Open Source Intelligence

Omer Usmani

Security Analyst

CCC Technology Center

California Community Colleges

OSINT

- Framework for gathering intelligence

OSINT Sources

- Information often found on social media, organization’s online directory, linux servers open to the internet, log files, etc.

Brief History

Why is OSINT important?

- Information from data breaches
- Find insecure devices connected to the internet
- Obsolete software
- Potential PII

End Goals

1) Social Engineering
2) Discovering potential attack vectors
3) Finding PII

Identifiers

- Name
- Email
- Birthday
- IP Address
- MAC Address
- Phone Number
- Home Address
- License Plate
- Etc.

Pivoting

- Searching for the same identifier across multiple datasets.

Workflow

Can be used offensively and defensively.

1) Identifying the source
2) Harvesting
3) Data Processing
4) Analysis
5) Reporting

OSINT Tools & Techniques

- Google Dorking
- Shodan
- SpiderFoot

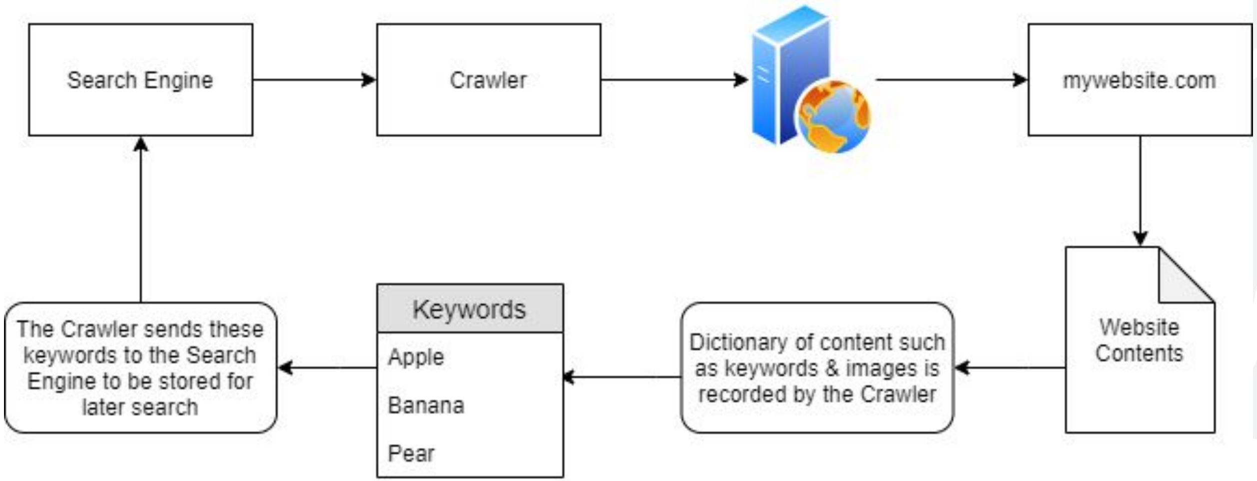
What is Google Dorking?

- Using the Google search engine to query for information that may or may not be intended to be available to the public.

What type of Information can be found?

- Exposed critical directories
- Vulnerable files and servers
- Files containing usernames and passwords
- Sensitive online shopping info

How do search engines work?



Search Engine

Crawler

mywebsite.com

Website Contents

Dictionary of content such as keywords & images is recorded by the Crawler

Keywords

Apple

Banana

Pear

The Crawler sends these keywords to the Search Engine to be stored for later search

Common Operators

- cache:
- allintext:
- allinurl:
- allintitle:
- link:
- site:
- filetype:
- *
- |
- +
- -

Google Dork Examples

- intitle: “webcamXP 5”
- allintext:username filetype:log
- intitle:”index of” inurl:ftp
- allintext:db_password filetype:env
- intitle:"report" ("nessus" | "nmap" | "burp") filetype:pdf

Preventing Google Dorks

- Encode/encrypt sensitive data
- Google Dork your own sites
- Create a robots.txt document on your webserver.

robots.txt

```
Disallow: /

Disallow: /admin/

Disallow: /privatearea/file.html

Disallow: /*?
```

Shodan

- Search engine for the IoT

Shodan Filters

- city
- country
- hostname
- net
- os
- port
- postal
- product
- version
- vuln

Shodan Demo

Open SSH (CLI)

```
shodan search port:22 city:"Portland"
```

Open VNC (Web)

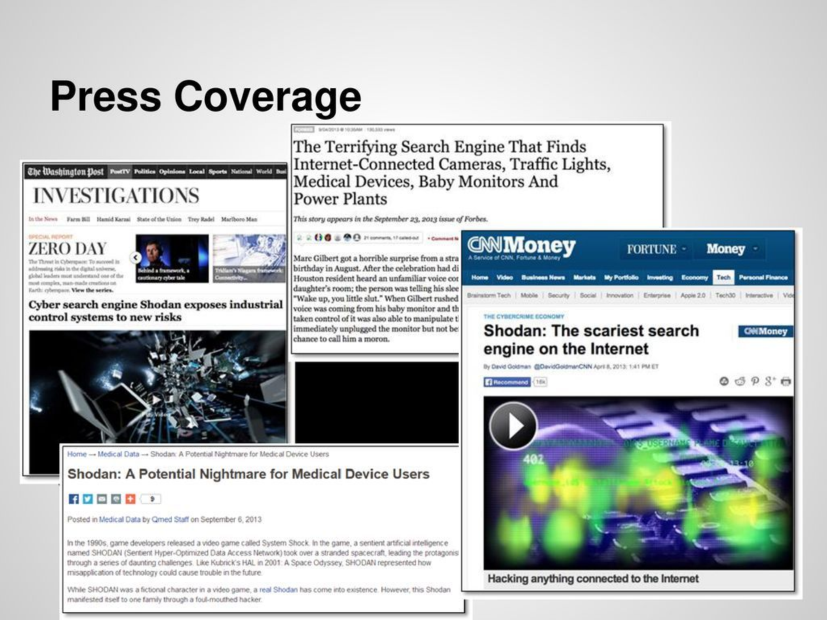
```
"authentication disabled" "RFB 003.008"
```

Open RDP (Web)

```
port:3389
```

```
port:3389 city:"Portland"
```

Preventing Shodan Searches



Press Coverage

The Washington Post
PostTV Politics Opinions Local Sports National World

INVESTIGATIONS

In the News Farm Bill Hamid Karzai State of the Union Trey Radel Marlboro Man
SPECIAL REPORT

ZERO DAY

The Threat in Cyberspace: To succeed in addressing risks in the digital universe, global leaders must understand one of the most complex, man-made creations on Earth: cyberspace. View the series.

Behind a framework, a cautionary cyber tale
Tridium's Niagara framework Connectivity...

Cyber search engine Shodan exposes industrial control systems to new risks

The Terrifying Search Engine That Finds Internet-Connected Cameras, Traffic Lights, Medical Devices, Baby Monitors And Power Plants

This story appears in the September 23, 2013 issue of Forbes.

Marc Gilbert got a horrible surprise from a stra
birthday in August. After the celebration had di
Houston resident heard an unfamiliar voice cor
daughter's room; the person was telling his slee
"Wake up, you little slut." When Gilbert rushed
voice was coming from his baby monitor and th
taken control of it was also able to manipulate t
immediately unplugged the monitor but not be
chance to call him a moron.

CNNMoney
A Service of CNN, Fortune & Money
FORTUNE
Money
Home Video Business News Markets My Portfolio Investing Economy Tech Personal Finance
Brainstorm Tech | Mobile | Security | Social | Innovation | Enterprise | Apple 2.0 | Tech30 | Interactive | Vide
THE CYBERCRIME ECONOMY

Shodan: The scariest search engine on the Internet

By David Goldman @DavidGoldmanCNN April 8, 2013: 1:41 PM ET

Hacking anything connected to the Internet

Home → Medical Data → Shodan: A Potential Nightmare for Medical Device Users

Shodan: A Potential Nightmare for Medical Device Users

Posted in Medical Data by Qmed Staff on September 6, 2013

In the 1990s, game developers released a video game called System Shock. In the game, a sentient artificial intelligence named SHODAN (Sentient Hyper-Optimized Data Access Network) took over a stranded spacecraft, leading the protagonis through a series of daunting challenges. Like Kubrick's HAL in 2001: A Space Odyssey, SHODAN represented how misapplication of technology could cause trouble in the future.

While SHODAN was a fictional character in a video game, a real Shodan has come into existence. However, this Shodan manifested itself to one family through a foul-mouthed hacker.

Common Default Passwords

- **ACTi**: *admin/123456* or *Admin/123456*
- **Axis (traditional)**: *root/pass*,
- **Axis (new)**: requires password creation during first login
- **Cisco**: No default password, requires creation during first login
- **Grandstream**: *admin/admin*
- **IQinVision**: *root/system*
- **Mobotix**: *admin/meinsm*
- **Panasonic**: *admin/12345*
- **Samsung Electronics**: *root/root* or *admin/4321*
- **Samsung Techwin (old)**: *admin/1111111*
- **Samsung Techwin (new)**: *admin/4321*
- **Sony**: *admin/admin*
- **TRENDnet**: *admin/admin*
- **Toshiba**: *root/ikwd*
- **Vivotek**: *root/<blank>*
- **WebcamXP**: *admin/ <blank>*

SpiderFoot Demo

Resources

- HaveIBeenPwned
- Intelligence X
- DeHashed