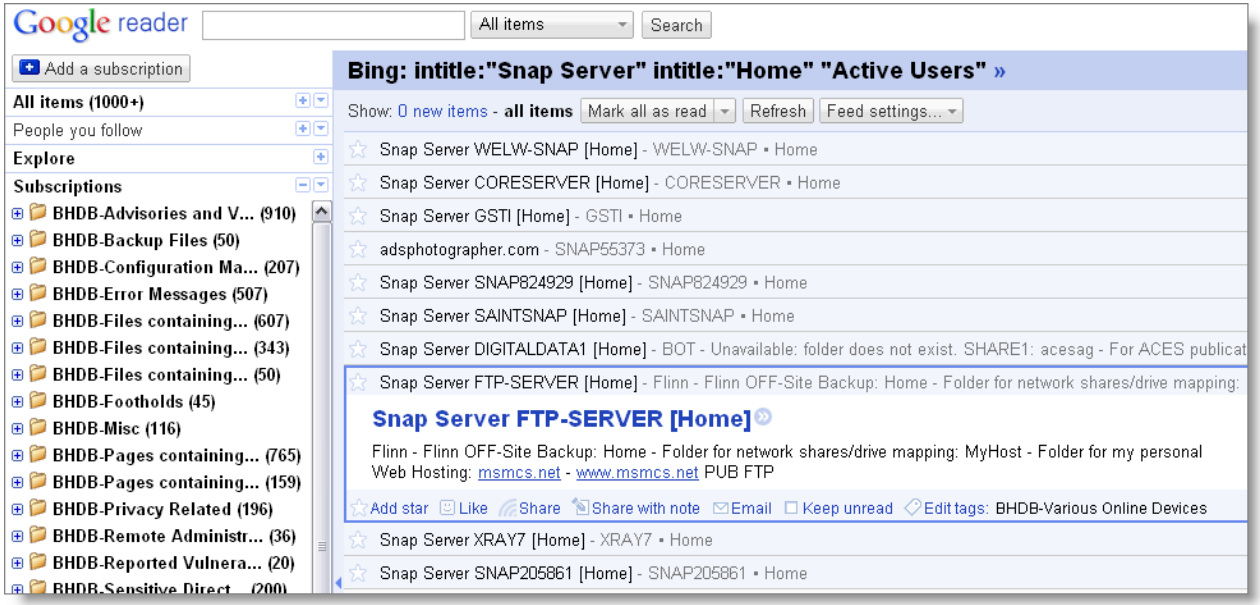
ADVANCED DEFENSES

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

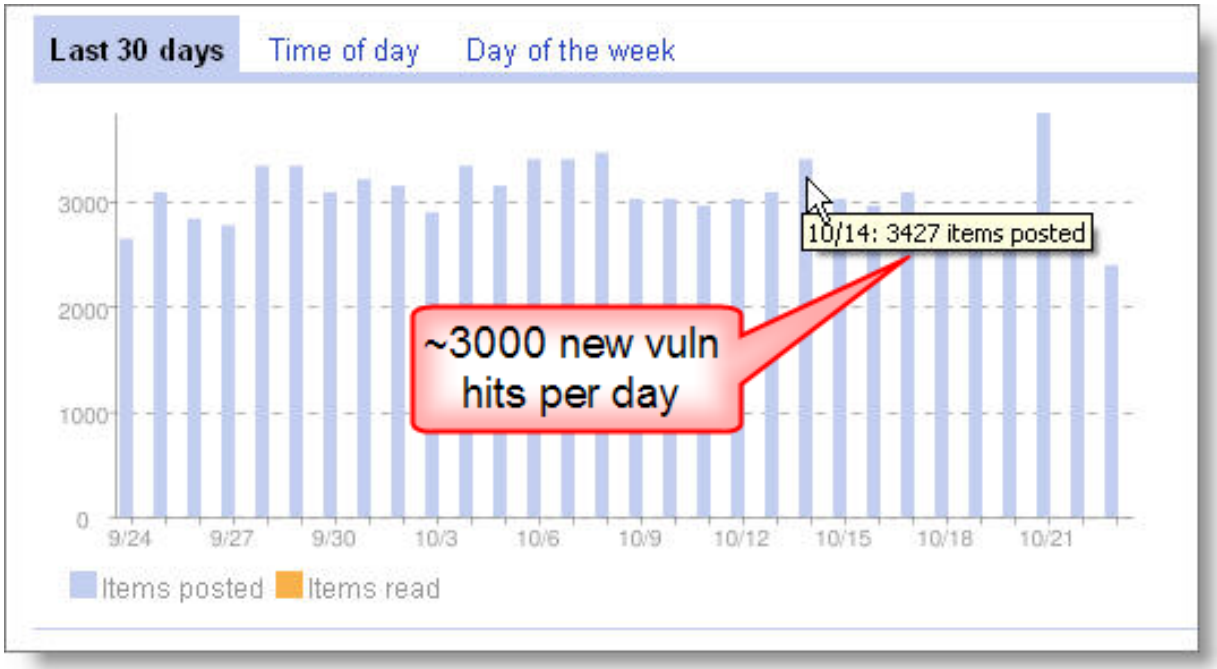


Bing/Google Alerts

LIVE VULNERABILITY FEEDS

World's Largest Live Vulnerability Repository

- Daily updates of *~3000 new hits per day*



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

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/