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**

- **Google**: maintains ~40-60 billion page index size

- **Bing**: ~11-12 billion pages indexed now

Around April 2012 - Bing makes major push in expanding their search index size
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)
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
Diggity Tools

PROJECT OVERVIEW

Google Hacking Diggity

HISTORY OF GOOGLE HACKING

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

## NEW ATTACK TOOLS

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

NEW ACROSS ALL ATTACK TOOLS
## Diggity Scraping

### Proxies Specification

<table>
<thead>
<tr>
<th>Bad: (36)</th>
<th>Untested: (15)</th>
<th>Good: (249)</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://119.73.47.165:8118">http://119.73.47.165:8118</a></td>
<td></td>
<td><a href="http://177.69.203.242:8080">http://177.69.203.242:8080</a></td>
</tr>
</tbody>
</table>

- **Auto-Find**: Automatically find open web proxies to use.
- **Test**: Test to ensure proxies are actually working and are fast.
Diggity Scraping

MANUAL PROXIES SPECIFICATION
Advanced Attacks

WHAT YOU SHOULD KNOW
Diggity Core 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

SLDB Updates in Progress

- Example: SharePoint Google Dictionary
New Features
IP ADDRESS RANGES

GoogleDiggity can now search for IP Address Ranges

GoogleDiggity automatically converts IP address ranges of different formats to site:10.1.1.* notation

GoogleDiggity now can search IP address ranges
New Features

TARGETING HTTP ADMIN CONSOLES

Searching for web admin interfaces on non-standard HTTP ports

[Google search examples showing how to search for web admin interfaces on non-standard HTTP ports]
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

[Image of the Google Diggity interface]

STACH&LIU
Hacking CSE’s

ALL TOP LEVEL DOMAINS

All Top Level Domains

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

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

'!' - 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

D I G G I T Y  C O R E  T O O L S

Demonstrating Bing's IP address reverse lookup feature
NEW GOOGLE HACKING TOOLS

Bing Hacking Database v2.0
BHDB v2.0 – Updates

• Bing hacking database

• Bing hacking limitations
  • Disabled \texttt{inurl}, \texttt{link} and \texttt{linkdomain} directives in March 2007
  • No support for \texttt{ext}, \texttt{allintitle}, \texttt{allinurl}
  • Limited \texttt{filetype} functionality
    • Only 12 extensions supported

• UPDATES (2012)
  • \texttt{ext}: functionality now added
  • \texttt{inurl}: work around by using \texttt{instreamset:url}

• New BHDB 2.0
  • Several thousand more Bing dorks!

Wordpress database passwords in config files
NEW GOOGLE HACKING TOOLS

NotInMyBackYard
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

Examples:

- Dump Monitor @dumpmon
- Slexy.org raws/2TU0ZWFr
- PasteBin.com raw.php?x=HlA

Twitter feed looking for passwords and sensitive info across PasteBin type sites.

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

Example, thousands of passwords found.
Cloud Docs Exposures

Public cloud storage document exposures

Looking for sensitive data leaks in Dropbox cloud storage

Database dump files on Microsoft SkyDrive

Cisco config files with passwords in Google Docs files
Cloud Docs Exposures

ROBOTS.TXT IS DEAD

Personal photo galleries exposed
Data Loss In The News

Major Data Leaks

• Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet

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 @elnormills

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

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

XLS IN CLOUD EXAMPLE

Look for the word “password”

Look at Amazon S3 cloud storage uploads

Look in all Microsoft Excel spreadsheets
Cloud Docs Exposures

Public cloud storage document exposures

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

Username and passwords for bank accounts, email, and everything else
NotInMyBackYard tool scours Web for your personal data

By Byron Acosta, USA TODAY

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.

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’.” NotInMyBackYard Diggity makes it easy to search for your sensitive information in third-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

Google search for site:/com.*

All non-port 80/443 HTTP admin consoles for .com

Google search for site:/216.75.*.*

IP address range search for HTTP admin interfaces on non-standard ports
Port Scanning

Targeting Port Ranges

Searching for specific port ranges

Site: com:* 8000..9000

Targeting ports 8000-9000

Site: com:* 5000..6000

Port scan 5000-6000
PortScanning

Targeting specific HTTP ports example

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

Found ~66k targets for Plesk Panel exploit.

KrebsonSecurity

Plesk 0Day For Sale As Thousands of Sites Hacked

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.
PortScan Diggity

Targeting HTTP Admin Consoles

Lists open ports per host

Looking for open ports on *.com

STACH&LIU
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`

<table>
<thead>
<tr>
<th>Code</th>
<th>Results 1 - 10 of about 2,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>post.asp</td>
<td></td>
</tr>
</tbody>
</table>

45: `strSql = "SELECT * from reply where reply_id = " & Request.QueryString("reply_id")`
46: `msg = "<br><br>"`  

57: `strSql = "SELECT T.Message from Topics where Topic_id = " & Request.QueryString("reply_id")`
58: `msg = "<br><br>"`

www.cnarts.net/web/download/software/bbs/tradeforum.zip - Unknown - ASP - More from tradeforum.zip »
CodeSearch Diggity

Amazon AWS Cloud keys stored in plaintext

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][^] chrome/content http://www.google.com/codesearch/p?hl=en#ulAl
Amazon Keys EC2 ec2[^d][^A-Z0-9][20][^] trunk/src/efaw 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#nF
Amazon Keys Amazon Amazon.^[^][^][^] trunk/lookups.py http://www.google.com/codesearch/p?hl=en#I420

Output

```<pre>  .ec2 ec2 = new J<b>ec2("AK[REDACTED]ZEHQ"</b>, "", ]+RClku0EeAD6");
</pre>```
Cloud Security

NO PROMISES...NONE

Amazon AWS Customer Agreement
• http://aws.amazon.com/agreement/#10

10. Disclaimers.

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

CREATE YOUR OWN SEARCH ENGINES

Web Data Extraction
Automate virtually anything you can do with a web browser

Query the World
Tap the web's massive database.

80legs
The most powerful web-crawler ever.
Google Code Search

VULNS IN OPEN SOURCE CODE

Develop Regex → Find Popular Web OSS → Verify Vulnerabilities

Publish Advisory
Update SLDB
Google Code Search

VULNS IN OPEN SOURCE CODE

Develop Regex → Find Popular Web OSS → Verify Vulnerabilities → Search Web

Mass Injection Attacks
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

```
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"
```

Default username is 'admin'

NAS storage devices located
SHODAN

Finding SCADA Systems

Using SHODAN to find SCADA web admin interfaces
Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software

MIAMI, Florida — A group of researchers said they have released vulnerabilities in industrial control systems used in critical infrastructures in order to teach a lesson about the importance of securing those systems.

The vulnerabilities were found in widely used software from companies like Rockwell Automation, Schneider Electric, and Honeywell.

10K Reasons to Worry About Critical Infrastructure

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.
Finding SCADA Systems via SHODAN Diggity

<table>
<thead>
<tr>
<th>Category</th>
<th>Search String</th>
<th>URL</th>
<th>Hostnames</th>
<th>City</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA</td>
<td>Niagara Web Server</td>
<td><a href="http://193.185.169.90/">http://193.185.169.90/</a></td>
<td></td>
<td></td>
<td>Finland</td>
</tr>
<tr>
<td>SCADA</td>
<td>Niagara Web Server</td>
<td><a href="http://12.171.57.87/">http://12.171.57.87/</a></td>
<td></td>
<td></td>
<td>United States</td>
</tr>
<tr>
<td>SCADA</td>
<td>Niagara Web Server</td>
<td><a href="http://216.241.207.94/">http://216.241.207.94/</a></td>
<td>sclop-ip94.schinernet. Colorado City</td>
<td>United States</td>
<td></td>
</tr>
<tr>
<td>SCADA</td>
<td>Niagara Web Server</td>
<td><a href="http://206.82.16.227/">http://206.82.16.227/</a></td>
<td>niagarafred.norleb.l1 Lancaster</td>
<td>United States</td>
<td></td>
</tr>
<tr>
<td>SCADA</td>
<td>Niagara Web Server</td>
<td><a href="http://184.187.11.158/">http://184.187.11.158/</a></td>
<td></td>
<td></td>
<td>Omaha United States</td>
</tr>
</tbody>
</table>

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
NEW GOOGLE HACKING TOOLS

Bing LinkFromDomainDiggity
Bing LinkFromDomain

Bing's linkfromdomain directive used to find external links on your sites

External links then sorted and extracted into: applications, host names, and domains
Bing LinkFromDomain

FOOTPRINTING LARGE ORGANIZATIONS

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

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

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

DLP Diggity
DLP Diggity

LOTS OF FILES TO DATA MINE

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

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

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

Bing
filetype:doc

Bing
filetype:pdf

1-10 of 146,000,000 results · Advanced
DLP Diggity

MORE DATA SEARCHABLE EVERY YEAR

Google Results for Common Docs

PDF  DOC  XLS  TXT

Data Loss In The News

MAJOR DATA LEAKS

• Groupon.com Leaks 300,000 users emails and passwords
  • filetype:sql hotmail gmail password
Data Loss In The News

**MAJOR DATA LEAKS**

- Yale Alumni 43,000 SSNs Exposed in Excel Spreadsheet

---

---

---
DLP Diggity

D I G G I T Y  T O O L K I T

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

PRACTICAL EXAMPLES

DLP Diggity - # 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 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.

Google CSE providing search access to XSS.CX vulnerability results

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

![FlashDiggity Toolkit](image-url)

```java
if (UserName.text == 'mizzico' && PassWord.text == 'furniture') {
  // Code snippet
}
```
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\n
• 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

STACH&LIU
NEW GOOGLE HACKING TOOLS

Baidu Diggity
BaiduDiggity
CHINA SEARCH ENGINE

• Fighting back

Finding vulns in Chinese government sites
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 Matthew J. Schwartz, InformationWeek
June 10, 2010

“Every time I load Jpost site, I get malware,” one user posted on Tuesday, referring to the Jerusalem Post. Sure enough, the Web sites of the Jerusalem Post and the Association of Christian Schools 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 Indiausa.org.
Mass Injection Attacks

Malware Distribution Woes – LizaMoon – April 2011

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

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..."
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 suggest
search results showed th

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, OMSCOMMERCE, WEB MALWARE
Watering Hole Attacks

Malware Gone Wild

Malware Distribution Woes – mysql.com - Sept 2011

• Popular websites victimized, become malware distribution sites to their own customers
Watering Hole Attacks

Malware Distribution Woes – LATimes.com - Feb2013

• Popular websites victimized, become malware distribution sites to their own customers
Watering Hole Attacks

MALWARE GONE WILD

Malware Distribution Woes – iphonedevsdk.com - Feb2013
• Popular websites victimized, become malware distribution sites to their own customers

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 Oday 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 Watering Hole breach.

Four days after the news on Facebook, the 19th February, the same "popular mobile developer Web forum" was victim of a "Watering Hole" attack. People briefed on the breach included defense contractors.

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

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 jQuery we can find an interesting submission, the 23 January, who reveal that some Java code was involved during the visit of
Inconvenient Truth

D**H E A D A L E R T S Y S T E M

Malware Black List Woes

• Average web administrator has no idea when their site gets black listed
Malware SaaS Services

CRIMINAL THIRD-PARTY SOLUTIONS

Service Automates Boobytrapping of Hacked Sites

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 quickly update lists of...
NEW GOOGLE HACKING TOOLS

Malware Diggity
MalwareDiggity

DIGGITY TOOLKIT

1. Leverages Bing’s \texttt{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**

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

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

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
Malware Diggity

D I A G N O S T I C S  I N  R E S U L T S

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

Site is listed as suspicious – visiting this website may harm your computer.

Part of this site was listed for suspicious activity a few days.

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).
NEW GOOGLE HACKING TOOLS

BingBinaryMalwareSearch (BBMS)
Bing Malware Search

Targeting known malware signatures

Malware: Trojan.Dropper.Vbs.Dummytag.A

www.terra.es
Time Date Stamp: 37fb2583. Symbols Pointer: 00000000 ... Address of Entry Point: 00001020
Base of Code: 00001000 ... Size of Image: 00008000. Size of Headers: 00000400
www.terra.es/personal7/sanchezsignes/PuRSuit.e_xe
Black Hat SEO

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

Black Hat SEO Recon

Top Google searches over past 8 years

Fake lyrics web sites setup to appear in Google search results, infect you with malware upon clicking

Lada Gaga, Rihanna lyrics sites used to foist Java exploit

Dan Kaplan April 14, 2010

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

Google announced they've searched their 'Insights for Search' tool, which contains a multitude of searches pertaining to elections.

Looking at the most popular searches, their official blog reported, adding, "We've looked at foreclosures, as well as immigration at the border with Mexico. We've even looked at some candidate's predicted vote totals, then used the error for other candidates. Oddly enough, the data was extremely accurate in one contest [in Florida], where the breaking news was making a difference in the personal vote of a different candidate.

Searching your way to the ballot box

10/27/2010 02:54:00 PM

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

Malware ads in search engines

Malware advertisements in "Sponsored sites"

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

- Identify Malware Links
- Mass Inject Competition
- Competition PageRank is 0
- Competition Black Listed
- Profit
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

Only a 8.5% 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 May 2012

• 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

- Identify External Links
- Identify Incoming Links
- Detect Infections
- Compare to Black List
- Alert
Monitoring Malware

Google Safe Browsing Alerts for Network Administrators

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

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.

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

HackAlert™
Secure Your Web Applications
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.
Disable Java

MALWARE DEFENSES

1. Type in "Java"
2. Click here

Un-check box
To disable Java in specific browsers only, go to advanced settings
Help from Google

Google releases “Help for Hacked Sites” – 12Mar2013
Non-Diggity Attack Tools

Other Search Hacking Tools
Maltego

INFORMATION GATHERING TOOL

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

INFORMATION GATHERING TOOL

Now we have a bunch of email addresses for our target microsoft.com

Double-click and change to 'microsoft.com'

We can try to find microsoft.com email addresses using 3 different info gather methods by clicking “All in this set” here.

Next, right click on the entry, and go to ‘Run Transform’
Maltego
INFORMATION GATHERING TOOL

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

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

FOOTPRINTING TOOL

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

Usage: theharvester options

-d: Domain to search or company name
-b: Data source (google, bing, bingapi, pgp, linkedin, google-profiles, people123, jigsaw, all)
-s: Start in result number X (default 0)
-v: Verify host name via dns resolution and search for virtual hosts
-f: Save the results into an HTML and XML file
-n: Perform a DNS reverse query on all ranges discovered
-c: Perform a DNS brute force for the domain name
-t: Perform a DNS TLD expansion discovery
-e: Use this DNS server
-l: Limit the number of results to work with (bing goes from 1 to 500, so default is 1)

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

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

- Tracking results...
  - 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
- 65.55.13.30:windowsupdate.microsoft.com
- 157.56.36.139:windows.microsoft.com
- 65.55.81.30:windows.microsoft.com
- 65.55.227.140:office.microsoft.com
- 65.55.11.139:schemas.microsoft.com
- 157.56.13.237:technet.microsoft.com
- 157.56.12.174:msdn.microsoft.com
- 131.107.115.214:mailb.microsoft.com
- 65.55.103.99:forums.microsoft.com
- 157.56.36.232:apps.microsoft.com
- 65.55.164.208:ie.microsoft.com
- 65.55.19.60:lync.microsoft.com
- 64.4.11.25:go.microsoft.com

Saving file
C:\theHarvester-2.2a>
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:\>
SpiderFoot 2.0

FOOTPRINTING TOOL

New Scan
Scan Name
Descriptive name for this scan.

Target Domain Name
e.g. scantarget.com

Modules

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

Run Scan
Note: Scan will be started immediately.
FOCA

INFO GATHERING AND METADATA
SHODAN

HACKER SEARCH ENGINE

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

FOOTPRINTING DNS SEARCH ENGINE

- DNS/IP Addr records hacker search engine

Deep Magic DNS

@deepmagicdns

A searchable DB of all 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

Twitter feed tracking public data leaks via PasteBin.com

Usernames, emails, and password hashes of compromised website posted to PasteBin.com
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)
Advanced Defenses

PROTECT YOUR 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

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

<table>
<thead>
<tr>
<th>Search terms</th>
<th>Type</th>
<th>How often</th>
<th>Email length</th>
<th>Deliver to</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Host=&quot;, intext:UserPassword=&quot;</code></td>
<td>Web</td>
<td>as-it-happens</td>
<td>up to 50 results</td>
<td>Feed</td>
</tr>
<tr>
<td>`&quot;Dumping data for table (username</td>
<td>password)&quot;`</td>
<td>Web</td>
<td>as-it-happens</td>
<td>up to 50 results</td>
</tr>
<tr>
<td><code>&quot;Dumping data for table&quot;</code></td>
<td>Web</td>
<td>as-it-happens</td>
<td>up to 50 results</td>
<td>Feed</td>
</tr>
<tr>
<td><code>&quot;phpMyAdmin MySQL-Dump &quot;INSERT INTO &quot;</code></td>
<td>Web</td>
<td>as-it-happens</td>
<td>up to 50 results</td>
<td>Feed</td>
</tr>
</tbody>
</table>

RSS Feeds generated that track new GHDB vulnerable pages in real-time.
Google Hacking Alerts

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

Several thousand GHDB/FSDB vuln alerts generated each day
Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Real-time vuln updates to >900 Bing hack queries via RSS
Bing/Google Alerts

LIVE VULNERABILITY FEEDS

World’s Largest Live Vulnerability Repository

- Daily updates of \(~3000\) new hits per day
ADVANCED DEFENSE TOOLS

Diggity Alert Fundle Bundle
FUNdle Bundle

ADVANCED DEFENSES

"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 piece 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? from 9/11/11

(New Hanover County) — New Hanover County and the City of Wilmington have been working closely with representatives of the Federal Emergency Management Agency (FEMA) to ensure that residents are well informed about the recovery process following Hurricane Irene.

www.nhcgov.com/News/_layout/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/00017421.pdf

3762 RSS feeds from GHDB, FSDB, SLDB all consolidated into 1 RSS feed using Google Reader Bundles.
ADVANCED DEFENSE TOOLS

SHODAN Alerts
SHODAN Alerts

FINDING SCADA SYSTEMS

Using SHODAN to find SCADA web admin interfaces
SHODAN Alerts

Finding SCADA Systems

10K Reasons to Worry About Critical Infrastructure
By Kim Zetter  January 24, 2012  6:30 am | Categories: Cybersecurity

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

SHODAN RSS FEEDS

Google reader

"SHODAN Alerts" bundle created by stach

Description: SHODAN RSS Alerts
A bundle is a collection of blogs and websites hand-selected on a particular topic or interest. You can keep up to date with the latest by subscribing in Google Reader.

There are 26 feeds included in this bundle

Google reader

SHODAN Alerts

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 Accept-Ranger...

- 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 Server:...

- 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:

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

- Google Alerts - "login: "*
  "password= "*
  filetype:xls

http://www.google.com/url?q=http://h30499.www3.hp.com/hpeb/attachments/hpeb/sws-20/1044/1/Attack%2520Statuss.XLS&ct=ga&cad=CACQRgBAEoATAAABAxvOQ8QRIAlgAYgVlbiTVUw&cd=YIV5QjTxm&usg=AFQjCNFzNr95HhqChmtMRucbi1ZmKU-g

- Google Alerts - intitle:Index.
of etc shadow
  1

- Google Alerts - "login: "* "password= "*
  filetype:xls
  1

Choose Action

Search Again

Email Results

Cancel
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
Connections: AlertDB
Tables: AlertTable

0001 select AlertTable.* from AlertTable
0002

Drag a column header here to group by that column

<table>
<thead>
<tr>
<th>PubDate</th>
<th>DateSRShared2</th>
<th>Title</th>
<th>URLClean</th>
<th>DiggityFeedSource</th>
</tr>
</thead>
</table>
Future Direction

I S N O W
Diggity Dashboards
COMING SOON

Google Charts

Mobile BI Apps

DIGGITY ALERTS
CLOUD DATABASE
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/