

Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing 18 MAY 2011 - TakeDownCon 2011 - Dallas, TX



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



Agenda

OVERVIEW

- Introduction/Background
- Advanced Attacks
 - Google/Bing Hacking
- Advanced Defenses
 - Google/Bing Hacking Alerts
- Other OSINT Attack Techniques
- Future Directions





Introduction/ Background

GETTING UP TO SPEED







Open Source Intelligence

SEARCHING PUBLIC SOURCES

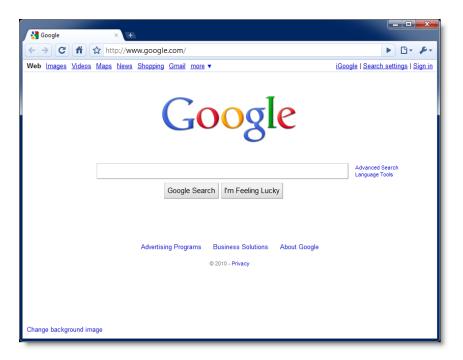
OSINT – is a form of intelligence collection management that involves finding, selecting, and acquiring information from *publicly available* sources and analyzing it to *produce actionable intelligence*.

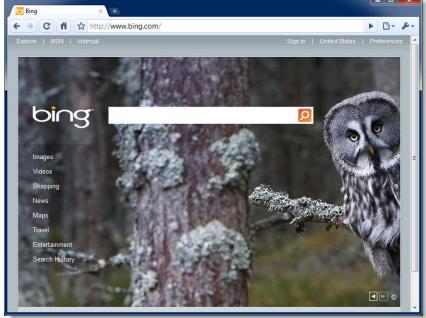




Google/Bing Hacking

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);
   }
}
```





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
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





Advanced Attacks

WHAT YOU SHOULD KNOW







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









SearchDiggity Updates



STACH & LIU TOOLS

New Features

- Auto-update for dictionaries
 - Will begin updating google/bing dorks
- Output formats
 - Now also XLS and HTML exports
- Help File chm file added



New Tool Tabs

- Bing LinkFromDomain Footprinting
 - Leverages linkfromdomain: directive to identify external links
 - Identify other apps, hosts, domains potentially belonging to target
- Google Code Search Diggity
 - Identifies code vulnerabilities within open source projects





NEW GOOGLE HACKING TOOLS



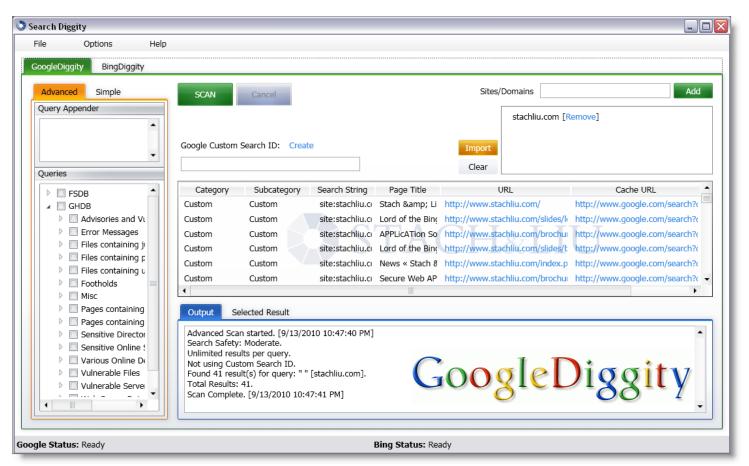




Google Diggity



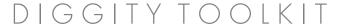
DIGGITY TOOLKIT



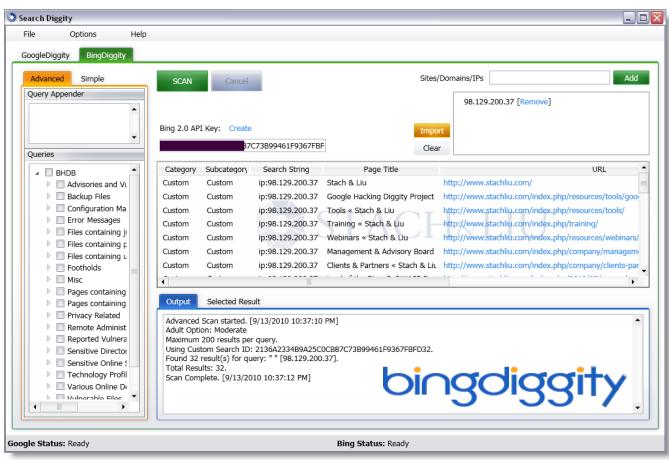




Bing Diggity











Auto-Update Feature

SLDB UPDATES



SLDB Updates in Progress

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







Auto-Update Feature

3rd party integration



New maintainers of the GHDB - 09 Nov 2010

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

Google Hacking Database Reborn

9th November 2010 - by admin

The incredible amount of information continuously leaked onto the Internet, and therefore accessible by Google, is of great use to penetration testers around the world. Johnny Long of Hackers for Charity started the Google Hacking Database (GHDB) to serve as a repository for search terms, called Google-Dorks, that expose sensitive information, vulnerabilities, passwords, and much more.



As Johnny is now pursing his mission in Uganda, he has graciously allowed us at The Exploit Database to pick up where the GHDB left off and resurrect it. It is with great excitement that we announce that the GHDB is now being hosted by us and actively maintained again. This will allow us to tie the GHDB directly into our database of exploits providing the most current information possible.

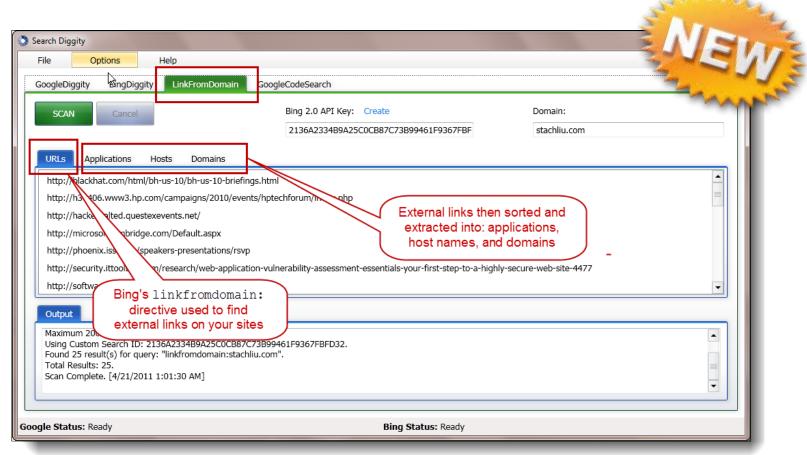




Bing LinkFromDomain



DIGGITY TOOLKIT







GoogleScrape Diggity

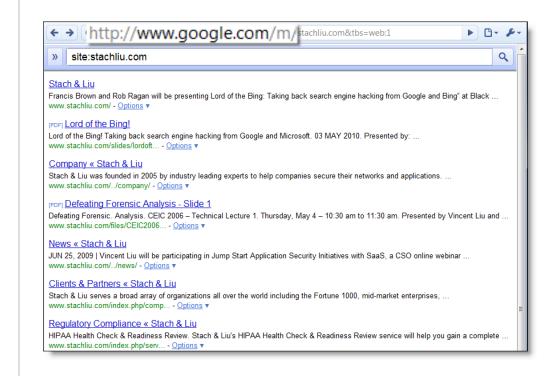


DIGGITY TOOLKIT

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









Bing Hack Database



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"







BaiduDiggity



CHINA SEARCH ENGINE

COMING SOON

COMING SOON!







BaiduDiggity

CHINA SEARCH ENGINE

Fighting back









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

"HACKYOURSELF"



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





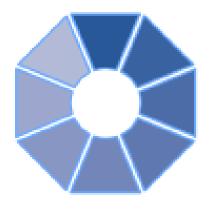


Advanced Defenses

NEW HOT SIZZLE

Stach & Liu now proudly presents:

- Google Hacking Alerts
 - SharePoint Hacking Alerts 118 dorks
- Bing Hacking Alerts







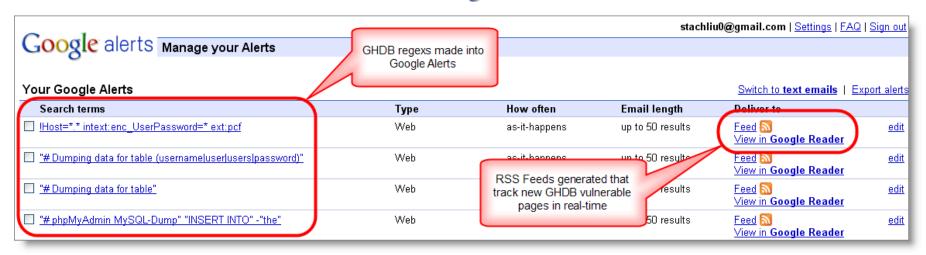
Google Hacking Alerts



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







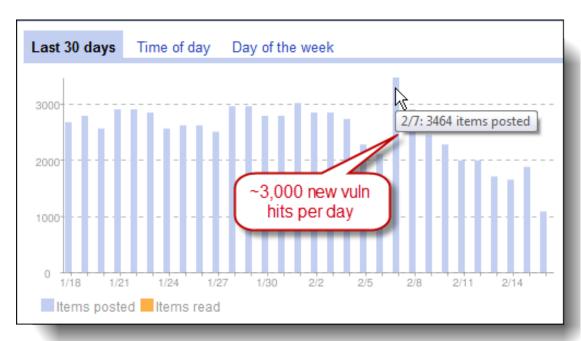
Bing/Google Alerts



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





New Defenses

"GOOGLE/BING HACK ALERTS"



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









Other OSINT Attacks

WHAT YOU SHOULD KNOW





Google Apps Explosion

SO MANY APPLICATIONS TO ABUSE

Google alerts

Google reader



Google custom search









Google calendar

Google news



Google docs

Google Insights for Search



Google blogs









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

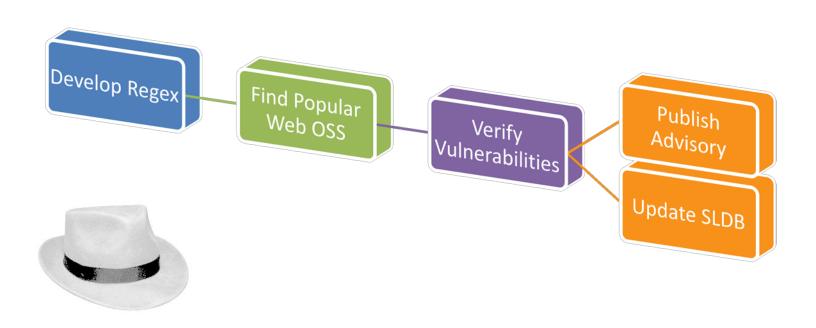






Google Code Search

VULNS IN OPEN SOURCE CODE



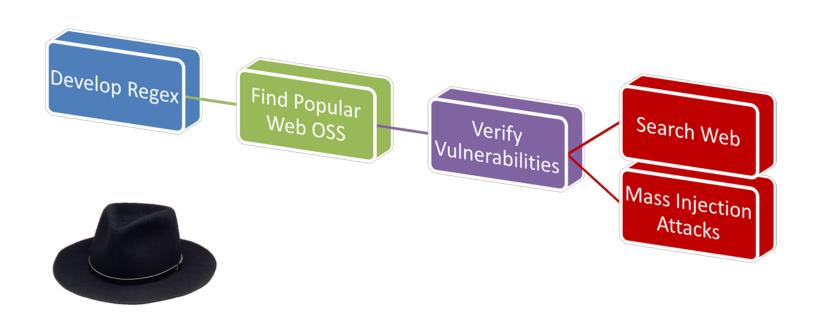






Google Code Search

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









BLACK HAT SEO RECON



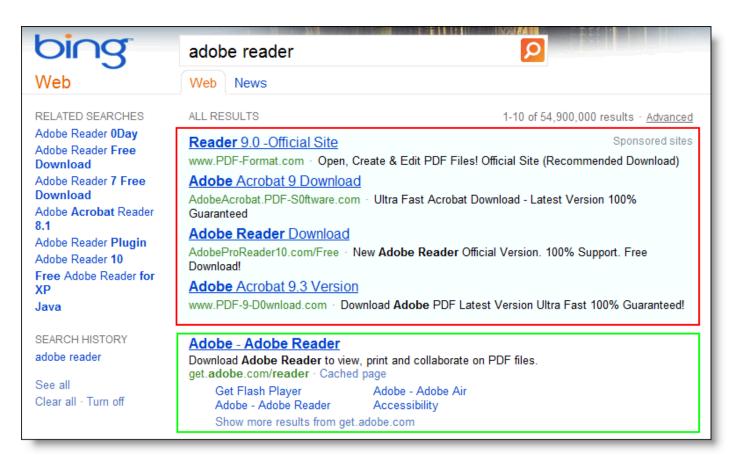




Malware Ads



BLACK HAT ADS







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

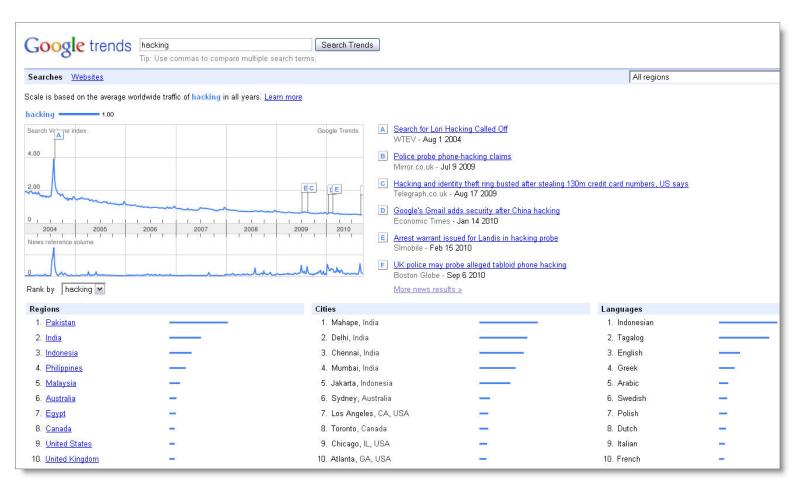








OTHER INTERESTING

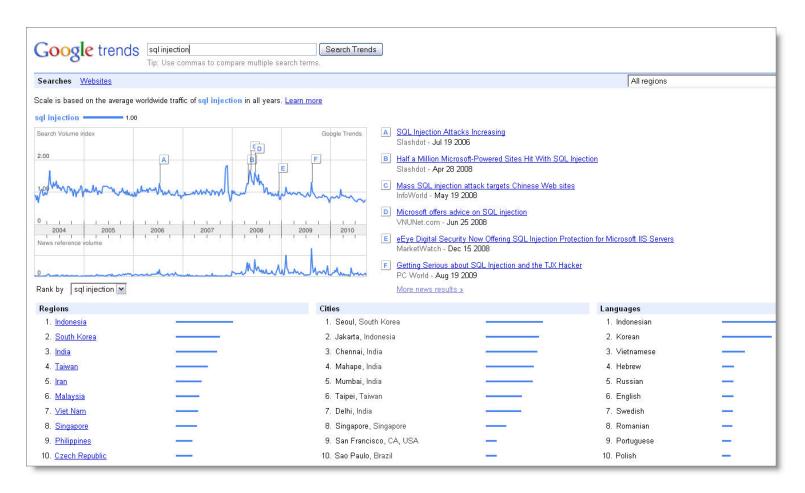








OTHER INTERESTING

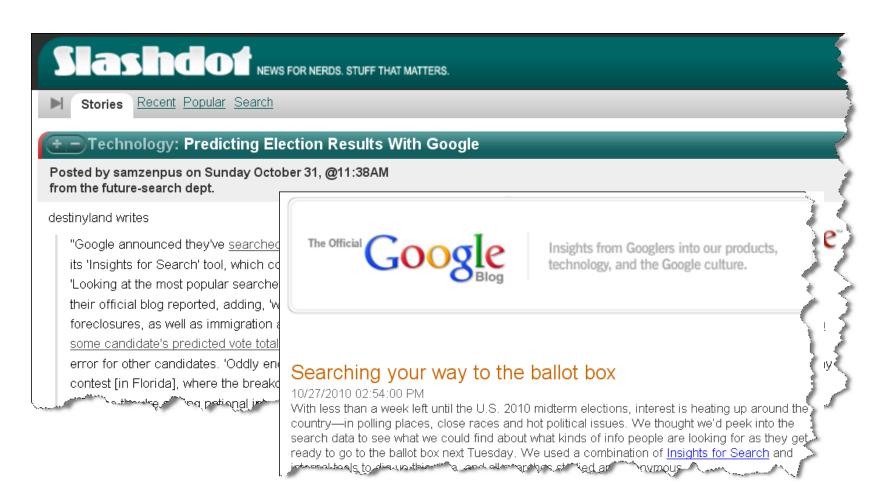








PREDICTING ELECTIONS







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/storp/chow4rtiple.ihtml2artipleID=22560024

"Every time I load Jpost site, I get nas on Tuesday, referring to the Jerusaler

Sure enough, the Web sites of the *Jet* and the Association of Christian Schosites 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 intijops.org.







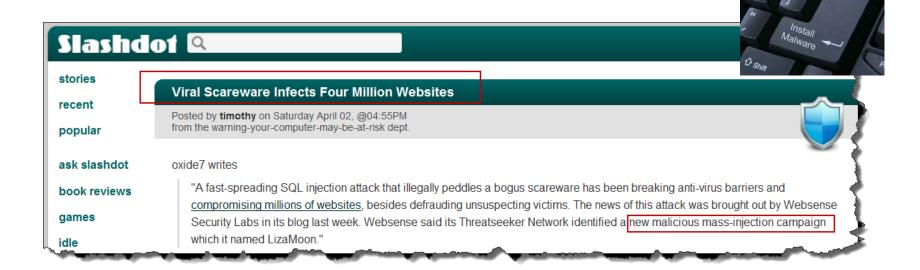
Mass Injection Attacks



MALWARE GONE WILD

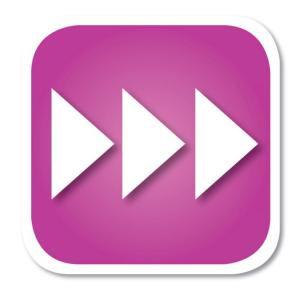
Malware Distribution Woes – LizaMoon – April2011

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





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







Predictions Update



GOOGLE REALTIME/INSTANT



Google About Google Instant

Learr

Google Instant is a new search enhancement that shows results as you type. We are pushing the limits of our technology and infrastructure to help you get better search results, faster. Our key technical insight was that people type slowly, but read quickly, typically taking 300 milliseconds between keystrokes, but only 30 milliseconds (a tenth of the time!) to glance at another part of the page. This means that you can scan a results page while you type.

The most obvious change is that you get to the right content much faster than before because you don't have to finish typing your full search term, or even press "search." Another shift is that seeing results as you type helps you formulate a better search term by providing instant feedback. You can now adapt your search on the fly until the results match exactly what you want. In time, we may wonder how search ever worked in any other way.









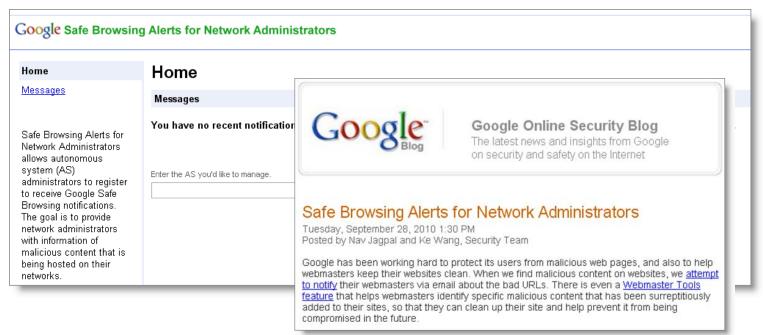
Predictions Update



SEEMS STRANGELY FAMILIAR

Google Safe Browsing Alerts for Network Administrators

- Google's new service which greatly resembles MalwareDiggity
- Imitation is the sincerest form of flattery...



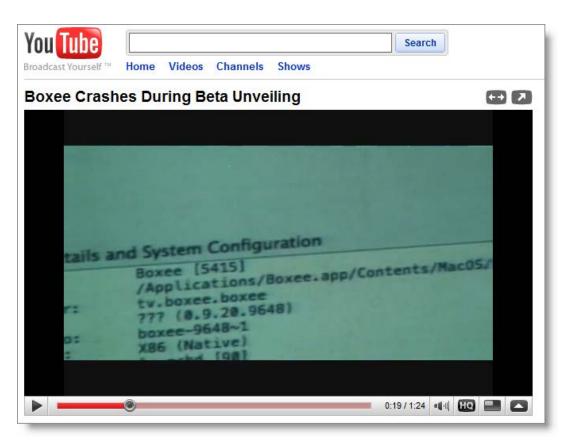




Youtube Info Leak



YOUTUBE + SENSITIVE INFO DISCLOSURE







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

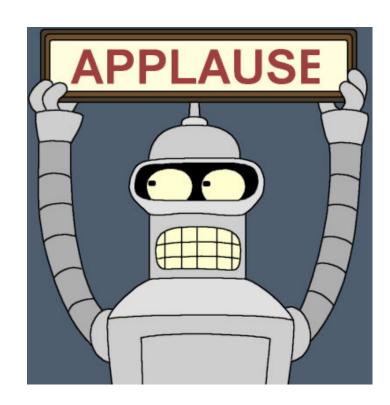
For more info:

Email: contact@stachliu.com Project: diggity@stachliu.com

Stach & Liu, LLC www.stachliu.com



Thank You



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

