Lord of the Bing

Taking Back Search Engine Hacking From Google and Bing

30 July 2010

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

STACH&LIU

Agenda

OVERVIEW

- Introduction
- Advanced Attacks
  - Google/Bing Hacking
  - Other OSINT Attack Techniques
- Advanced Defenses
- Future Directions

Goals

DESIRED OUTCOME

- *To understand* Google Hacking
  - Attacks and defenses
  - Advanced tools and techniques
- *To think differently* about exposures caused by publicly available sources
- To blow your mind!

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*.

Quick History

GOOGLE HACKING RECAP

Dates	Event
2004	Google Hacking Database (GHDB) begins
May 2004	Foundstone SiteDigger v1 released
2005	Google Hacking v1 released by Johnny Long
Jan. 2005	Foundstone SiteDigger v2 released
Feb. 13, 2005	Google Hack Honeypot first release
Jan. 10, 2005	MSNPawn v1.0 released
Dec. 5, 2006	Google stops issuing Google SOAP API keys
…	…

Quick History

GOOGLE HACKING RECAP

Dates	Event
Mar. 2007	Bing disables inurl: link: and linkdomain:
Nov. 2, 2007	Google Hacking v2 released
Mar. 2008	cDc Goolag - gui tool released
June 3, 2009	Bing goes online
Sept. 7, 2009	Google shuts down SOAP Search API
Nov. 2009	Binging tool released
Dec. 1, 2009	FoundStone SiteDigger v 3.0 released
2010	Googlag.org disappears

Threat Areas

WHAT YOU SHOULD KNOW

Google/Bing Hacking

SEARCH ENGINE ATTACKS

- Our favorites are **Google** and **Bing**
- **Crawl** and **Index**
- **Cache** and **RSS** are forever
- **Query** modifiers
  - site:target.com
  - related:target.com
  - filetype:xls
  - ip:69.63.184.142

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)

Attack Targets

GOOGLE HACKING DATABASE

Examples

Error Messages

- filetype:asp + "[ODBC SQL"
- "Warning: mysql_query()" "invalid query"

Files containing passwords

- inurl:passlist.txt

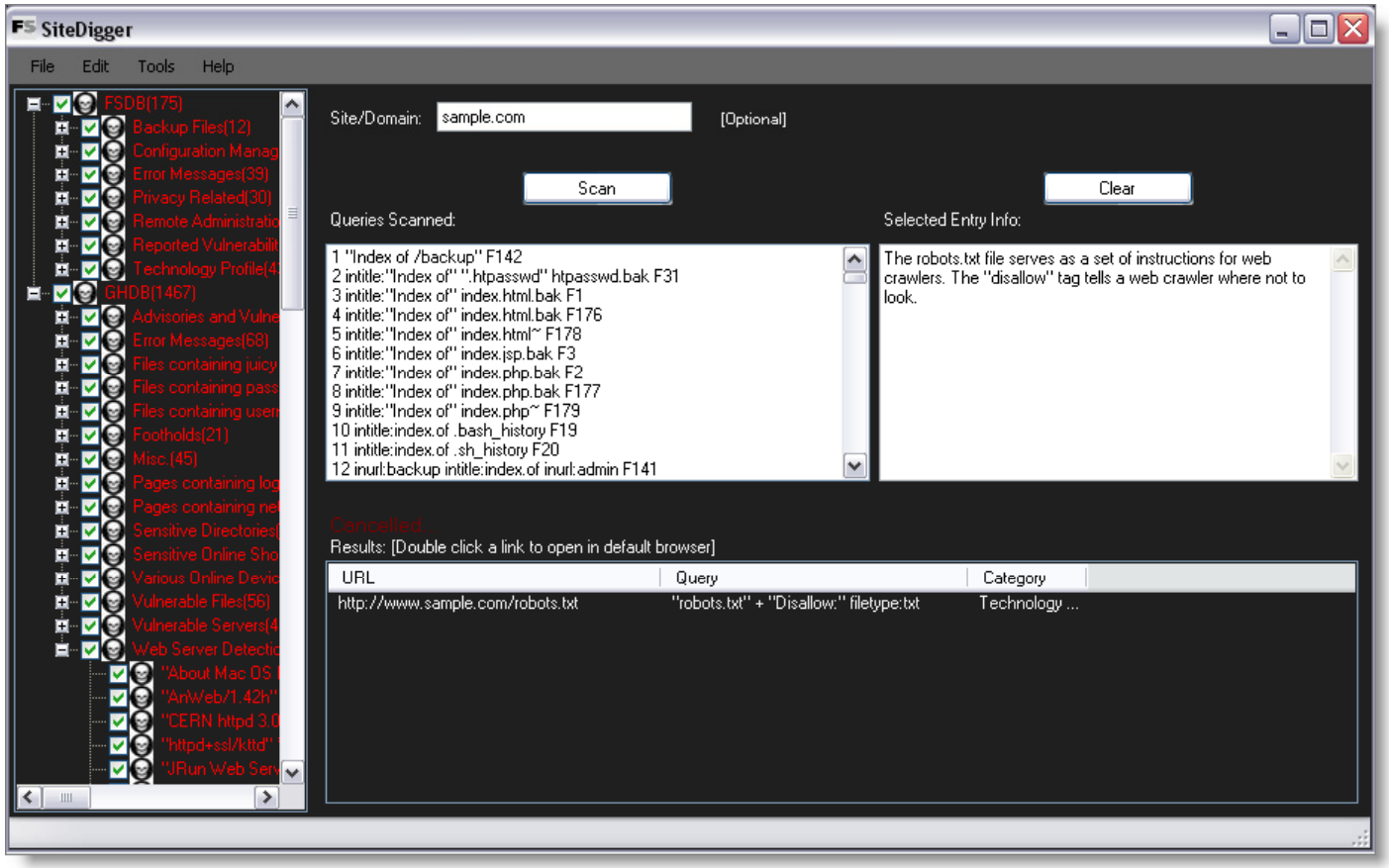
Google Hacking Toolkit

STATE OF THE ART

- SiteDigger v3.0
  - Uses Google AJAX API
    - Not blocked by Google
    - But restricted to 64 results/query
- Binging
  - Uses Microsoft Bing search engine
  - Limited domain/ip profiling utils
- Gooscan, Goolag
  - Work still, but get blocked by Google bot detection
  - Download sites no longer around

Google Hacking Toolkit

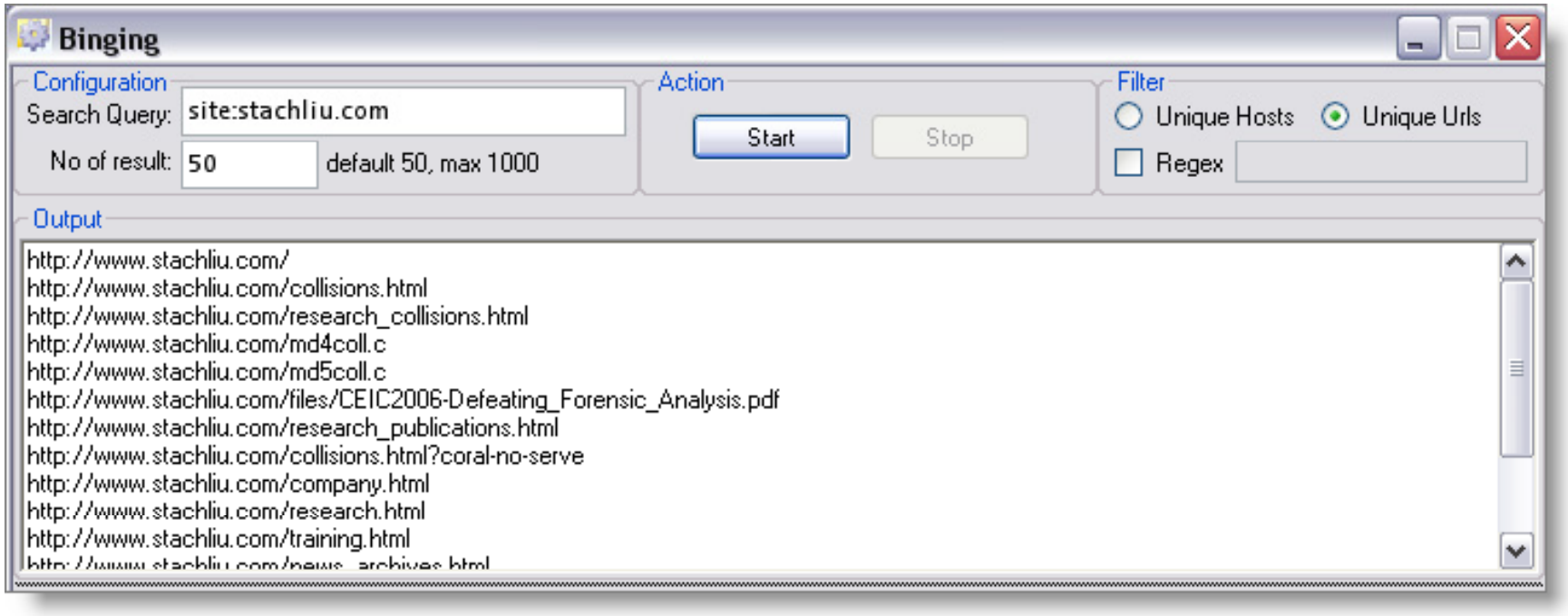
FOUNDSTONE SITEDIGGER



STACH&LIU

Google Hacking Toolkit

BINGING



NEW GOOGLE HACKING TOOLS

DEMO

New Toolkit

STACH & LIU TOOLS

GoogleDiggity

- Uses Google AJAX API
  - Not blocked by Google bot detection
- Can Leverage Google custom search

BingDiggity

- Company/Webapp Profiling
  - Enumerate: URLs, IP-to-virtual hosts, etc.
- Bing Hacking Database (BHDB)
  - Regexs in Bing format

New Toolkit

GOOGLEDIGGITY

```
C:\GoogleDigity\bin\Debug>GoogleDiggity.exe /?

        +============================================================+
        |               GoogleDiggity - Version 0.1                  |
        |       Google Hacking Utility - Using Google AJAX API       |
        |               By: Fran Brown  and  Rob Ragan               |
        |       Stach & Liu, LLC - http://www.stachliu.com           |
        +============================================================+

        ** Note: Google AJAX API won't block you, but does limit you to 64 results per query.

        Usages: GoogleDiggity.exe [-q Google_Search_Query] [-d Target_Domain] [-k Google_CustomSearchEngine_ID]
                GoogleDiggity.exe [-f Google_Search_Query_File] [-d TargetDomain] [-k GoogleCustomSearchEngineID]

        -q  [Google search query]
            Optional, can alternatively load queries from file using the -f option.
        -f  [Google Hack queries file]
            Optional, text file contain Google search queries, one per line.
            GHDB and FSDB txt files provided (e.g. "Error Messages.txt", "Files containing passwords.txt", etc.).
        -d  [Domain to search]
            Optional, example: whatever.com
        -k  [Google Custom Search Engine ID]
            Optional, this can also be set in the configuration file.
            Note, to use the Google CSE ID in the config file, specify the -k option without any params.
            For more info, go to http://www.google.com/cse/

        Examples:
        GoogleDiggity.exe -q test -d stachliu.com
        GoogleDiggity.exe -f "Error Messages.txt" -k 006113852371342063645:ytae6rpigi4
        GoogleDiggity.exe -f "Error Messages.txt" -k
```

New Toolkit

BINGDIGGITY

```
C:\BingDigity\bin\Debug>BingDiggity.exe /?

        +============================================================+
        |               BingDiggity - Version 0.1                    |
        |       Bing Hacking Utility - Using Bing 2.0 API            |
        |               By: Fran Brown  and  Rob Ragan               |
        |       Stach & Liu, LLC - http://www.stachliu.com           |
        +============================================================+

        Usages: BingDiggity.exe [-q Bing_Search_Query] [-d Target_Domain] [-m Max_Search_Results] [-k Bing_2.0_App_ID]
                BingDiggity.exe [-f Bing_Search_Query_File] [-d TargetDomain] [-k Bing_2.0_App_ID]
                BingDiggity.exe [-i IP_Address | -r IP_Address_Range] [-m Max_Search_Results] [-k Bing_2.0_App_ID]

        -q  [Bing search query]
            Optional, can alternatively load queries from file using the -f option.
        -f  [Bing Hack queries file]
            Optional, text file contain Bing search queries, one per line.
        -d  [Domain to search]
            Optional, example: whatever.com
        -i  [IP address to search]
            Optional, example: 10.1.1.1
        -r  [IP address range to search]
            Optional, example: 10.1.1.1-10.1.1.15
        -m  [Max # of results to return per query]
            Optional, note Bing 2.0 doesnt limit your # of queries per day.
        -k  [Bing 2.0 App ID]
            Required, this can also alternatively be set in the configuration file.
            To obtain a Bing 2.0 App ID, go to http://www.bing.com/developer

        Examples:
        BingDiggity.exe -q "mySQL error with query"
        BingDiggity.exe -d stachliu.com -k 2136A233ASDFGHC0CB87C73B9946PFJRYGBVFD32
        BingDiggity.exe -q test -d stachliu.com
        BingDiggity.exe -i 10.1.1.1
        BingDiggity.exe -r 10.1.1.1-10.1.1.15
```

Defenses

GOOGLE/BING HACKING DEFENSES

- "Google Hack yourself" organization
  - Employ tools and techniques used by hackers
- Policy and Legal Restrictions
- Regularly update your robots.txt
- Data Loss Prevention/Extrusion Prevention Systems
  - Free Tools: OpenDLP, Senf
- Social Sentry
  - Service to monitor employee FaceBook and Twitter for $2-$8 per employee (MySpace, YouTube, and LinkedIn support by summer)

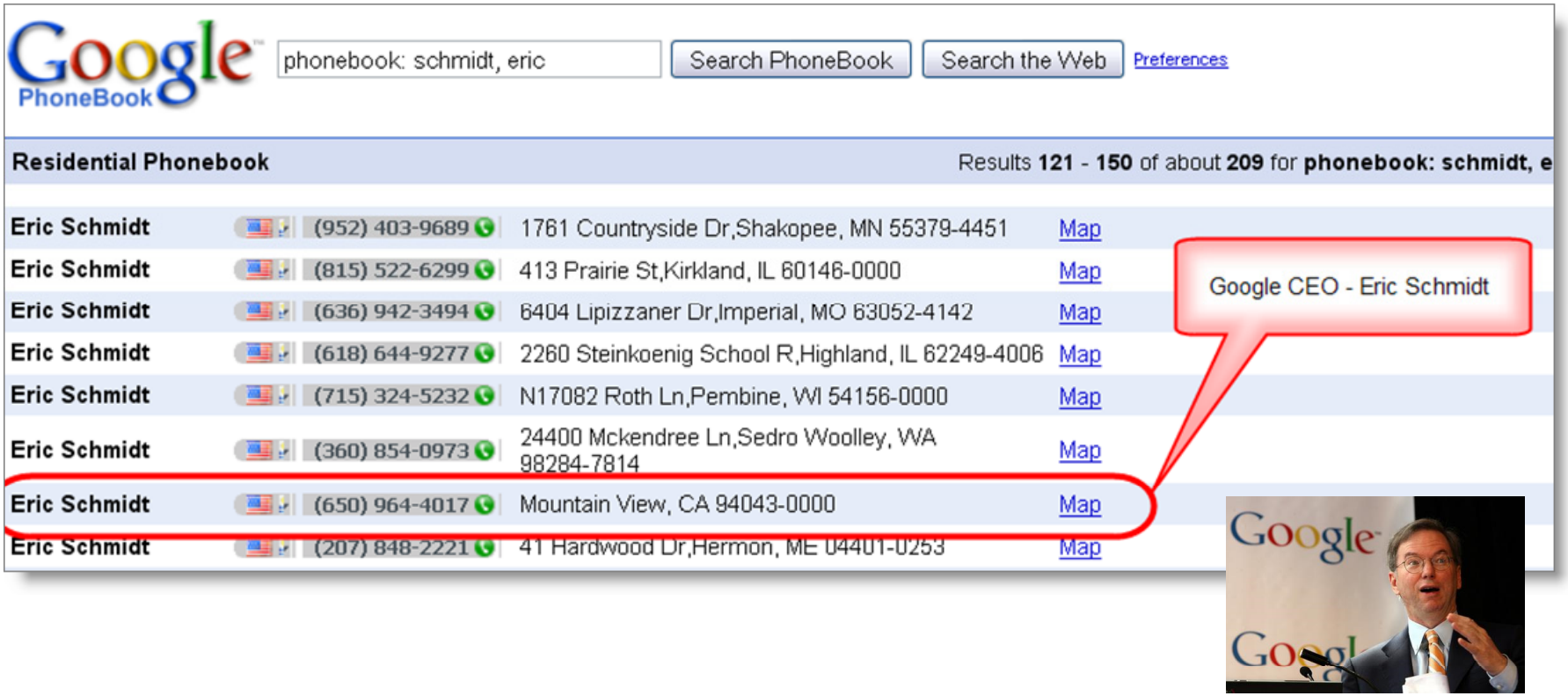
Google Apps Explosion

SO MANY APPLICATIONS TO ABUSE

STACH&LIU

Google PhoneBook

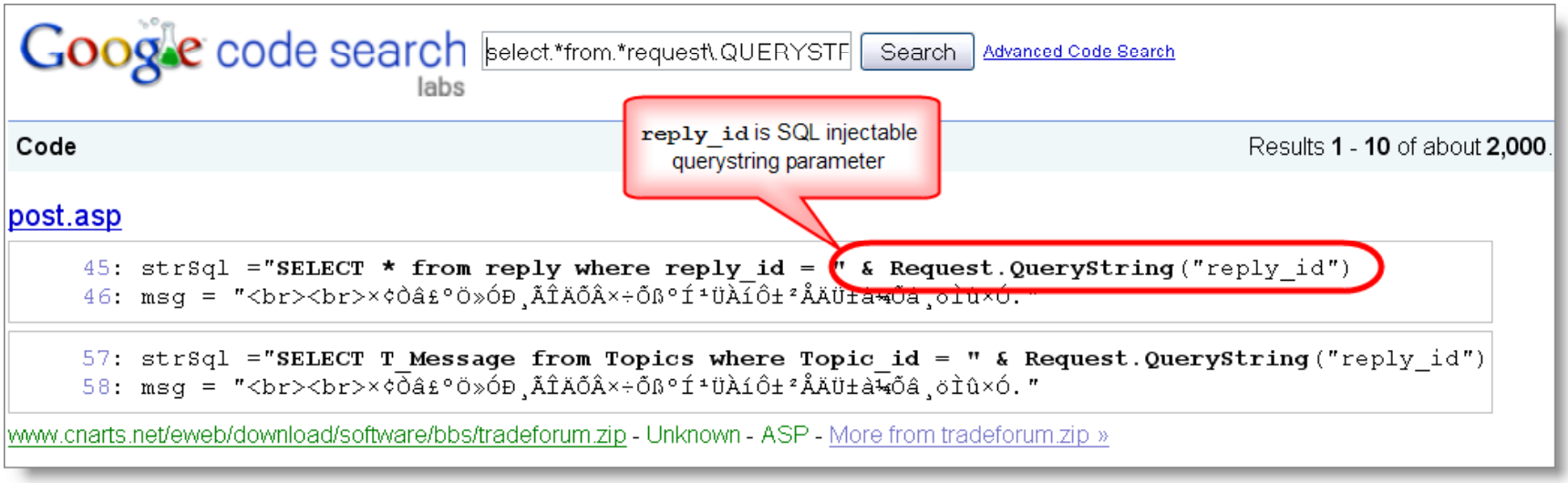
SPEAR PHISHING



Google Code Search

VULNS IN OPEN SOURCE CODE

- Regex search for vulnerabilities in public code
- Example: SQL Injection in ASP querystring
  - select.*from.*request\.QUERYSTRING



GOOGLE CODE SEARCH HACKING

DEMO

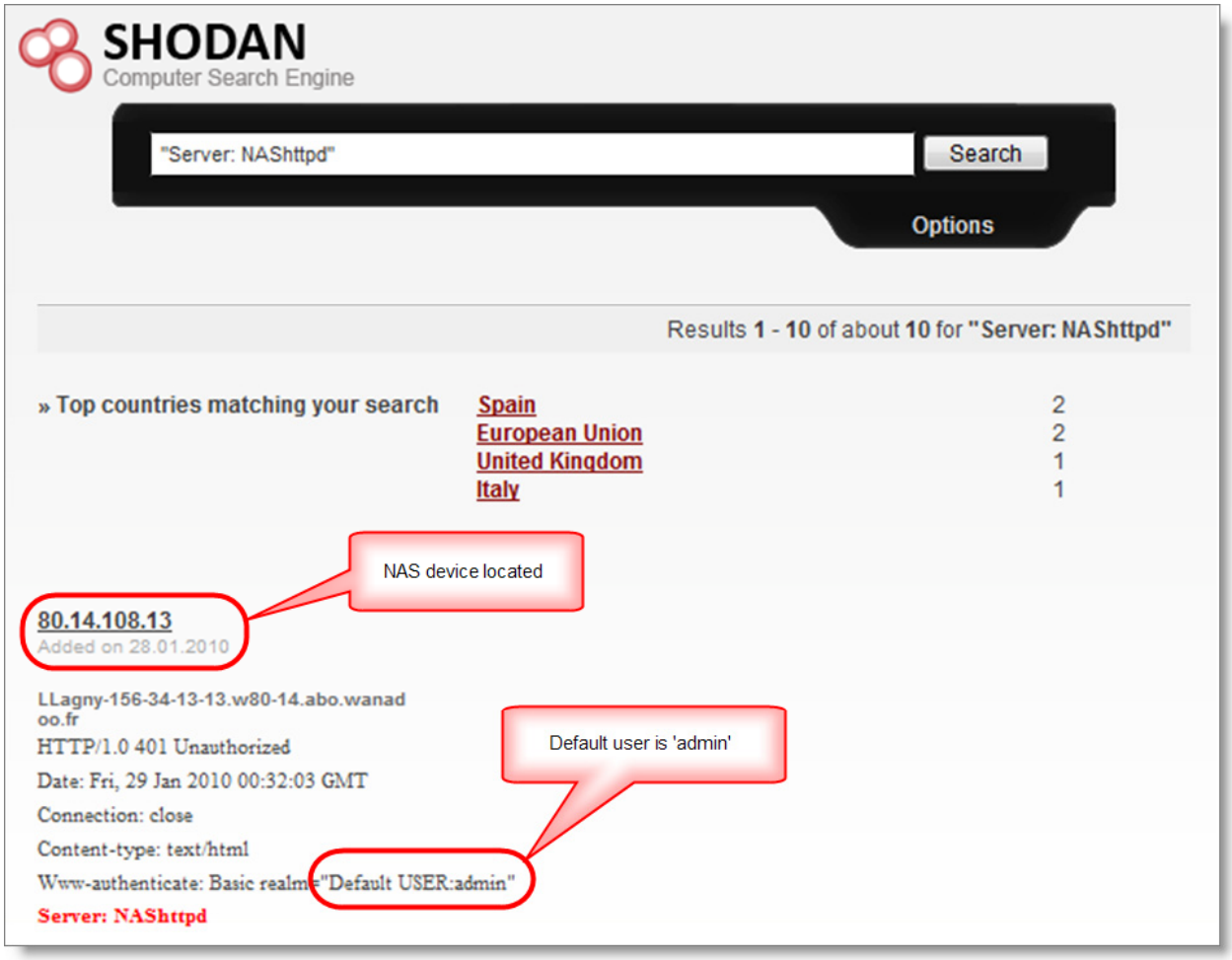
SHODAN

HACKER SEARCH ENGINE

SHODAN Computer Search Engine

- Scans and probes the Internet for open HTTP ports and indexes the headers returned in the response
- Profile a target without directly probing their systems
- Discover specific network appliances
- Easily find vulnerable systems!

Target NAS Appliances



Target SCADA

SHODAN
Computer Search Engine

CRITICAL INFRASTRUCTURE SECURITY

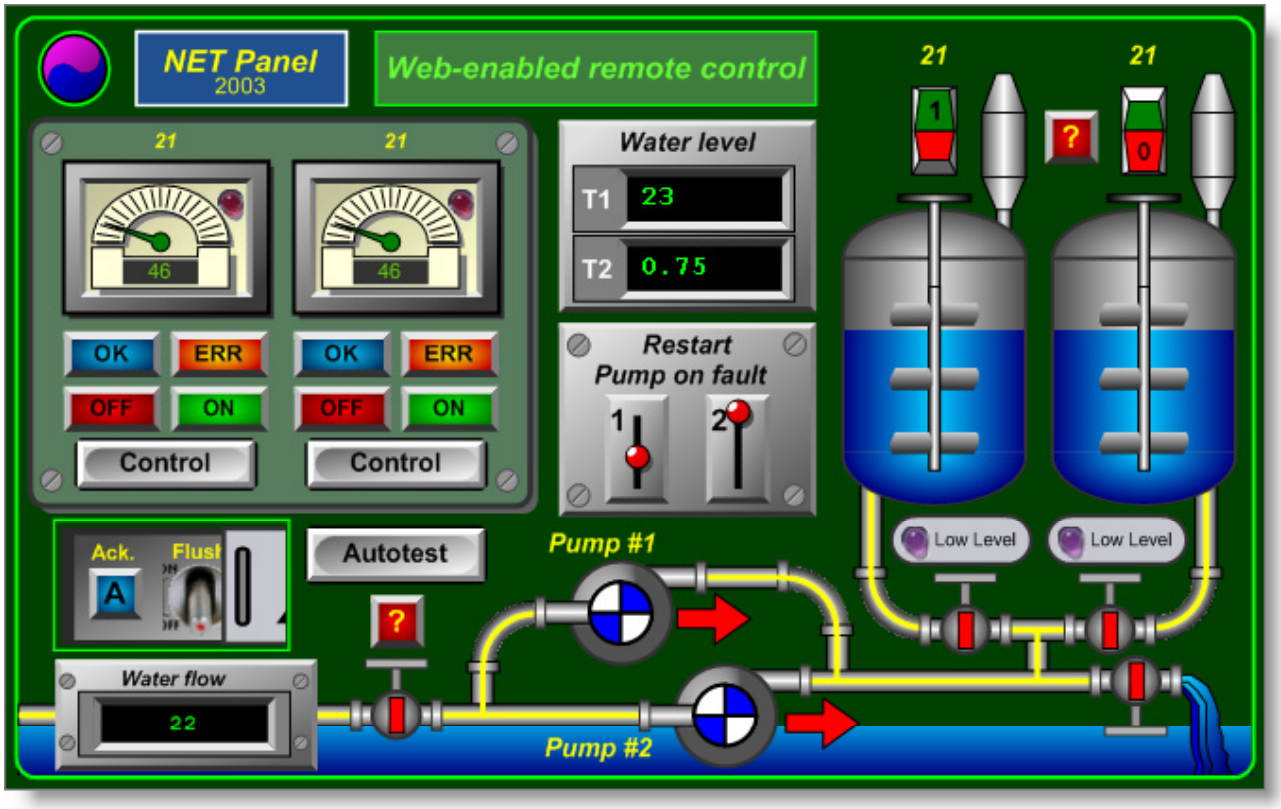
- Supervisory control and data acquisition

Target SCADA

SHODAN
Computer Search Engine

CRITICAL INFRASTRUCTURE SECURITY

- SHODAN: Target Aquired!



STACH&LIU

Black Hat SEO

SEARCH ENGINE OPTIMIZATION

- Why use real news events?
- Black hats make their own fake news
- Faux celebrity sex tape anyone?
- Send to college students
- It works!
- Other scammers imitate what works

Google Trends

BLACK HAT SEO RECON

Defenses

BLACKHAT SEO DEFENSES

- Google SafeBrowsing plugin
- Microsoft SmartScreen Filter
- No-script and Ad-block browser plugins
- Install software security updates
- Stick to reputable sites!
  - Google results aren't safe.

Metadata Attacks

DATA ABOUT DATA

- It's everywhere!
  - In documents (doc, xls, pdf)
  - In images
- What can be data mined?
  - Usernames, emails
  - File paths
  - Operating systems, software versions
  - Printers
  - Network information
  - Device information

FOCA

AUTO METADATA MINING

- Automated doc search via Google/Bing
- Specify domains to target
- Automated download and analysis of docs

Defenses

METADATA MINING DEFENSES

- Implement a policy to review files for sensitive metadata before they're released
- Run metadata extraction tools on your resources
- Utilize metadata cleaning tools
- Digital Rights Management (DRM) tools

Advanced Defenses

PROTECT YO NECK

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 Hacking Alerts
- Bing Hacking Alerts

ADVANCED DEFENSE TOOLS

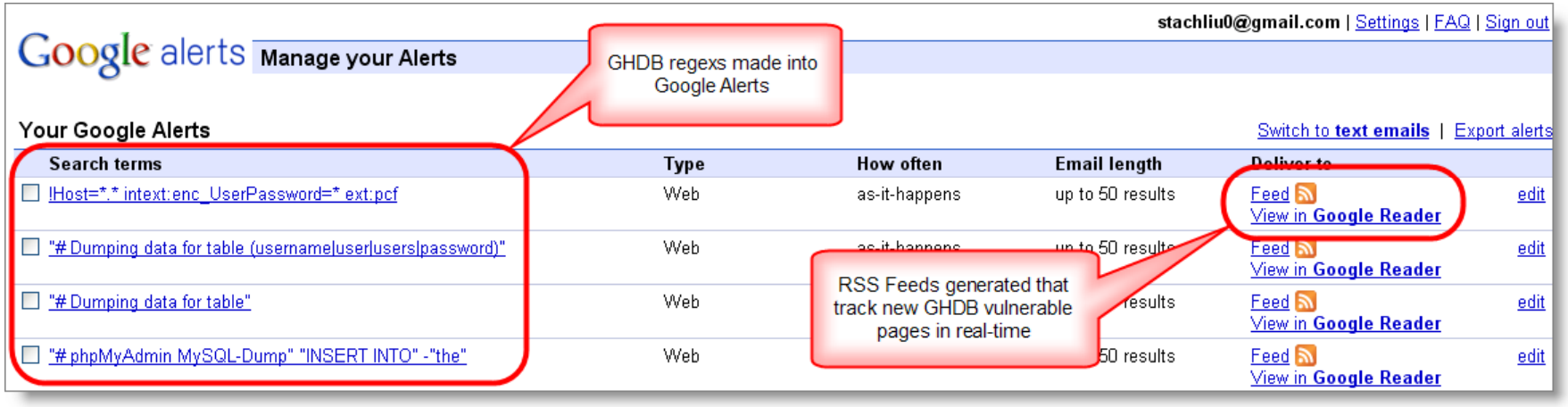
DEMO

Advanced Defenses

GOOGLE HACKING ALERTS

Google Hacking Alerts

- All GHDB/FSDB regexs using Google alerts
- Real-time vuln updates to 1623 hack queries via RSS
- Organized and available via Google reader importable file



Advanced Defenses

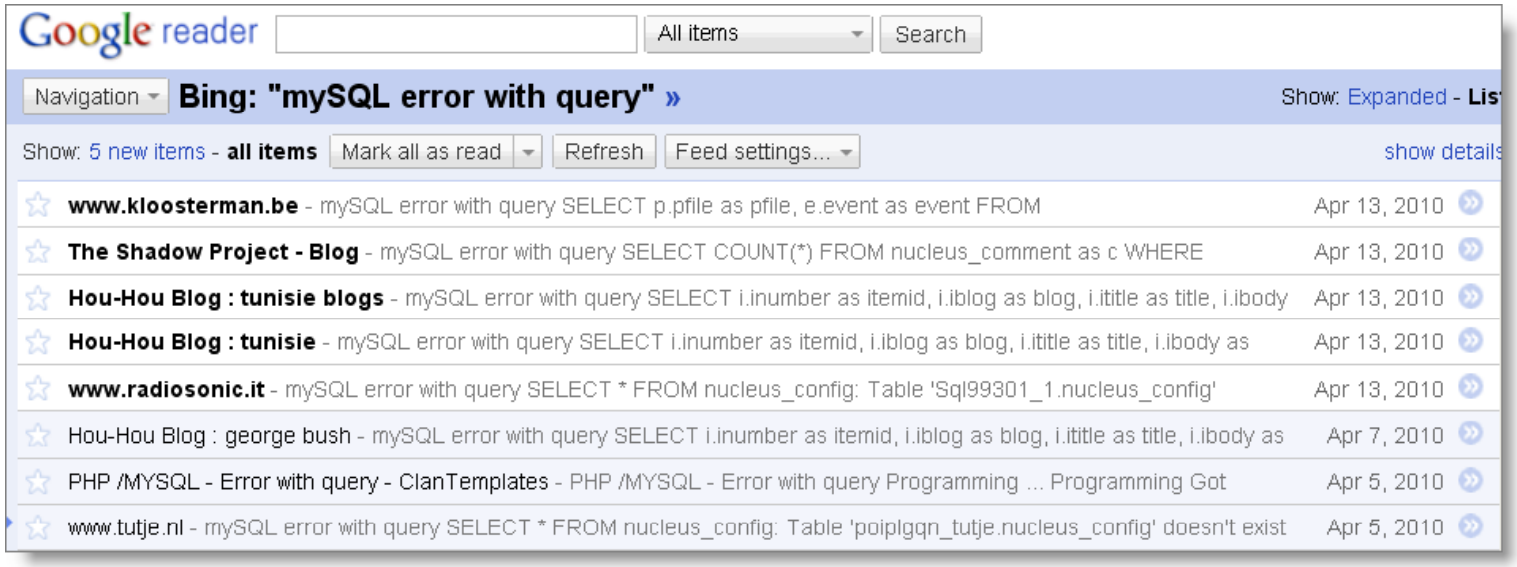
GOOGLE HACKING ALERTS

Advanced Defenses

BING HACKING ALERTS

Bing Hacking Alerts

- Bing searches with regexs from BHDB
- Leverage '&format=rss' directive to turn into update feeds



Future Direction

PREDICTIONS

Future Directions

PREDICTIONS

Data Explosion

- More data indexed, searchable
- Real-time, streaming updates
- Faster, more robust search interfaces

Google Involvement

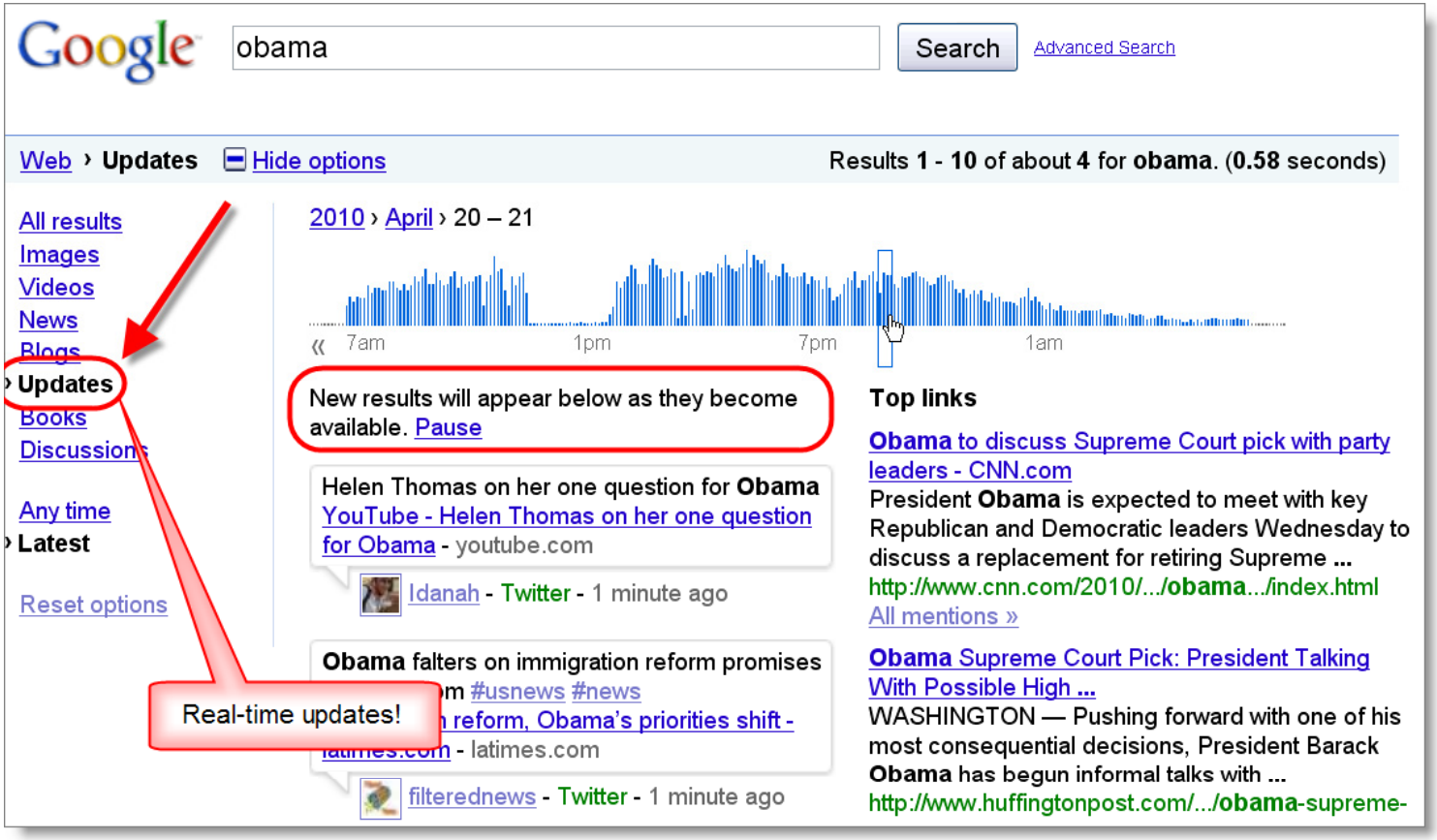
- Filtering of search results
- Better GH detection and tool blocking

Renewed Tool Dev

- Google Ajax API based
- Bing/Yahoo/other engines
  - Search engine aggregators
- Google Code and Other Open Source Repositories
  - MS CodePlex, SourceForge, …
- More automation in tools
  - Real-time detection and exploitation
  - Google worms

Future Directions

REAL-TIME UPDATES



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

For more info:
Email: contact@stachliu.com
Stach & Liu, LLC
www.stachliu.com

STACH&LIU

Thank You