



Pulp Google Hacking

The Next Generation Search Engine Hacking Arsenal

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



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

Agenda

OVERVIEW



- Introduction/Background
- Advanced Attacks
 - Google/Bing Hacking - Core Tools
 - **NEW** Diggity Attack Tools
- Advanced Defenses
 - Google/Bing Hacking Alert RSS Feeds
 - **NEW** Diggity Alert Feeds and Updates
 - **NEW** Diggity Alert RSS Feed Client Tools
- Future Directions

Introduction/ Background

GETTING UP TO SPEED





Open Source Intelligence

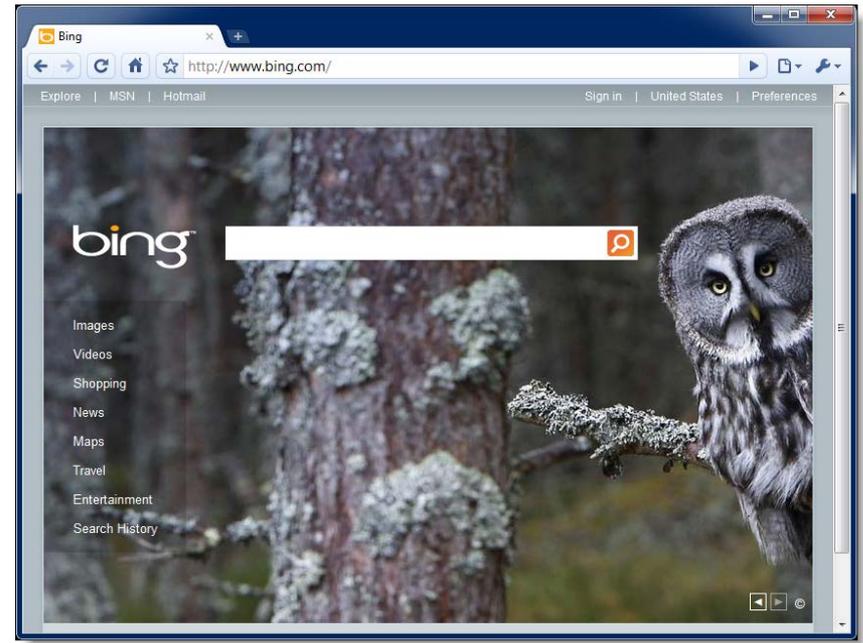
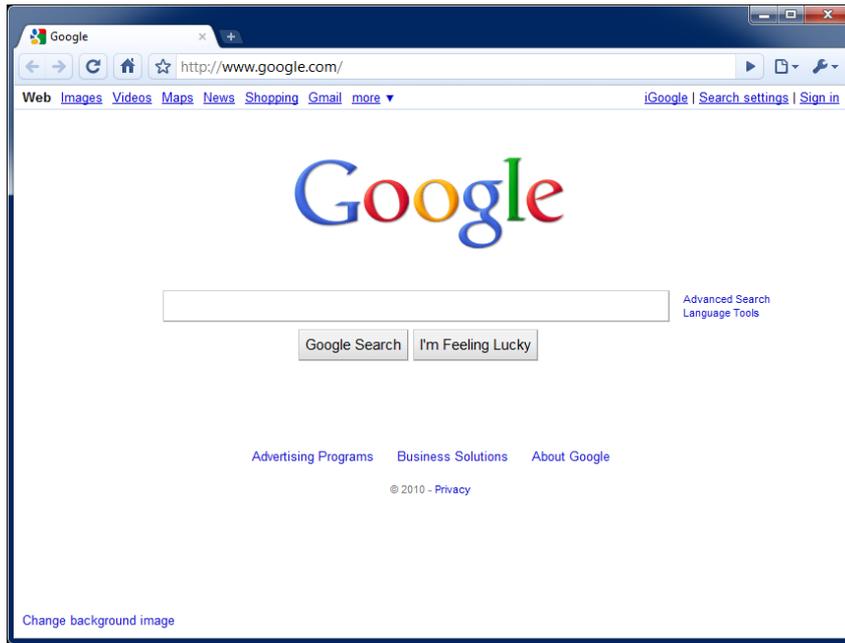
SEARCHING PUBLIC SOURCES

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



Google/Bing Hacking

SEARCH ENGINE ATTACKS





Google/Bing Hacking

SEARCH ENGINE ATTACKS

Bing's source leaked!



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

Attack Targets

GOOGLE HACKING DATABASE



- Advisories and Vulnerabilities (215)
- Error Messages (58)
- Files containing juicy info (230)
- Files containing passwords (135)
- Files containing usernames (15)
- Footholds (21)
- Pages containing login portals (232)
- Pages containing network or vulnerability data (59)
- Sensitive Directories (61)
- Sensitive Online Shopping Info (9)
- Various Online Devices (201)
- Vulnerable Files (57)
- Vulnerable Servers (48)
- Web Server Detection (72)



Google Hacking = Lulz

REAL WORLD THREAT

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



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

- A-Team, 28 June 2011



Google Hacking = Lulz

REAL WORLD THREAT

22:14 <@kayla> Sooooo...using the link above and the *google hack string*.
!Host=. * intext:enc_UserPassword=* ext:pcf* Take your pick of VPNs you want access too. Ugghh.. *Aaron Barr CEO HBGary Federal Inc.*

22:15 <@kayla> download the pcf file

22:16 <@kayla> then use <http://www.unix-ag.uni-kl.de/~massar/bin/cisco-decode?enc=> to clear text it

22:16 <@kayla> = *free VPN*



The screenshot shows a Google search interface. The search bar contains the query: `!Host=*. * intext:enc_UserPassword=* ext:pcf`. Below the search bar, it indicates "About 877 results (0.24 seconds)".

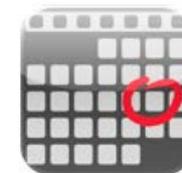
On the left side, there are navigation links: "Everything", "Images", "Videos", "News", "Shopping", and "More".

The search results list two items:

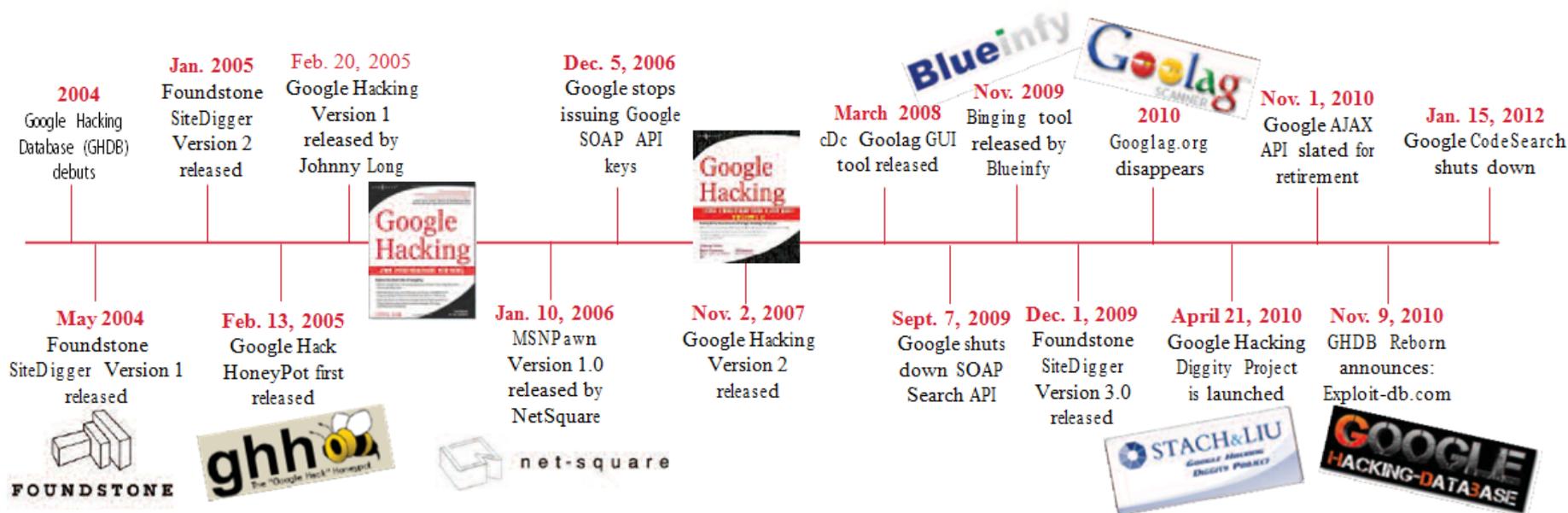
- DentsuVPN.pcf**
www.net-root.com/files/Cisco/DentsuVPN.pcf - United Kingdom - Cached
 [main] Description= **Host=109.204.23.27** AuthType=1 ... UserPassword=**enc_UserPassword=** NTDomain= EnableBackup=0 BackupServer= EnableMSLogon=1 MSLogonType=0 ...
- csd-kerb.pcf**
www.cs.umd.edu/~ntg/csvpn/csd-kerb.pcf - Cached
 [main] Description= **Host=vpn.cs.umd.edu** AuthType=1 GroupName=csd-kerb GroupPwd= ... Username= SaveUserPassword=1 UserPassword= **enc_UserPassword=** NTDomain= ...

A red speech bubble on the right side of the screenshot contains the text: "Google Hacking search used by Kayla of LulzSec".

Quick History

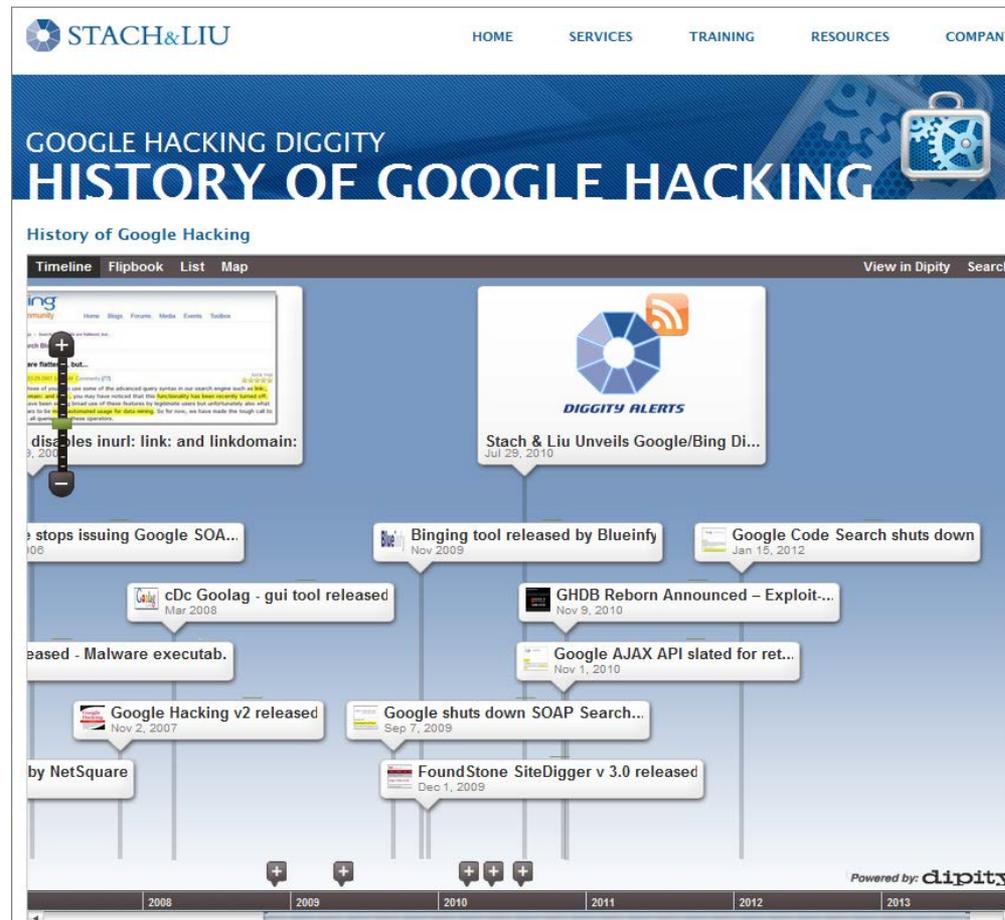


GOOGLE HACKING RECAP



Quick History

GOOGLE HACKING RECAP





Advanced Attacks

WHAT YOU SHOULD KNOW





Diggity Core Tools

STACH & LIU TOOLS



Google Diggity

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



Bing Diggity

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





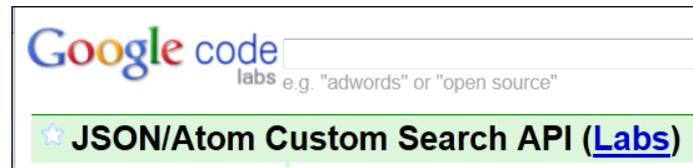
New Features



DIGGITY CORE TOOLS

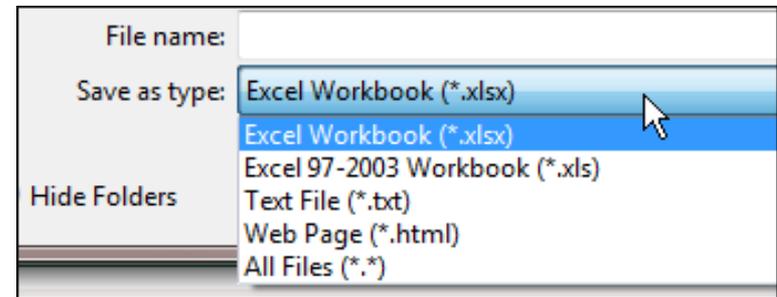
Google Diggity - New API

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



Misc. Feature Upgrades

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





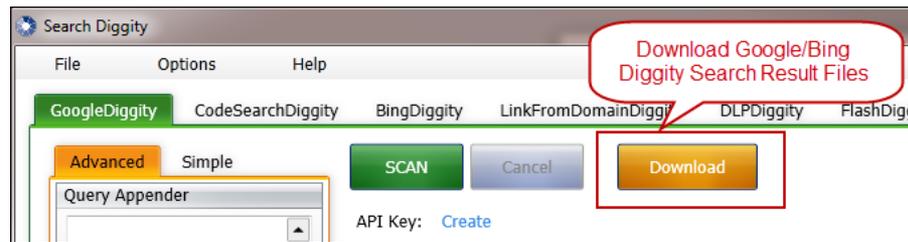
New Features



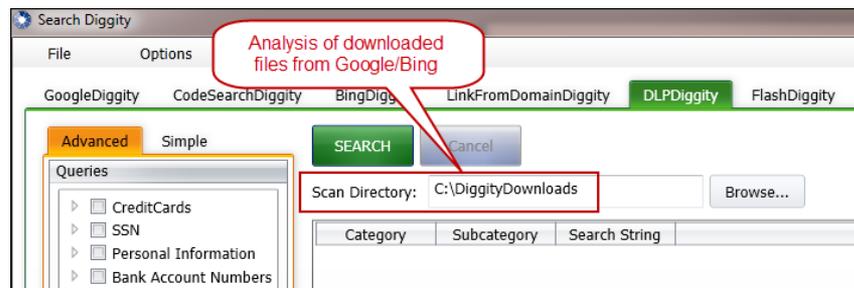
DOWNLOAD BUTTON

Download Buttons for Google/Bing Diggity

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



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

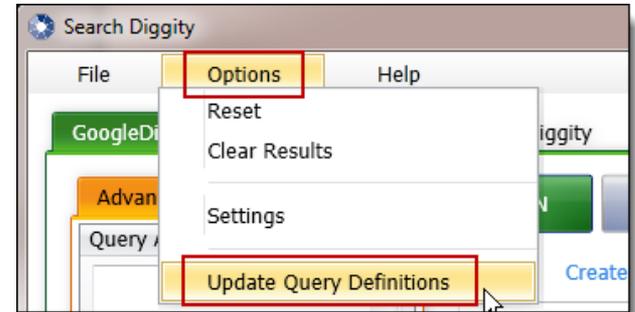




New Features



AUTO-UPDATES



SLDB Updates in Progress

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

Google search for `"/_vti_bin/lists.aspx" filetype:asmx` showing **About 98,300 results (0.21 seconds)**. The search results list several **Lists Web Service** entries, with a callout indicating **98,000 exposed SharePoint "Lists Web Service"**.





New Features

IP ADDRESS RANGES

GoogleDiggity can now search for IP Address Ranges

GoogleDiggity automatically converts IP address ranges of different formats to `site:10.1.*.*` notation

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 screenshots of Google search results. The left screenshot shows a search for `site:/com:*` with a callout box stating: "All non-port 80/443 HTTP admin consoles for .com". The right screenshot shows a search for `site:/216.75.*:**` with a callout box stating: "IP address range search for HTTP admin interfaces on non-standard ports".

Left Screenshot: Search query: `site:/com:*`. Results include:

- Twimbow - Colored Thought: <https://www.twimbow.com:5223/>
- Tribe.VastSpot.Com - Server: <https://server-triburile.com:81/>
- Davidsons Motors - Denver: <https://davidsonsmotors.com:16>

Right Screenshot: Search query: `site:/216.75.*:**`. Results include:

- SmarterMail Login - SmarterMail: 216.75.63.101:9998/
- SHOUTcast Administrator: 216.75.172.130:8015/
- Prolinkweb - Web Mail: 216.75.20.82:32000/mail/



Dictionary Updates

3RD PARTY INTEGRATION



New maintainers of the GHDB – 09 Nov 2010

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

Google Hacking Database Reborn

9th November 2010 - by admin

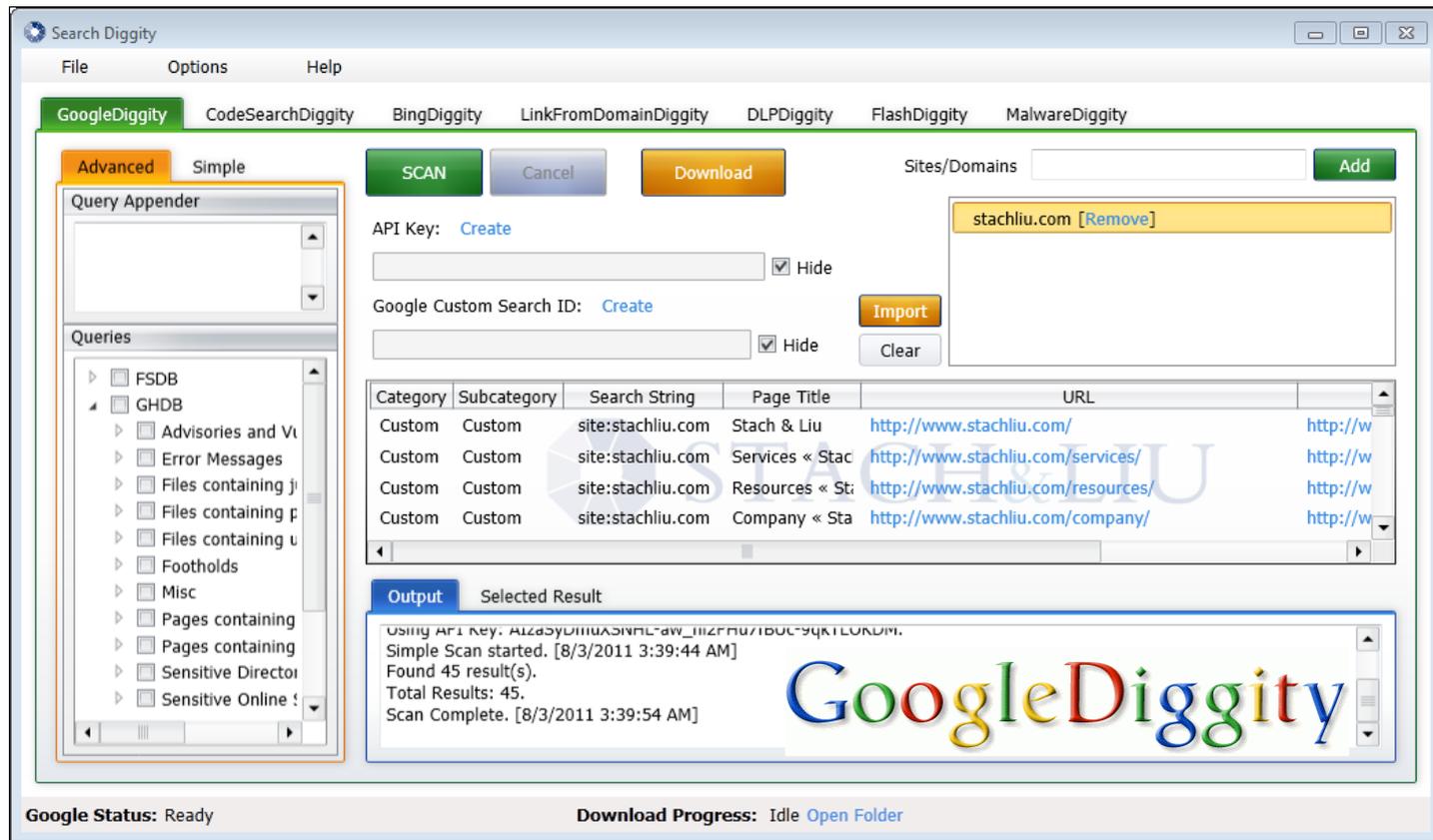
The incredible amount of information continuously leaked onto the Internet, and therefore accessible by Google, is of great use to penetration testers around the world. Johnny Long of [Hackers for Charity](#) started the Google Hacking Database (GHDB) to serve as a repository for search terms, called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

GOOGLE
HACKING-DATABASE

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

Google Diggity

DIGGITY CORE TOOLS



The screenshot shows the Google Diggity application window. The interface includes a menu bar (File, Options, Help), a tabbed interface with 'GoogleDiggity' selected, and a main workspace. On the left, there are 'Advanced' and 'Simple' tabs, a 'Query Appender' field, and a tree view of 'Queries' with 'GHDB' expanded. The main area contains a 'SCAN' button, 'Cancel', and 'Download' buttons. Below these are fields for 'API Key' and 'Google Custom Search ID', each with a 'Create' link and a 'Hide' checkbox. To the right, there's a 'Sites/Domains' list with 'stachliu.com [Remove]' and an 'Add' button. Below the list are 'Import' and 'Clear' buttons. A table displays search results with columns for Category, Subcategory, Search String, Page Title, and URL. The 'Output' tab shows a log of the scan process, including the API key, start time, number of results found, and completion time. The 'Google Diggity' logo is visible in the bottom right of the output area. The status bar at the bottom shows 'Google Status: Ready' and 'Download Progress: Idle Open Folder'.

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

```
Using API Key: ALZa5yDIIUASIVNLC-aw_1IuzFNU7tDUC-9qKI-EURDM.  
Simple Scan started. [8/3/2011 3:39:44 AM]  
Found 45 result(s).  
Total Results: 45.  
Scan Complete. [8/3/2011 3:39:54 AM]
```

Bing Diggity

DIGGITY CORE TOOLS



The screenshot shows the Bing Diggity application window. The 'BingDiggity' tab is selected. The interface includes a menu bar (File, Options, Help), a toolbar with 'SCAN', 'Cancel', and 'Download' buttons, and a search input field containing '98.129.200.37'. Below the search field, there is a 'Bing 2.0 API Key' field with a 'Create' link and a 'Hide' checkbox. The main area displays a table of search results. A red box highlights the search string 'ip:98.129.200.37' in the second row. A red callout bubble points to the IP address in the search input field with the text 'Demonstrating Bing's IP address reverse lookup feature'. The 'Output' section at the bottom shows the scan results, including the API key and the number of results found.

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

Output Selected Result

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

Bing Status: Ready Download Progress: Idle Open Folder



Bing Hacking Database



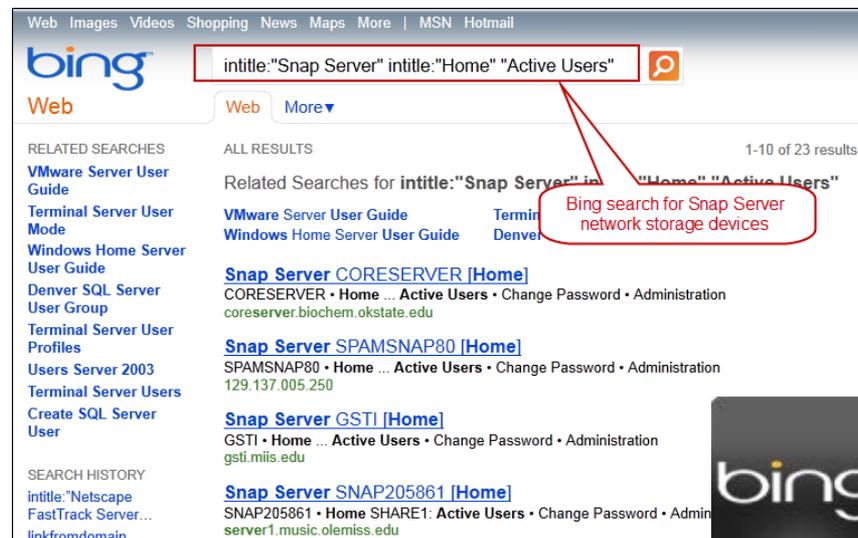
STACH & LIU TOOLS

BHDB – Bing Hacking Data Base

- First ever Bing hacking database
- Bing hacking limitations
 - Disabled **inurl:**, **link:** and **linkdomain:** directives in March 2007
 - No support for **ext:**, **allintitle:**, **allinurl:**
 - Limited **filetype:** functionality
 - Only 12 extensions supported

Example - Bing vulnerability search:

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





Hacking CSE's



ALL TOP LEVEL DOMAINS

GoogleDiggity

Google custom search

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 »](#)



NEW GOOGLE HACKING TOOLS

Code Search Diggity

Google Code Search



VULNS IN OPEN SOURCE CODE

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



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

The screenshot shows a Google Code Search interface. The search query is `select.*from.*request\..QUERYSTRING`. The search results show a file named `post.asp`. A red callout box points to the `reply_id` parameter in the SQL query, stating "reply_id is SQL injectable querystring parameter". The SQL query is: `SELECT * from reply where reply_id = " & Request.QueryString("reply_id")`. The search results also show a link to `www.cnarts.net/eweb/download/software/bbs/tradeforum.zip`.

CodeSearch Diggity

AMAZON CLOUD SECRET KEYS



Search Diggity

File Options Help

GoogleDiggity **CodeSearchDiggity** BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity MalwareDiggity

Advanced Simple

SCAN Cancel

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

Amazon AWS Cloud keys stored in plaintext

Output Selected Result

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



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 Docs Exposures

PUBLIC CLOUD SEARCHING

Public cloud storage document exposures



Dropbox

Google docs

Google search results for the query: `intext:"name" intext:"address" intext:"taxpayer" site:dl.dropbox.com`. The search returned 7 results in 0.23 seconds. A callout bubble points to the search query with the text: "Looking for sensitive data leaks in Dropbox cloud storage". One result is highlighted: "[PDF] ... W-9" with the URL `https://dl.dropbox.com/s/.../CTMUN_W9_Request_For_TaxID.pdf?...`. A second search is shown below, for the query: `site:live.com "skydrive" ext:dmp`, returning about 2,700 results in 0.41 seconds. A callout bubble points to this search with the text: "Database dump files on Microsoft SkyDrive". One result is highlighted: "Windows Live SkyDrive" with the URL `https://skydrive.live.com/embedicon.as...` and the filename `Open 060510-38688-01.dmp`.

Google search results for the query: `intext:"enable password" inurl:docid site:docs.google.com`. The search returned 4 results in 0.13 seconds. A callout bubble points to the search query with the text: "Cisco config files with passwords in Google Docs files". One result is highlighted: "nepsi-sw22" with the URL `https://docs.google.com/View?docid=0AbKTT...1...1...`. The snippet shows: `boot-end-marker ! enable secret 5 1Bhsg$izpAqHDuLzEWCqfP/leT/ enable password 7 0455254C5F765C ! no aaa new-model. system mtu routing 1500 ...`. Another result is highlighted: "ncepsi-sw21-01-04-10" with the URL `https://docs.google.com/View?docid=0AbKTT...1...1...`. The snippet shows: `enable secret 5 1P6du$.NRbLzz5WIKER5mgw.t7r enable password 7 000A3D4C540C1B ! no aaa new-model. system mtu routing 1500. ip subnet-zero ...`. A third result is highlighted: "ncepsi-rt06-01-04-10" with the URL `https://docs.google.com/View?docid=0AbKTT...1...1...`. The snippet shows: `logging buffered 51200 warnings. enable secret 5 1.7N$Ru28/DDfSHrAgq5bhUFz enable password 7 151C2546547D25 ! no aaa new-model ! resource ...`. The page footer includes "Tempe, AZ" and "Change location".



linkFromDomainDiggity

NEW GOOGLE HACKING TOOLS

Bing LinkFromDomainDiggity

Bing LinkFromDomain

DIGGITY TOOLKIT



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



Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

The screenshot shows the LinkFromDomainDiggity tool interface. At the top, there are several tabs: GoogleDiggity, CodeSearchDiggity, BingDiggity, LinkFromDomainDiggity (highlighted with a red box), DLPDiggity, FlashDiggity, and MalwareDiggity. Below the tabs is a 'Query Appender' section with a text input field containing 'site:gov.cn' (highlighted with a red box) and buttons for 'SCAN' and 'Cancel'. To the right, there is a 'Sites/Domains' section with a text input field containing 'www.gov.cn' (highlighted with a red box) and an 'Add' button. Below this, there are 'Import' and 'Clear' buttons. The main display area has tabs for 'URLs', 'Applications', 'Hosts' (selected), and 'Domains'. Under the 'Hosts' tab, a list of hostnames is displayed, including '2010.visithainan.gov.cn', 'app.mps.gov.cn', 'bg.mofcom.gov.cn', 'bjsat.gov.cn', 'bjyouth.gov.cn', 'catf.agri.gov.cn', and 'cc.fjkl.gov.cn' (all highlighted with a red box). At the bottom, there is an 'Output' section with a text area containing the following text: 'Using [redacted] F9367FBFD32. Advanced Scan started. [9/10/2011 2:16:54 PM] Found 445 result(s) for query: "linkfromdomain:www.gov.cn site:gov.cn". Total Results: 445. Scan Complete. [9/10/2011 2:17:26 PM]'. The 'linkfromdomaindiggity' logo is visible in the bottom right corner of the interface.

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

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

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



NEW GOOGLE HACKING TOOLS

DLP Diggity



DLP Diggity



LOTS OF FILES TO DATA MINE

Google search interface showing the query `filetype:pdf` and the result count: "About 513,000,000 results (0.25 seconds)".

Google search interface showing the query `filetype:doc` and the result count: "About 84,500,000 results (0.10 seconds)".

Google search interface showing the query `filetype:xls` and the result count: "About 17,300,000 results (0.13 seconds)".

Bing search interface showing the query `filetype:doc`. The results section shows "1-10 of 26,900,000 results" and includes a link to "Advanced" search options.

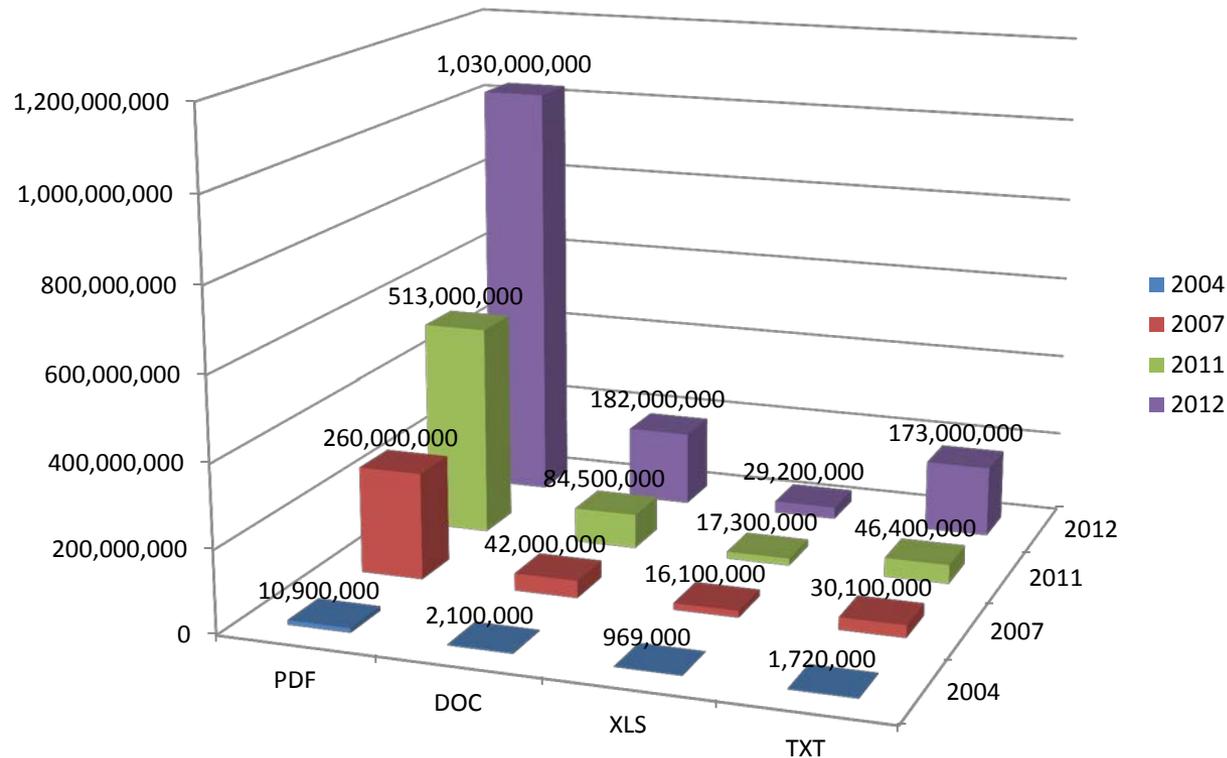
Bing search interface showing the query `filetype:pdf`. The results section shows "1-10 of 146,000,000 results" and includes a link to "Advanced" search options.



DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR

Google Results for Common Docs





Data Loss In The News

MAJOR DATA LEAKS

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

The image shows a screenshot of a Slashdot article and a Google search result. The Slashdot article is titled "Groupon Deal of the Day: 300,000 Customer Accounts" and is posted by samzenpus on Wednesday June 29 2011, @01:11PM. The article text mentions that the customer database of Groupon's Indian subsidiary was published, unsecured and unencrypted, on the company's site for long enough to be indexed by Google. The Google search result shows the query "filetype:sql hotmail gmail password" and a result from "www.sos-asta.com/uploaded/user/xyz.sql" in India.



Data Loss In The News

MAJOR DATA LEAKS

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet



DLP Diggity

DIGGITY TOOLKIT



GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity **DLPDiggity** FlashDiggity Mal...

Advanced Simple

SEARCH Cancel

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

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

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
```

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



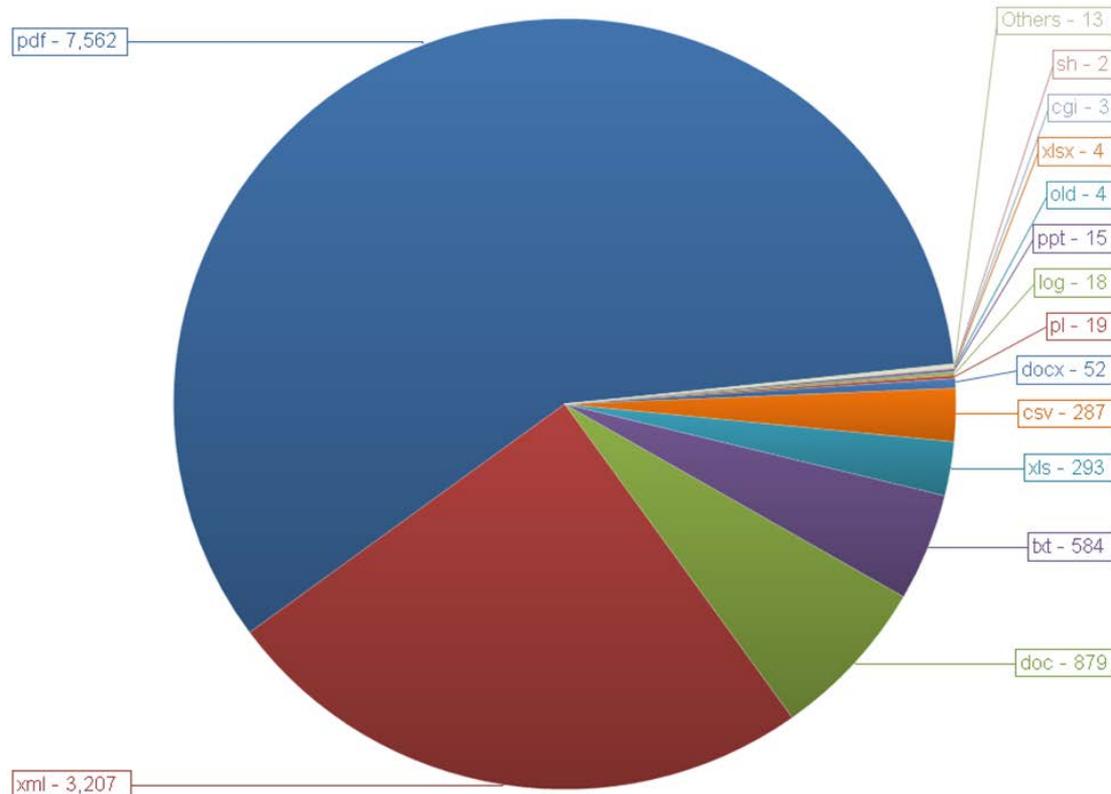
DLP Reporting

PRACTICAL EXAMPLES



DLPDiggity - # of Files Analyzed per File Extension

Total = 12,943 files



DLP Reporting

PRACTICAL EXAMPLES



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

Updated October 8, 2011

Executive Summary

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

General Information

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

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

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

Google custom search

XSS.CX Research

Google™ Site Search Search

Google CSE providing search access to XSS.CX vulnerability results

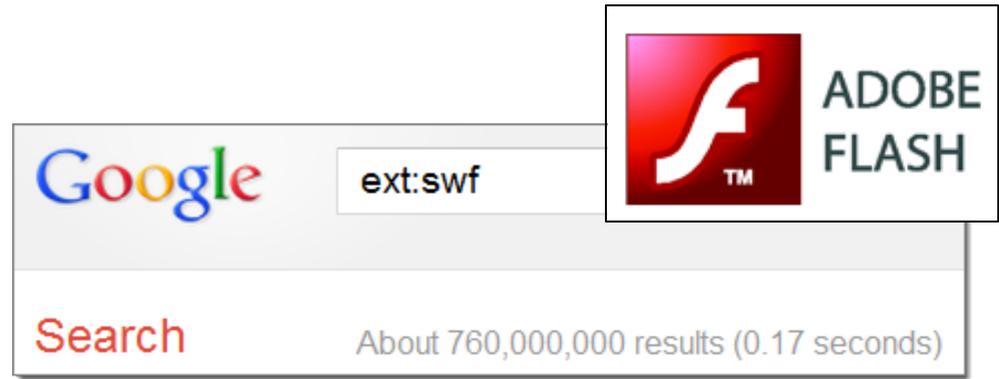
Search engine details

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

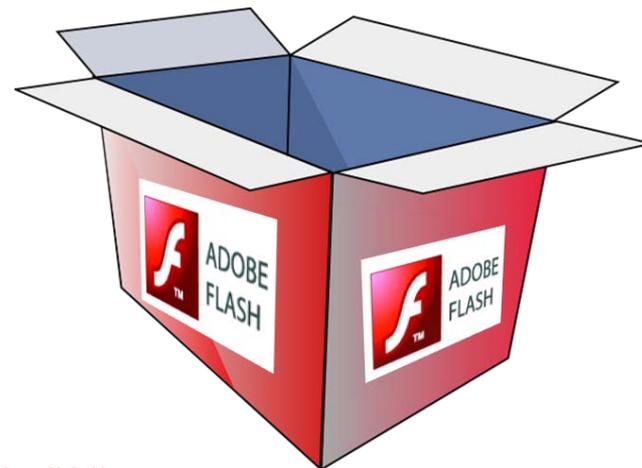


NEW GOOGLE HACKING TOOLS

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



GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity **FlashDiggity** MalwareDiggity

Advanced Simple

SEARCH Cancel

Queries

- Insecure Application De
- ActionScript Source
- Application Source /
- Sensitive Data
- PGP Private Key Blo
- PGP Public Key Bloc
- RSA Private Key Blo
- Internal IP Disclosui
- MD5 Hash Detected
- Possible Credit Card
- Possible Server Pat
- Possible Social Secu
- SHA-0/SHA-1 Hash
- Keywords
 - User Account Info
 - Potentially Interesti
 - Application

Scan Directory: C:\DiggityDownloads Browse...

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

Output Selected Result

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

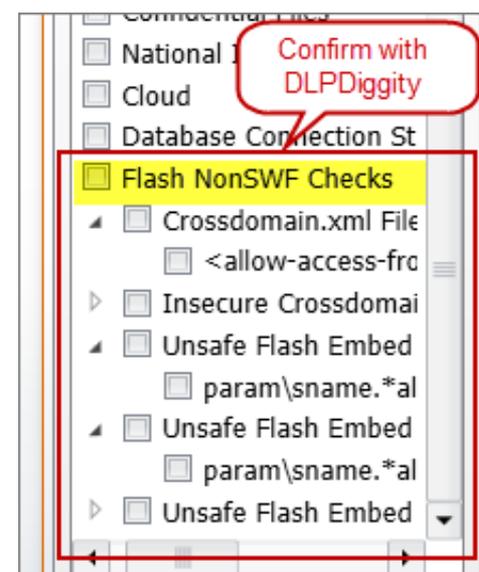
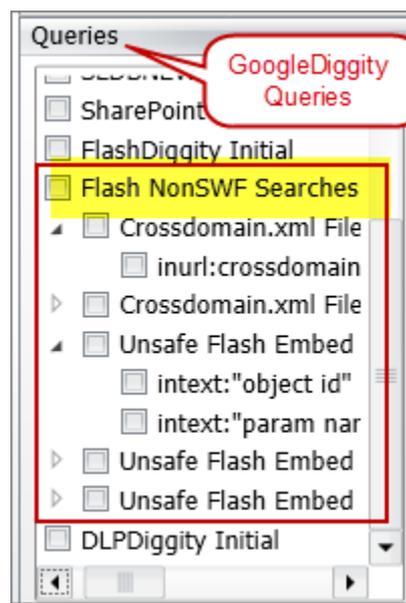
Hardcoded usernames and passwords in cleartext in SWF file

Flash Non-SWF Hacking



OTHER FLASH HACKING

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





NEW GOOGLE HACKING TOOLS

DEMO

GoogleScrape Diggity

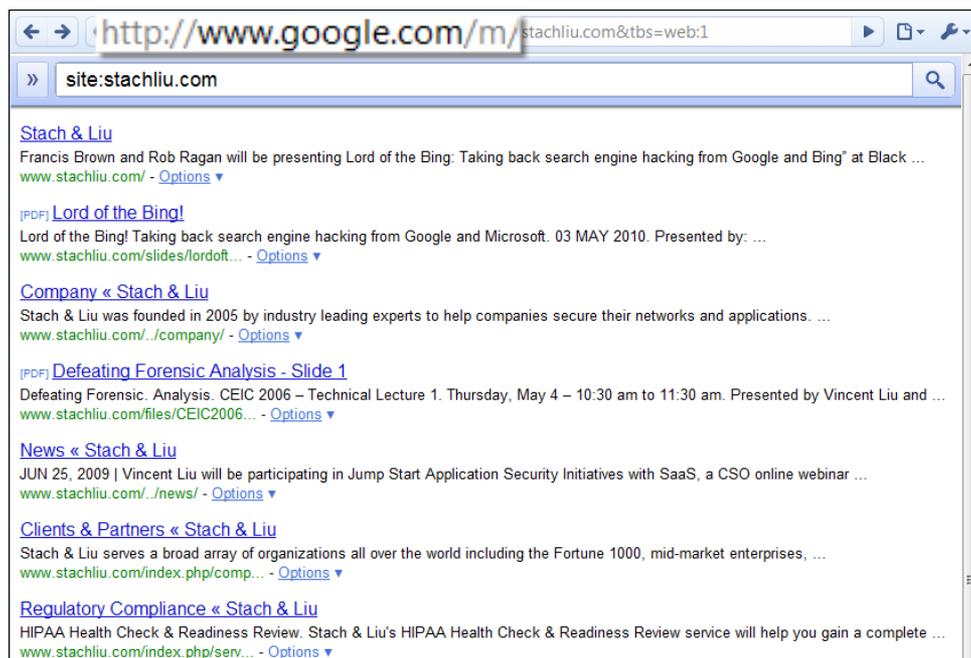
DIGGITY TOOLKIT



GoogleScrape Diggity

- Uses Google mobile interface
 - Light-weight, no advertisements
 - *Violates* Terms of Service
- Bot detection avoidance
 - Distributed via proxies
 - Spoofs User-agent and Referer headers
 - Random `&userip=` value
 - Across Google servers

COMING SOON





NEW GOOGLE HACKING TOOLS

Baidu Diggity

BaiduDiggity

CHINA SEARCH ENGINE



- Fighting back

COMING SOON

百度搜索_"supplied argu... x

www.baidu.com/s?bs=intitle%3A"Snap+Server"+intitle%3A"Home"+"Active+Use

Baidu 百度 新闻 网页 贴吧 知道 MP3 图片 视频 地图 更多

"supplied argument is not a valid MySQL result resource" site:gov.cn 百度一下

去掉""获得更多 [supplied argument is not a valid MySQL result resource site:gov.cn](#) 的搜索结果(于双引号)

信息内容添加

: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in D:\apache\phpmysql\htdocs\news\adm\newgl\newstj.php on line 11
[www.xjpi.gov.cn/news/adm/newgl/newstj.php](#) 2011-...

[中山市五桂山区办事处信息网](#)
Warning: mysql_free_result(): supplied argument is not a valid MySQL result resource in E:\site\phpsite\wgs\public\navigation.php on line 18...
[www.wuguishan.gov.cn/zhzx/zhzx_content.ph](#) ... 2011-2-17 - 百度快照

[堵河水电专业气象服务](#)
: mysql_num_rows(): supplied argument is not a valid MySQL result resource in E:\wwwroot\qxwv-shiyan.gov\web\duhe\inc_online.php...
[qxwv.shiyan.gov.cn/duhe/sdgk_dianzhan_xin](#) ... 2011-4-14 - 百度快照

[中山市五桂山区办事处信息网](#)
Warning: mysql_free_result(): supplied argument is not a valid MySQL result resource in E:\

Finding vulns in Chinese government sites



NEW GOOGLE HACKING TOOLS

Malware Diggity



Rise of Malware

NO SITES ARE SAFE

SOPHOS - Security Threat Report 2012

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

Online threats

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

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



Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – WSJ.com – June 2010

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

Massive Malware Hits Media Web Sites

Security researchers estimate that roughly 7,000 Web pages were compromised in a SQL injection attack this week, including *The Wall Street Journal* and *Jerusalem Post*.

By Mathew J. Schwartz, [InformationWeek](#)

June 10, 2010

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=225600247>

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

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



From: www.itworld.com

Mass Web attack hits Wall Street Journal, Jerusalem Post

by Robert McMillan

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

Estimates of the total number of compromised Web sites vary between 7,000 and 114,000, according to security experts. Other compromised sites include servicewomen.org and intijobs.org.



Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – LizaMoon – April 2011

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



Slashdot

stories **Viral Scareware Infects Four Million Websites**

recent

popular

ask slashdot

book reviews

games

idle

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 targets [osCommerce](#) store-management systems, is spreading rapidly. When researchers from [Armorize](#) searched for [osCommerce](#) search results suggested that the attack was spreading. Search results showed that the attack was spreading to over 5 million pages.

Armorize Malware Blog



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

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





Mass Injection Attacks

MALWARE GONE WILD

Malware Distribution Woes – mysql.com - Sept2011

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



Slashdot

stories
recent
popular
ask slashdot
book reviews
games
idle

mysql.com Hacked, Made To Serve Malware

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

Orome1 writes

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

th
g

FILED UNDER: INSECURITY COMPLEX | SECURITY

Hacked MySQL.com used to serve Windows malware

By: Elinor Mills
SEPTEMBER 26, 2011 6:10 PM PDT

Malware SaaS Services

CRIMINAL 3RD PARTY SOLUTIONS

KrebsonSecurity

In-depth security news and investigation

Service Automates Boobytrapping of Hacked Sites

101 tweets

retweet

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

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

At the very least, a decent iFramer service will allow customers to verify large lists of

The screenshot shows a dark-themed interface for an 'iFramer Service'. It features several sections:

- Security:** A list of bullet points including 'We are professionals in the field of information security...', 'Advanced algorithms for content analysis and automatic detection of the correct method of implementation.', 'Successful work with PHP, ASP and static files.', 'Daily and weekly implementation of frames in CMS Wordpress, Joomla, Joomla and many other.', 'The introduction of extensive engines.', 'Interception through Facebook.', 'Back loading of scripts on the web.', 'Determination of http-urls considerable complexity to specify the name of the script placed randomly, or static pattern.'
- Automation:** A list of bullet points including 'Maintain a list of all to generate the frame.', 'Automatic change out.', 'Automatic script being introduced frame.', 'Processing on schedule.', 'Check through IP.', 'Job file notification.', 'Automatic registration and billing.'
- Anti-virus scan:** A list of bullet points including 'Health protection of domain frame to blacklist and its databases of your group.', 'Advanced logs storage frame.'

At the bottom, there is a 'Support' button and a list of social media links: Facebook, Twitter, LinkedIn, and YouTube.



MalwareDiggity



DIGGITY TOOLKIT

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



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



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

Malware Diggity

DIGGITY TOOLKIT



GoogleDiggity CodeSearchDiggity BingDiggity LinkFromDomainDiggity DLPDiggity FlashDiggity **MalwareDiggity**

SCAN Cancel

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

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

Sites/Domains

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

Import Clear

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

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

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

Output

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

Malware Diggity



DIGGITY TOOLKIT

interpark.com does appear to have links to www.michoo.co.kr

Links to michoo.co.kr

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	6,100,000
903	zumi.pl	Business & P	6,100,000
904	natwest.com	Banking	6,100,000
905	peixurbano.com.br	Coupons & Discount Offers	6,100,000
906	soundcloud.com	Music Equipment & Technology	6,100,000
907	interpark.com	Shopping	6,100,000
908	hotpepper.jp	Dining Guides	6,100,000

Malware Diggity



DIAGNOSTICS IN RESULTS

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

Safe Browsing
Diagnostic page for michoo.co.kr

Advisory provided by Google

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

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

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

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

Black Hat SEO



SEARCH ENGINE OPTIMIZATION

- Use popular search topics du jour
- Pollute results with links to badware
- Increase chances of a successful attack



Google Trends



BLACK HAT SEO RECON

The screenshot shows the Google Insights for Search interface. The search terms are set to "All search terms" for the United States from 2004 to the present. The top search results are "facebook", "lyrics", and "you". A red callout points to the "lyrics" result, stating: "Fake lyrics web sites setup to appear in Google search results, infect you with malware upon clicking". Another red callout points to the time range dropdown, stating: "Top Google searches over past 8 years". A third red callout points to a search result snippet titled "Lada Gaga, Rihanna lyrics sites used to foist Java exploit", which includes a date of April 14, 2010, and a description of a zero-day Sun Java vulnerability.

Google Insights for Search beta

Help | Sign in | Dow

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

Web Search

United States | All subregions | All metro

2004 - present

All Categories

Web Search Interest

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

- facebook
- lyrics
- 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

lyspate

3. youtube Break

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 Plus
Adobe Reader

ALL RESULTS 1-10 of 54,900,000 results · [Advanced](#)

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

Adobe Acrobat 9 Download
[AdobeAcrobat.PDF-Software.com](#) · Ultra Fast Acrobat Download Latest Version 100% Guaranteed

Adobe Reader Download
[AdobeProReader10.com/Free](#) · New Adobe Reader Official version. 100% Support. Free Download!

Adobe Acrobat 9.3 Version
[www.PDF-9-Download.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 Adobe - Adobe Reader Accessibility
Show more results from [get.adobe.com](#)

Malware advertisements in "Sponsored sites"

Letter O replaced with 0 (zero)

Malware Defenses

BLACKHAT SEO DEFENSES

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





NON-DIGGITY ATTACK TOOLS

Other Search Hacking Tools

Maltego

INFORMATION GATHERING TOOL



The screenshot displays the Maltego Client 3.0 BETA interface. At the top, there is a title bar with the text "Maltego Client 3.0 BETA". Below the title bar is a menu bar with "Investigate" and "Manage". The main interface is divided into several sections:

- Toolbar:** Contains various icons for clipboard operations (Paste, Clear, Copy, Cut, Delete), transformation (Number of Results), search (Quick Find), selection (Select All, Invert Selection, Select parents, Add parents, Select children, Add children, Select neighbours, Add neighbours), and zooming (Zoom in, Zoom out, Zoom to fit).
- Palette:** A vertical sidebar on the left with categories like "Infrastructure" (AS, DNS Name, Domain, IPv4 Address, Location, MX Record, NS Record, Netblock, Website) and "Personal" (Email Address, Person, Phone Number, Phrase).
- Main View:** A large central area showing a network diagram. The diagram features a central node "guillaume.prigent@diateam.net" with several outgoing arrows to other nodes like "jean-baptiste.rouault@diateam.net", "florian.vichot@diateam.net", "actes.sstic.org", "blog.hynesim.org", "www.bridnet.fr", "www.ossir.org", "2009.hack.lu", "www.hynesim.fr", "diateam.net", "diateam.fr", and "diateam.com". A red arrow points from "diateam.net" back to "guillaume.prigent@diateam.net". Other nodes include "lists.trolltech.com", "libvirt.org", "vbox.innotek.de", "frederic.paul@diateam.net", and "webmaster@diateam.net".
- Detail View:** A sidebar on the right showing details for a selected entity, "actes.sstic.org". It includes a description, a link to "www.hynesim.fr", and other related information.
- Footer:** A search bar and several checkboxes for "Bookmark results", "Search all properties", "Search notes", and "Search display info".

theHarvester



FOOTPRINTING TOOL

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

```
C:\theHarvester-ng-blackhat>python theHarvester.py

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

Usage: theharvester options

-d: Domain to search or company name
-b: Data source (google,bing,bingapi,pgp,linkedin,google-profiles)
-s: Start in result number X (default 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS bruteforce for the domain name
-t: Perform a DNS TTL bruteforce
-e: Use this DNS server (ip)
-l: Limit the number of results (default 100, goes from 50 to 1000)
-h: use SHODAN data (ip) (default google 100 to 1000, option)

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

theHarvester

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

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

theHarvester



FOOTPRINTING EXAMPLE

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

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

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

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

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

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

theHarvester-ng-blackhat/microsoft.output.html

theHarvester results for :microsoft.com

Dashboard:

6	38	0	0	0
Emails	hosts	Vhost	TLD	Shodan

E-mails names found:

- mikemr@microsoft.com
- cnfrmprom@microsoft.com
- wvblog@microsoft.com
- nntp@microsoft.com
- domains@microsoft.com
- MVADean@e-mail.microsoft.com

Hosts found:

- 207.46.19.254:www.microsoft.com
- 207.46.225.250:support.microsoft.com
- 65.55.27.219:windowsupdate.microsoft.com

FOCA



INFO GATHERING AND METADATA

FOCA Free 3.0

Project Tools Options TaskList About Donate

No project

- Network
 - Clients (0)
 - Servers (0)
- Domains
- Roles
- Vulnerabilities
- Metadata
 - Documents (0/0)
 - Metadata Summary

FOCA

Select search type

- Web Searcher
- DNS Search
- Transfer Zone
- Dictionary Search
- IP Bing
- PTR Scanning
- Shodan & Robtex

Web Searcher

Using a web searcher like Google or Bing the program searches links pointing to the domain site to identify new subdomains.

Select the web search engine to use:

- GoogleWeb
- GoogleWeb
- GoogleAPI
- BingWeb
- BingAPI
- Exalead

Current search: None

Skip Start

Time	Source	Severity	Message

Conf Deactivate AutoScroll Clear Save log to File

SHODAN



HACKER SEARCH ENGINE

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

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

Italy	20
China	14
United States	7
Spain	6
Greece	5

Below the table, a search result is displayed for the IP address **123.116.195.215**. The result includes the following information:

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

Red callout boxes highlight specific details: "NAS storage devices located" points to the IP address; "Default username is 'admin'" points to the WWW-Authenticate header; and "Default USER:admin" points to the realm value in the WWW-Authenticate header.

Advanced Defenses

PROTECT YO NECK





Traditional Defenses

GOOGLE HACKING DEFENSES

- “Google Hack yourself” organization
 - Employ tools and techniques used by hackers
 - Remove info leaks from Google cache
 - <http://www.google.com/remove.html>
- Regularly update your robots.txt
 - Or robots meta tags for individual page exclusion
- Data Loss Prevention/Extrusion Prevention Systems
 - Free Tools: OpenDLP, Senf
- Policy and Legal Restrictions





Existing Defenses

"HACK YOURSELF"



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



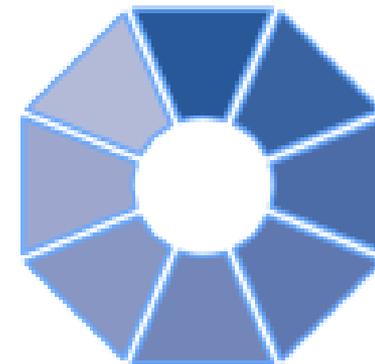
Advanced Defenses

NEW HOT SIZZLE



Stach & Liu now proudly presents:

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



Google Hacking Alerts

ADVANCED DEFENSES



Google Hacking Alerts

- All hacking database queries using **Google alerts**
- Real-time vuln updates to >2400 hack queries via RSS
- Organized and available via **Google reader** importable file

Google alerts Manage your Alerts [email]@gmail.com | Settings | FAQ

Your Google Alerts

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

GHDB regexs made into Google Alerts

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

Google Hacking Alerts

ADVANCED DEFENSES



Google reader

All items (1000+)

People you follow

Explore

Subscriptions

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

Google Alerts - "mysql error with query"

Show: 11 new items - all items

Mark all as read

Refresh

Feed settings...

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

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

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

Add star Like Share Share with note Email Add tags

Several thousand GHDB/FSDB vuln alerts generated each day

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

Bing Hacking Alerts

ADVANCED DEFENSES



Bing Hacking Alerts

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

The screenshot shows a Google Reader interface with a list of subscriptions on the left and a feed of items on the right. The top of the feed shows a search query: **Bing: intitle:"Snap Server" intitle:"Home" "Active Users" »**. Below this, several items are listed, including "Snap Server WELW-SNAP [Home]", "Snap Server CORESERVER [Home]", "Snap Server GSTI [Home]", "adsphotographer.com - SNAP55373", "Snap Server SNAP824929 [Home]", "Snap Server SAINTSNAP [Home]", "Snap Server DIGITALDATA1 [Home]", and "Snap Server FTP-SERVER [Home]". A red callout box points to the "Snap Server FTP-SERVER [Home]" item with the text "SNAP network attached storage servers exposed".



Bing/Google Alerts

LIVE VULNERABILITY FEEDS



World's Largest Live Vulnerability Repository

- Daily updates of *~3000 new hits per day*





Diggity Alerts

One Feed to Rule Them All

ADVANCED DEFENSE TOOLS

Diggity Alert Fundle Bundle



FUNdle Bundle

ADVANCED DEFENSES



 **Google reader** DIGGITY HACKING ALERTS

"Diggity Hacking Alerts" bundle created by Stach

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

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

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

[Sign in](#) to subscribe

[Get started with Google Reader](#)

[Atom feed](#)

[OPML file](#)

Debris Removal - News & Information

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

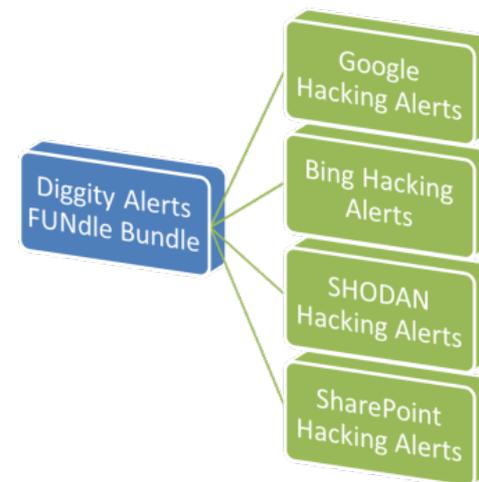
(New Hanover County)--- New Hanover County and municipal of ... with representatives of the Federal Emergency Management Agency ...
www.nhcgov.com/News/_layouts/listform.aspx?...

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



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

1 subscriber



☆ Bing NEW: intitle:"BadBlu:	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:"BadBlu:	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:"BadBlu:	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-	6:32 AM	⌵
☆ Bing NEW: intitle:"AppSen	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:"AppSen	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:"AppSen	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:"AppSen	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:"AppSen	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:"AppSen	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 r	Search - © 2011 ILO Portal - ILO Decent Work Team and Office for the ... Powered by mnoGoSearch - free web search engine software	6:26 AM	⌵
☆ Bing NEW: "Powered by r	Google Hacks - PawnGame.com - Multiplayer Flash Gaming - "Powered by mnoGoSearch - free web search engine software" "powered by openbsd" +"powered by	6:26 AM	⌵
☆ Bing NEW: "Powered by r	Circuit Breaker Reset Philosophies for aircraft - CB reset philosophy ... Powered by mnoGoSearch - free web search engine software	6:26 AM	⌵

FUNdle Bundle

MOBILE FRIENDLY



Google Reader

Diggity Hacking Alerts

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

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

Google reader

« Feeds **Diggity Hacking Alerts**  

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



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



ADVANCED DEFENSE TOOLS

SHODAN Alerts



SHODAN Alerts



FINDING SCADA SYSTEMS

SHODAN

» Top countries matching your search

Canada	13
Finland	12
United States	8
Sweden	6
Denmark	6

Using SHODAN to find SCADA web admin interfaces

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="i**SCADA** 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
 dsl-main-66-18-233-232-

SHODAN Alerts

FINDING SCADA SYSTEMS



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

THREAT LEVEL

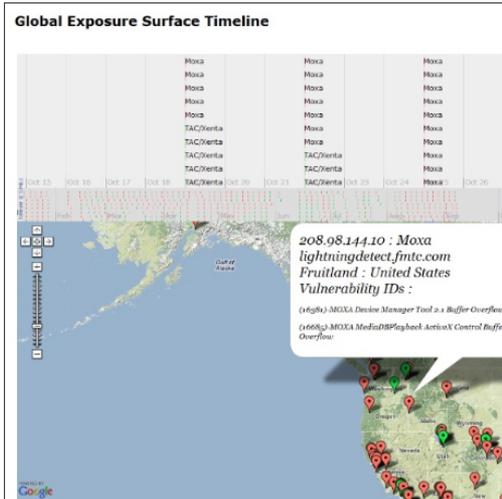
PRIVACY, CRIME AND SECURITY ONLINE

10K Reasons to Worry About Critical Infrastructure

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

708 83 140
Tweet +1 Share

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

SHODAN ALERTS

"SHODAN Alerts" bundle created by stach

Description: SHODAN RSS Alerts

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

There are [26 feeds](#) included in this bundle

[+ Subscribe](#)

[67.228.99.229:80](#)
via [SHODAN - Search: Server: LiteSpeed country:CN](#) on 8/2/11

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

[184.172.42.27:80](#)
via [SHODAN - Search: Server: LiteSpeed country:CN](#) on 8/2/11

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

SHODAN Alerts

« Feeds

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

Bing/Google Alerts

THICK CLIENTS TOOLS



Google/Bing Hacking Alert Thick Clients

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



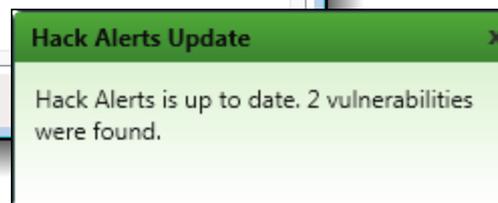
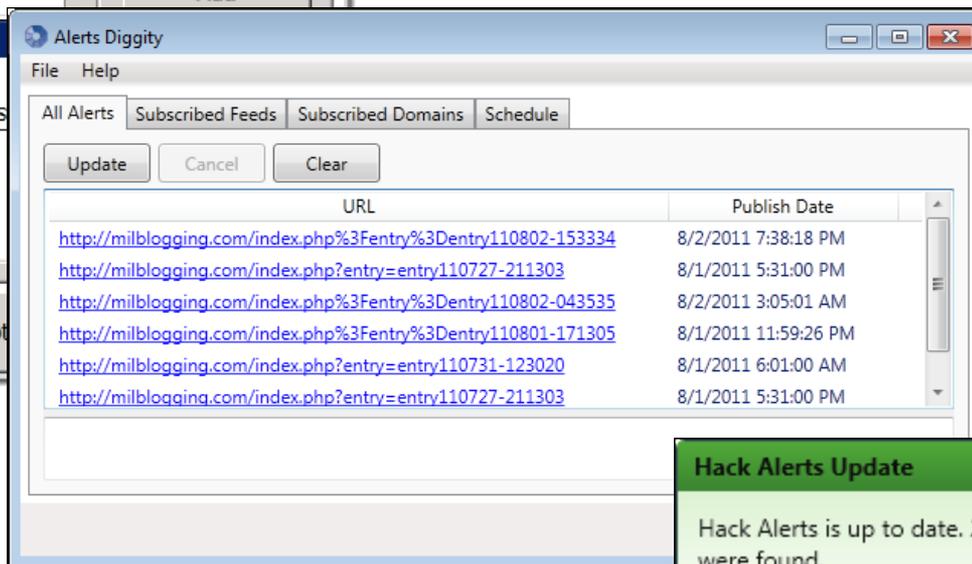
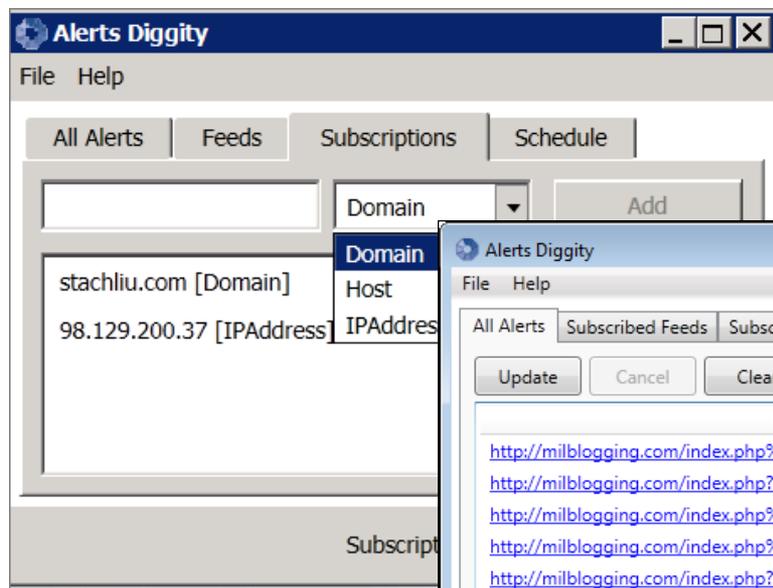


ADVANCED DEFENSE TOOLS

Alert Diggity

Alerts Diggity

ADVANCED DEFENSES



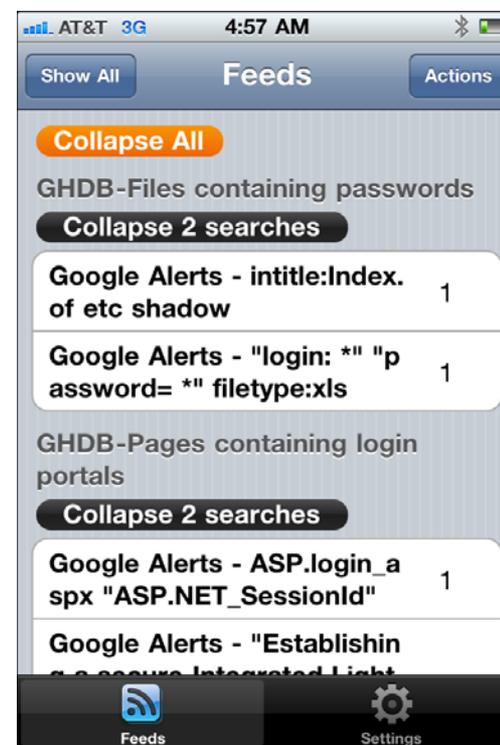
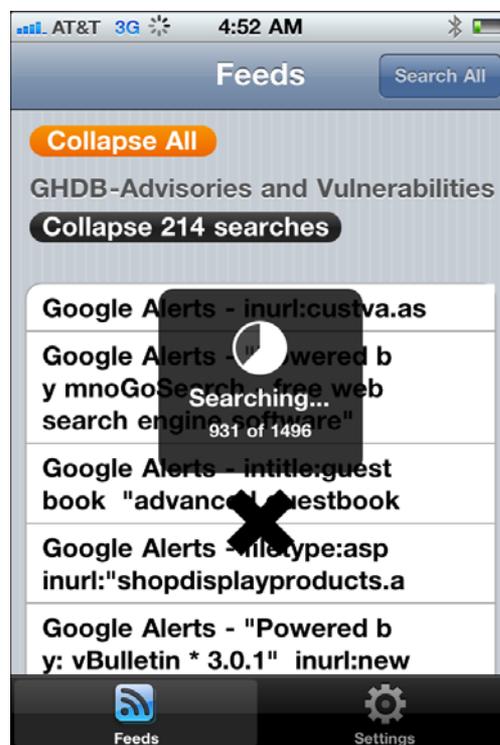
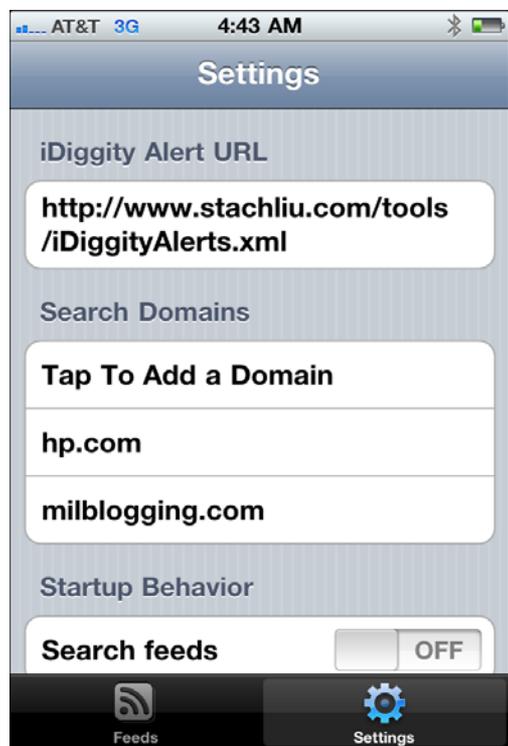


ADVANCED DEFENSE TOOLS

iDiggity Alerts

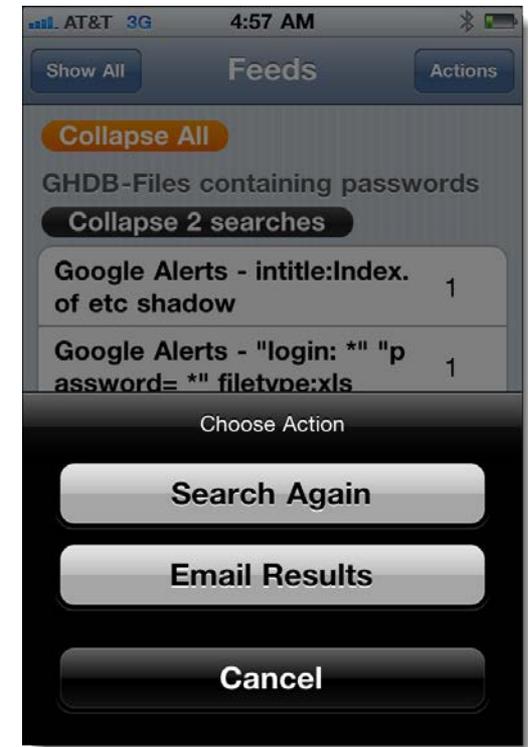
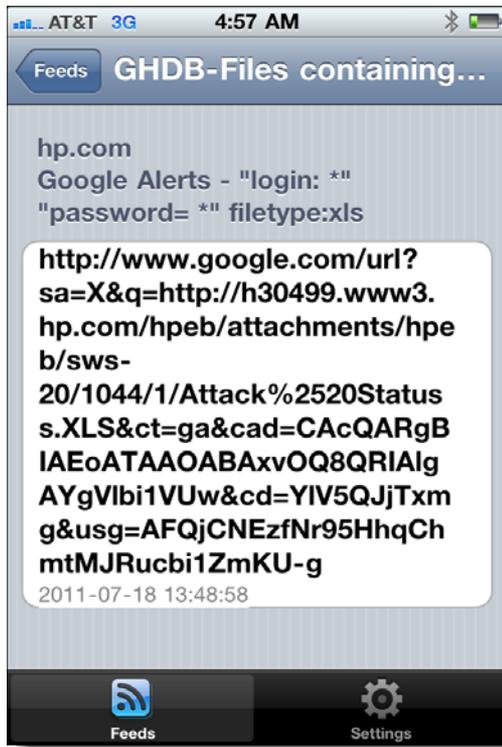
iDiggity Alerts

ADVANCED DEFENSES



iDiggity Alerts

ADVANCED DEFENSES



New Defenses

"GOOGLE/BING HACK ALERTS"

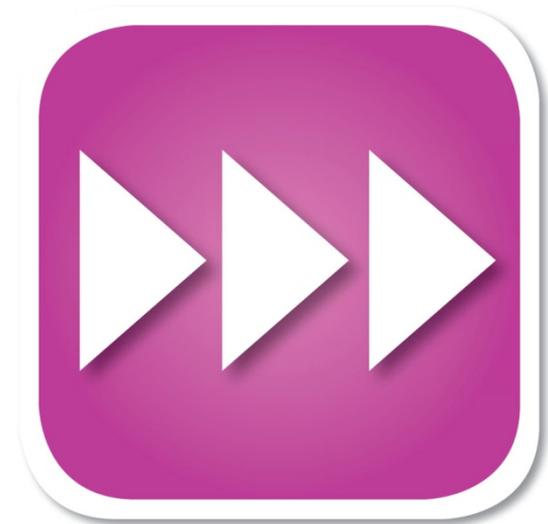


- ✓ Tools exist
- ✓ Convenient
- ✓ Real-time updates
- ✓ Multi-engine results
- ✓ Historical archived data
- ✓ Multi-domain searching



Future Direction

IS NOW



Diggity Alert DB

DATA MINING VULNS



Database Browser

File View Connections Execute Help

Connections: x 0001 select AlertTable.* from AlertTable
0002

AlertDB

Tables:

AlertTable

Drag a column header here to group by that column

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

0001 select AlertTable.* from AlertTable
0002

Drag a column header here to group by that column

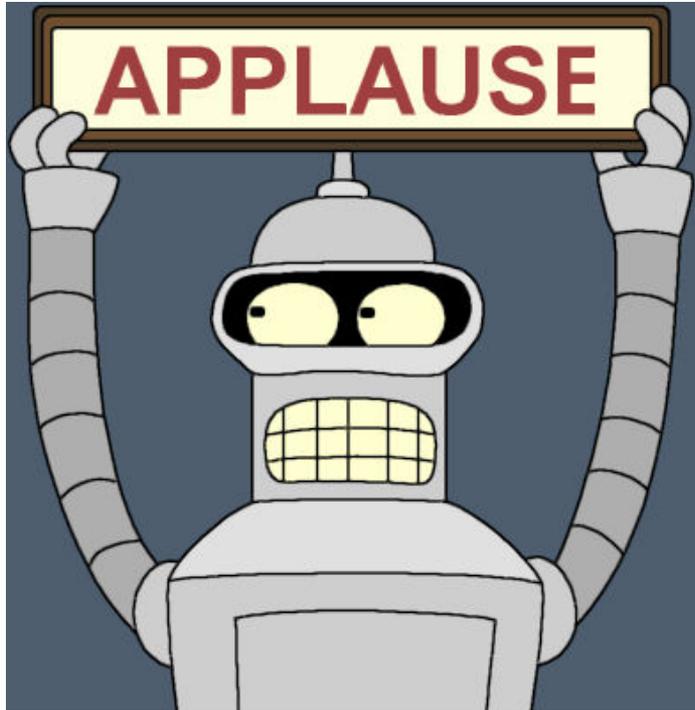
PubDate	DateGRShared2	Title	URLClean	DiggityFeedSource
2011-07-31T00:23:07Z	Sat Jul 30 17:23:07 2011	PHP Tutorials: Form Data Display and Sec	http://blog.phpmoz.org/php-tutorials-form-data-display-and-security	Google Alerts - data filety
2011-07-30T23:41:34Z	Sat Jul 30 16:41:34 2011	error_log	http://celestedesignsusa.com/error_log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



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/>