Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

15 May 2012 – ISSA LA - Fourth Annual Information Security Summit – Los Angeles, CA

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

STACH&LIU

Agenda

OVERVIEW

- 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

Introduction/ Background

GETTING UP TO SPEED

STACH&LIU

Open Source Intelligence

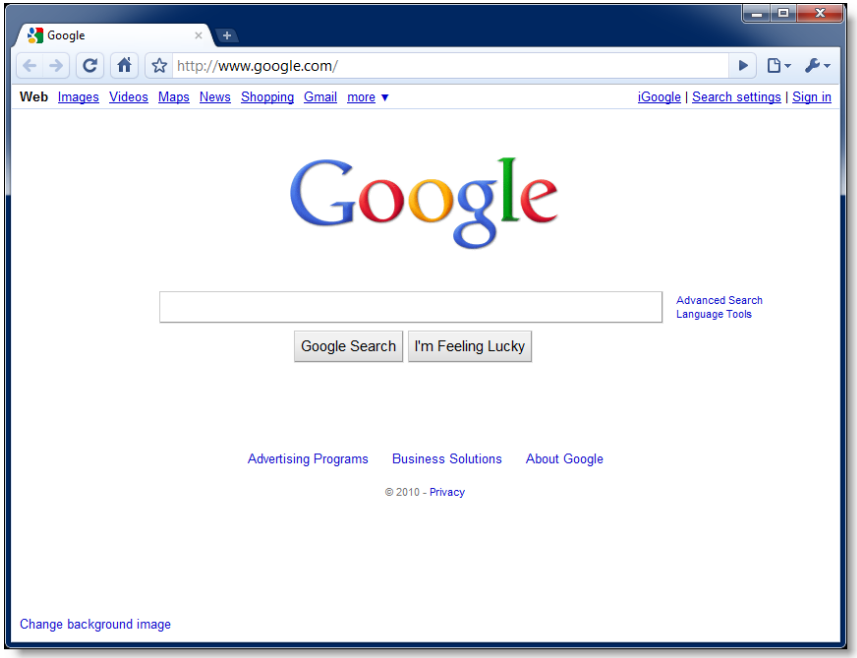
SEARCHING PUBLIC SOURCES

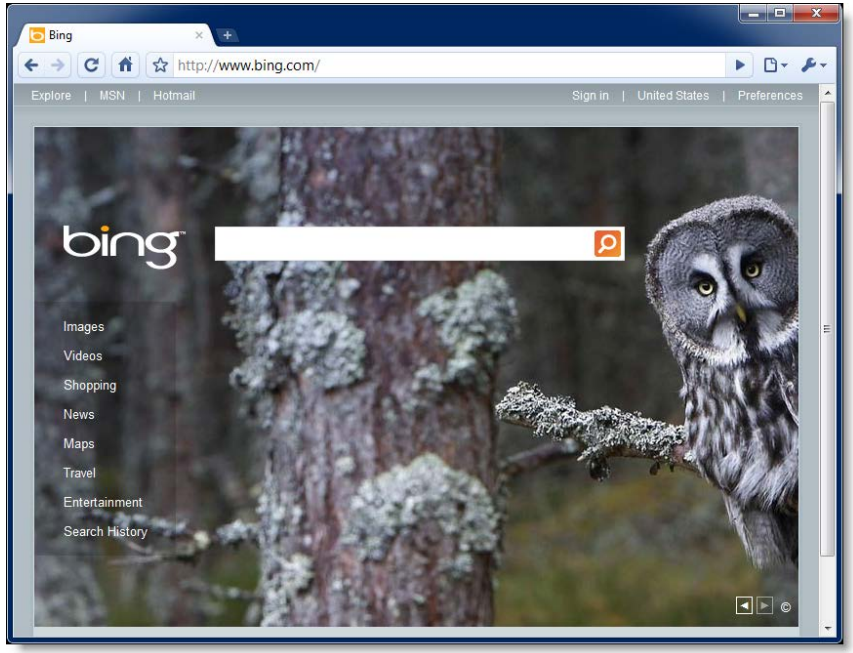
OSINT – is a form of intelligence collection management that involves finding, selecting, and acquiring information from *publicly available* sources and analyzing it to *produce actionable intelligence*.

STACH&LIU

Google/Bing Hacking

SEARCH ENGINE ATTACKS





STACH&LIU

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)

Google Hacking = Lulz

REAL WORLD THREAT

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

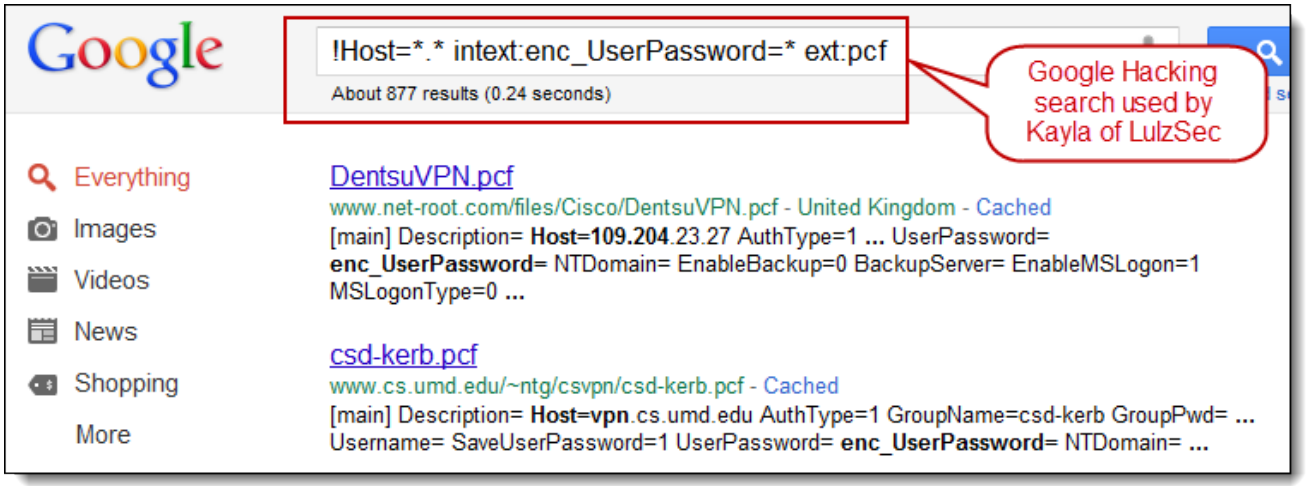
Their releases have nothing to do with their goals or their lulz. It's purely based on whatever they find with their "google hacking" queries and then release it.

– A-Team, 28 June 2011

Google Hacking = Lulz

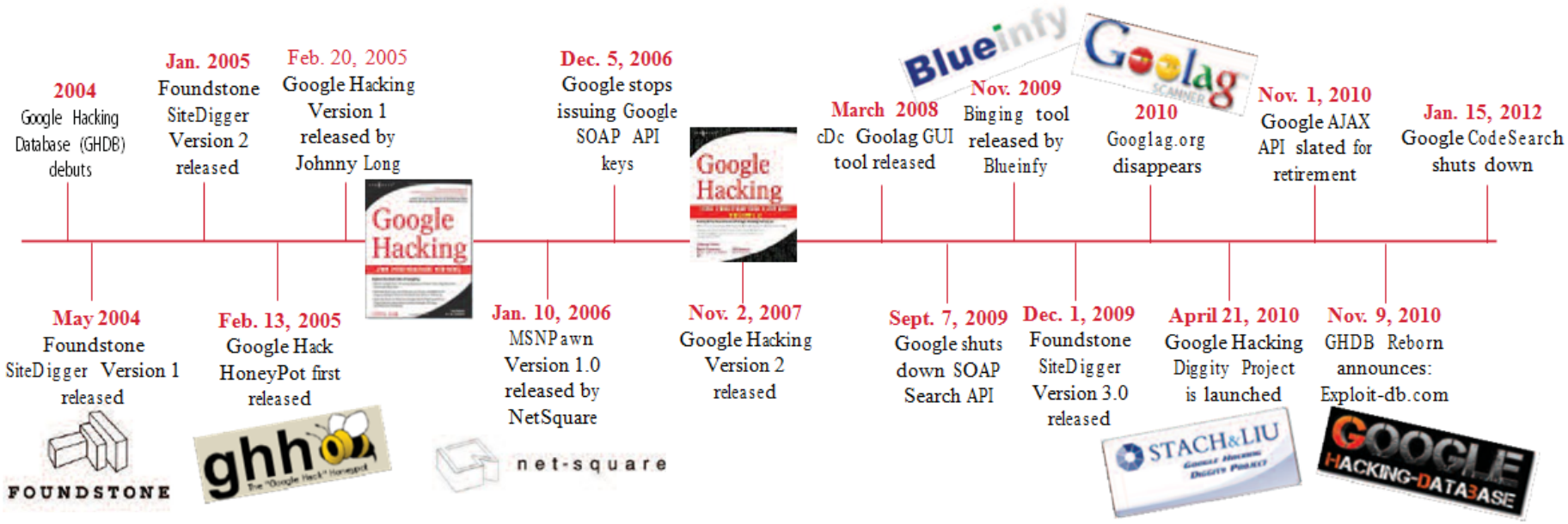
REAL WORLD THREAT

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



Quick History

GOOGLE HACKING RECAP

Advanced Attacks

WHAT YOU SHOULD KNOW

Diggity Core Tools

STACH & LIU TOOLS

Google Diggity

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

Bing Diggity

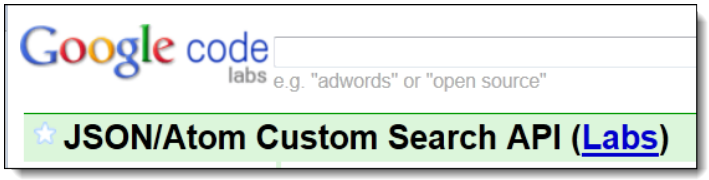
- Uses Bing 2.0 SOAP API
- Company/Webapp Profiling
  - Enumerate: URLs, IP-to-virtual hosts, etc.
- Bing Hacking Database (BHDB)
  - Vulnerability search queries in Bing format

New Features

DIGGITY CORE TOOLS

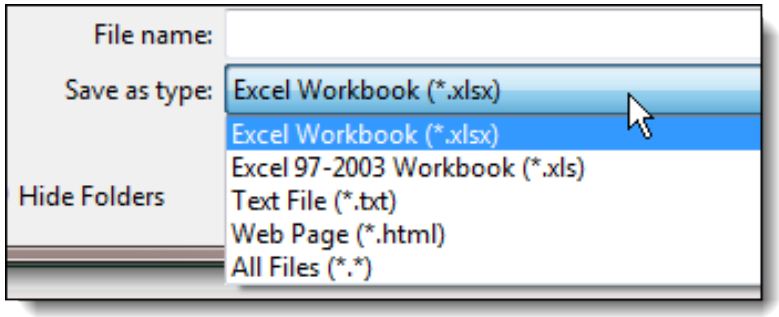
Google Diggity - New API

- 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

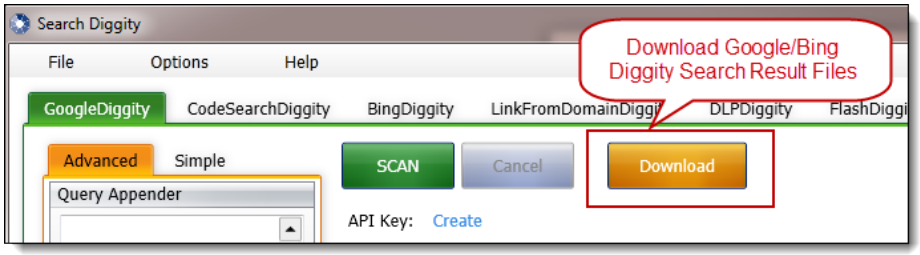


New Features

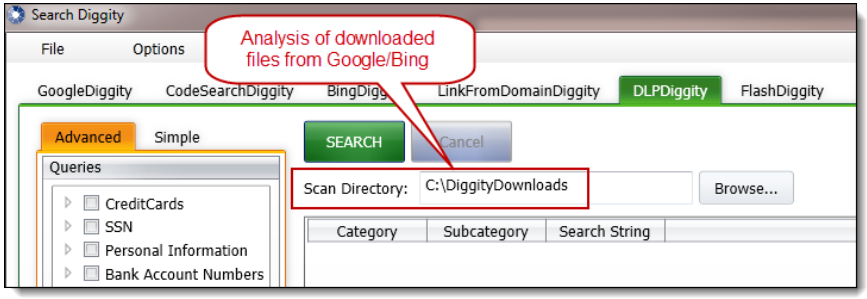
DOWNLOAD BUTTON

Download Buttons for Google/Bing Diggity

- Download actual files from Google/Bing search results
  - Downloads to default: `C:\DiggityDownloads\`



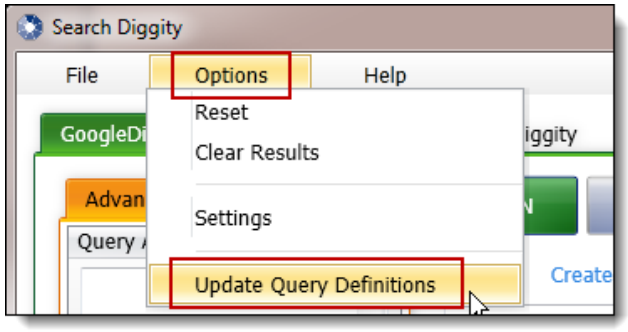
- Used by other tools for file download/analysis:
  - FlashDiggity, DLP Diggity, MalwareDiggity,…



New Features

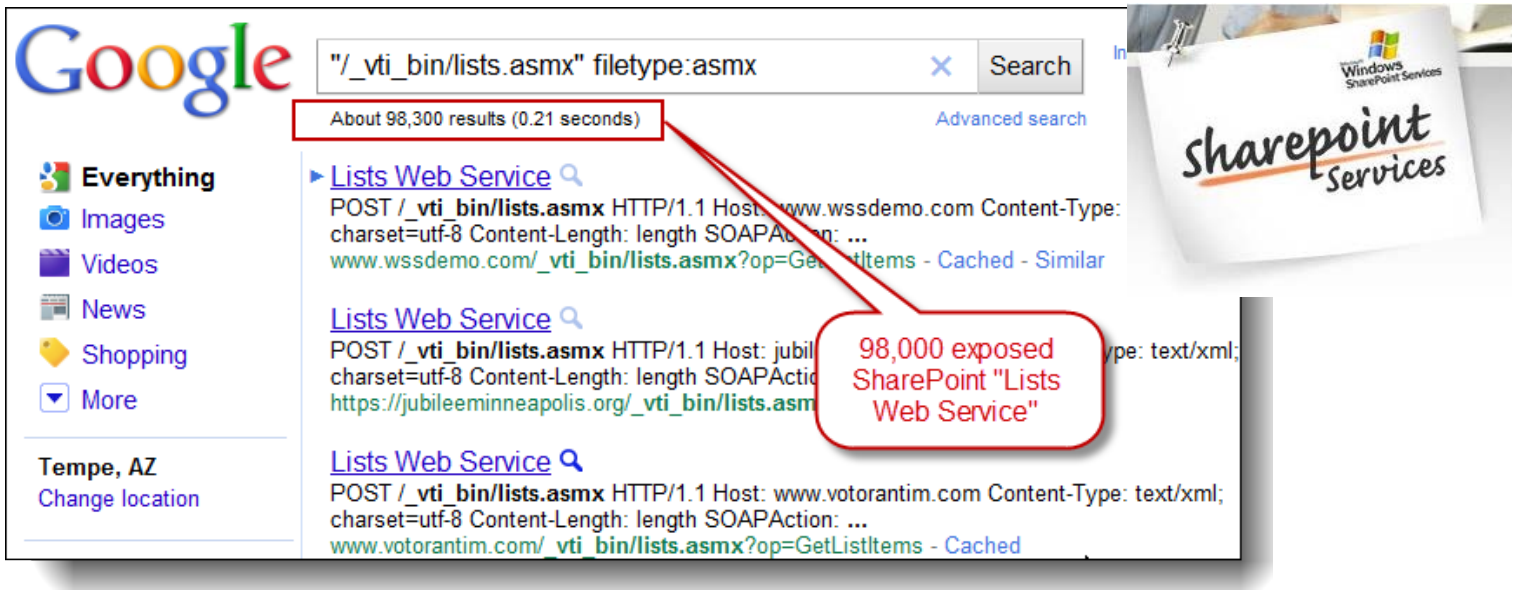
NEW

AUTO-UPDATES



SLDB Updates in Progress

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

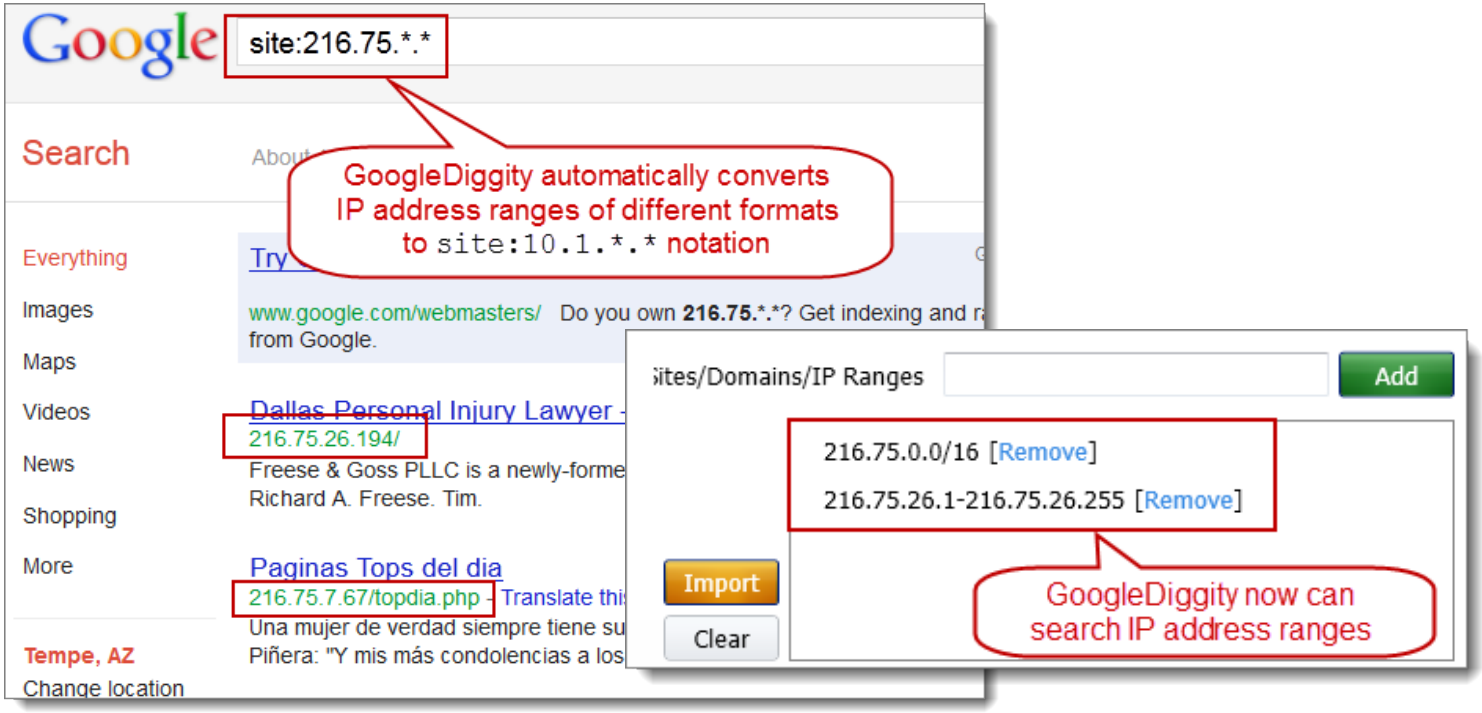


New Features

NEW

IP ADDRESS RANGES

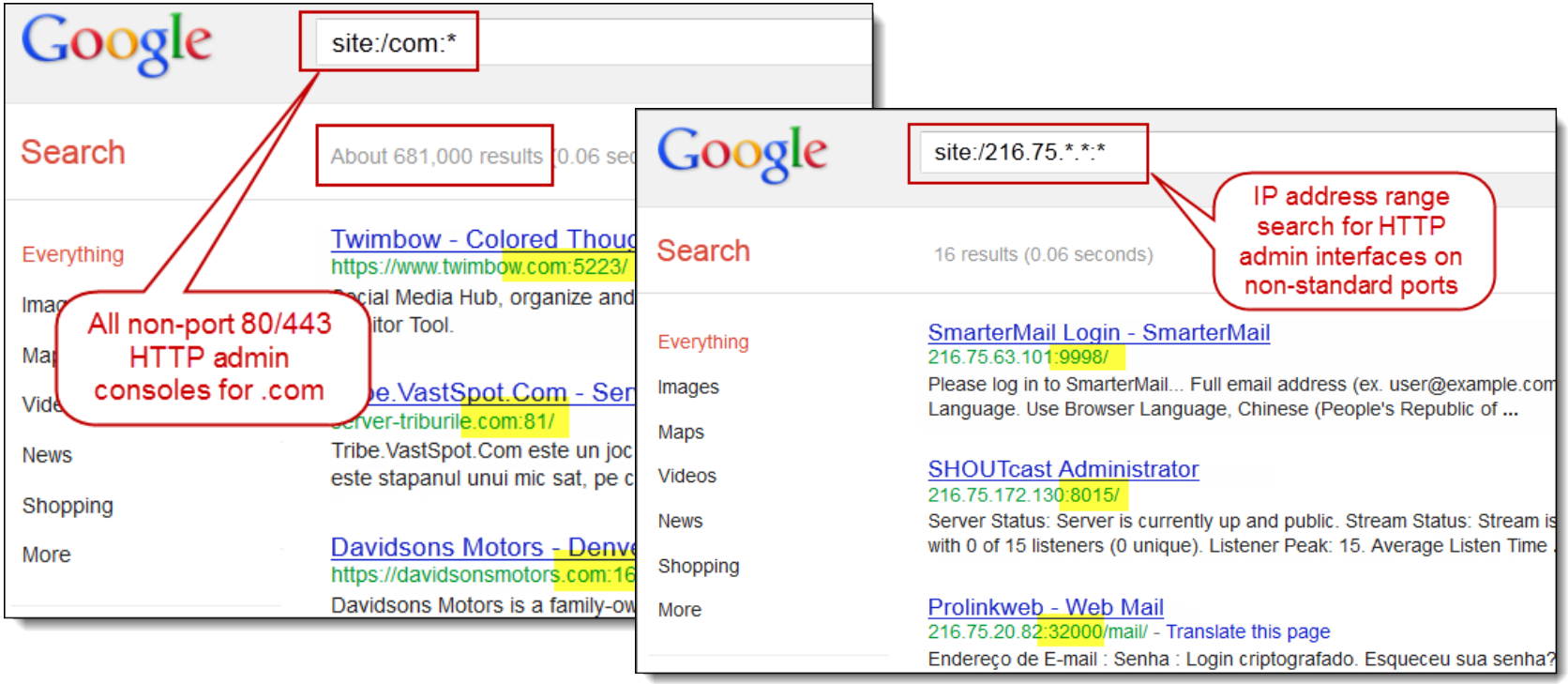
GoogleDiggity can now search for IP Address Ranges



New Features

TARGETING HTTP ADMIN CONSOLES

Searching for web admin interfaces on non-standard HTTP ports



Dictionary Updates

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

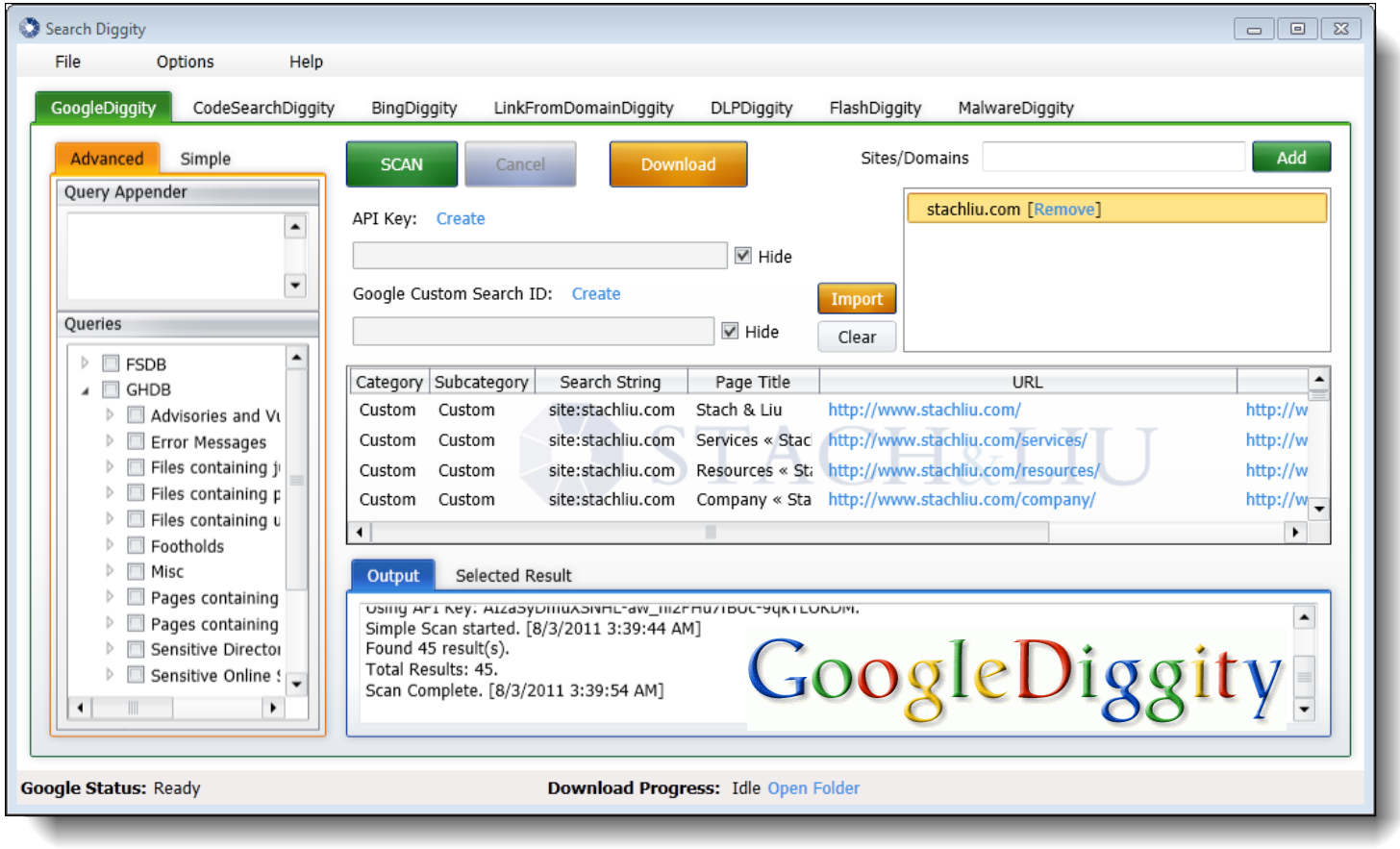
The incredible amount of information continuously leaked onto the Internet, and therefore accessible by Google, is of great use to penetration testers around the world. Johnny Long of Hackers for Charity started the Google Hacking Database (GHDB) to serve as a repository for search terms, called Google-Dorks,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

GOOGLE HACKING-DATABASE

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.

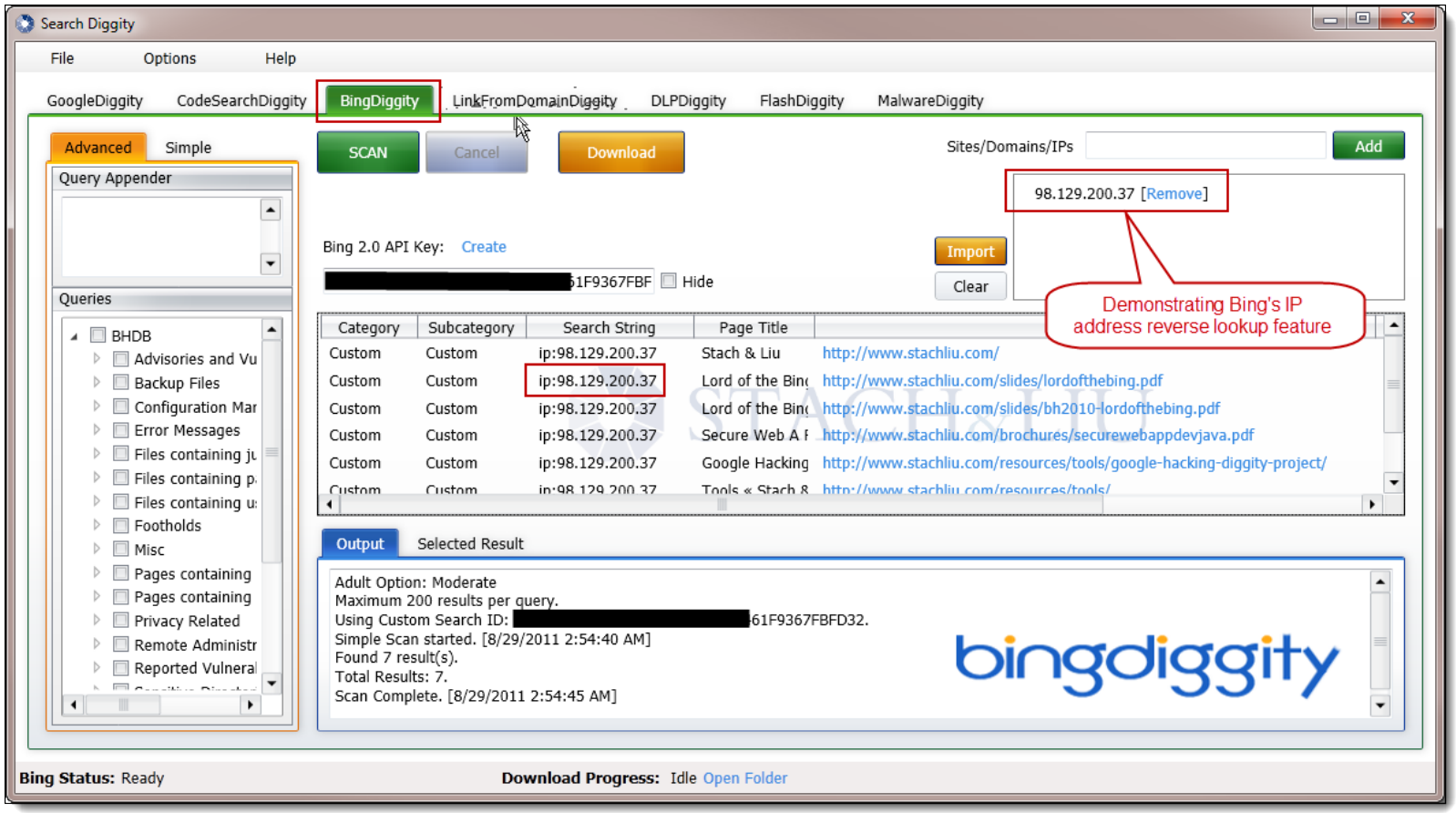
Google Diggity

DIGGITY CORE TOOLS



Bing Diggity

DIGGITY CORE TOOLS



Bing Hacking Database

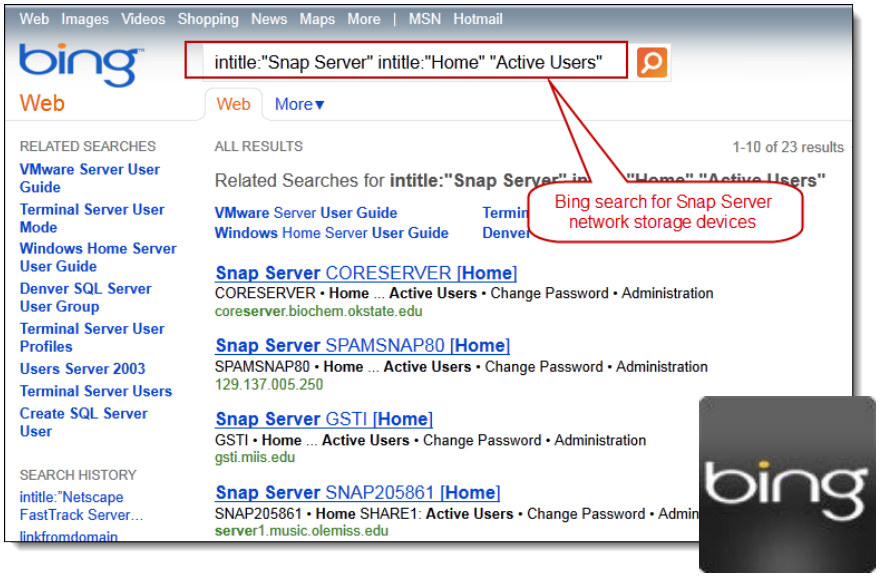
STACH & LIU TOOLS

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

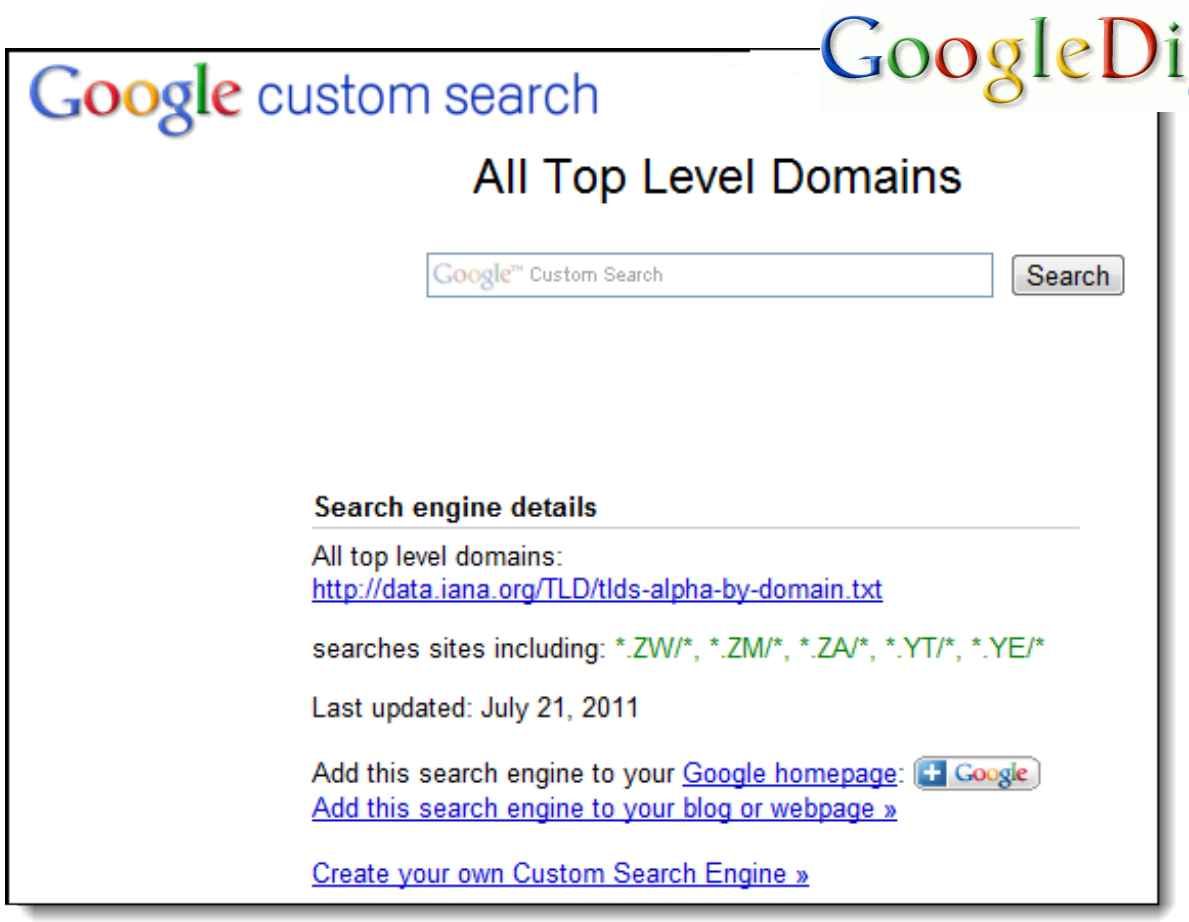
Example - Bing vulnerability search:

- GHDB query
  - `"allintitle:Netscape FastTrack Server Home Page"`
- BHDB version
  - `intitle:"Netscape FastTrack Server Home Page"`



Hacking CSE's

ALL TOP LEVEL DOMAINS



NEW GOOGLE HACKING TOOLS

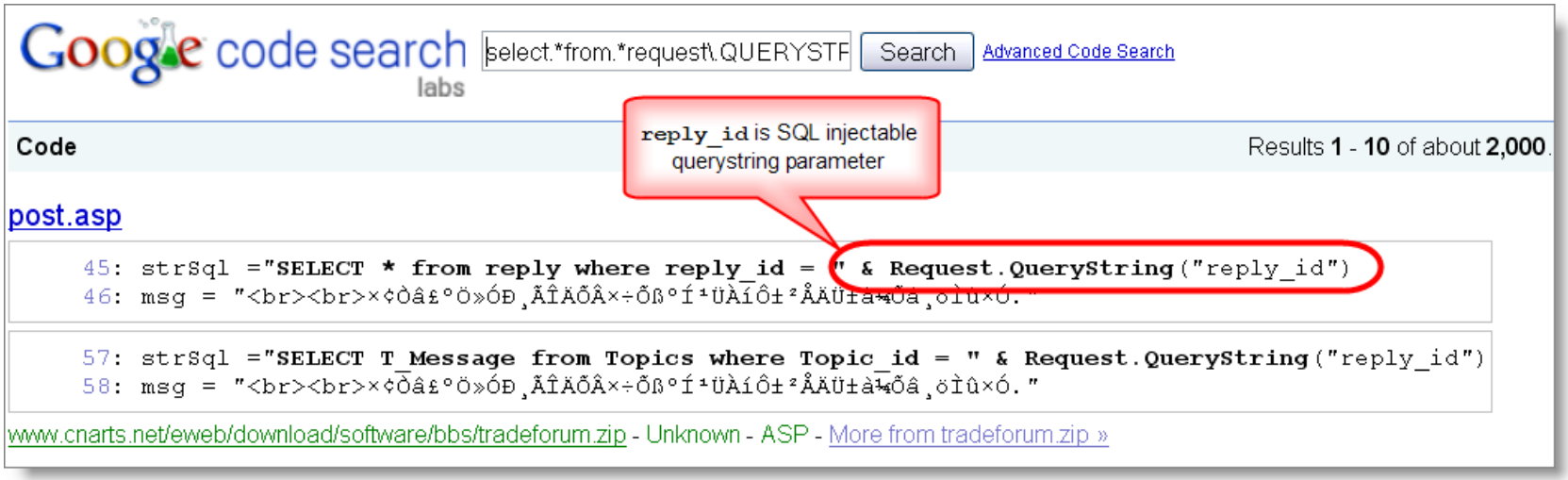
Code Search Diggity

Google Code Search

VULNS IN OPEN SOURCE CODE

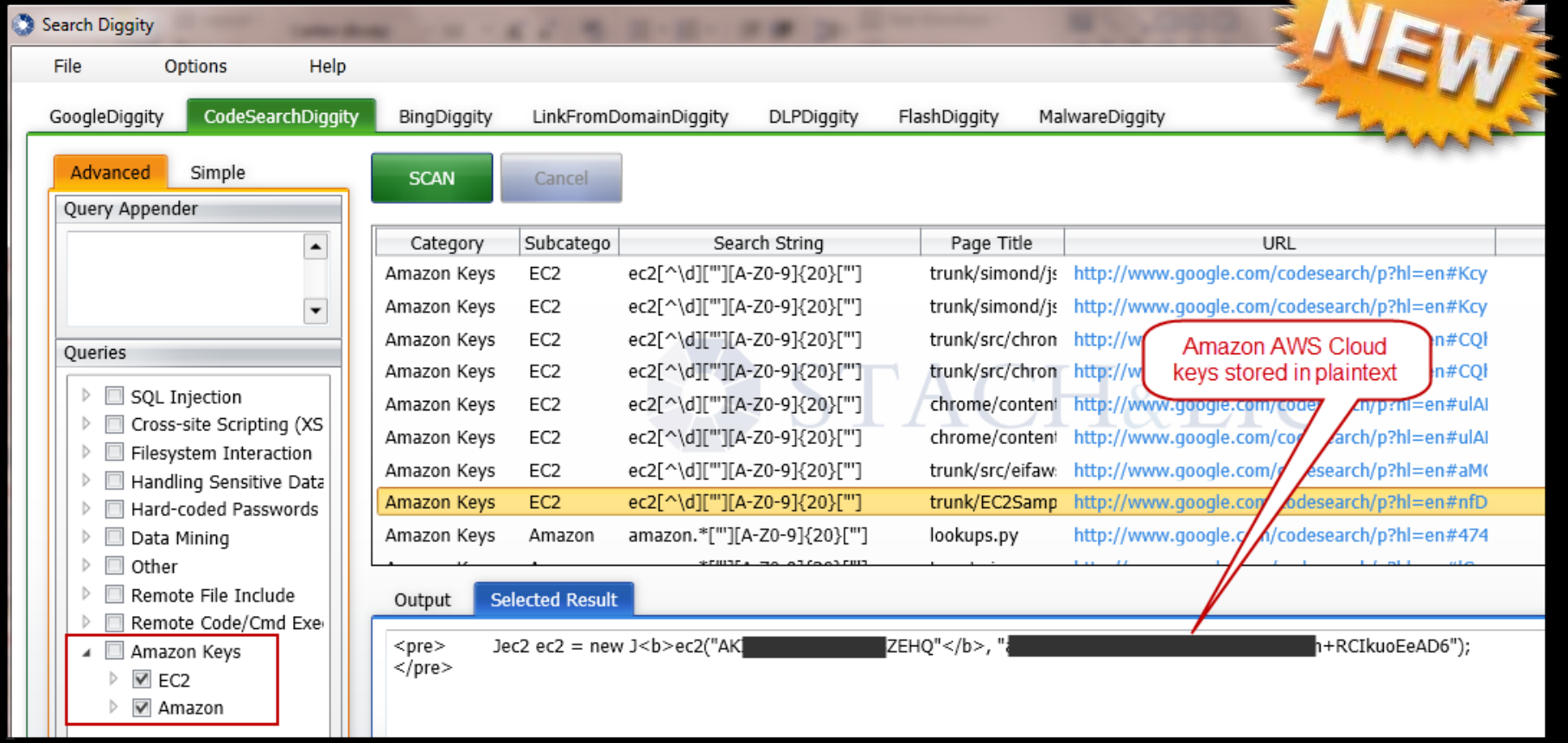
- Regex search for vulnerabilities in indexed public code, including popular open source code repositories:

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



CodeSearch Diggity

AMAZON CLOUD SECRET KEYS



Cloud Security

NO PROMISES. . .NONE

amazon web services™

Amazon AWS Customer Agreement

- http://aws.amazon.com/agreement/#10

10. Disclaimers.

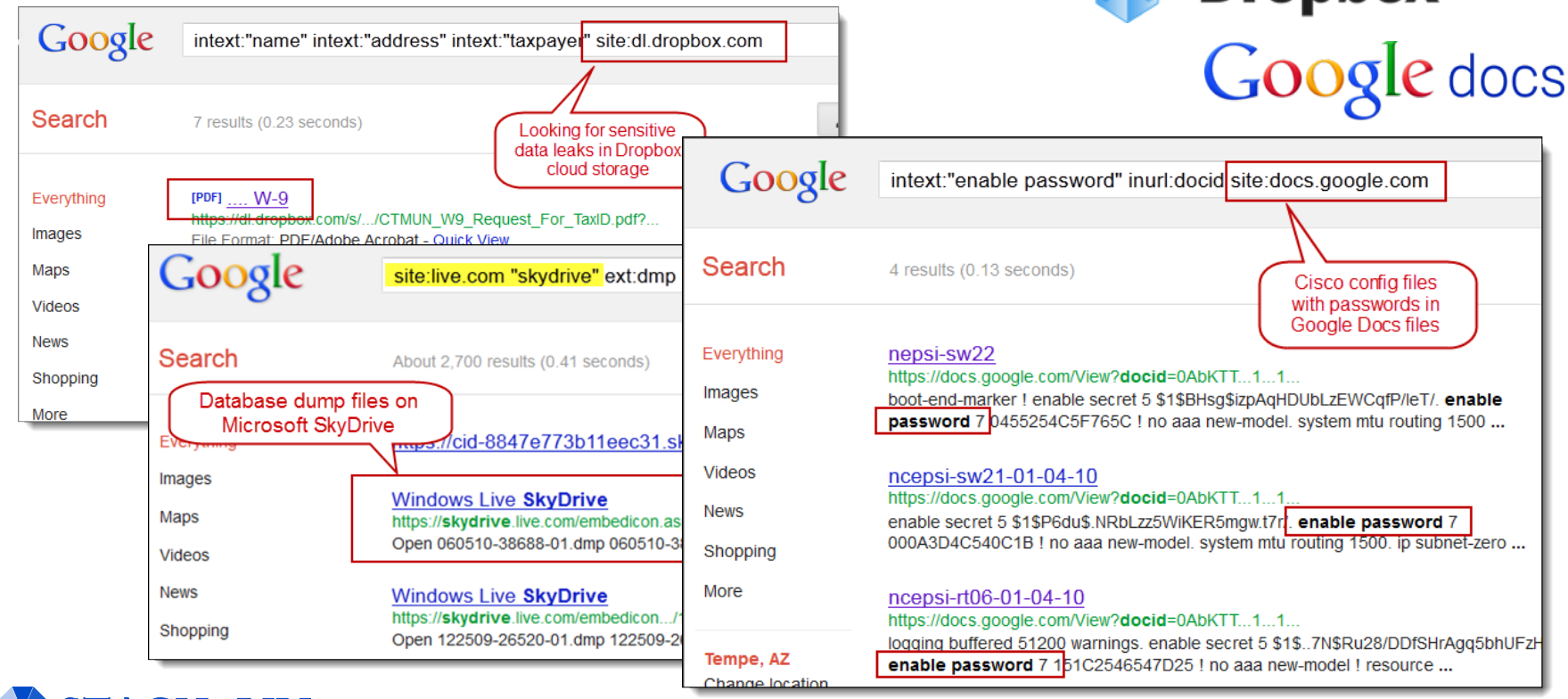
No guarantee of confidentiality, integrity, or availability (the CIA security triad) of your data in any way

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT OR THE THIRD PARTY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

Cloud Docs Exposures

PUBLIC CLOUD SEARCHING

Public cloud storage document exposures



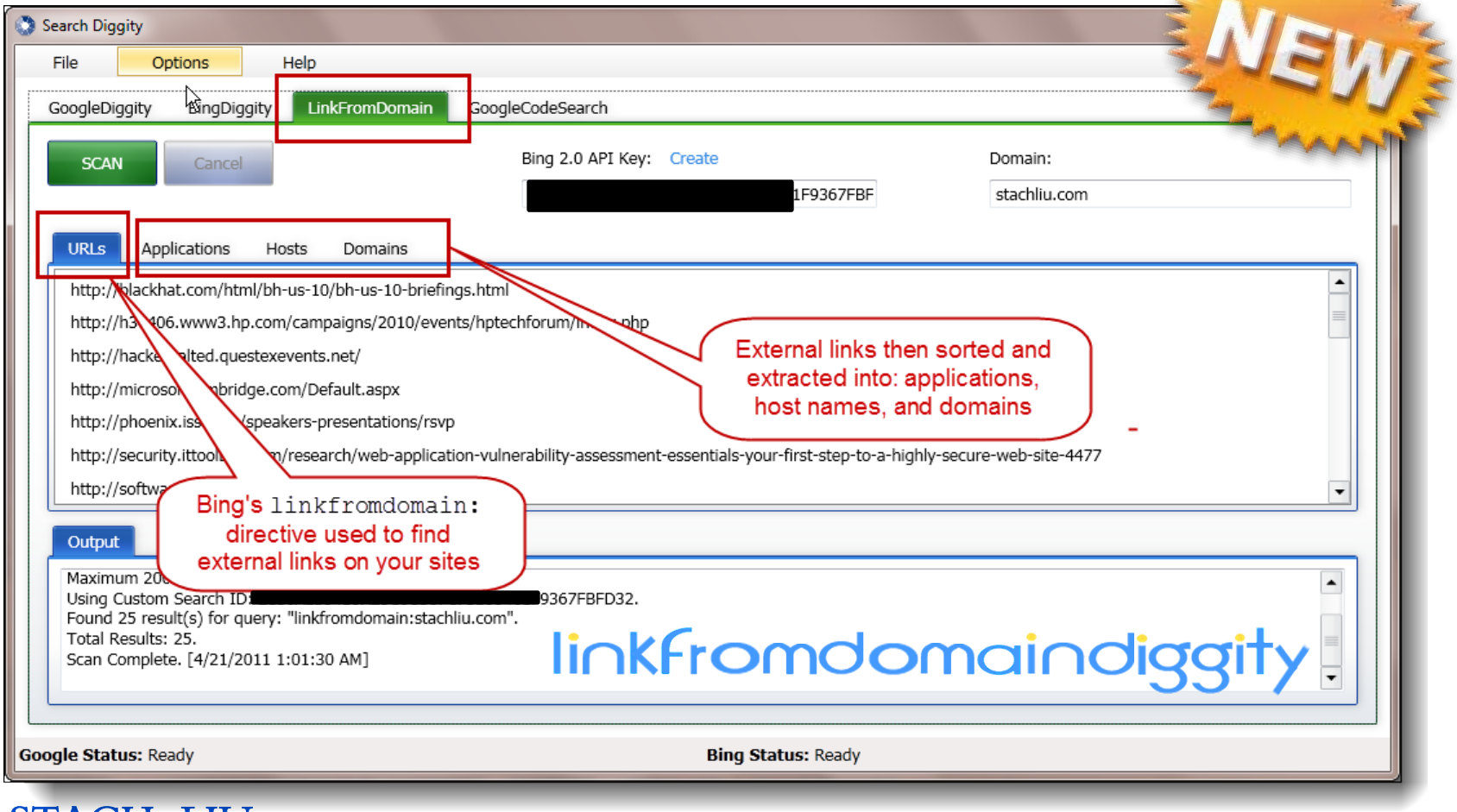
linkfromdomaindiggity

NEW GOOGLE HACKING TOOLS

Bing LinkFromDomainDiggity

Bing LinkFromDomain

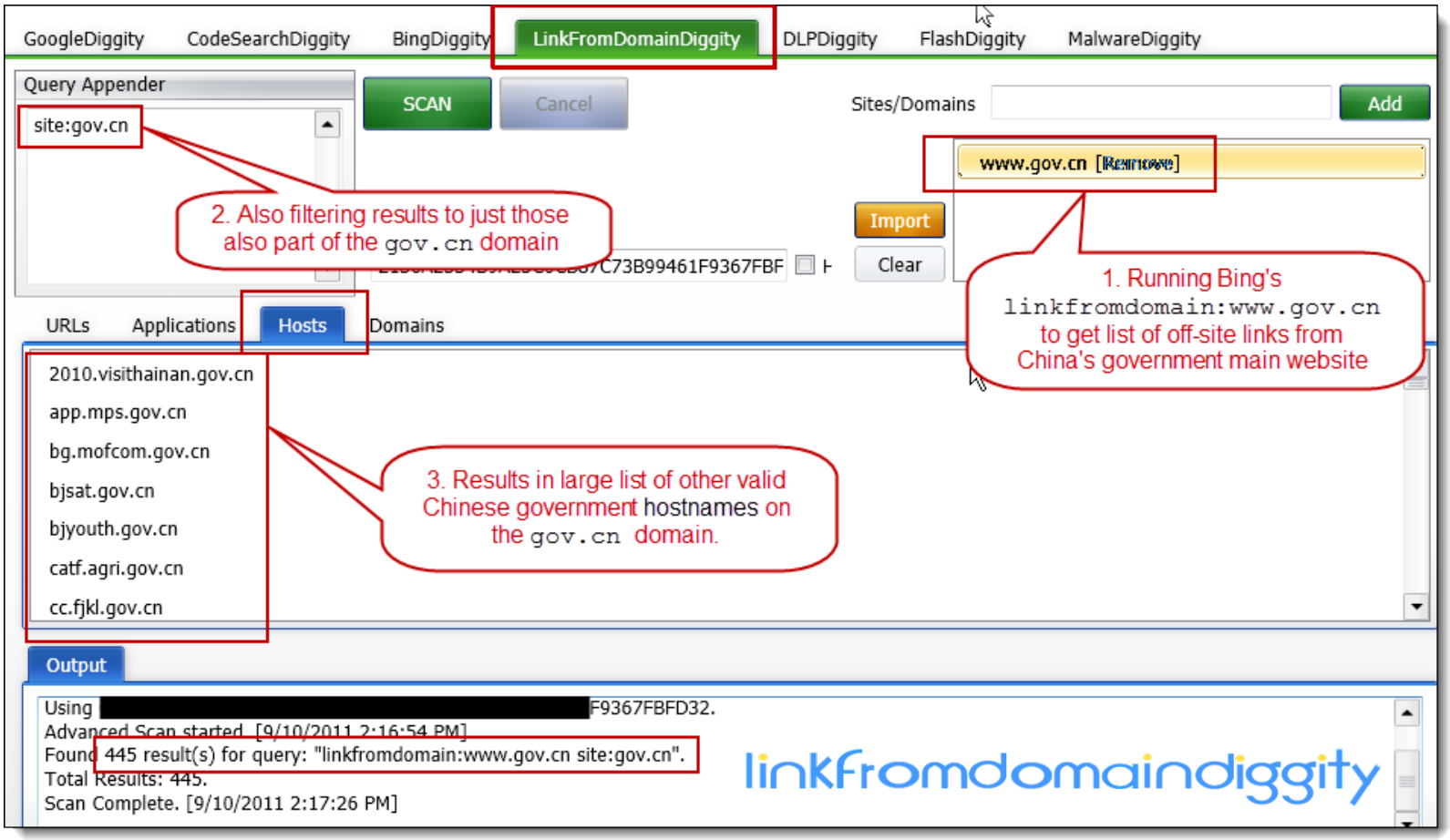
DIGGITY TOOLKIT



NEW

Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

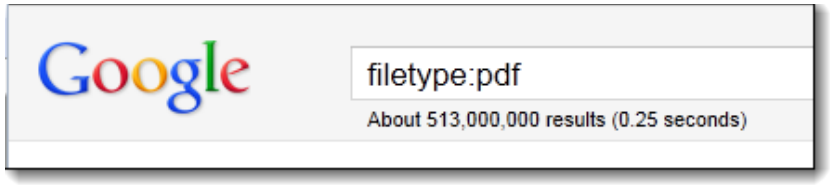


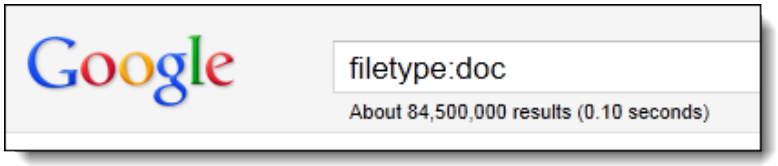
NEW GOOGLE HACKING TOOLS

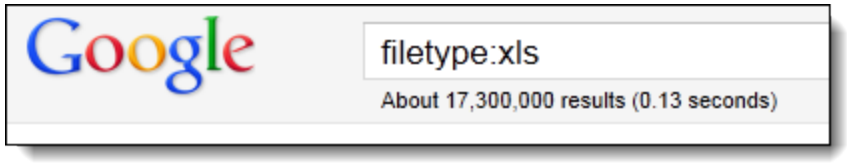
DLP Diggity

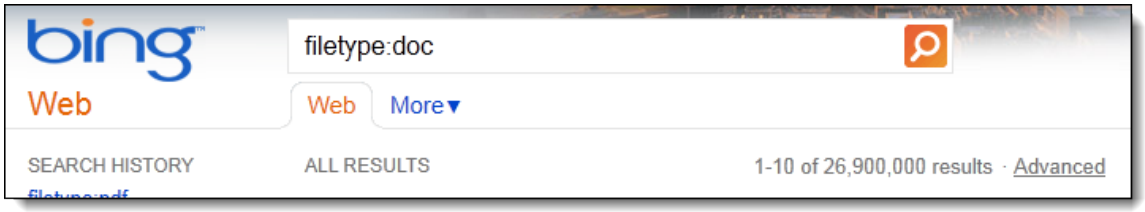
DLP Diggity

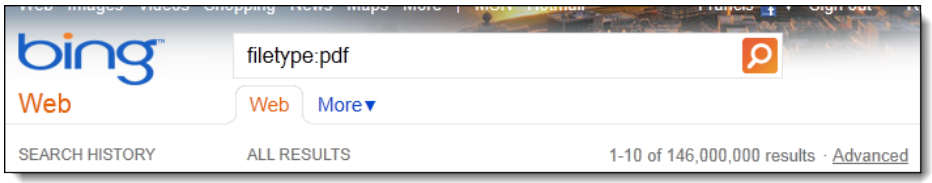
LOTS OF FILES TO DATA MINE







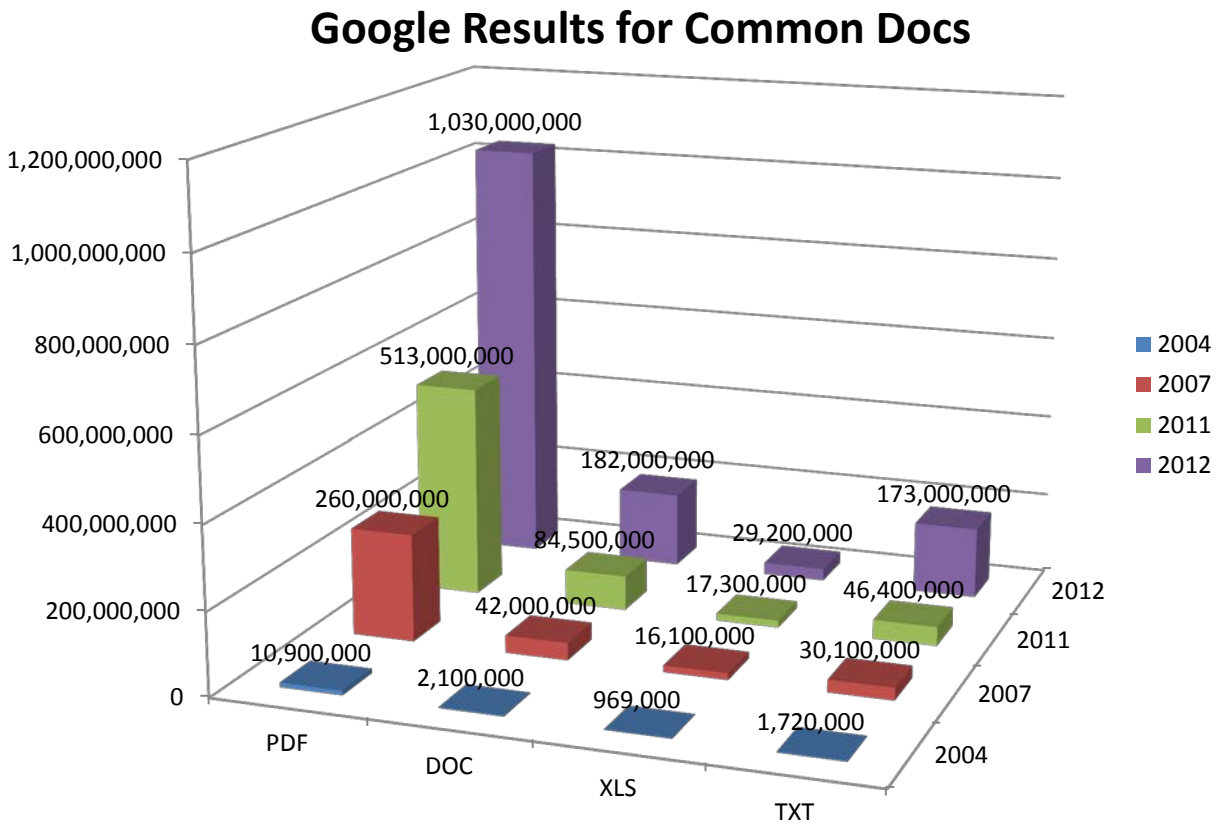




STACH&LIU

DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR



Data Loss In The News

MAJOR DATA LEAKS

- Groupon.com Leaks 300,000 users emails and passwords
  - `filetype:sql hotmail gmail password`

Slashdot

stories
recent
popular
ask slashdot
book reviews
games

Groupon Deal of the Day: 300,000 Customer Accounts

Posted by **samzenpus** on Wednesday June 29 2011, @01:11PM
from the good-deal dept.

itwbennett writes

"The customer database of Groupon's Indian subsidiary was published, unsecured and unencrypted, on the company's site for long enough to indexed

Google

filetype:sql hotmail gmail password [redacted]

3 results (0.10 seconds)

Everything
Images
Videos

CREATE TABLE `phase2_users` (`id` int(11) NOT NULL auto_increment ...
[redacted]
www.sos-asta.com/uploaded/user/xyz.sql - India

Data Loss In The News

MAJOR DATA LEAKS

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet

DLP Diggity

DIGGITY TOOLKIT

GoogleDiggity | CodeSearchDiggity | BingDiggity | LinkFromDomainDiggity | DLPDiggity | FlashDiggity | Ma

NEW

Advanced | Simple

SEARCH | Cancel

Queries

- CreditCards
- SSN
- PII
- Bank Account Numbers
- TaxID
- Patient Records
- National ID Numbers
- Tech Data Mining
- Encryption Related
- Passwds
- Passwds Various Langu
- Keywords

Scan Directory: C:\DiggityDownloads\ Browse...

Category	Subcategory	Search String	File
SSN	Social Security	[^A-Za-z0-9_]([0-6]\d{	C:\DiggityDownloads\PIITutorial.doc
SSN	SSN LANL	(ss(n)?|social(\s*securi	C:\DiggityDownloads\PIITutorial.doc

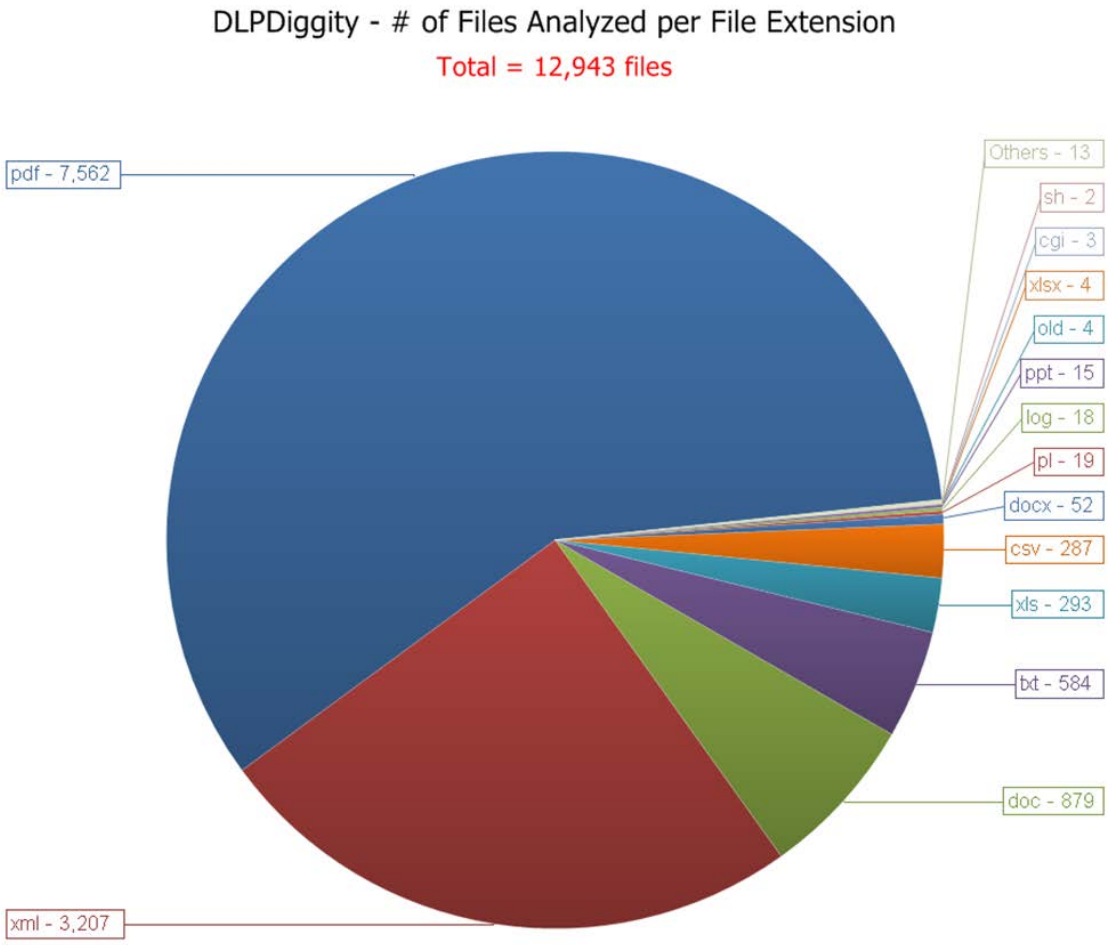
Search through downloaded files from GoogleDiggity and BingDiggity for data leaks such as SSNs, credit cards, etc.

Output | Selected Result

21 Jerry,
22 This is Mary. I forgot to include my social security number in those clearance documents I su
Would you mind adding it in for me? My SSN is 123-45-6789. Thanks a lot!
23 - Mary
24

DLP Reporting

PRACTICAL EXAMPLES



STACH&LIU

DLP Reporting

PRACTICAL EXAMPLES

Automagic Removal Process, DORK, GHDB, XSS.CX, Vulnerability Management, Best Practices

Updated October 8, 2011

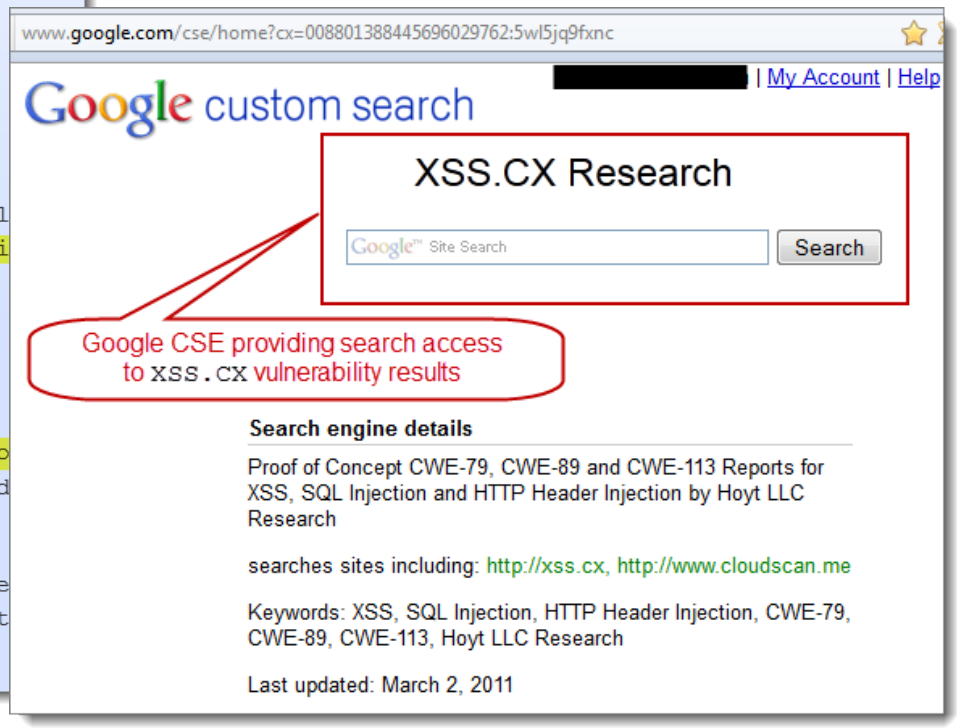
Executive Summary

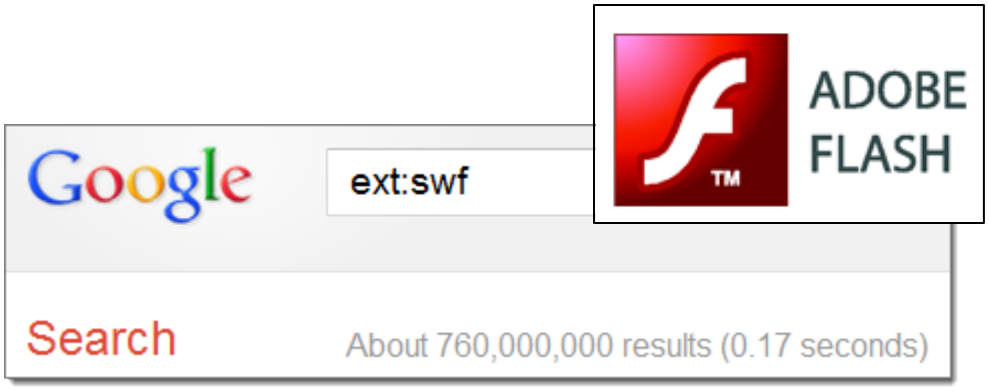
XSS.CX is an automated Anti-Phishing Execution Robot defined as a SCAP Expert System performing Vulnerabil Execution, Risk Analysis and Reporting into the Publi Domain for the public convenience and necessity of securing personally identifying information.

General Information

The Anti-Phishing Web Crawler publishes Vulnerable Ho reports into the Public Domain which are then indexed Search Engines.

Companies with external facing Vulnerability Manageme Programs then identify the XSS.CX Report, resolving t vulnerability in the normal course of business.



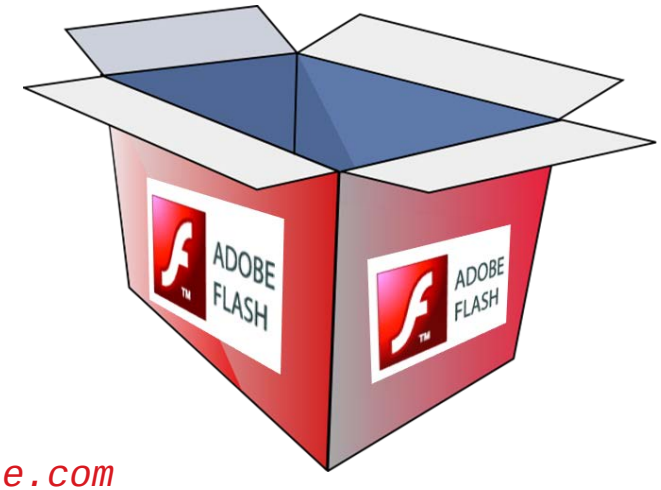


NEW GOOGLE HACKING TOOLS

FlashDiggity

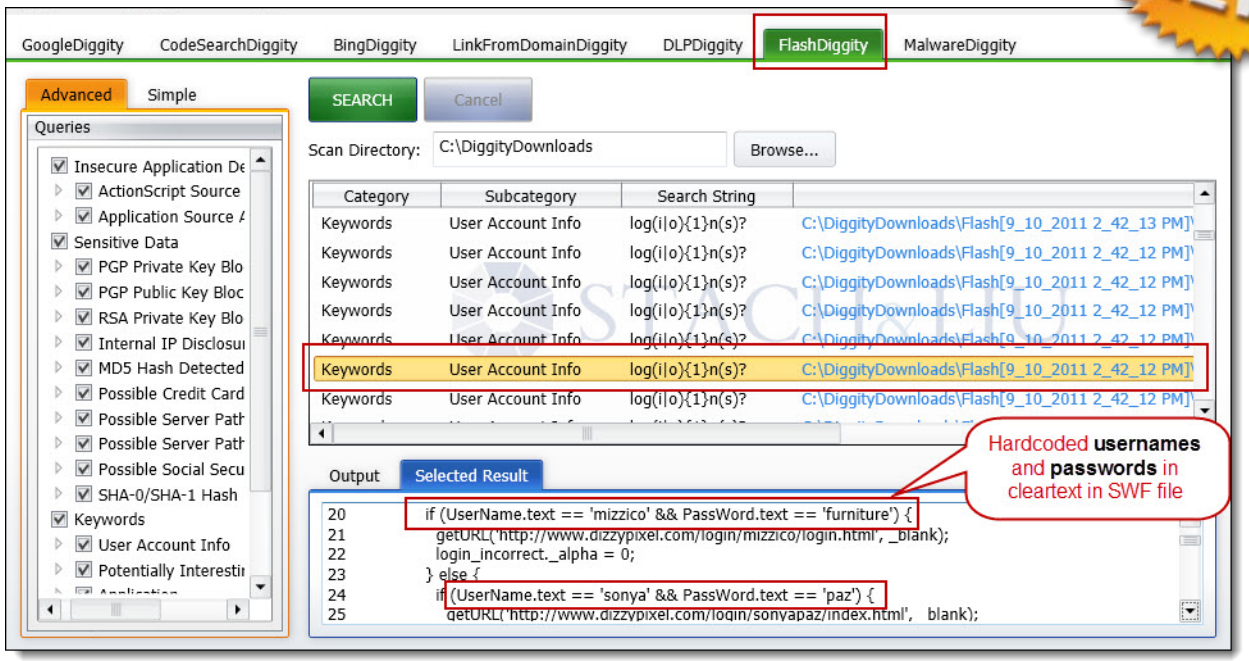
FlashDiggity

DIGGITY TOOLKIT



- Google/Bing 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

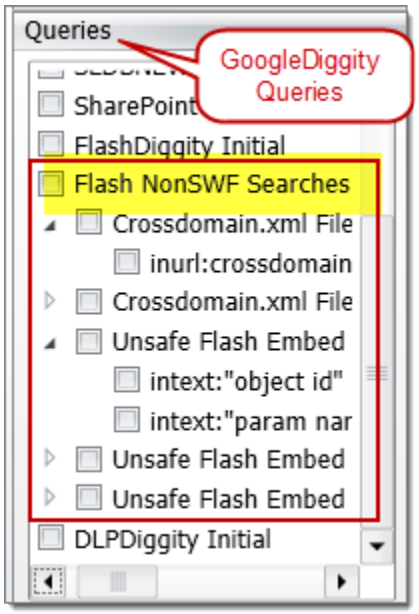
NEW

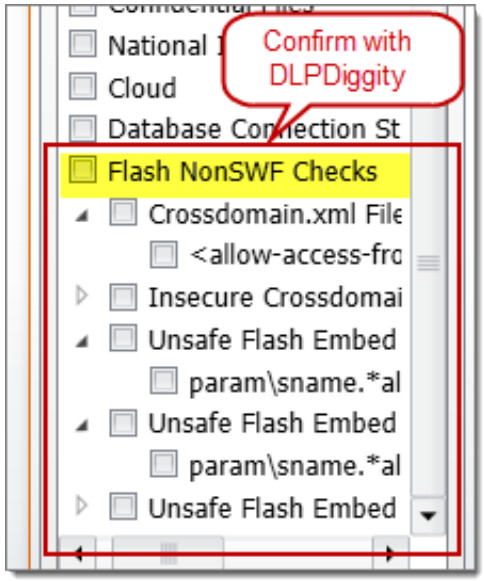


Flash Non-SWF Hacking

OTHER FLASH HACKING

- Google/Bing for Non-SWF files on target domains, but related to Flash. Example queries:
  - `inurl:crossdomain.xml ext:xml intext:"secure" intext:"false"`
  - `intext:"swf" intext:"param name" intext:"allowNetworking * all"`
- Download Non-SWF files to `C:\DiggityDownloads\`
- Use DLPDiggity to analyze for non-SWF Flash vulnerabilities, such as:
  - Crossdomain.xml Insecure Settings
    - Secure flag set to false
    - Open * wildcard used
  - Unsafe Flash HTML Embed Settings:
    - AllowScriptAccess always
    - AllowNetworking all
    - AllowFullScreen true





ADOBE FLASH

STACH&LIU

NEW GOOGLE HACKING TOOLS

DEMO

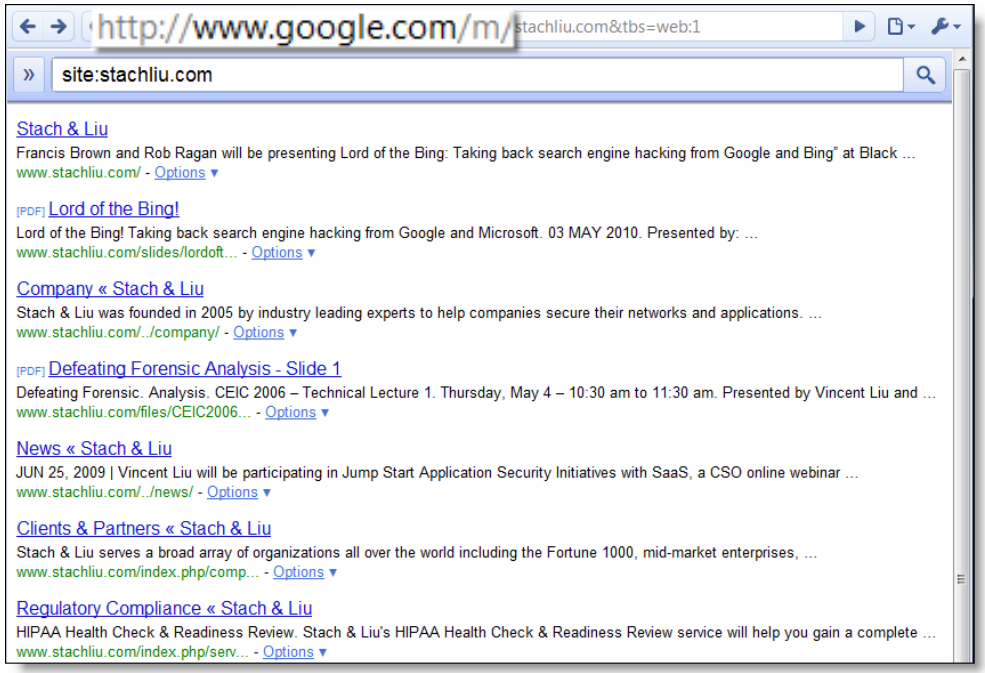
GoogleScrape Diggity

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



NEW GOOGLE HACKING TOOLS

Baidu Diggity

BaiduDiggity

CHINA SEARCH ENGINE

- Fighting back

COMING SOON

STACH&LIU

NEW GOOGLE HACKING TOOLS

Malware Diggity

Rise of Malware

NO SITES ARE SAFE

SOPHOS - Security Threat Report 2012

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

Online threats

Cybercriminals constantly launch attacks designed to penetrate your digital defenses and steal sensitive data. And almost no online portal is immune to threat or harm.

According to SophosLabs more than 30,000 websites are infected every day and 80% of those infected sites are legitimate. Eighty-five percent of all malware, including viruses, worms, spyware, adware and Trojans, comes from the web.[11] Today, drive-by downloads have become the top web threat. And in 2011, we saw one drive-by malware rise to number one, known as Blackhole.

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/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.

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."

Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – willysy.com - August2011

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

Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – mysql.com - Sept2011

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

Slashdot

stories
recent
popular
ask slashdot
book reviews
games

Mysql.com Hacked, Made To Serve Malware

Posted by **Soulskill** on Monday September 26, @06:52PM
from the high-profile-problems dept.

Orome1 writes

"Mysql.com was compromised today, redirecting visitors to a page serving malware. Security firm Armorize detected the compromise through its website malware monitoring platform HackAlert, and has analyzed how

FILED UNDER: INSECURITY COMPLEX | SECURITY

Hacked MySQL.com used to serve Windows malware

By: Elinor Mills

SEPTEMBER 26, 2011 6:10 PM PDT

Print E-mail

Malware SaaS Services

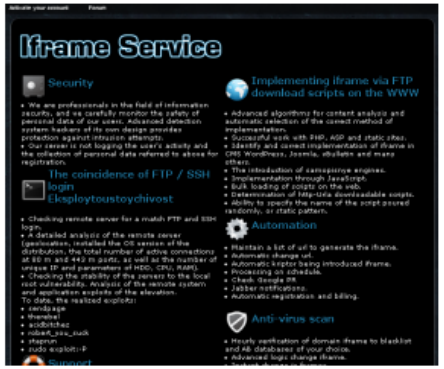
CRIMINAL 3RD PARTY SOLUTIONS

KrebsonSecurity
In-depth security news and investigation

Service Automates Boobytrapping of Hacked Sites

101 tweets retweet

Hardly a week goes by without news of some widespread compromise in which thousands of Web sites that share a common vulnerability are hacked and seeded with malware. Media coverage of these mass hacks usually centers on the security flaw that allowed the intrusions, but one aspect of these crimes that's seldom examined is the method by which attackers automate the booby-trapping and maintenance of their hijacked sites.



Regular readers of this blog may be unsurprised to learn that this is another aspect of the cybercriminal economy that can be outsourced to third-party services. Often known as "iFramers," such services can simplify the task of managing large numbers of hacked sites that are used to drive traffic to sites that serve up malware and browser exploits.

At the very least, a decent iFramer service will al

STACH&LIU

MalwareDiggity

DIGGITY TOOLKIT

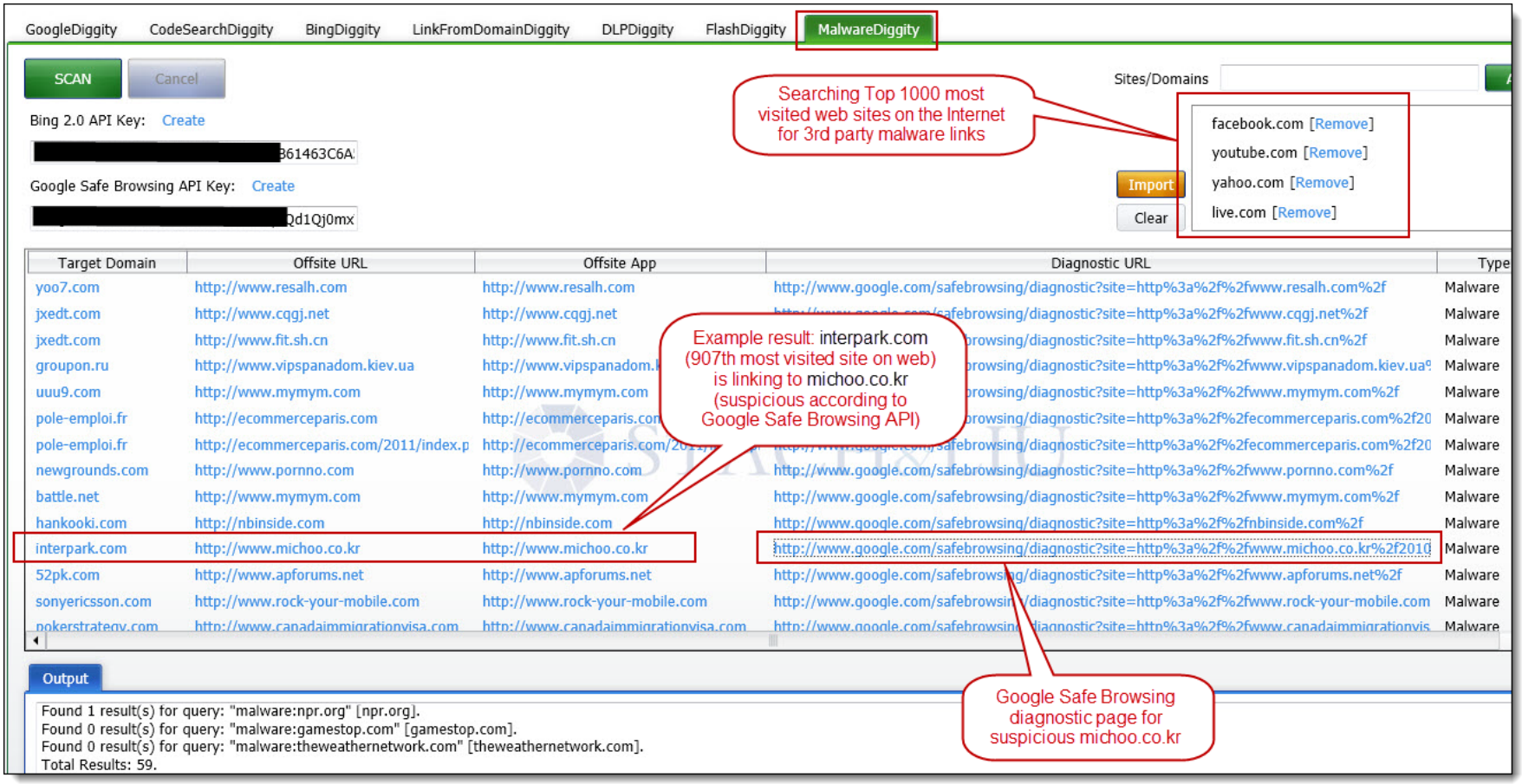
1. Leverages Bing's `linkfromdomain:` search operator to find off-site links of target applications/domains

2. Runs off-site links against Google's Safe Browsing API to determine if any are malware distribution sites

3. Return results that identify malware sites that your web applications are directly linking to

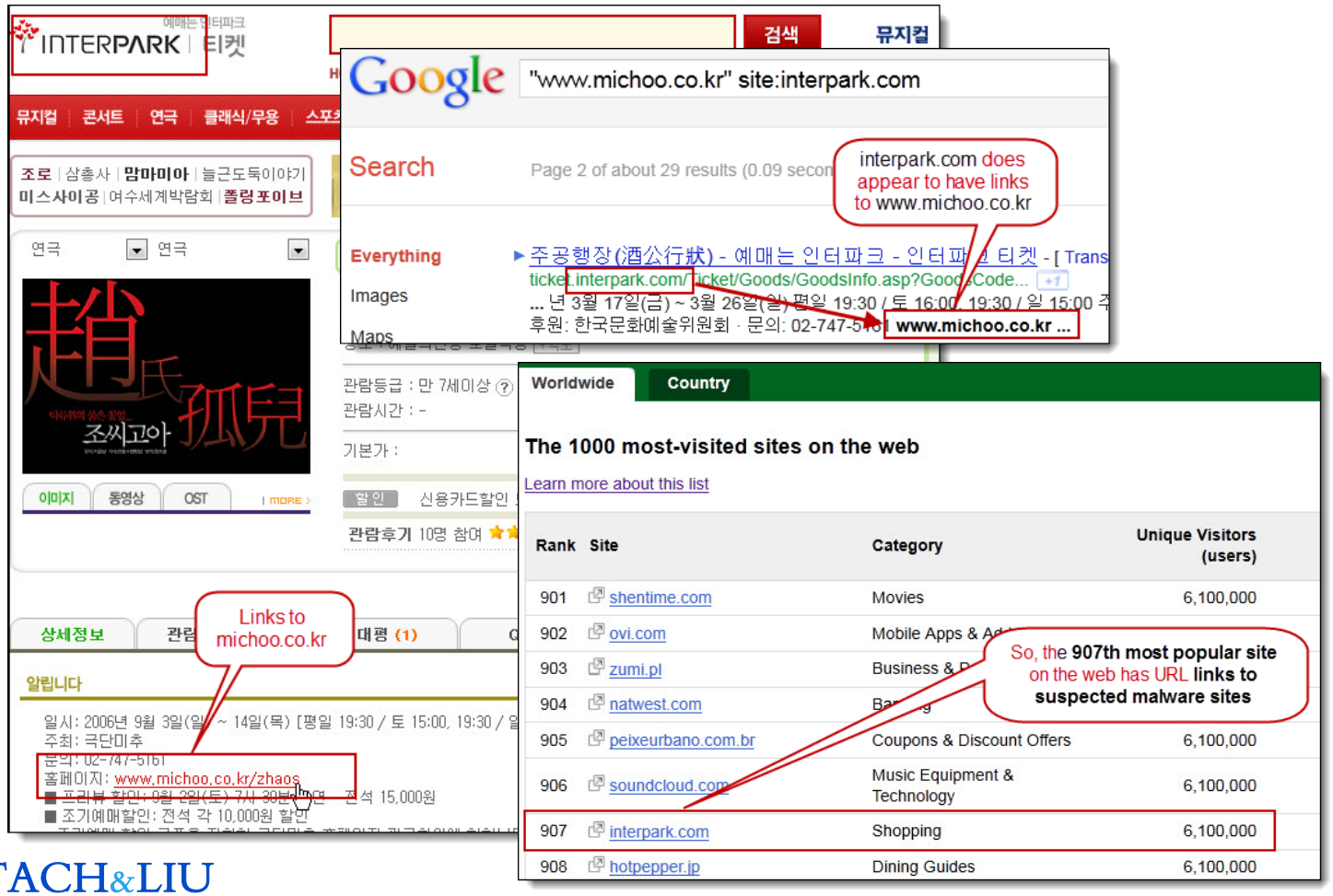
Malware Diggity

DIGGITY TOOLKIT



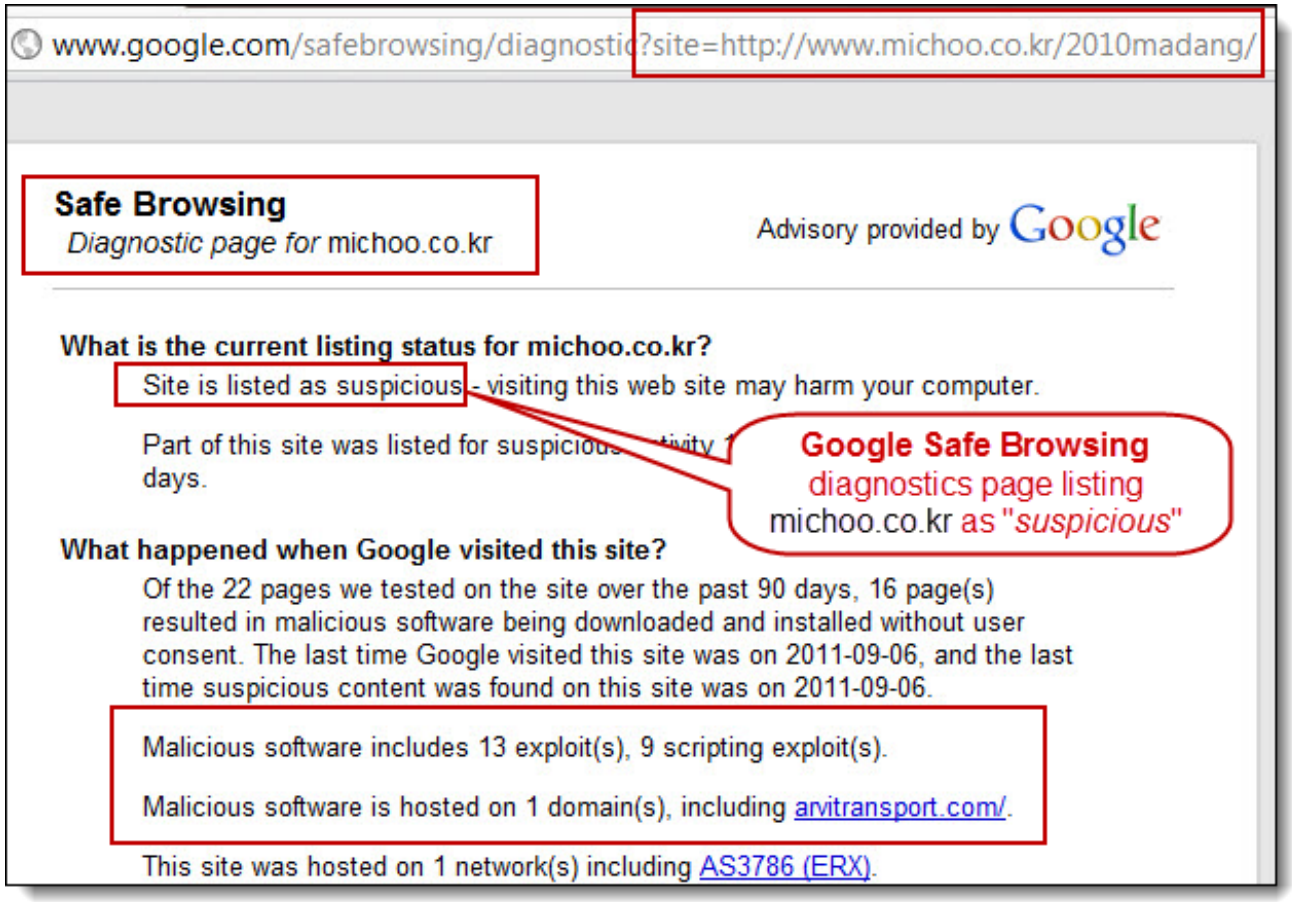
Malware Diggity

DIGGITY TOOLKIT



Malware Diggity

DIAGNOSTICS IN RESULTS



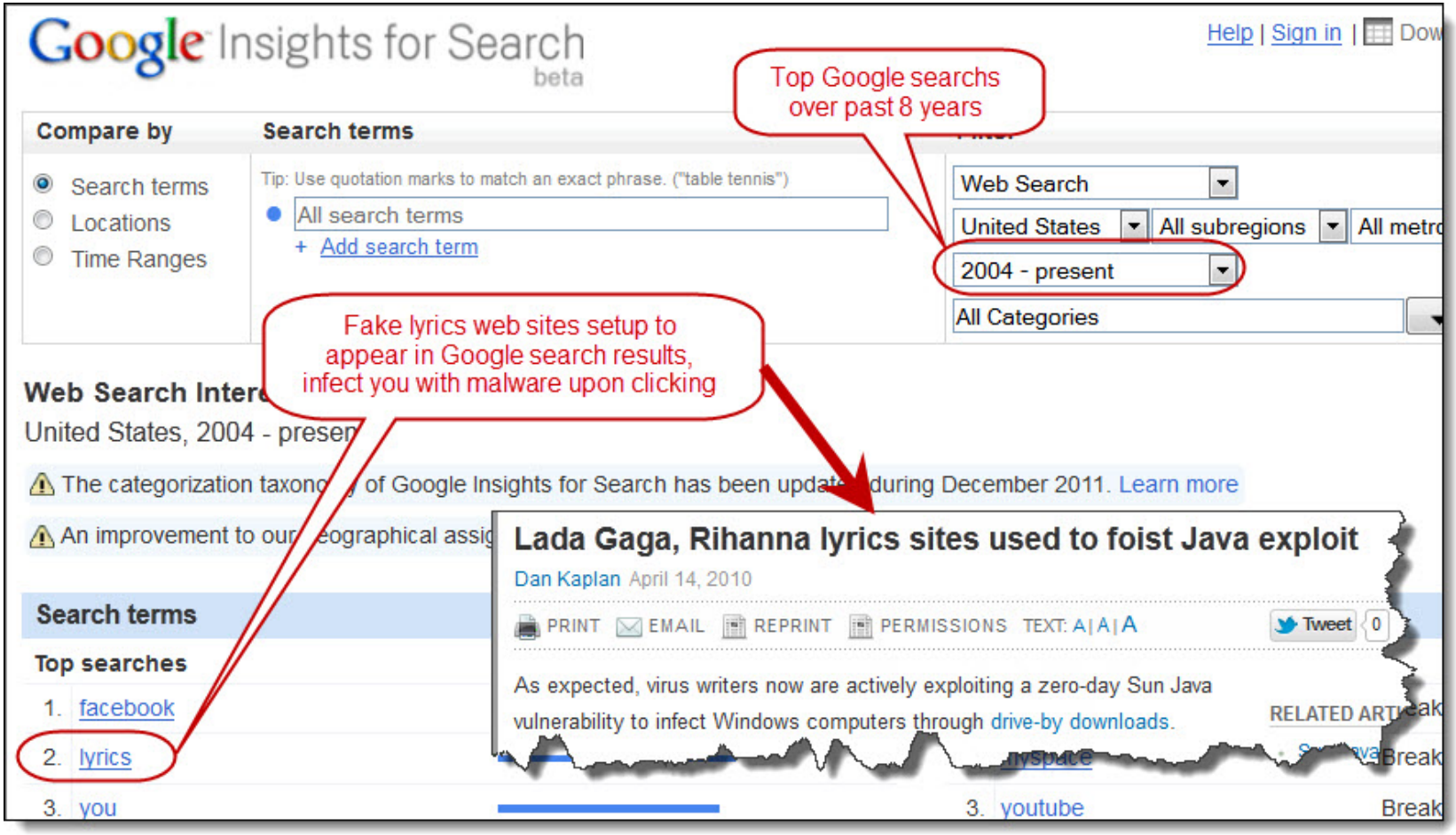
Black Hat SEO

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



STACH&LIU

Malvertisements

MALWARE ADS IN SEARCH ENGINES

bing

adobe reader

Web | News

RELATED SEARCHES

Adobe Reader 0Day
Adobe Reader Free Download
Adobe Reader 7 Free Download
Adobe Acrobat Reader 8.1
Adobe Reader Plu...
Adobe Reader ...

adobe reader

See all
Clear all · Turn off

ALL RESULTS 1-10 of 54,900,000 results · Advanced

Sponsored sites

Reader 9.0 -Official Site
www.PDF-Format.com · Open, Create & Edit PDF Files! Official Site (Recommended Download)

Adobe Acrobat 9 Download
AdobeAcrobat.PDF-S0ftware.com · Ultra Fast Acrobat Download - Latest Version 100% Guaranteed

Adobe Reader Download
AdobeProReader10.com/Free · New **Adobe Reader** Official Version. 100% Support. Free Download!

Adobe Acrobat 9.3 Version
www.PDF-9-D0wnload.com · Download **Adobe** PDF Latest Version Ultra Fast 100% Guaranteed!

Adobe - Adobe Reader
Download **Adobe Reader** to view, print and collaborate on PDF files.
get.**adobe**.com/**reader** · Cached page

Get Flash Player
Adobe - Adobe Reader
Adobe - Adobe Air
Accessibility
Show more results from get.adobe.com

Malware advertisements in "Sponsored sites"

Letter O replaced with 0 (zero)

Malware Defenses

BLACKHAT SEO DEFENSES

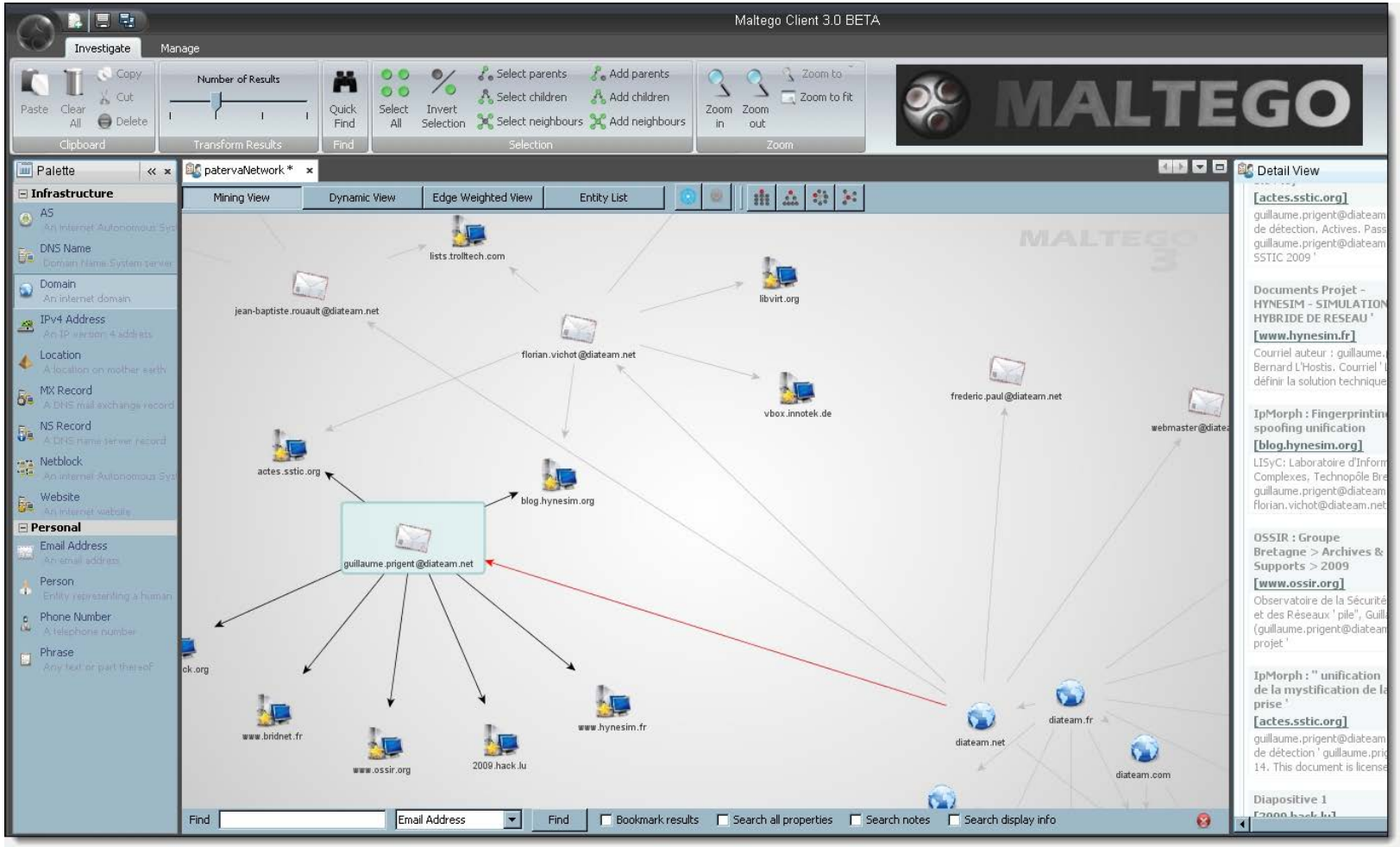
- Malware Warning Filters
  - Google Safe Browsing
  - Microsoft SmartScreen Filter
  - Yahoo Search Scan
- Sandbox Software
  - Sandboxie (sandboxie.com)
  - Dell KACE - Secure Browser
  - Office 2010 (Protected Mode)
  - Adobe Reader Sandbox (Protected Mode)
  - Adobe Flash Sandbox (Protected Mode) – NEW May2012
- No-script and Ad-block browser plugins

NON–DIGGITY ATTACK TOOLS

Other Search Hacking Tools

Maltego

INFORMATION GATHERING TOOL

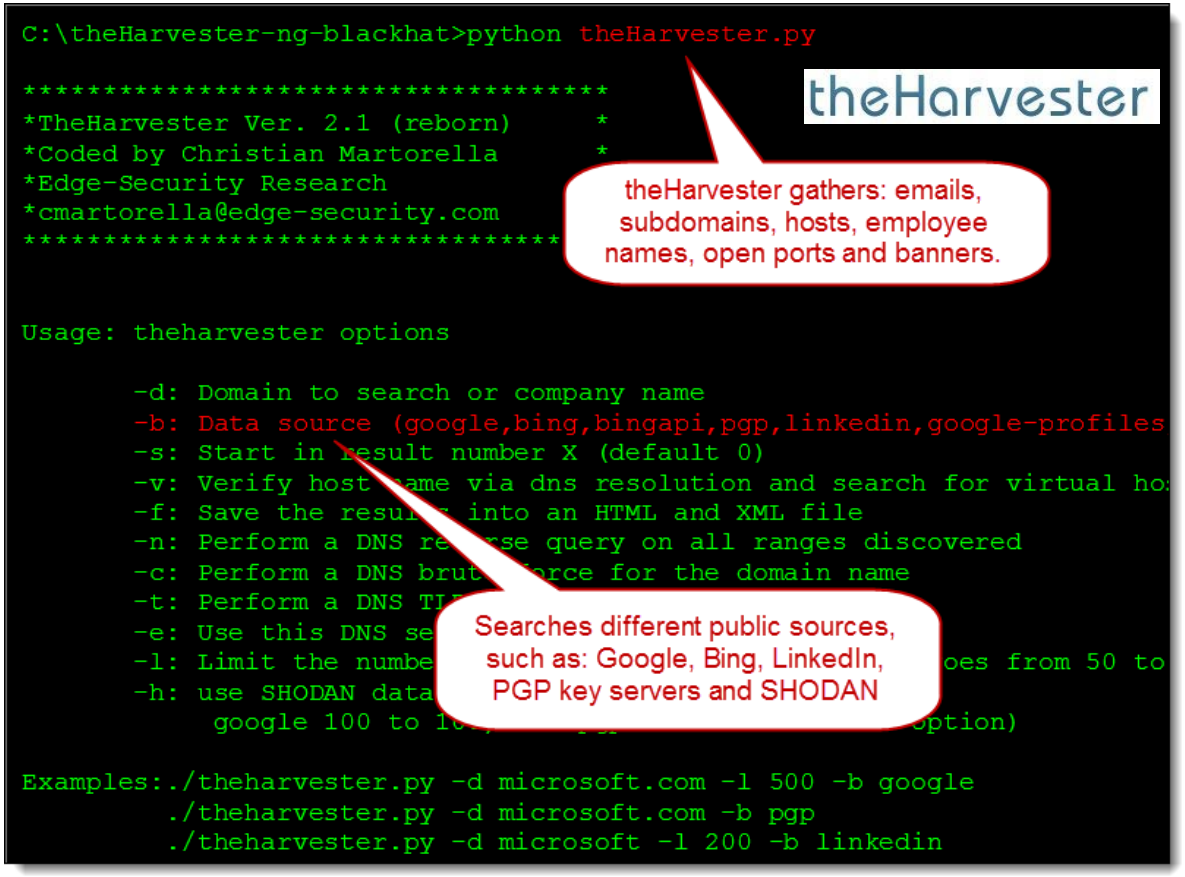


STACH&LIU

theHarvester

FOOTPRINTING TOOL

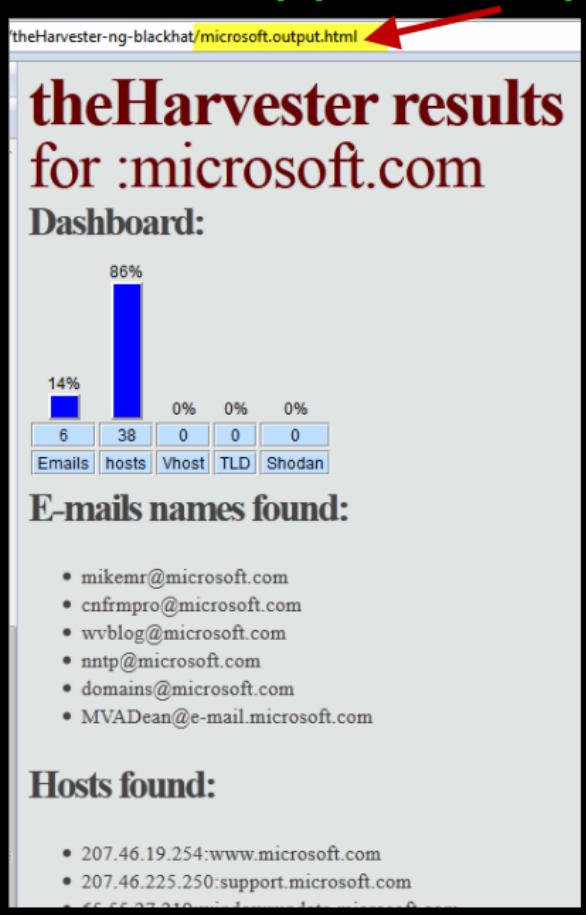
- Gathers e-mail accounts, user names and hostnames, and subdomains



theHarvester

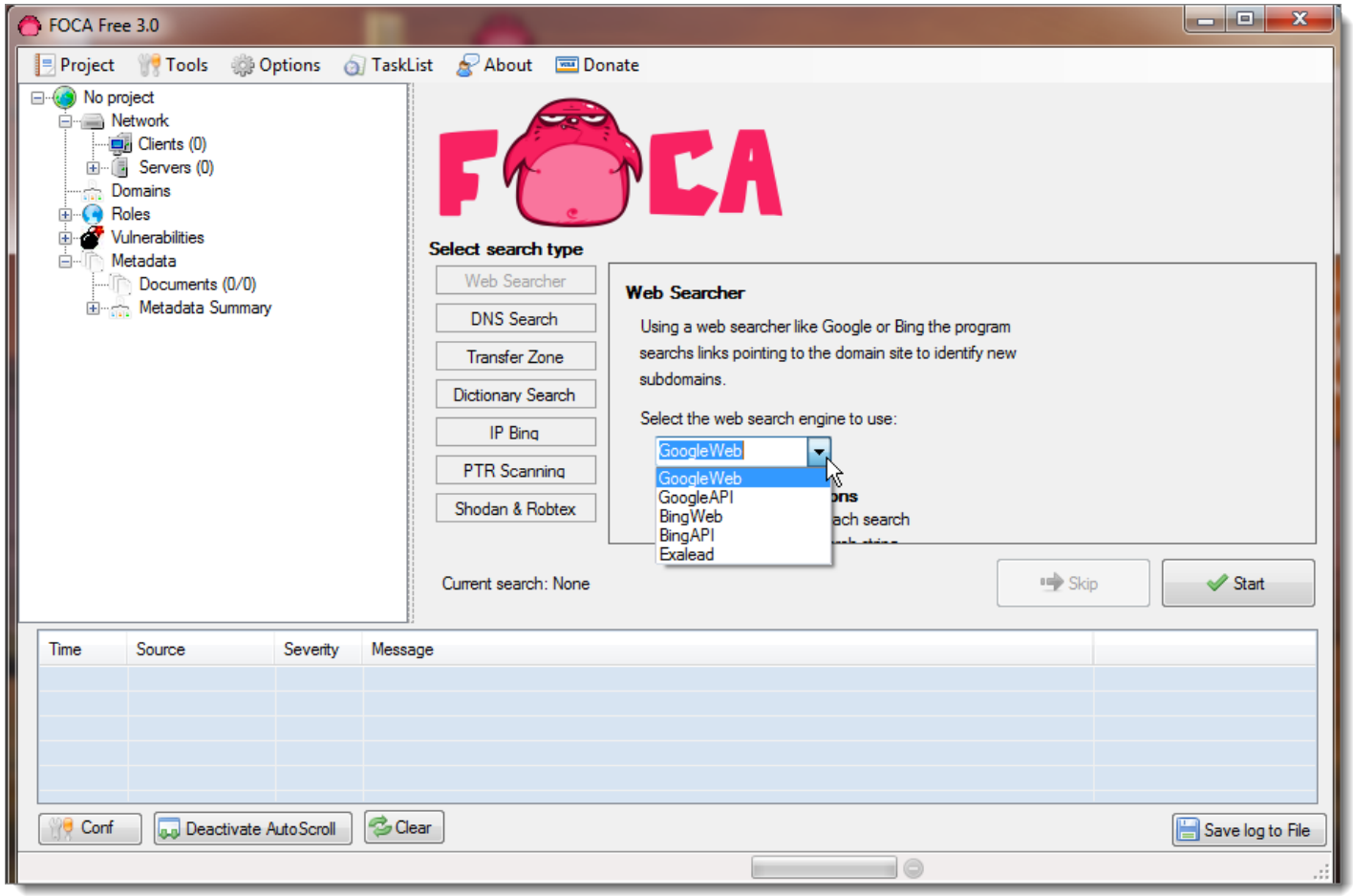
FOOTPRINTING EXAMPLE

```
C:\theHarvester>python theharvester.py -d microsoft.com -l 200 -b google -f microsoft.output.html

**************************************
*TheHarvester Ver. 2.1 (reborn)      *
*Coded by Christian Martorella       *
*Edge-Security Research              *
*cmartorella@edge-security.com       *
**************************************


[-] Searching in Google:
        Searching 0 results...
        Searching 100 results...
        Searching 200 results...

[+] Emails found:
------------------
mikemr@microsoft.com
cnfrmpro@microsoft.com
wvblog@microsoft.com
nntp@microsoft.com
domains@microsoft.com
MVADean@e-mail.microsoft.com

[+] Hosts found in search engines:
----------------------------------
207.46.19.254:www.microsoft.com
207.46.225.250:support.microsoft.com
65.55.27.219:windowsupdate.microsoft.com

...

65.55.11.238:schemas.microsoft.com
65.52.103.84:connect.microsoft.com

[+] Proposed SET
---------------
[]
Saving file
```



FOCA

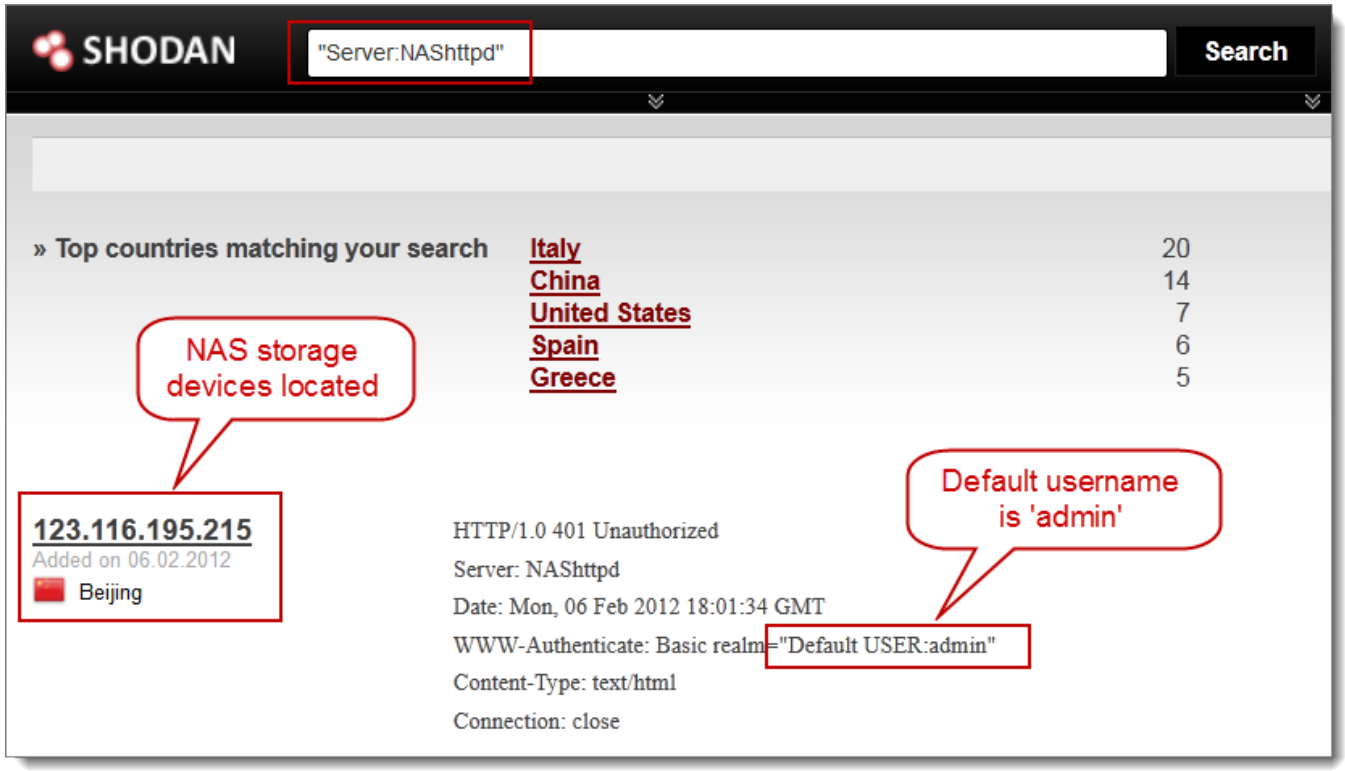
INFO GATHERING AND METADATA



SHODAN

HACKER SEARCH ENGINE

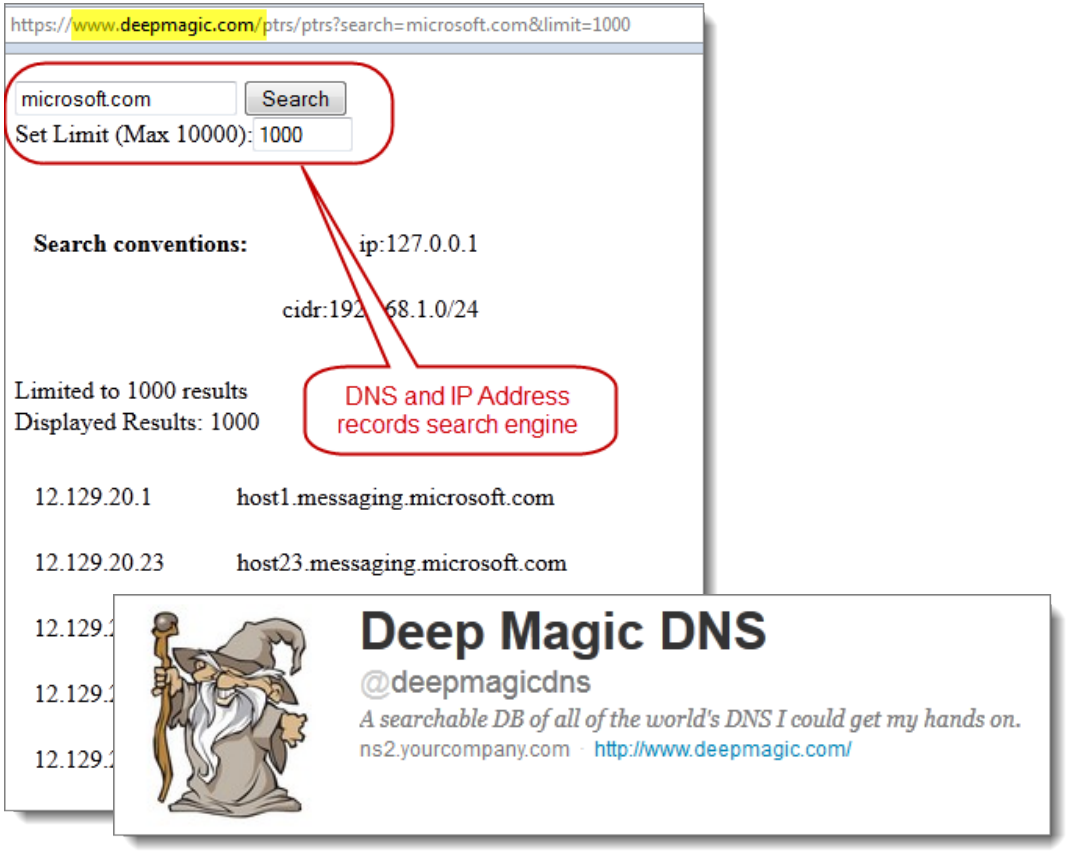
- Indexed service banners for whole Internet for HTTP (Port 80), as well as some FTP (23), SSH (22) and Telnet (21) services



DeepMagic DNS

FOOTPRINTING DNS SEARCH ENGINE

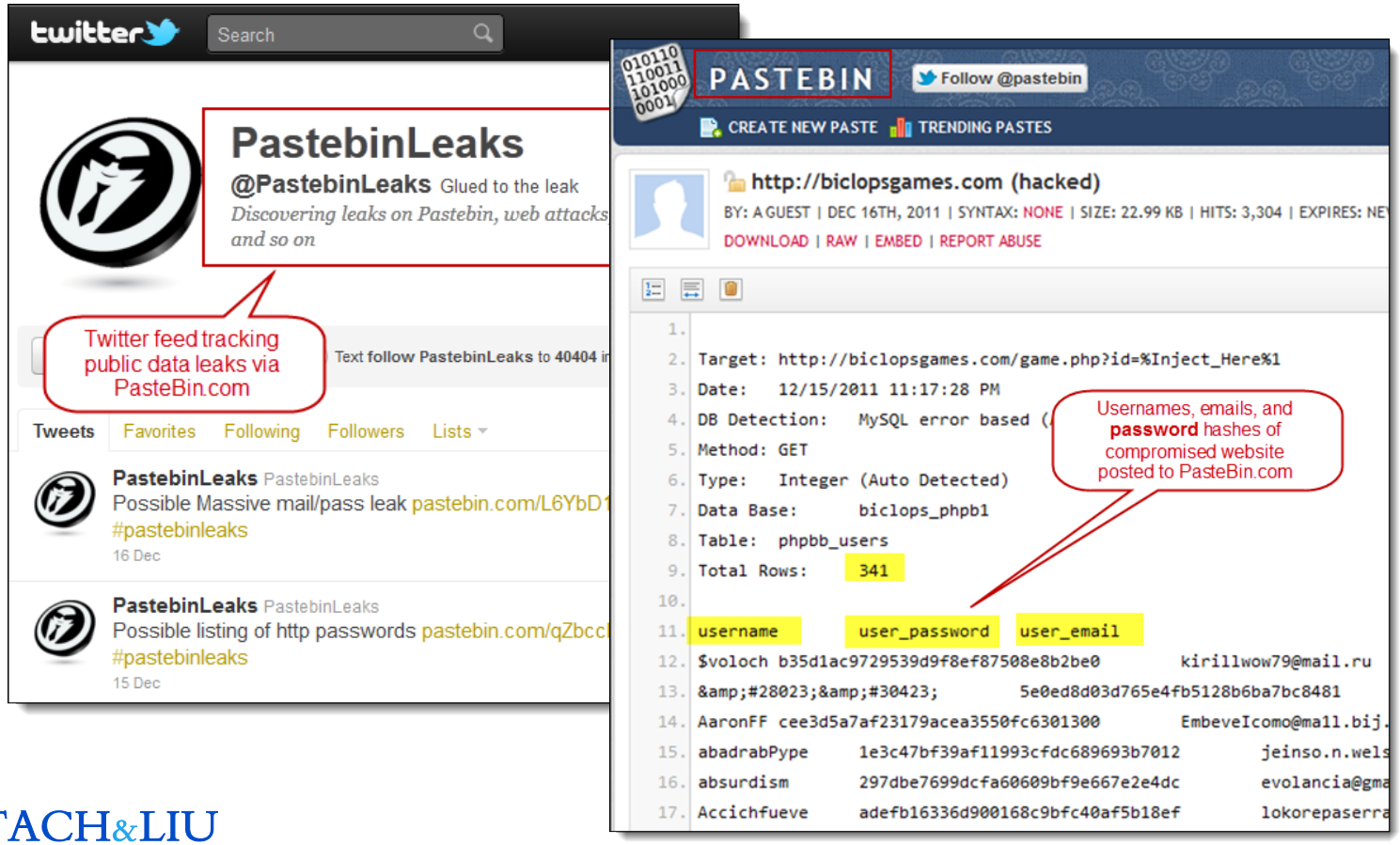
- DNS/IP Addr records hacker search engine



PasteBin Leaks

PASSWORDS IN PASTEBIN.COM POSTS

- Twitter feed tracking passwords leaked via PasteBin



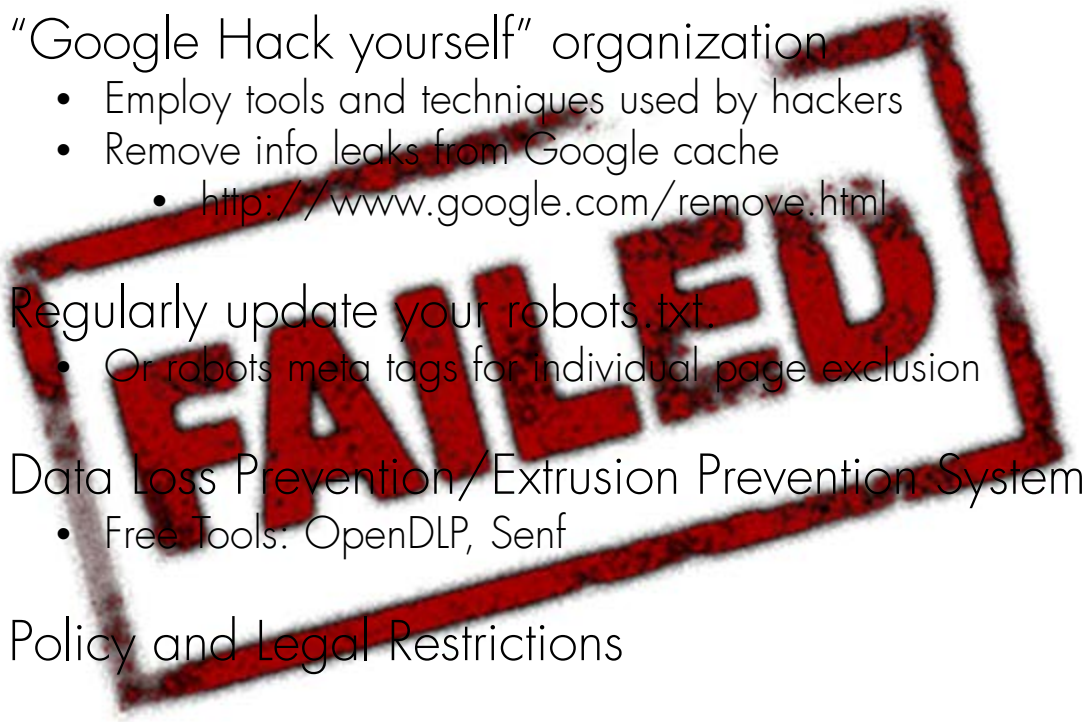
Advanced Defenses

PROTECT YO NECK

Traditional Defenses

GOOGLE HACKING DEFENSES

- "Google Hack yourself" organization
  - Employ tools and techniques used by hackers
  - Remove info leaks from Google cache
    - http://www.google.com/remove.html
- 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



Existing Defenses

"HACK YOURSELF"

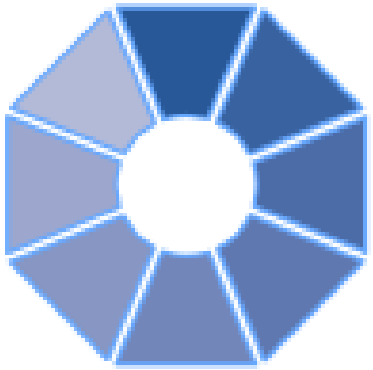
- ✓ Tools exist
- ✘ Convenient
- ✘ Real-time updates
- ✘ Multi-engine results
- ✘ Historical archived data
- ✘ Multi-domain searching

Advanced Defenses

NEW HOT SIZZLE

Stach & Liu now proudly presents:

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

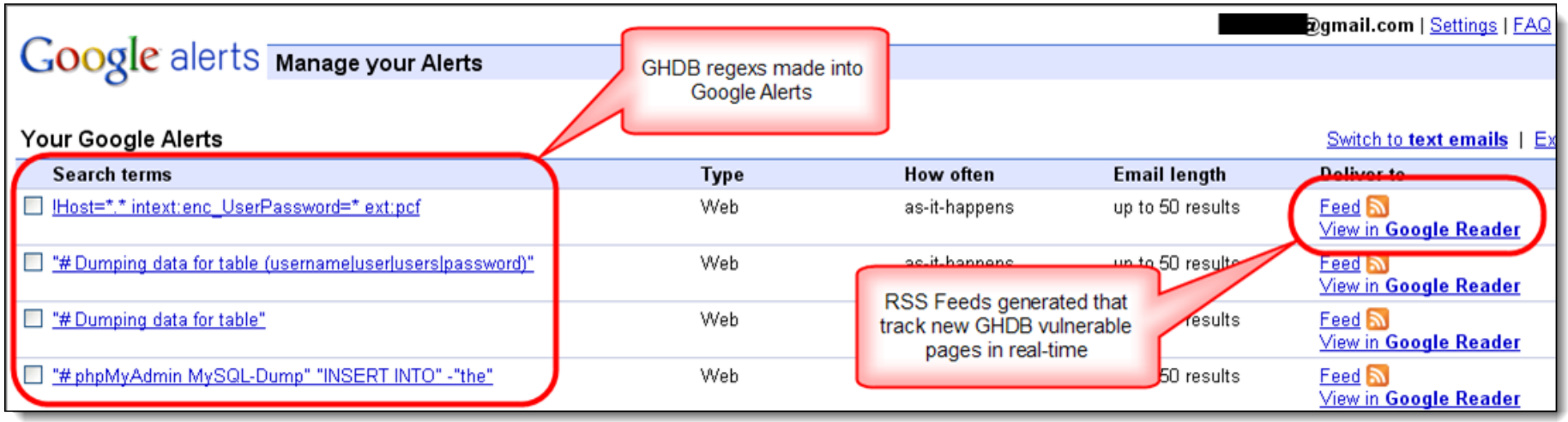


Google Hacking Alerts

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

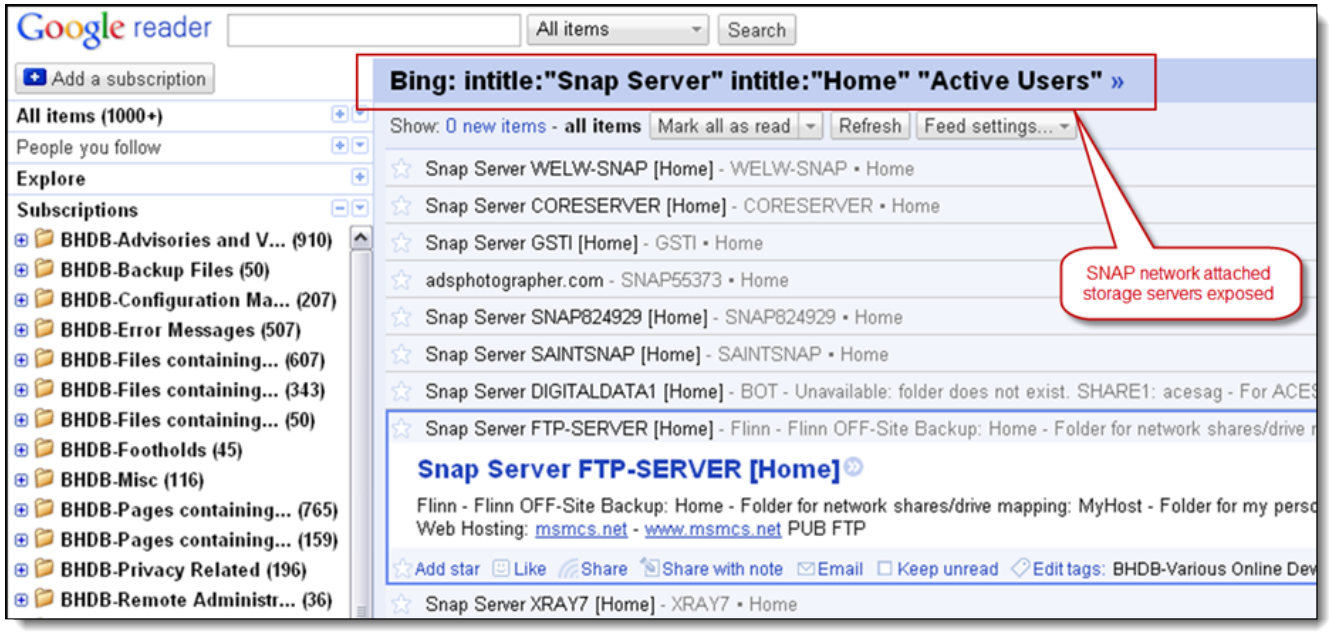
ADVANCED DEFENSES

Bing Hacking Alerts

ADVANCED DEFENSES

Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Leverages http://api.bing.com/rss.aspx
- Real-time vuln updates to >900 Bing hack queries via RSS

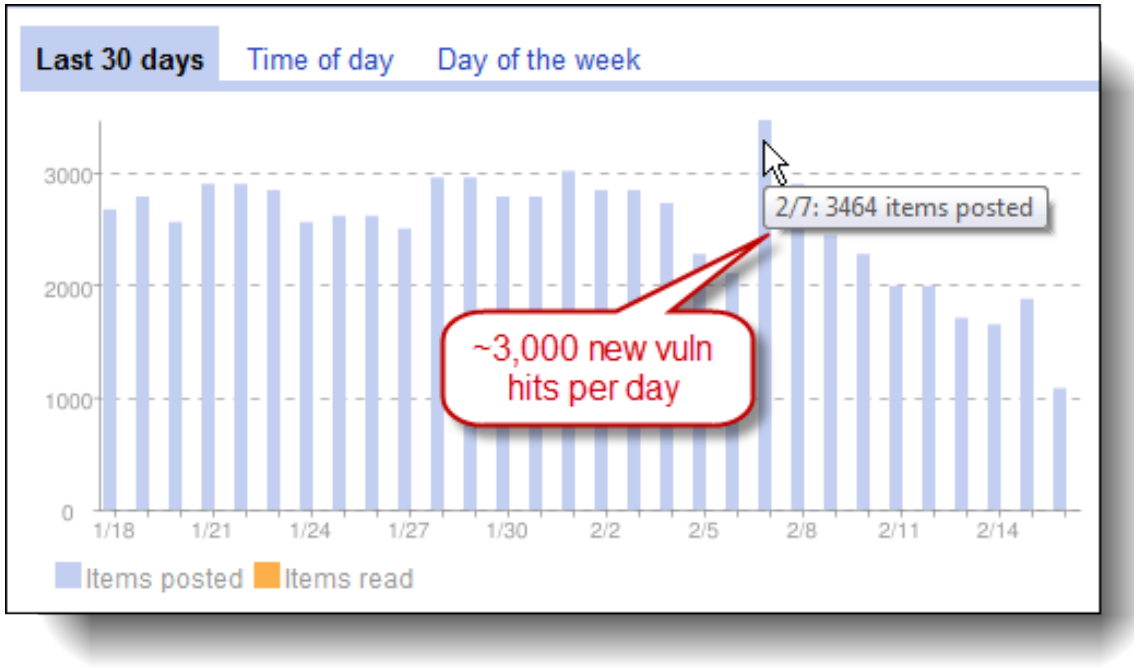


Bing/Google Alerts

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

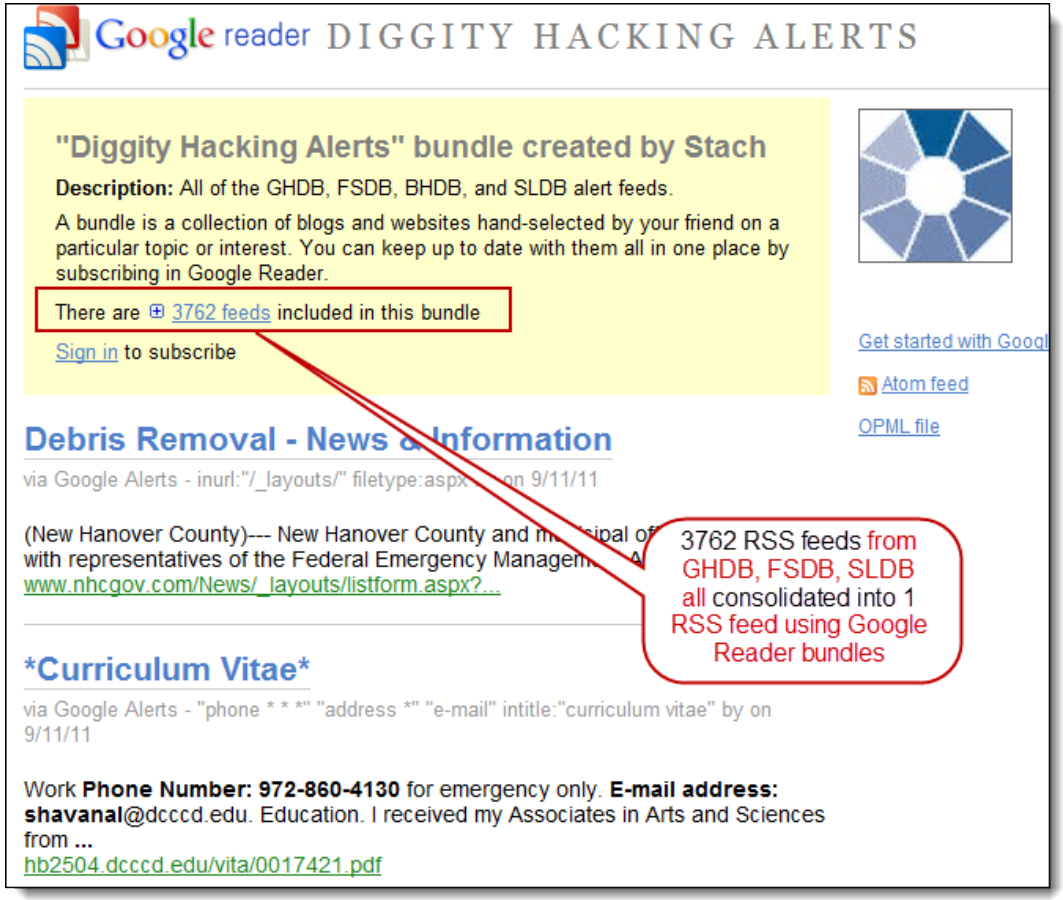
ADVANCED DEFENSE TOOLS

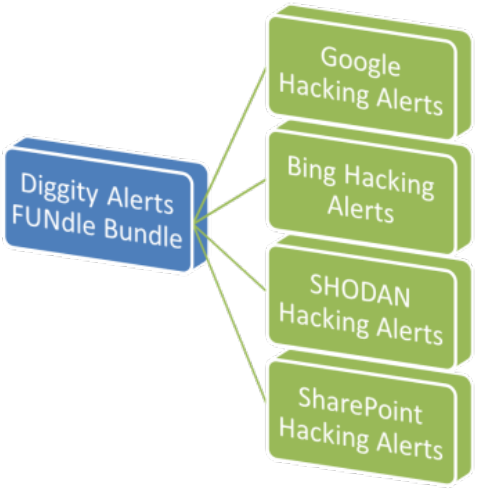
Diggity Alert Fundle Bundle

STACH&LIU

FUNdle Bundle

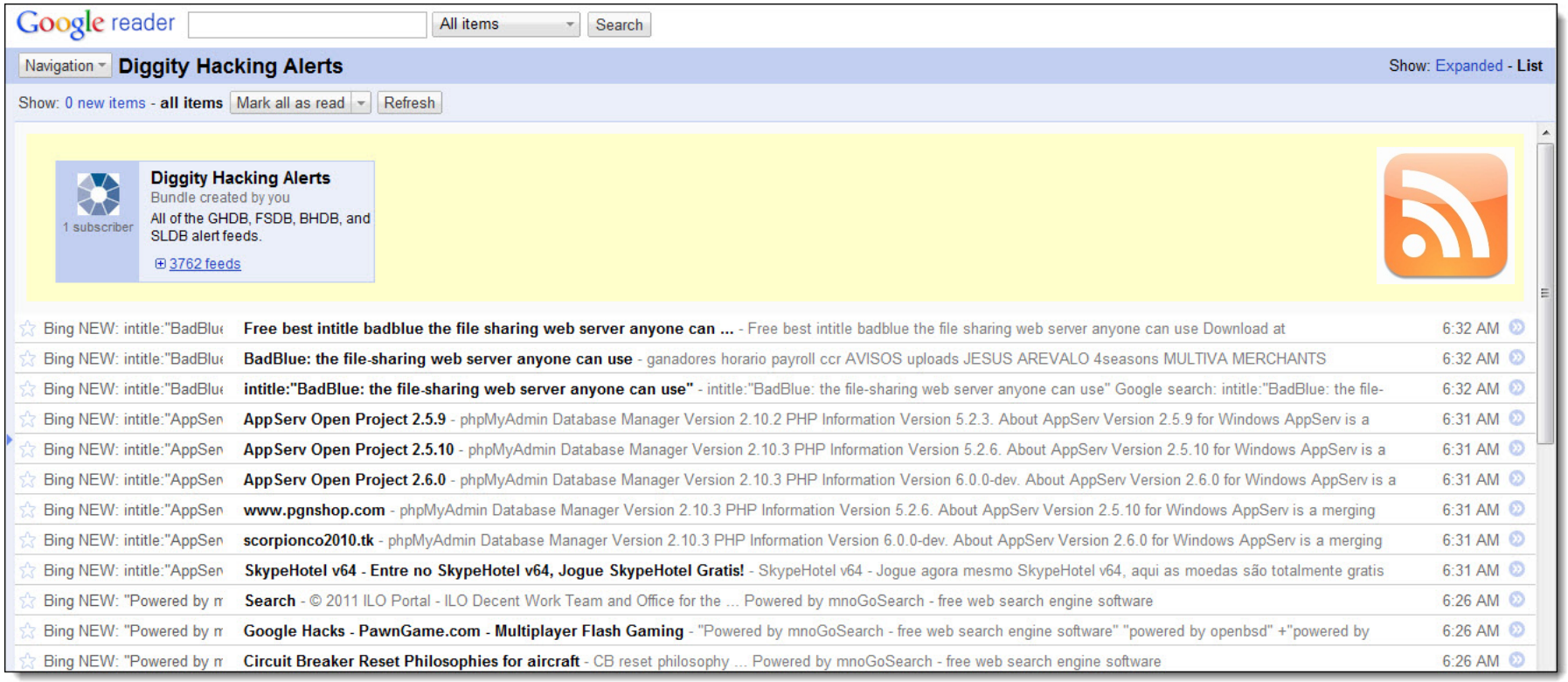
ADVANCED DEFENSES





FUNdle Bundle

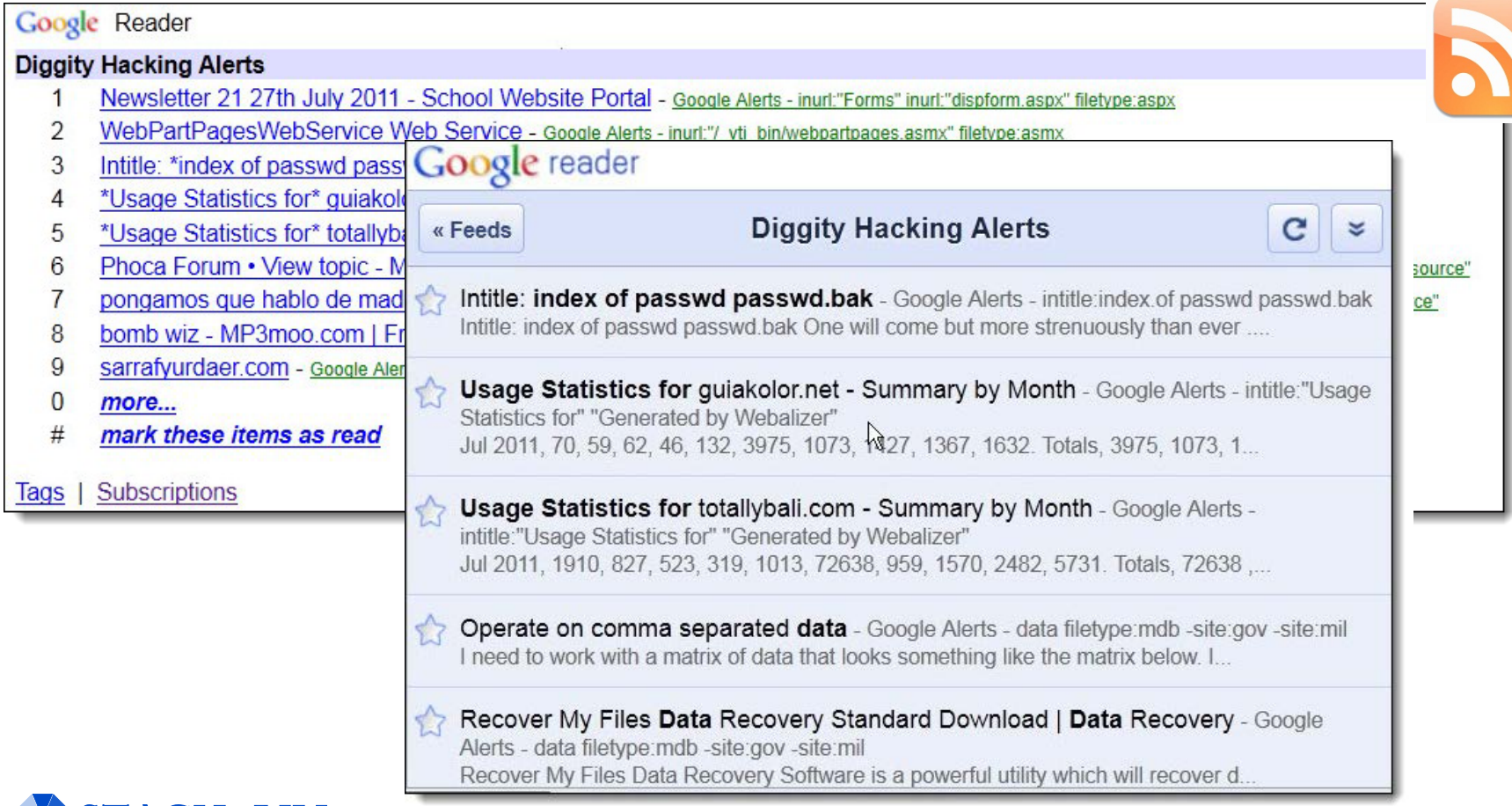
ADVANCED DEFENSES



STACH&LIU

FUNdle Bundle

MOBILE FRIENDLY



STACH&LIU

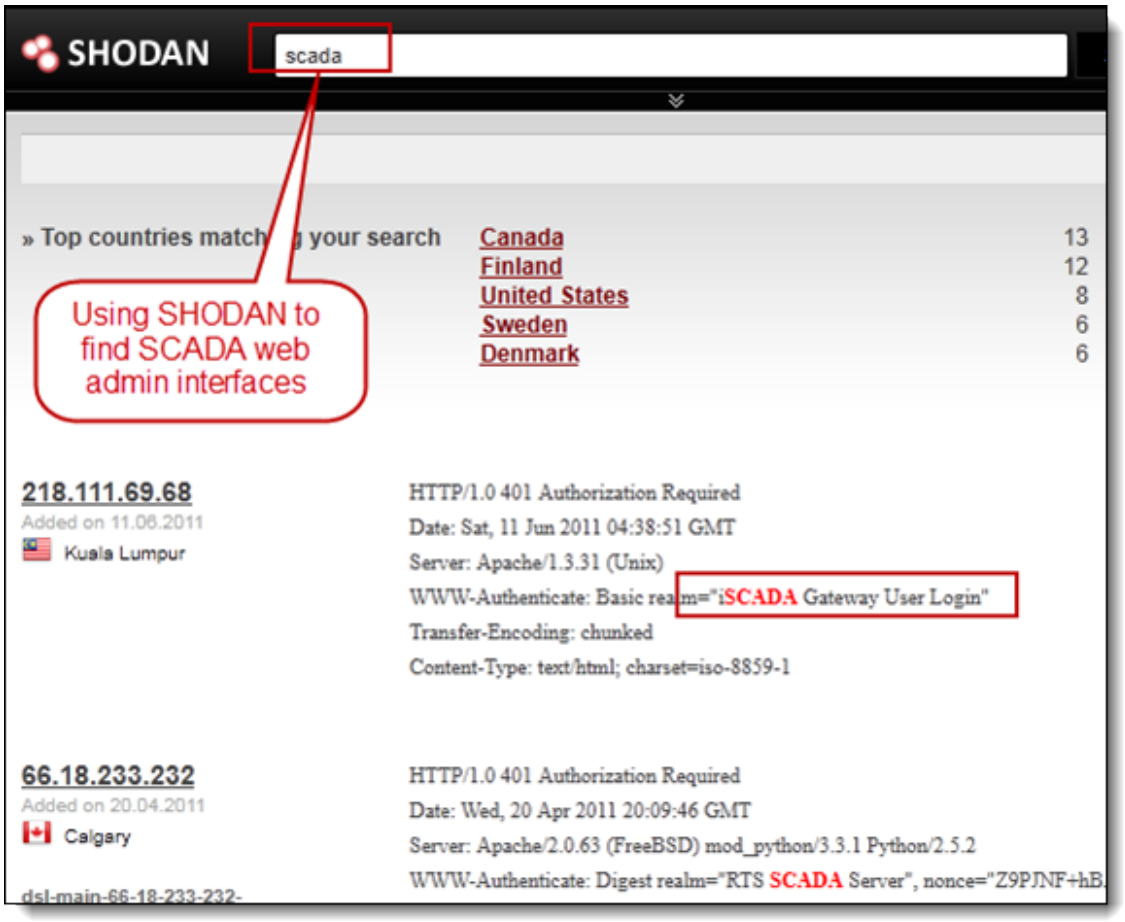
ADVANCED DEFENSE TOOLS

SHODAN Alerts

SHODAN Alerts

SHODAN Computer Search Engine

FINDING SCADA SYSTEMS



STACH&LIU

SHODAN Alerts

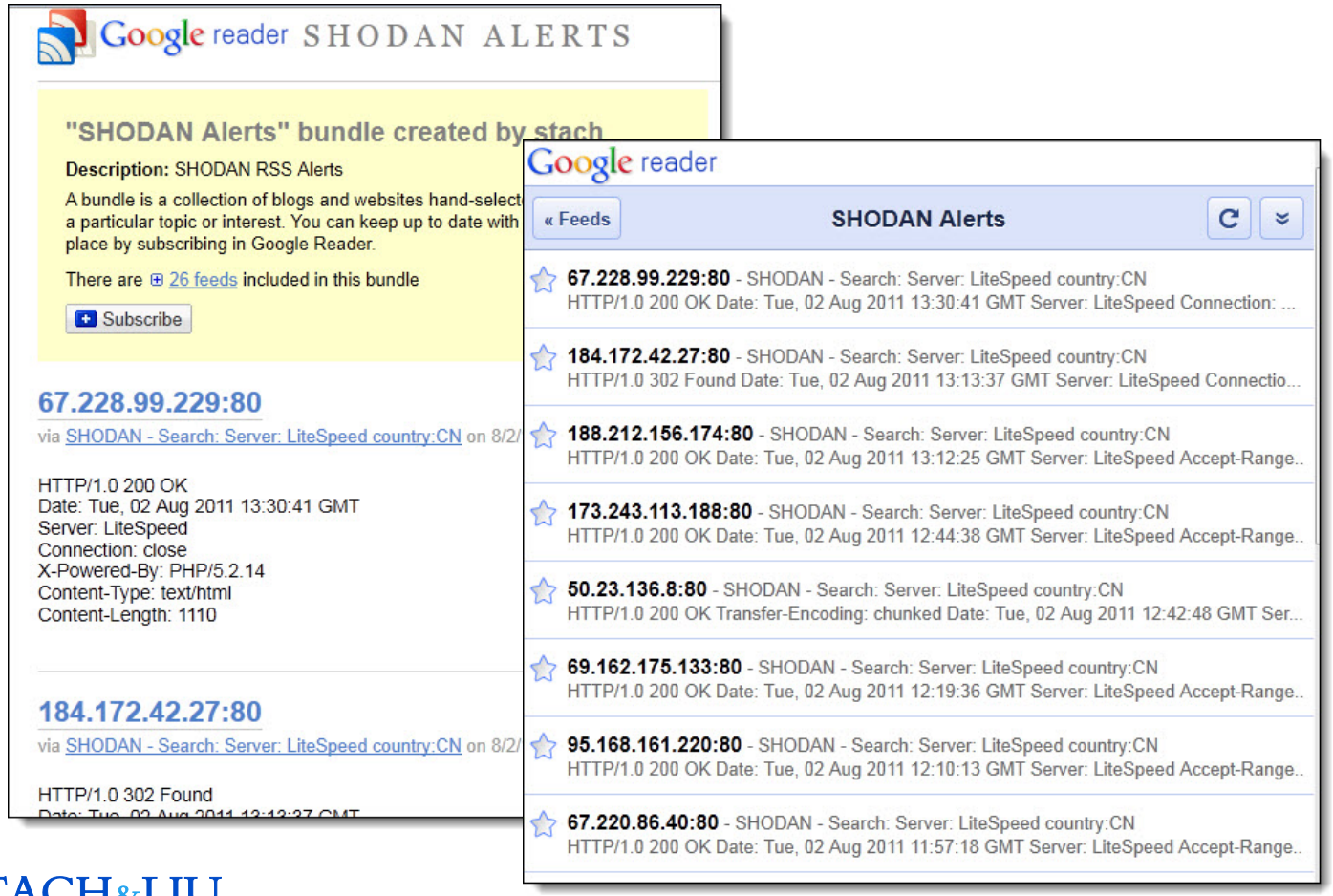
FINDING SCADA SYSTEMS

SHODAN
Computer Search Engine

Screenshot showing an industrial control system in Idaho that's connected to the internet. The red tag indicates there are known vulnerabilities for the device that might be exploitable. Two known vulnerabilities are listed at the bottom of the text bubble.

SHODAN Alerts

SHODAN RSS FEEDS



Bing/Google Alerts

THICK CLIENTS TOOLS

Google/Bing Hacking Alert Thick Clients

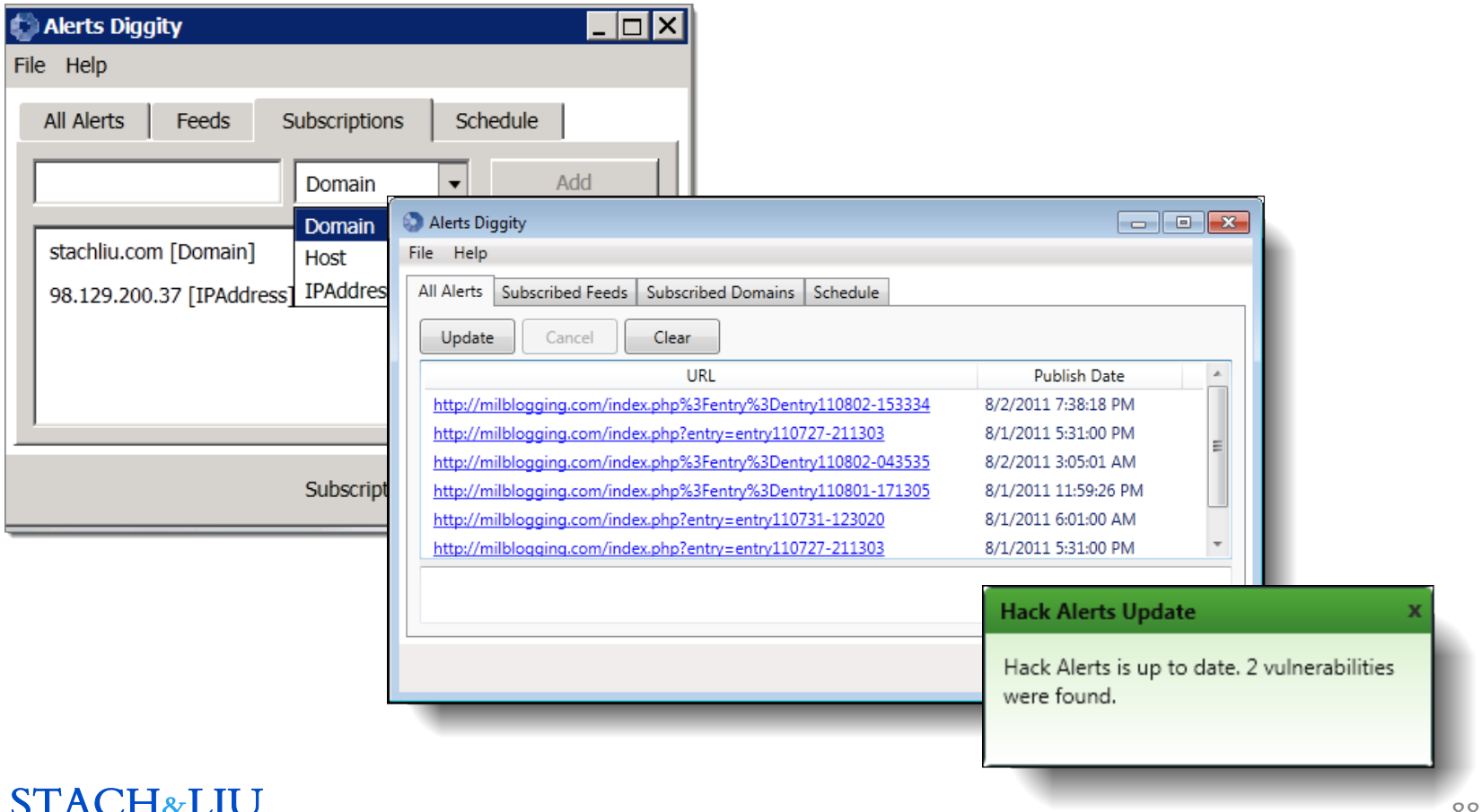
- Google/Bing Alerts *RSS feeds as input*
- Allow user to *set one or more filters*
  - e.g. *"yourcompany.com"* in the URL
- Several *thick clients* being released:
  - Windows Systray App
  - Droid app (coming soon)
  - iPhone app

ADVANCED DEFENSE TOOLS

Alert Diggity

Alerts Diggity

ADVANCED DEFENSES



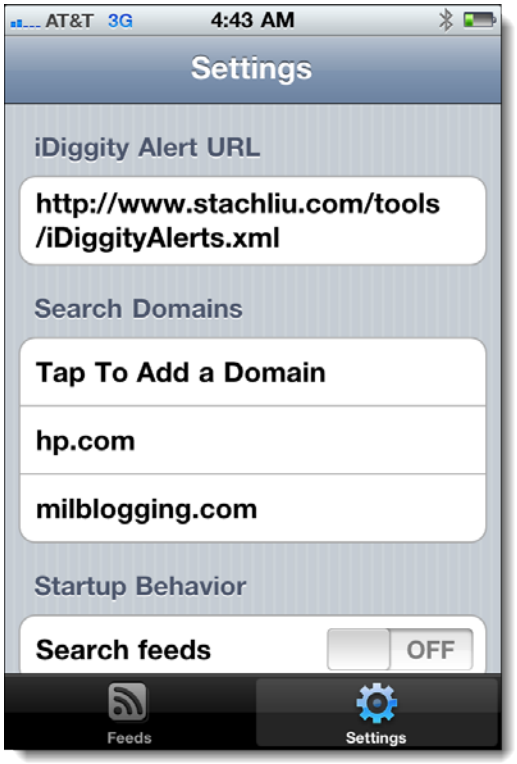
STACH&LIU

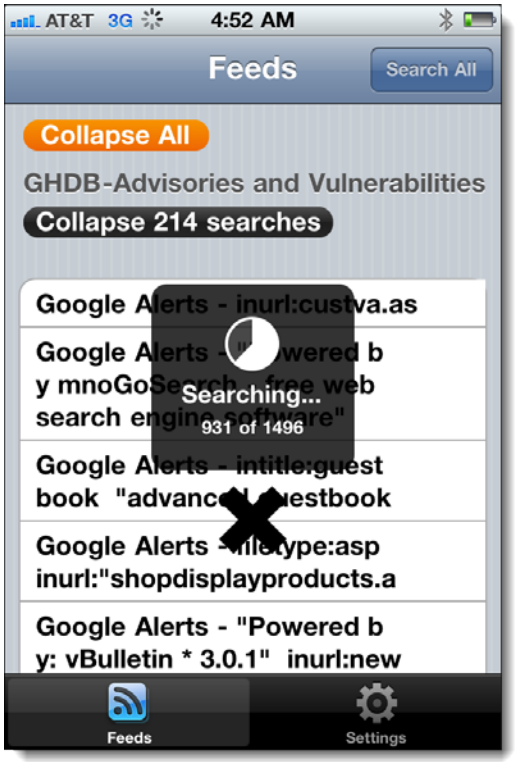
ADVANCED DEFENSE TOOLS

iDiggity Alerts

iDiggity Alerts

ADVANCED DEFENSES

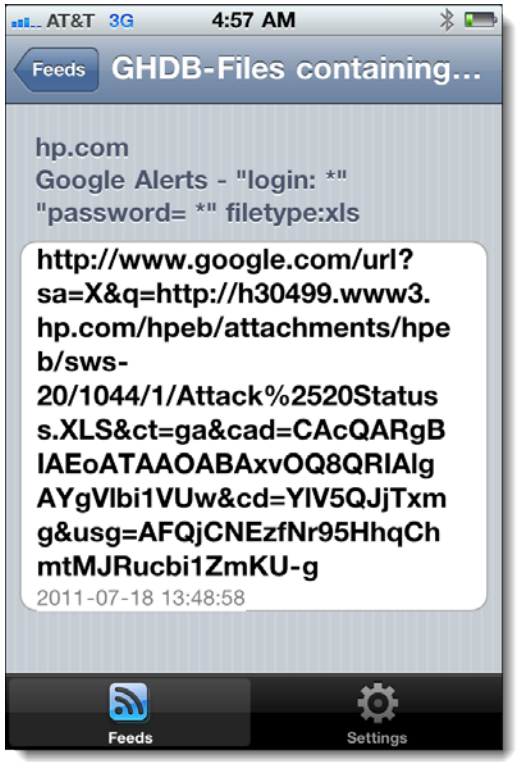


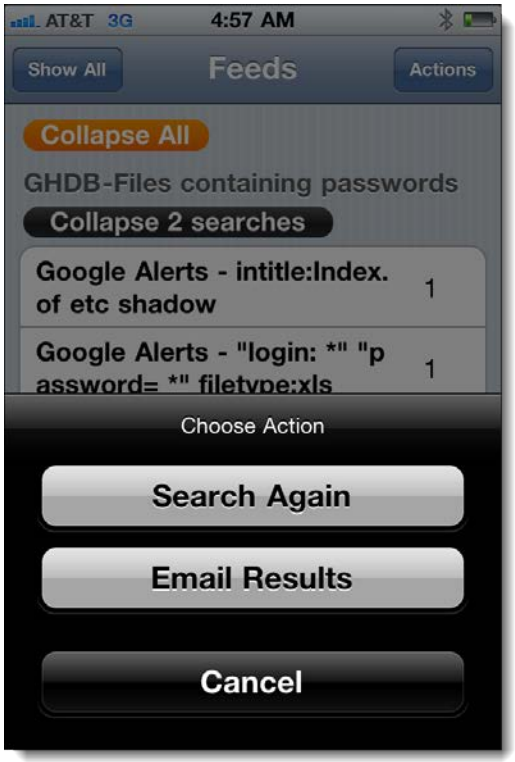


STACH&LIU

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

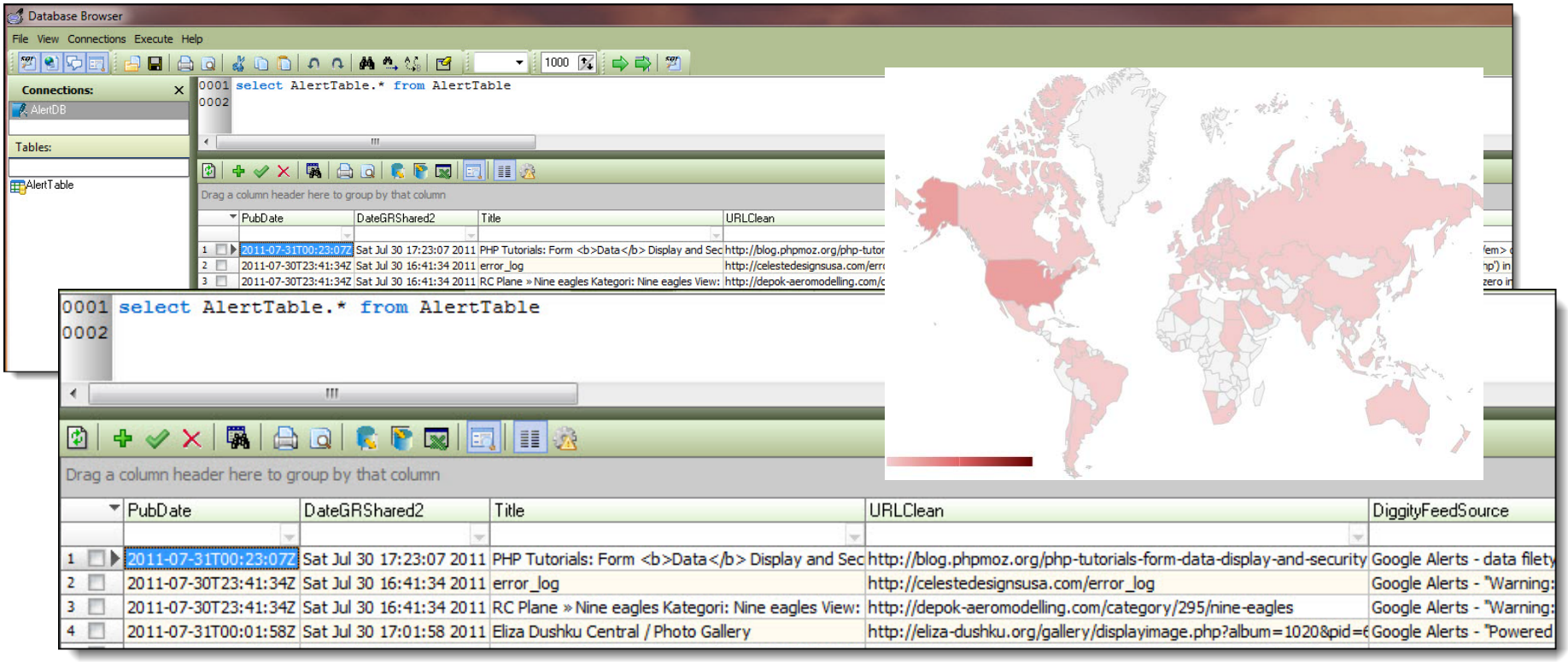
Future Direction

IS NOW

STACH&LIU

Diggity Alert DB

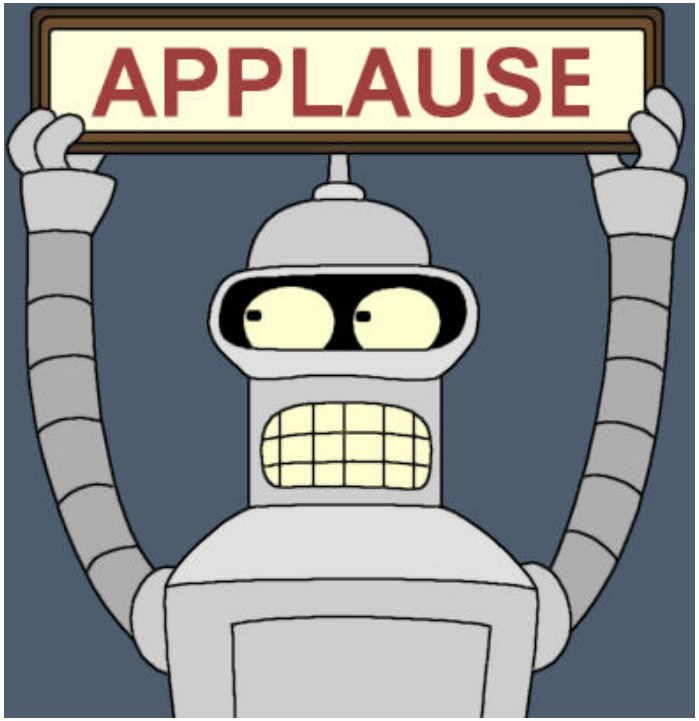
DATA MINING VULNS



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

For more info:
Fran Brown
Rob Ragan (@sweepthatleg)
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/