Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

3 August 2011 – Black Hat 2011 – Las Vegas, NV

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

blackhatusa+2011
EMBEDDING SECURITY

STACH&LIU

Agenda

- Introduction/Background

- Advanced Attacks
  - Google/Bing Hacking - Core Tools
  - NEW Diggity Attack Tools

- Advanced Defenses
  - Google/Bing Hacking Alert RSS Feeds
    - NEW Diggity Alert Feeds and Updates
  - NEW Diggity Alert RSS Feed Client Tools

- Future Directions

**STACH&LIU**

Introduction/Background

GETTING UP TO SPEED

STACH&LIU

Open Source Intelligence

SEARCHING PUBLIC SOURCES

OSINT – is a form of intelligence collection management that involves finding, selecting, and acquiring information from *publicly available* sources and analyzing it to *produce actionable intelligence*.

Google/Bing Hacking

SEARCH ENGINE ATTACKS
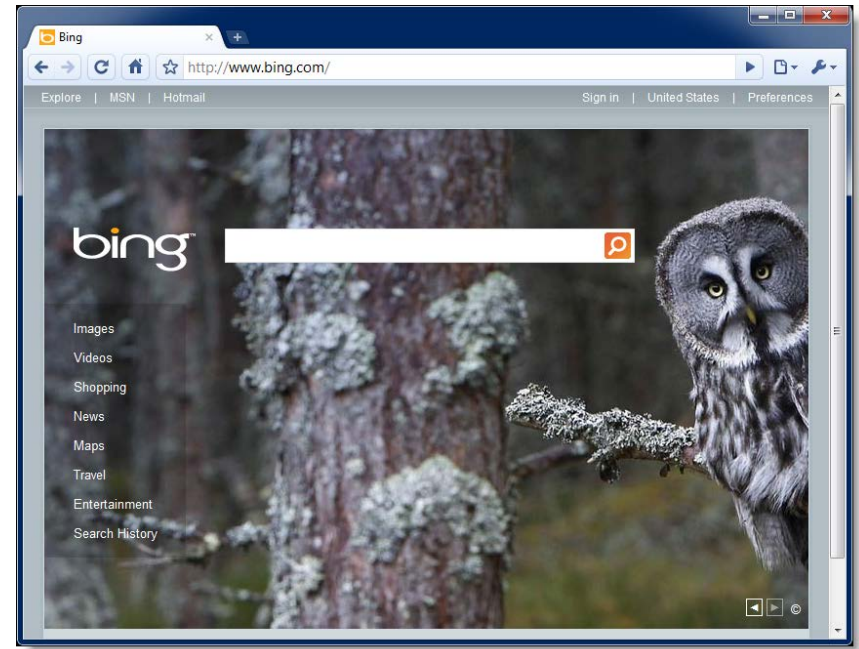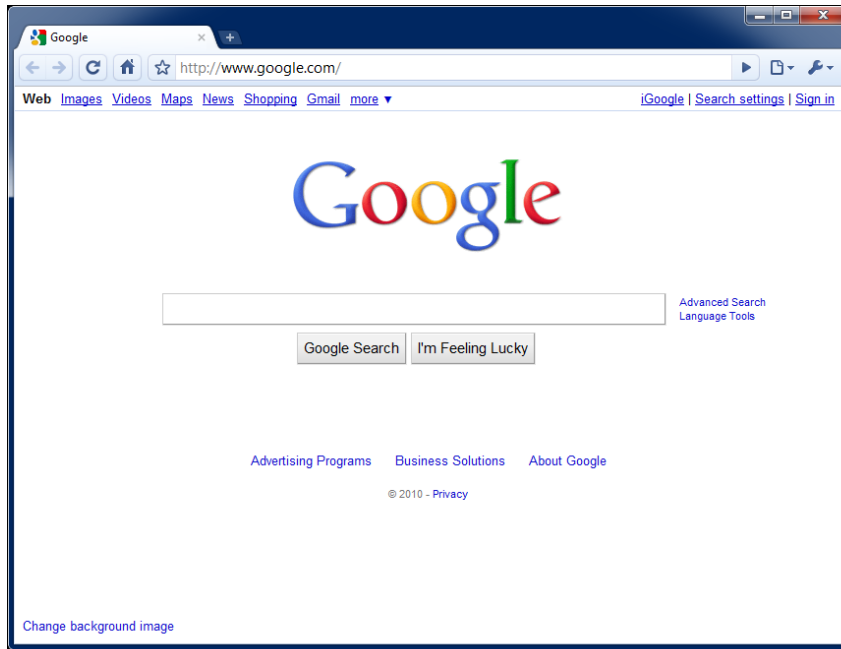
Google/Bing Hacking

SEARCH ENGINE ATTACKS

Bing's source leaked!

```
class Bing {
   public static string Search(string
   query)
   {
      return Google.Search(query);
   }
}
```

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)

STACH&LIU

Google Hacking = Lulz

REAL WORLD THREAT

LulzSec and **Anonymous** believed to use **Google Hacking** as a primary means of identifying vulnerable targets.

Their releases have nothing to do with their goals or their lulz. *It's purely based on whatever they find with their "google hacking" queries and then release it.*

– A-Team, 28 June 2011

STACH&LIU

Google Hacking = Lulz
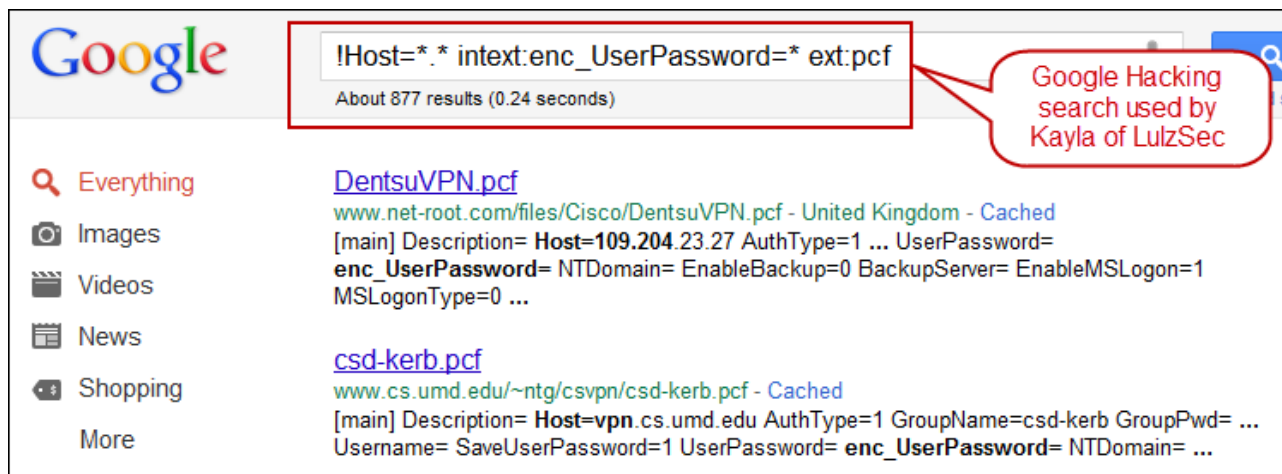
REAL WORLD THREAT

*22:14 <@kayla> Sooooo…using the link above and the google hack string.
!Host=*.* intext:enc_UserPassword=* ext:pcf Take your pick of VPNs you
want access too. Ugghh.. Aaron Barr CEO HBGary Federal Inc.
22:15 <@kayla> download the pcf file
22:16 <@kayla> then use http://www.unix-ag.uni-
kl.de/~massar/bin/cisco-decode?enc= to clear text it
22:16 <@kayla> = free VPN*

Quick History

GOOGLE HACKING RECAP

Dates	Event
2004	Google Hacking Database (GHDB) begins
May 2004	Foundstone SiteDigger v1 released
Jan 2005	Foundstone SiteDigger v2 released
Feb 13, 2005	Google Hack Honeypot first release
Feb 20, 2005	Google Hacking v1 released by Johnny Long
Jan 10, 2006	MSNPawn v1.0 released by NetSquare
Dec 5, 2006	Google stops issuing Google SOAP API keys
Mar 2007	Bing disables inurl: link: and linkdomain:
Nov 2, 2007	Google Hacking v2 released

STACH&LIU

Quick History...cont.

Dates	Event
Mar 2008	cDc Goolag - gui tool released
Sept 7, 2009	Google shuts down SOAP Search API
Nov 2009	Binging tool released by Blueinfy
Dec 1, 2009	FoundStone SiteDigger v 3.0 released
2010	Googlag.org disappears
April 21, 2010	**Google Hacking Diggity Project initial releases**
Nov 1, 2010	Google AJAX API slated for retirement
Nov 9, 2010	GHDB Reborn Announced – Exploit-db.com
July 2011	Bing ceases `&format=rss` support

STACH&LIU

Advanced Attacks

WHAT YOU SHOULD KNOW

STACH&**LIU**

Diggity Core Tools
S T A C H & L I U T O O L S

Google Diggity
- Uses Google JSON/ATOM API
  - Not blocked by Google bot detection
  - Does not violate Terms of Service
- Required to use 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

STACH&LIU

New Features

DIGGITY CORE TOOLS

Google Diggity - New API
- Updated to use Google JSON/ATOM API
- Due to deprecated Google AJAX API
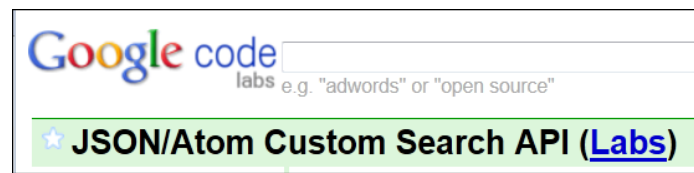
Misc. Feature Uprades
- Auto-update for dictionaries
- Output export formats
  - Now also XLS and HTML
- Help File – chm file added

STACH&LIU
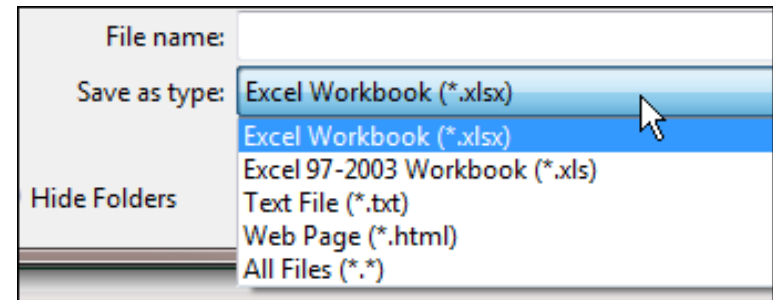
New Features

DOWNLOAD BUTTON

Download Buttons for Google/Bing Diggity
- Download actual files from Google/Bing search results
  - Downloads to default: `C:\DiggityDownloads\`
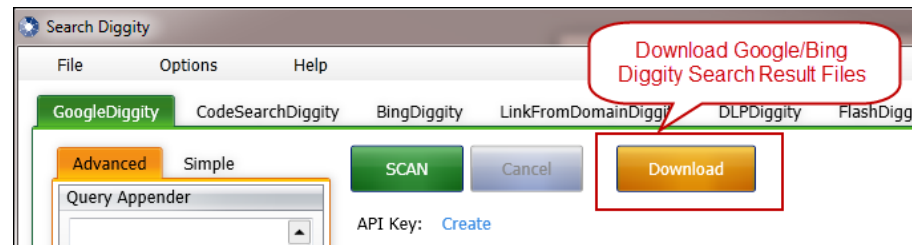
- Used by other tools for file download/analysis:
  - FlashDiggity, DLP Diggity, MalwareDiggity,…
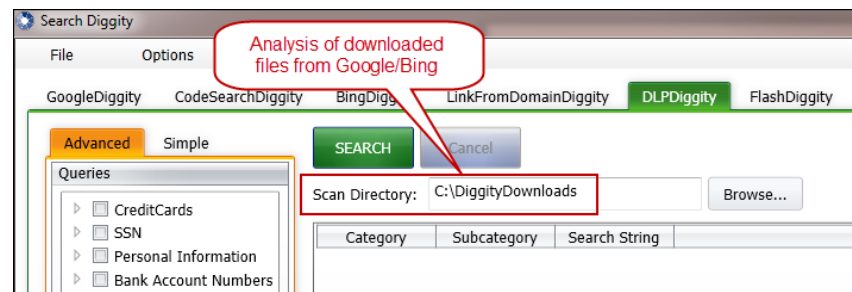
New Features

AUTO-UPDATES
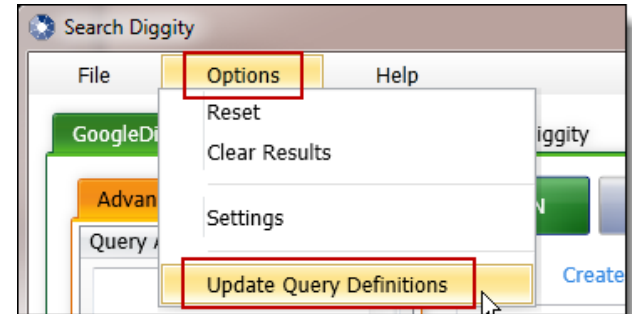
SLDB Updates in Progress

- Example: SharePoint Google Dictionary
  - http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/#SharePoint – GoogleDiggity Dictionary File

STACH&LIU

Google Diggity

DIGGITY CORE TOOLS

Bing Diggity
DIGGITY CORE TOOLS

Bing Hacking Database

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

Hacking CSE's

STACH&LIU

NEW GOOGLE HACKING TOOLS

Code Search Diggity

STACH&LIU

Google Code Search

VULNS IN OPEN SOURCE CODE

- Regex search for vulnerabilities in indexed public code, including popular open source code repositories:

- Example: SQL Injection in ASP querystring
  - select.*from.*request\.QUERYSTRING

CodeSearch Diggity

AMAZON CLOUD SECRET KEYS

NEW GOOGLE HACKING TOOLS

Bing LinkFromDomainDiggity

STACH&LIU

Bing LinkFromDomain

DIGGITY TOOLKIT

Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

NEW GOOGLE HACKING TOOLS

Malware Diggity

STACH&LIU

MalwareDiggity

D I G G I T Y   T O O L K I T

1. Leverages Bing's `linkfromdomain:` search directive to find off-site links of target applications/domains
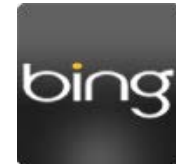
2. Runs off-site links against Google's Safe Browsing API to determine if any are malware distribution sites

Google code labs   e.g. "adwords" or "open source"

Google Safe Browsing API (Labs)
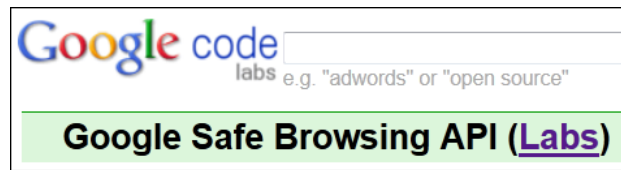
3. Return results that identify malware sites that your web applications are directly linking to

STACH&LIU

Mass Injection Attacks
MALWARE GONE WILD

Malware Distribution Woes – WSJ.com – June2010

- 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 *Jer*[...]
and the Association of Christian Scho[...]
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.
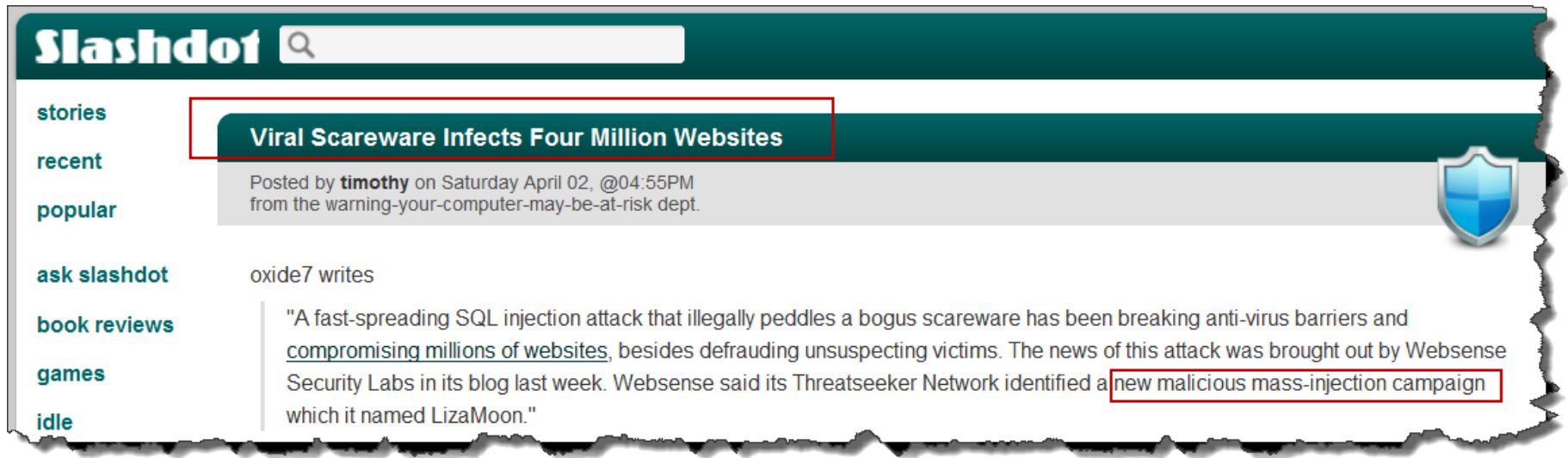
Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include Servicewomen.org and Intljobs.org.

Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – LizaMoon – April2011

- Popular websites victimized, become malware distribution sites to their own customers

Slashdot

stories
recent
popular

ask slashdot
book reviews
games
idle

Viral Scareware Infects Four Million Websites

Posted by **timothy** on Saturday April 02, @04:55PM
from the warning-your-computer-may-be-at-risk dept.

oxide7 writes

"A fast-spreading SQL injection attack that illegally peddles a bogus scareware has been breaking anti-virus barriers and compromising millions of websites, besides defrauding unsuspecting victims. The news of this attack was brought out by Websense Security Labs in its blog last week. Websense said its Threatseeker Network identified a new malicious mass-injection campaign which it named LizaMoon."

STACH&LIU

Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – willysy.com - August2011
- Popular websites victimized, become malware distribution sites to their own customers

Malware attack spreads to 5 million pages (and counting)
Unpatched sites turn on visitors

By **Dan Goodin in San Francisco** · **Get more from this author**

Posted in Malware, 2nd August 2011 18:07 GMT

An attack that targets a popular online commerce application has infected almost 5 million webpages with scripts that attempt to install malware on their visitors' computers.

The mass attack, which
osCommerce store-mar
When researchers from
search results suggeste
search results showed t

Armorize Malware Blog

armorize
Secure Your Web Applications

willysy.com Mass Injection ongoing, over 8 million infected pages, targets osCommerce sites

POSTED BY: CHRIS ON 7.25.2011 / CATEGORIES: DRIVE-BY DOWNLOAD, HACKALERT, MASS INJECTION, OSCOMMERCE, WEB MALWARE

STACH&LIU

Malware Diggity

DIGGITY TOOLKIT

Malware Diggity

DIGGITY TOOLKIT

Malware Diggity

DIAGNOSTICS IN RESULTS

NEW GOOGLE HACKING TOOLS

DLP Diggity

DLP Diggity

LOTS OF FILES TO DATA MINE

DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR

Google Results for Common Docs

Legend:
- 2004
- 2007
- 2011

Data points:
- 513,000,000
- 260,000,000
- 84,500,000
- 42,000,000
- 17,300,000
- 46,400,000
- 10,900,000
- 16,100,000
- 30,100,000
- 2,100,000
- 969,000
- 1,720,000

Categories: PDF, DOC, XLS, TXT

DLP Diggity

DIGGITY TOOLKIT

NEW GOOGLE HACKING TOOLS

FlashDiggity

STACH&LIU

Flash Diggity

DIGGITY TOOLKIT

- **Google for SWF** files on target domains
  - Example search: `filetype:swf site:example.com`
- **Download** SWF files to `C:\DiggityDownloads\`
- **Disassemble** SWF files and **analyze** for Flash vulnerabilities

NEW GOOGLE HACKING TOOLS

DEMO

GoogleScrape Diggity
DIGGITY TOOLKIT

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

STACH&LIU
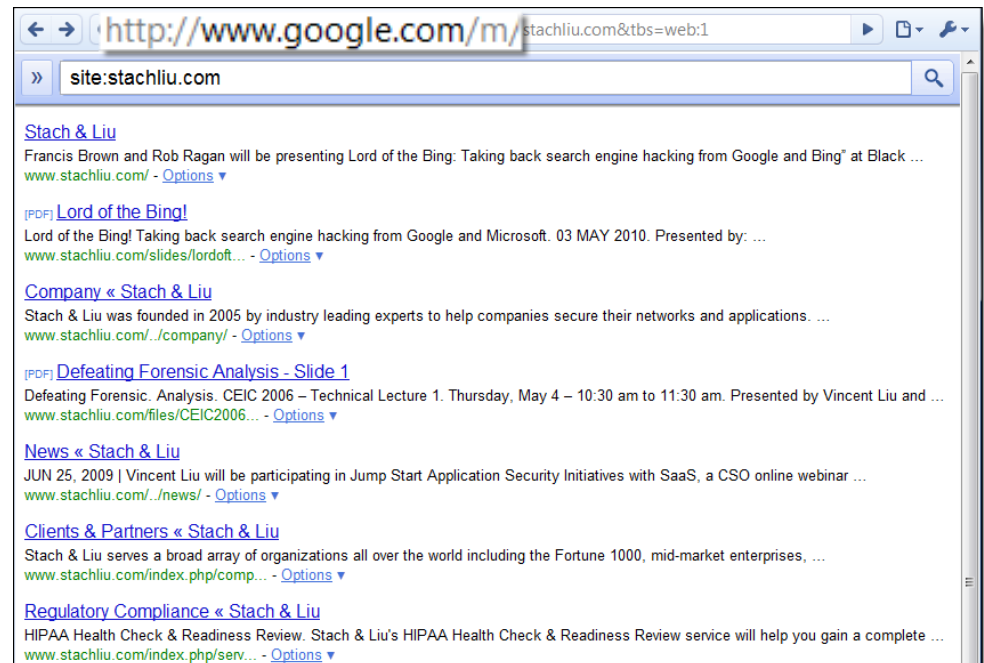
NEW GOOGLE HACKING TOOLS

Baidu Diggity

BaiduDiggity

CHINA SEARCH ENGINE

- Fighting back

Finding vulns in Chinese government sites

Advanced Defenses

PROTECT YO NECK

STACH&LIU

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

STACH&LIU

Existing Defenses

✔ Tools exist

✖ Convenient

✖ Real-time updates

✖ Multi-engine results

✖ Historical archived data

✖ Multi-domain searching

STACH&LIU

Advanced Defenses

NEW HOT SIZZLE

Stach & Liu now proudly presents:

- Google and Bing Hacking Alerts
  - SharePoint Hacking Alerts – 118 dorks
  - SHODAN Hacking Alerts – 26 dorks
- Diggity Alerts FUNdle Bundles
  - Consolidated alerts into 1 RSS feed
- Alert Client Tools
  - Alert Diggity – Windows systray notifications
  - iDiggity Alerts – iPhone notification app

STACH&LIU
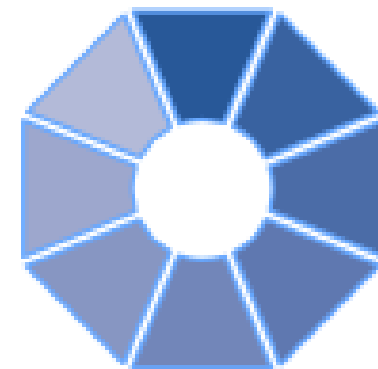
Google Hacking Alerts

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

STACH&LIU

Google Hacking Alerts

Bing Hacking Alerts

ADVANCED DEFENSES

Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Leverages http://api.bing.com/rss.aspx
- 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*
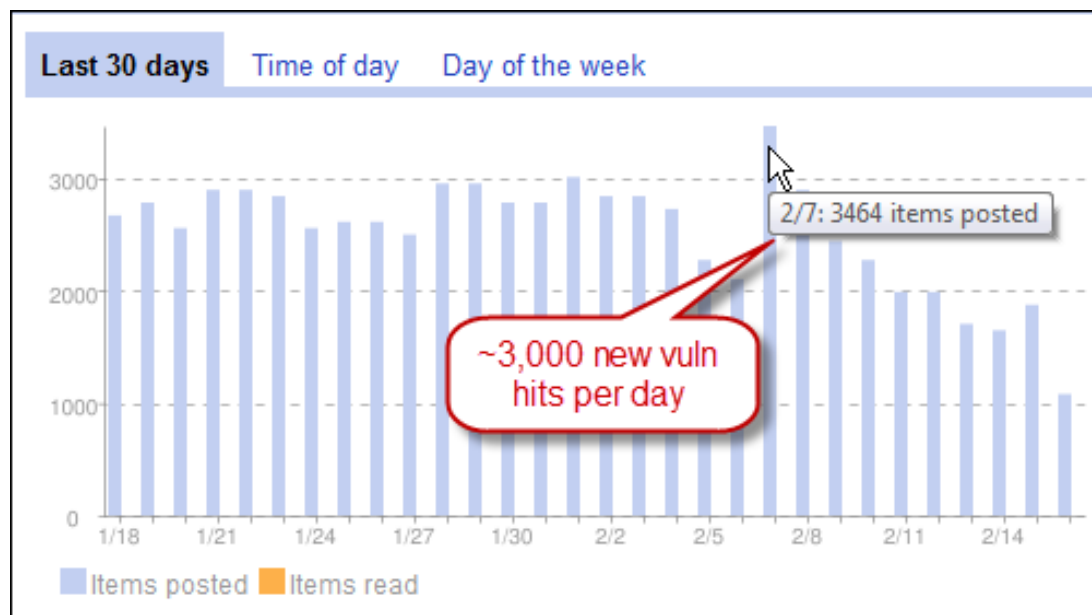
Diggity Alerts
One Feed to Rule Them All

ADVANCED DEFENSE TOOLS

Diggity Alert Fundle Bundle

STACH&LIU

FUNdle Bundle

FUNdle Bundle

A D V A N C E D   D E F E N S E S

FUNdle Bundle

MOBILE FRIENDLY

ADVANCED DEFENSE TOOLS

SHODAN Alerts

SHODAN Alerts

FINDING SCADA SYSTEMS

SHODAN Alerts

SHODAN RSS FEEDS

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:
    - Windows Systray App
    - Droid app (coming soon)
    - iPhone app

STACH&LIU

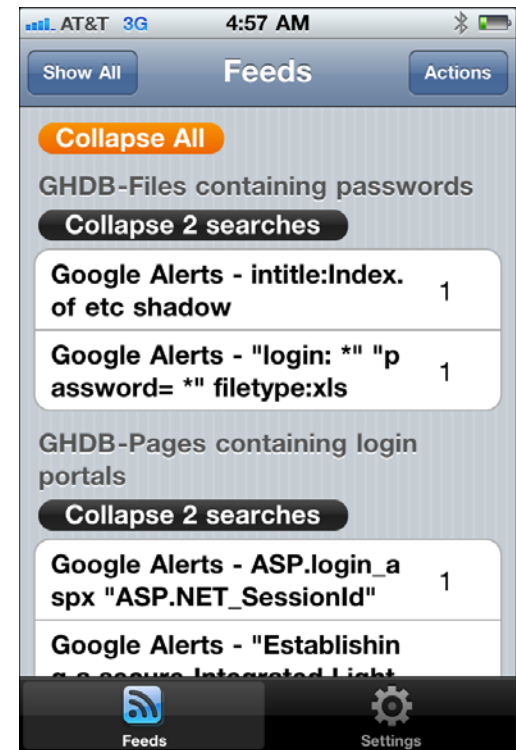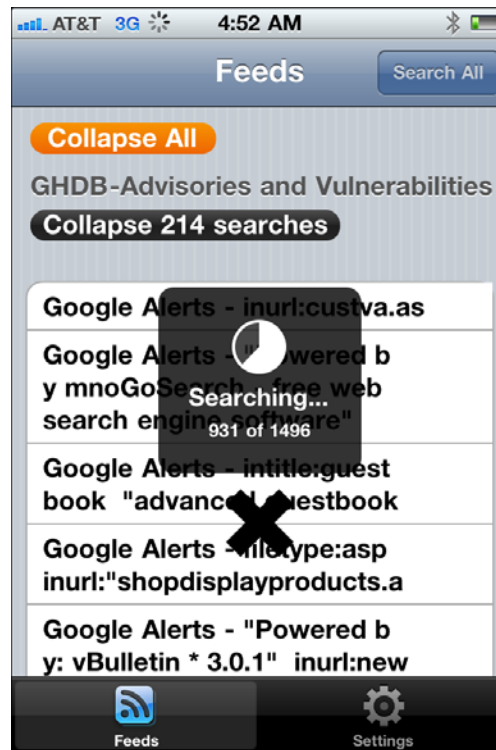ADVANCED DEFENSE TOOLS

Alert Diggity

STACH&LIU

Alerts Diggity

ADVANCED DEFENSES

ADVANCED DEFENSE TOOLS

iDiggity Alerts
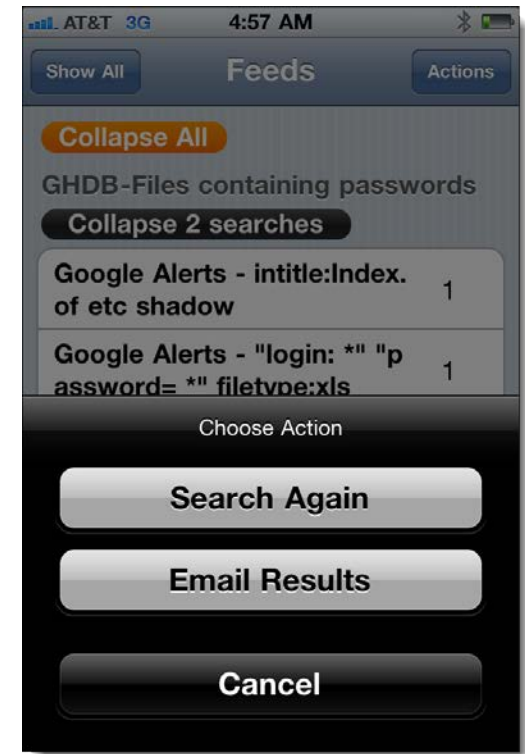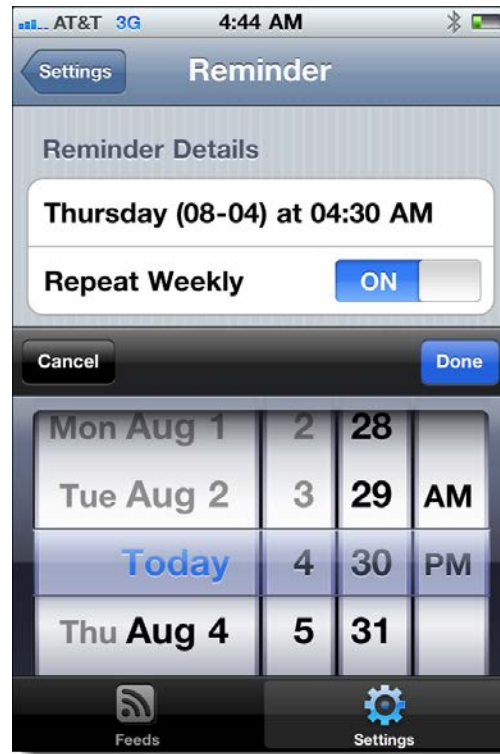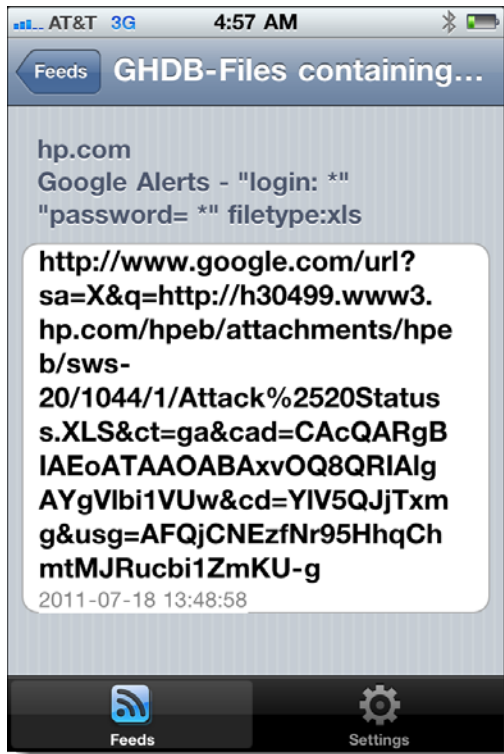
STACH&LIU

iDiggity Alerts
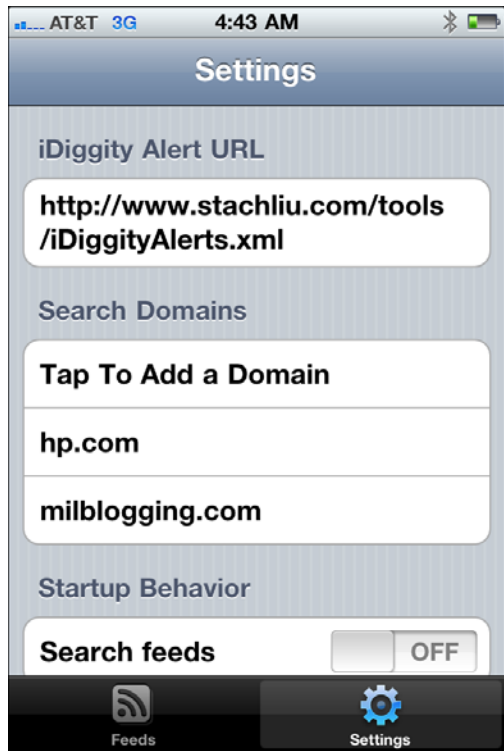
ADVANCED DEFENSES

iDiggity Alerts

ADVANCED DEFENSES

New Defenses

"GOOGLE/BING HACK ALERTS"

✓ Tools exist

✓ Convenient

✓ Real-time updates

✓ Multi-engine results

✓ Historical archived data

✓ Multi-domain searching

STACH&LIU

Future Direction

IS NOW

Diggity Alert DB

DATA MINING VULNS

DIGGITY ALERTS DATABASE

STACH&LIU

Dictionary Updates

New maintainers of the GHDB – 09 Nov 2010

- http://www.exploit-db.com/google-hacking-database-reborn/

STACH&LIU

Special Thanks

Oscar "The Bull" Salazar
Brad "BeSickWittIt" Sickles
Nick "King Luscious" Harbin
Prajakta "The Flasher" Jagdale
Ruihai "Ninja" Fang
Jason "Blk-majik" Lash

STACH&LIU

Questions?
Ask us something
We'll try to answer it.

STACH&LIU

Thank You

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

STACH&LIU