Cybersecurity Management
Information Gathering

marc.ruiz-ramirez@upc.edu

Contents

- Information types
- Network Information Gathering
- People Information Gathering
- People Hacking
- Extra Resources

Information Gathering

- **Information is power**: Having critical information, at the right time, and especially knowing how to use it, can be a great source of power.
- **Reconnaissance** is the information gathering stage of ethical hacking where data about a target network or system is collected.
  - Data includes anything from network infrastructure to employee contact details.
- **Reconnaissance goal**: Identify as many potential attack vectors as possible.

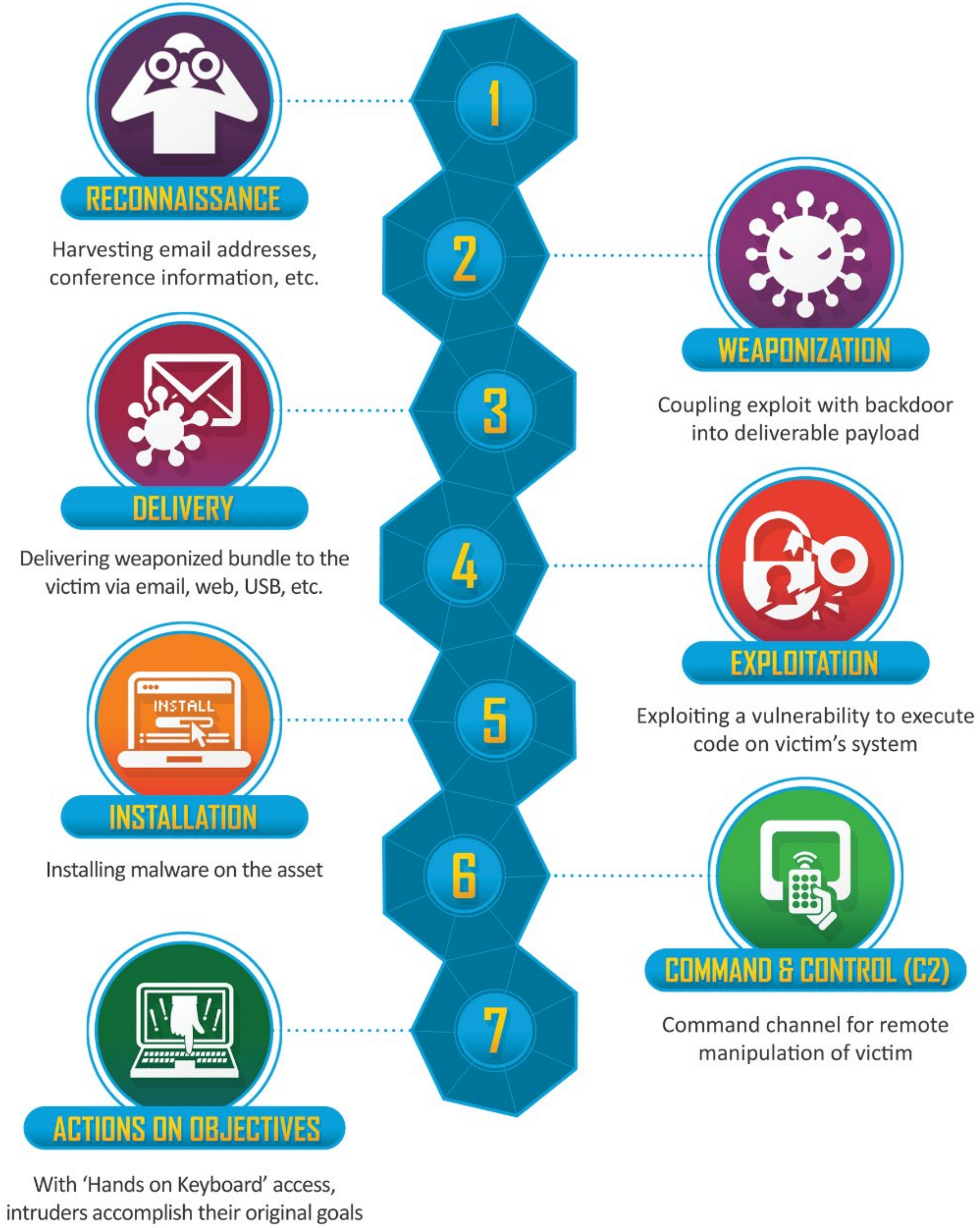
Reconnaissance

- “*A process (sequence of actions) performed by adversaries to gather as much information as possible about target networks and systems that can be used to conduct various types of malicious activity (unauthorized access or denial of service)*”
- Reconnaissance is performed by:
  - Adversaries
    - Black/grey hat hackers
  - Security researchers
    - White hat hackers, blue teams for security testing purposes

Cyber Kill Chain: Describes the technical aspects and a sequential step-by-step model to understand the movement of Advanced Persistent Threats (APTs).

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Reconnaissance: Adversaries collect information about targets using different **tactics, techniques, and procedures (TTP)**.


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Advanced Persistent Threat (APT)

Source: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/

- An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time.
- An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar.
- Requires a higher degree of customization and sophistication than a traditional attack. Adversaries are typically well-funded, experienced teams of cybercriminals that target high-value organizations.
- Spent significant time and resources researching and identifying vulnerabilities within the organization.

Example of APT: https://www.bbc.com/news/world-asia-china-57889981

Cyber Kill Chain stages

- **1. Reconnaissance** involves researching potential targets before carrying out any penetration testing.
  - Identifying potential targets, their vulnerabilities, third parties are connected to them, and entry points.
- 2. **Weaponization** stage consists on the creation of malware to be used against an identified target.
- 3. In the **Delivery** stage, cyberweapons are used to infiltrate a target's network and reach users.
  - Sending phishing emails containing malware attachments or hacking into an organization's network and exploiting a hardware or software vulnerability to infiltrate it.
- 4. In the **Exploitation** stage, attackers take advantage of the discovered vulnerabilities to further infiltrate a target's network and achieve their objectives.
  - Cybercriminals often move laterally across a network to reach their targets.
- 5. In the **Installation** stage, malware is installed onto the target network to take control of its systems and exfiltrate valuable data.
  - Malwares can be installed using Trojan horses, backdoors, or command-line interfaces.
- 6. In the **Command and Control** stage, cybercriminals communicate with the malware they've installed onto a target's network to instruct the installed tools to carry out their objectives.
- 7. In the **Actions on Objectives** stage, cybercriminals carry out their cyberattack objectives.

Reconnaissance phases

- Reconnaissance is present in different forms throughout the attack process:
  - Provides key information to execute subsequent phases

1. Selection of the target organization and creation of an effective plan for initial access:
   - Collect as much information as possible using externally available sources (using scanning, and social engineering techniques)
2. Access to the internal network:
   - One host has been compromised a secure channel is created between an installed backdoor and a command and control server
   - System commands and custom tools are used to collect more information about the network to engage in lateral movement and compromise other resources.
     - Using passive scanning techniques such as sniffing packets to obtain a network view and discover system architectures, protocol mappings, and exploitable vulnerabilities.
       - Helps adversaries to remain undetected for extended periods of time.
       - Adversaries can exploit vulnerabilities using the collected information to compromise other hosts to get closer to the target resources

Information types

- Different types of information is collected by adversaries depending on their objectives and capabilities.
    - It is highly interconnected and it may need to be acquired sequentially.
- What types of information do adversaries seek?
    - **Non-technical (Social) Information***:* useful for performing social engineering and initial access planning
        - Ex: people contact details, physical security, etc.
    - ***Technical Information****:* used for finding vulnerabilities to compromise specific systems, escalate privileges, establish durable footholds (to maintain access to their targets) or move laterally (to extend access to other hosts or applications in an organization) in networks
        - Ex: host or network configurations

Target Information					
Non-technical Information		**Technical Information**			
Organization details	**Employee information**	**User Information**	**Network Information**	**Host Information**	**Application Information**
Organization location	Contact details	Account details	Domain Names	System Processes	Frameworks and Environment
Organization infrastructure	Background	User credentials	Remote Hosts and Network Topology	System Platform	Security Tools and Applications
Physical security	Habitual behaviour		Network Protocols and Services	System Configuration	Application or Package Configuration
Logistic details			Network Devices	System Hardware and Peripheral Devices	Cloud Dashboard and API
				Security Environment	
				Files and Directories	

Non-technical information (I)

- *Organization Background and Details*
  - Organization’s information, resources, employee contacts and work details, physical access and security policies
    - **Physical Attributes**
      - Lead to effective social engineering attacks: gaining physical access using reverse social engineering.
    - **Logistics Details**
- *Personal Information.*
  - Employees information (contact details, technical or financial background, habits, and behavioral traits)
    - Collected to analyze people’s weaknesses
    - Useful for applying social engineering techniques to gain remote access to the victims’ machines or online accounts
  - **Contact Details:** Adversaries can collect contact details such as email addresses, phone numbers, identity information.
    - theHarvester: Open source tool that can collect email addresses given a domain name
      - https://github.com/laramies/theHarvester

Non-technical information (II)

- *Personal Information.*
  - **Personal Background:** Information related to the technical or financial background is useful for social engineering attacks.
    - The technical background reveals what information and organization resources they may have access to. It can be found on the organization website, an employee’s LinkedIn profile, etc.)
  - **Habitual Behavior**
    - Adversaries attempt to learn their targets’ habits to perform social engineering (ex. phishing) attacks.
  - **Emotional States and Blackmail**
    - Adversaries observe people’s emotional states.
      - Spy people through webcams in compromised hosts.
      - Take photos of victims to blackmail them.

Technical information

- Information about networks, hosts, applications, and users.
- Technical details are especially useful once adversaries have access to the target organization’s internal network.
- Basic technical information can be obtained from an external network, but adversaries usually need to breach the target network or system to be able to gather more accurate details

Network-level Information (I)

- Essential for planning remote attacks to penetrate an organization’s network and for lateral movement and avoiding detection once an internal network is breached
- Adversaries look for network-level information (topology, protocols, devices, and services) to understand the local network.
  - Effective techniques: Scanning and sniffing
- Botnet-based attacks compromise systems remotely and then maintain command channels to execute commands on the compromised systems.
  - Channels include various protocols (Telnet, SSH) used by the remote shell client software

Network-level Information (II)

- Most common network-level information that adversaries attempt to obtain:
  - **Domain Names:** Domain and hostnames are identifiers that adversaries can use to map which hosts belong to a particular domain
  - **Remote Hosts and Network Topology:** Adversaries try to obtain the list of reachable IP addresses to map the whole network view (hosts, routers, switches, firewalls, etc.)
  - **Network Protocols and Services:** Running services can be identified from outside the organization's network by interacting with the server or sniffing packets for public-facing servers or compromised hosts.
  - **Network Devices:** Device information is useful for adversaries when employing exploits that target known vulnerabilities.
    - NetworkWatcher: Tool for identifying device information (hardware device manufacturer or vendor, operating systems and version, manufacturer settings, networking configurations)
- Adversaries also look for network security measures (firewalls, IDSs, honeypots, etc.).

Host-level Information

- Software configurations, running processes, files and directories, and security environments is very useful to adversaries for performing advanced stages of attacks.
    - Specific details can be obtained once a host machine is compromised.
- Common host-level information that adversaries look for:
    - **System Processes**: Information regarding details of installed software (presence of security software or environments, development frameworks, etc.)
    - **System Platform**: The type of operating system and its version.
        - Using old versions creates more opportunities for attackers to utilize known tools to exploit.
    - **System Configuration**:
        - Adversaries gather information from the Windows registry system using remote access tools and learn about running programs, their configurations, presence of antivirus or sandbox.
    - **System Hardware and Peripheral Devices**:
        - Device information helps adversaries to identify known vulnerabilities in a vendor’s product and devise exploitation strategies.
    - **Security Environment**:
        - Adversaries learn about security environments (virtualization or sandbox) by querying registry values, system services, BIOS information, process list, and system information (as hardware configuration).
    - **Files and Directories**

Application-level Information

- Security vulnerabilities at the application depend on three factors: exploitability, detectability, and impact of damage.
- To exploit application level vulnerabilities (e.g., SQL injection, cross-site scripting, broken access control, etc.), adversaries collect application-level information from a system or a network.
- Most common application-level information adversaries look for:
  - **Frameworks and Environments**: names, version, and runtime configuration information of frameworks that are installed on a system
    - Development frameworks and environments can have vulnerabilities.
    - Misconfiguration (weakness) that creates loopholes and attract adversaries
  - **Security Tools and Applications**
    - Identification of anti-malware and forensic tools by querying the default software installation directory or by querying registry, and running processes.
  - **Application or Package Configuration:**
    - Adversaries learn about the configuration of installed software and applications on a host. This information can be used to develop exploits or use existing exploits in the dark web.
    - Application configuration information can reveal access tokens and user credentials
  - **Cloud Dashboard and API**
    - Adversaries gather information about virtual machines, cloud tools, services, and other cloud assets accessible from the compromised host

User-level Information

- It is useful in different stages from gaining initial foothold in an internal network to privilege escalation on a compromised host.
- **Account Details**: User and group information includes the list of users and groups, their login types, access control policies, group permissions, and so on.
    - APTs can gather information about domain and account information (account ID, token information, etc.) by observing the list of running processes.
    - APTs are capable of querying information from account associated directories and enumerating local and domain users.
- **User Credentials**: Most common practices of obtaining user credentials are:
    - Social engineering attacks (e.g., phishing) against target users
    - Installing keyloggers on the users' machines
    - Use spyware to collect user profile data or login information stored in a browser cache (ex: APT: Machete).
    - Take advantage of web browser vulnerabilities to collect user-level information
        - Installing a malware extension and stealing sensitive information when the user fills out a web form
        - Potential for compromising other services (users often use the same passwords for multiple accounts)

Reconnaissance Techniques

- Network information gathering
  - Whois Lookup
  - DNS Interrogation
  - Domains and subdomains (Passive and actives techniques)
  - Search Engines
  - Scanning techniques
- People information gathering
  - Search Engines
  - Social Engineering

Summary of selected tools and sources

- WHOIS, Reverse WHOIS
- Google Dorks
- crt.sh
- Wappalyzer
- sitemap.xml, robots.txt
- Wayback Machine
- Shodan
- Zoomeye
- GHDB
- The Harvester
- OSINT framework
- Rubber Ducky
- Keyloggers / Screenloggers

This is an small but variate set of available SW and HW tools for Information Gathering and OSINT.

You should know what they are and what kind of information they provide.

Network Information Gathering

Widening the scope and reducing the unknown

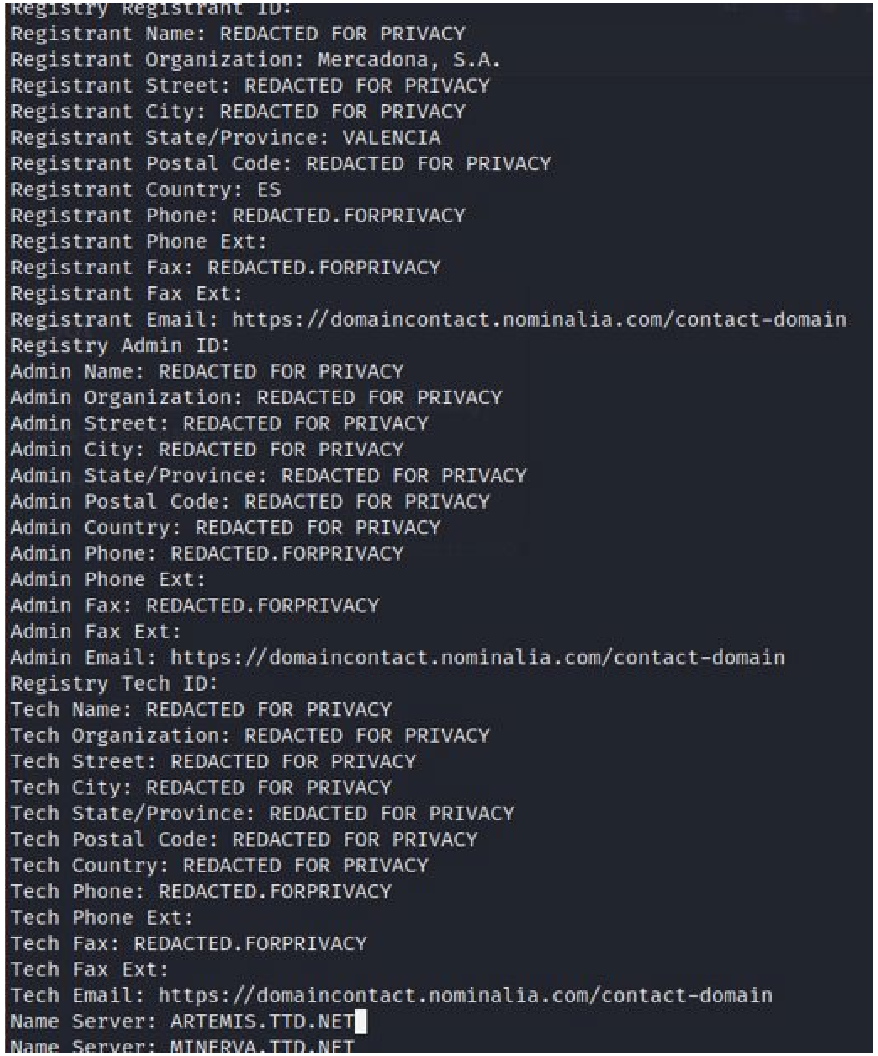
WHOIS Lookup

- WHOIS databases: stores WHOIS records and are maintained by regional Internet registries.
- WHOIS record: Contains details about the owner of a domain, physical addresses, email addresses and other related information
- Adversaries perform WHOIS lookup to find administrative information (domain name details, the contact information of the owner, name servers, etc.)
  - This information is used to perform social engineering attacks to obtain further information about the target

WHOIS and Reverse WHOIS

- WHOIS query by domain
- WHOIS query by IP
- Reverse WHOIS query by registrant
- Reverse WHOIS query by company
- Reverse WHOIS query by registrant's email

RIR (Regional Internet Registry)	Organisation
Europe, Russia, Asia (Central, West)	RIPE
USA, Canada	ARIN
Oceania, Asia (South and East)	APNIC
Latin America	LACNIC
Africa	AFRINIC



```
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Mercadona, S.A.
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: VALENCIA
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: ES
Registrant Phone: REDACTED.FORPRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED.FORPRIVACY
Registrant Fax Ext:
Registrant Email: https://domaincontact.nominalia.com/contact-domain
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED.FORPRIVACY
Admin Phone Ext:
Admin Fax: REDACTED.FORPRIVACY
Admin Fax Ext:
Admin Email: https://domaincontact.nominalia.com/contact-domain
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED.FORPRIVACY
Tech Phone Ext:
Tech Fax: REDACTED.FORPRIVACY
Tech Fax Ext:
Tech Email: https://domaincontact.nominalia.com/contact-domain
Name Server: ARTEMIS.TTD.NET
Name Server: MINERVA.TTD.NET
```

DNS Interrogation tools

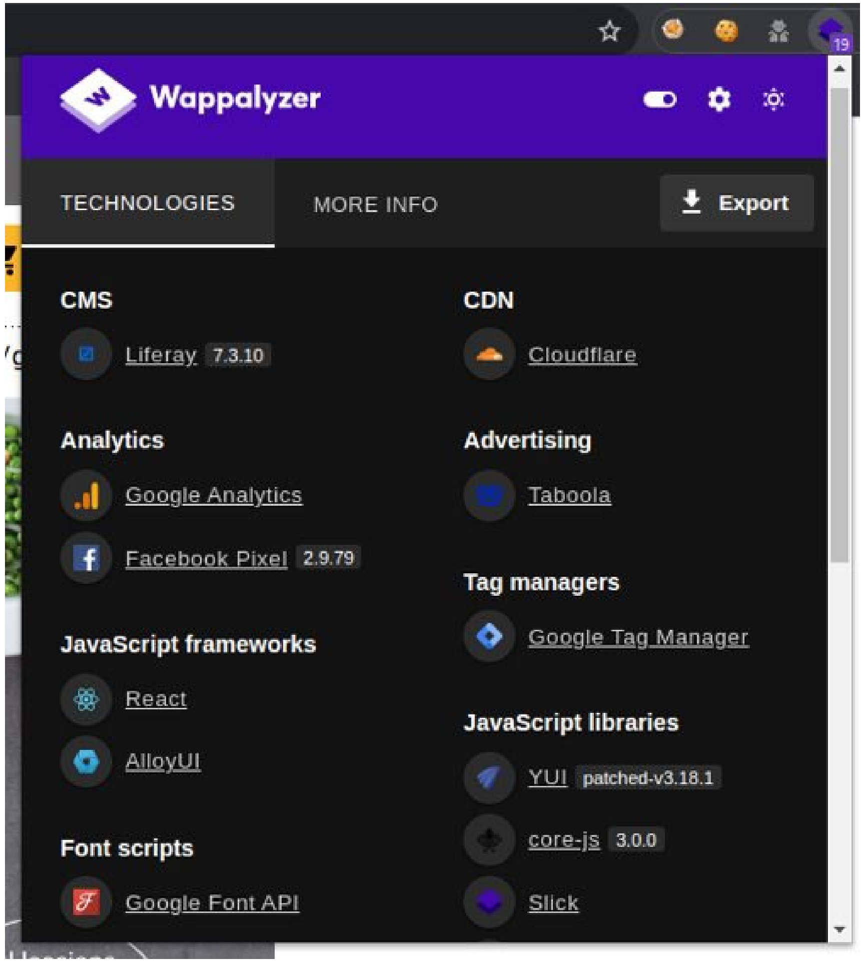
- Are used to search for hosts in a network to obtain an interal view of the network.
- Several online tools leverage the opportunity to perform a lookup to find additional hosts inside the network.
- NSLookup is the most common tool for DNS interrogation.
- Adversaries can find potential targets by obtaining records of CNAME, PTR, MX, HINFO, and AXFR if misconfigured by administrators.

Domains and Subdomains

- **Passive**: Obtain information without direct interaction with the target (using search engines).
  - Manual: Google dorks, pages (like crt.sh).
  - Automated: amass, dnsenum, dnsrecon, sublist3r, etc.
- **Active**: Obtain information by directly interacting with the target. This stage would usually require authorization to test.
  - Zone transfer (it should be vulnerable)
    - Attacker gather the DNS records to select targets for exploitation
  - DNS Zone Walk (it should be vulnerable)
    - Technique used to find subdomains using domains whose NSEC records are set
  - Crawling, some good tools: ZAProxy, BurpSuite, FortiPenTest
    - Allows automatic numbering of all active subdirectories of a web page by automating the visit to the application's internal links.
    - Objective: find all the indexed routes of the web page, to see if there are vulnerabilities in them.
  - Brute force, some tools: gobuster, ffuf, wfuzz
    - Brute force with subdomain
      - Guess possible combination to get a subdomain that is resolved to IP address
      - Subdomains not indexed on search engines (not available on online DNS aggregators sites)
    - Brute force with HTTP Host header

Technologies in Use

- Useful to search for vulnerabilities
- Tools
  - Browser Extensions: Wappalyzer
  - Allows you to identify the technology used to build a website:
    - Data about an application's servers, programming languages, databases, etc.
  - Command-line interface: WhatWeb
  - Open source program for collecting information about a web application.
    - New generation scanner that detects the technologies used in the development of a web page.



CMS
Liferay 7.3.10

CDN
Cloudflare

Analytics
Google Analytics
Facebook Pixel 2.9.79

Advertising
Taboola

Tag managers
Google Tag Manager

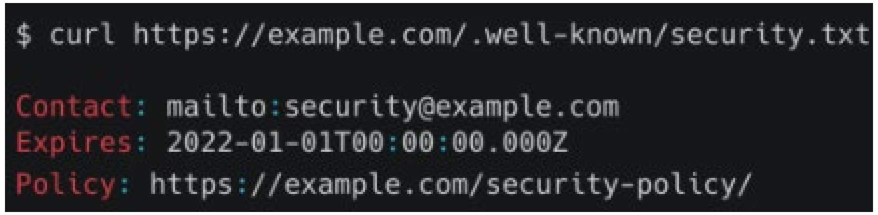
JavaScript frameworks
React
AlloyUI

JavaScript libraries
YUI patched-v3.18.1
core-js 3.0.0
Slick

Font scripts
Google Font API

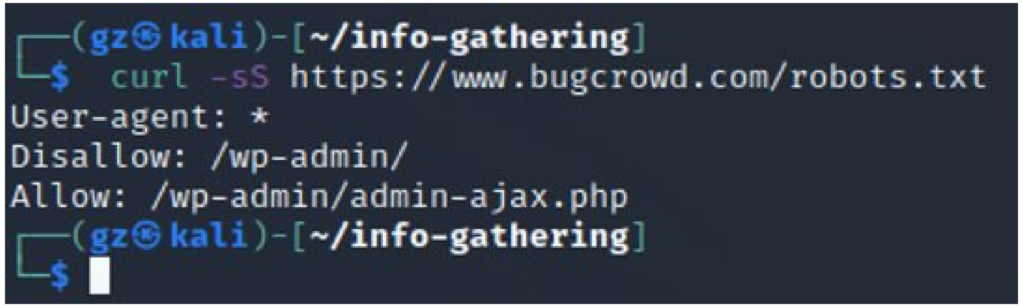
Resources – Special Files

- sitemap.xml
- robots.txt
- humans.txt
- security.txt
- .well-known/



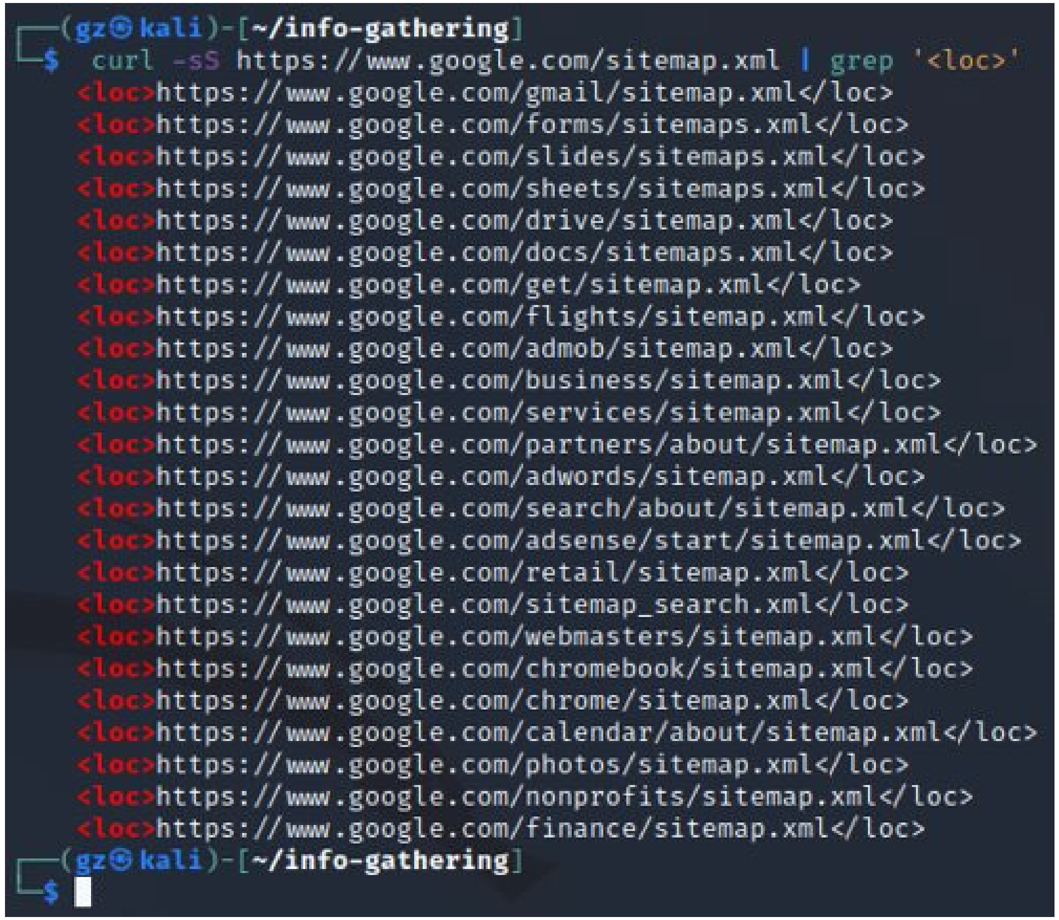
```
$ curl https://example.com/.well-known/security.txt

Contact: mailto:security@example.com
Expires: 2022-01-01T00:00:00.000Z
Policy: https://example.com/security-policy/
```



```
┌──(gz㉿kali)-[~/info-gathering]
└─$ curl -sS https://www.bugcrowd.com/robots.txt
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
┌──(gz㉿kali)-[~/info-gathering]
└─$ 
```

Specifies the URLs a search engine crawler can access



```
┌──(gz㉿kali)-[~/info-gathering]
└─$ curl -sS https://www.google.com/sitemap.xml | grep '<loc>'
   <loc>https://www.google.com/gmail/sitemap.xml</loc>
   <loc>https://www.google.com/forms/sitemaps.xml</loc>
   <loc>https://www.google.com/slides/sitemaps.xml</loc>
   <loc>https://www.google.com/sheets/sitemaps.xml</loc>
   <loc>https://www.google.com/drive/sitemap.xml</loc>
   <loc>https://www.google.com/docs/sitemaps.xml</loc>
   <loc>https://www.google.com/get/sitemap.xml</loc>
   <loc>https://www.google.com/flights/sitemap.xml</loc>
   <loc>https://www.google.com/admob/sitemap.xml</loc>
   <loc>https://www.google.com/business/sitemap.xml</loc>
   <loc>https://www.google.com/services/sitemap.xml</loc>
   <loc>https://www.google.com/partners/about/sitemap.xml</loc>
   <loc>https://www.google.com/adwords/sitemap.xml</loc>
   <loc>https://www.google.com/search/about/sitemap.xml</loc>
   <loc>https://www.google.com/adsense/start/sitemap.xml</loc>
   <loc>https://www.google.com/retail/sitemap.xml</loc>
   <loc>https://www.google.com/sitemap_search.xml</loc>
   <loc>https://www.google.com/webmasters/sitemap.xml</loc>
   <loc>https://www.google.com/chromebook/sitemap.xml</loc>
   <loc>https://www.google.com/chrome/sitemap.xml</loc>
   <loc>https://www.google.com/calendar/about/sitemap.xml</loc>
   <loc>https://www.google.com/photos/sitemap.xml</loc>
   <loc>https://www.google.com/nonprofits/sitemap.xml</loc>
   <loc>https://www.google.com/finance/sitemap.xml</loc>
┌──(gz㉿kali)-[~/info-gathering]
└─$ 
```

Website's essential pages Google can find and crawl them all.

Helps search engines understand your website structure.

Resources – "Hidden" Resources

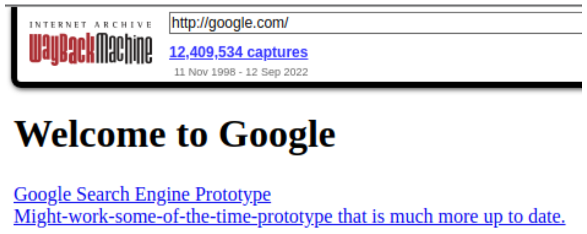
- No link pointing to them
- They are found by brute force
  - The response differ in some properties
    - Status code
    - Size
    - Words
    - Lines
    - Characters
    - Response time
- Tools: ffuf, gobuster, feroxbuster, wfuzz, etc.
  - Discover hidden files, directories, and other web application vulnerabilities by performing recursive and brute-force searches.
  - https://infosecwriteups.com/attacking-web-applications-with-ffuf-solving-the-ctf-challenge-c22263cf67e1

Resources – Open Source Projects

- Open Source hosting platforms
  - GitHub
  - GitLab
  - BitBucket
- There might be sensitive information
  - Credentials
  - Emails
  - API keys
- Do not forget other branches and previous commits
- GitHub Dorks (list, keywords, tools)

Resources – Archive

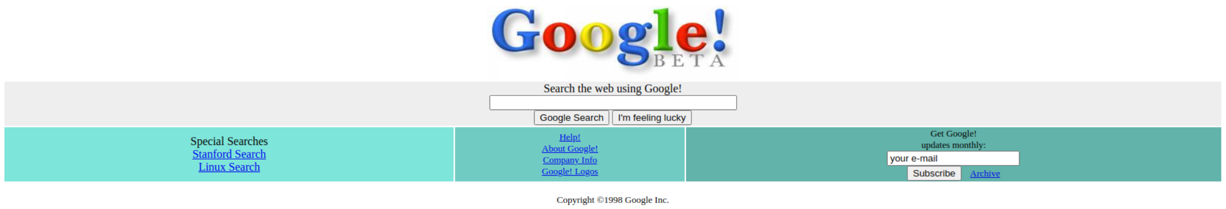
- Previous versions may contain sensitive information
- Internet Archives: WaybackMachine
- Cached websites (Google dork)
- Automated tools: waybackurls
  - Obtain URL from archived versions of websites available on the WaybackMachine service



Welcome to Google

Google Search Engine Prototype
Might-work-some-of-the-time-prototype that is much more up to date.

11/11/1998: Google in alpha version



Search the web using Google!

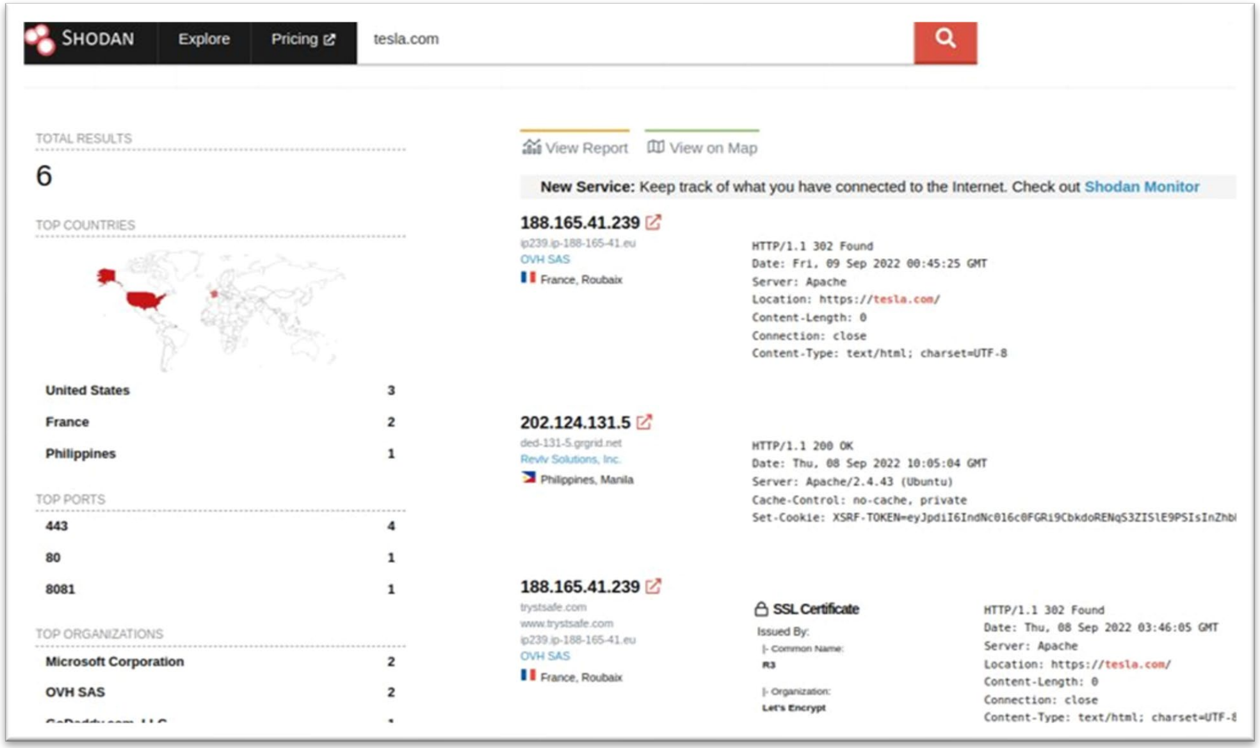
Get Google! updates monthly:

Copyright ©1998 Google Inc.

02/12/1998: Google in beta version

More than just Web

- IoT Search Engines: Shodan, Censys, ZoomEye
- CLI option: shodan (API key needed)



TOTAL RESULTS

6

TOP COUNTRIES

United States	3
France	2
Philippines	1

TOP PORTS

443	4
80	1
8081	1

TOP ORGANIZATIONS

Microsoft Corporation	2
OVH SAS	2
GoDaddy.com, LLC	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

188.165.41.239
ip239.ip-188-165-41.eu
OVH SAS
France, Roubaix

```
HTTP/1.1 302 Found
Date: Fri, 09 Sep 2022 00:45:25 GMT
Server: Apache
Location: https://tesla.com/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

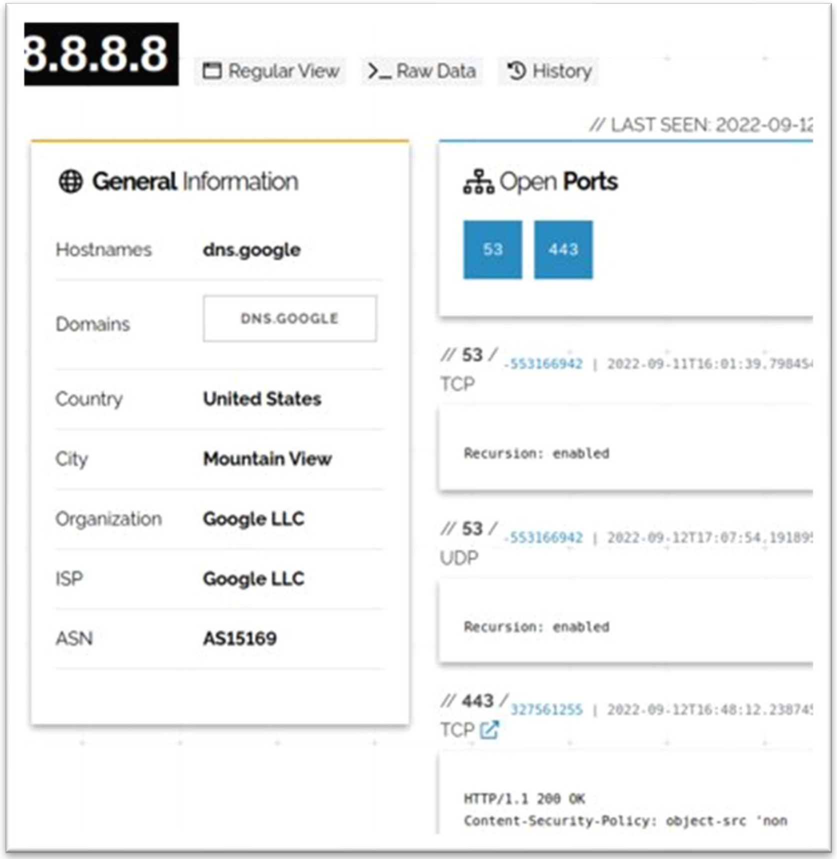
202.124.131.5
ded-131-5.grgrid.net
Reviv Solutions, Inc.
Philippines, Manila

```
HTTP/1.1 200 OK
Date: Thu, 08 Sep 2022 10:05:04 GMT
Server: Apache/2.4.43 (Ubuntu)
Cache-Control: no-cache, private
Set-Cookie: XSRF-TOKEN=eyJpdiI6IndNc016c0FGRi9CbkdoRENqS3ZISlE9PSIsInZhb
```

188.165.41.239
trystsafe.com
www.trystsafe.com
ip239.ip-188-165-41.eu
OVH SAS
France, Roubaix

SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt

```
HTTP/1.1 302 Found
Date: Thu, 08 Sep 2022 03:46:05 GMT
Server: Apache
Location: https://tesla.com/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```



// LAST SEEN: 2022-09-1

General Information

Hostnames	dns.google
Domains	DNS.GOOGLE
Country	United States
City	Mountain View
Organization	Google LLC
ISP	Google LLC
ASN	AS15169

Open Ports

53 443

// 53 / -553166942 | 2022-09-11T16:01:39.79845
TCP

```
Recursion: enabled
```

// 53 / -553166942 | 2022-09-12T17:07:54.19189
UDP

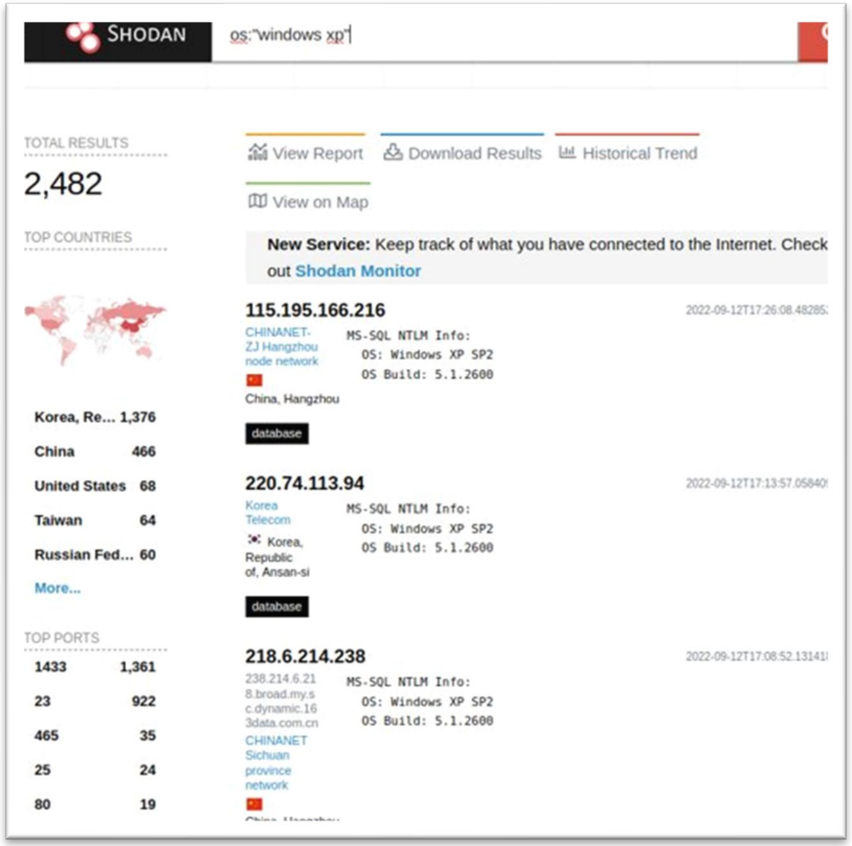
```
Recursion: enabled
```

// 443 / 327561255 | 2022-09-12T16:48:12.23874
TCP

```
HTTP/1.1 200 OK
Content-Security-Policy: object-src 'non
```

More than just Web

- Shodan Dorks (API key needed)



os:"windows xp"

TOTAL RESULTS

2,482

View Report · Download Results · Historical Trend

View on Map

TOP COUNTRIES

Korea, Re...	1,376
China	466
United States	68
Taiwan	64
Russian Fed...	60

More...

TOP PORTS

1433	1,361
23	922
465	35
25	24
80	19

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

115.195.166.216 2022-09-12T17:26:08.48285

CHINANET-ZJ Hangzhou node network

China, Hangzhou

```
MS-SQL NTLM Info:
  OS: Windows XP SP2
  OS Build: 5.1.2600
```

database

220.74.113.94 2022-09-12T17:13:57.05840

Korea Telecom

Korea, Republic of, Ansan-si

```
MS-SQL NTLM Info:
  OS: Windows XP SP2
  OS Build: 5.1.2600
```

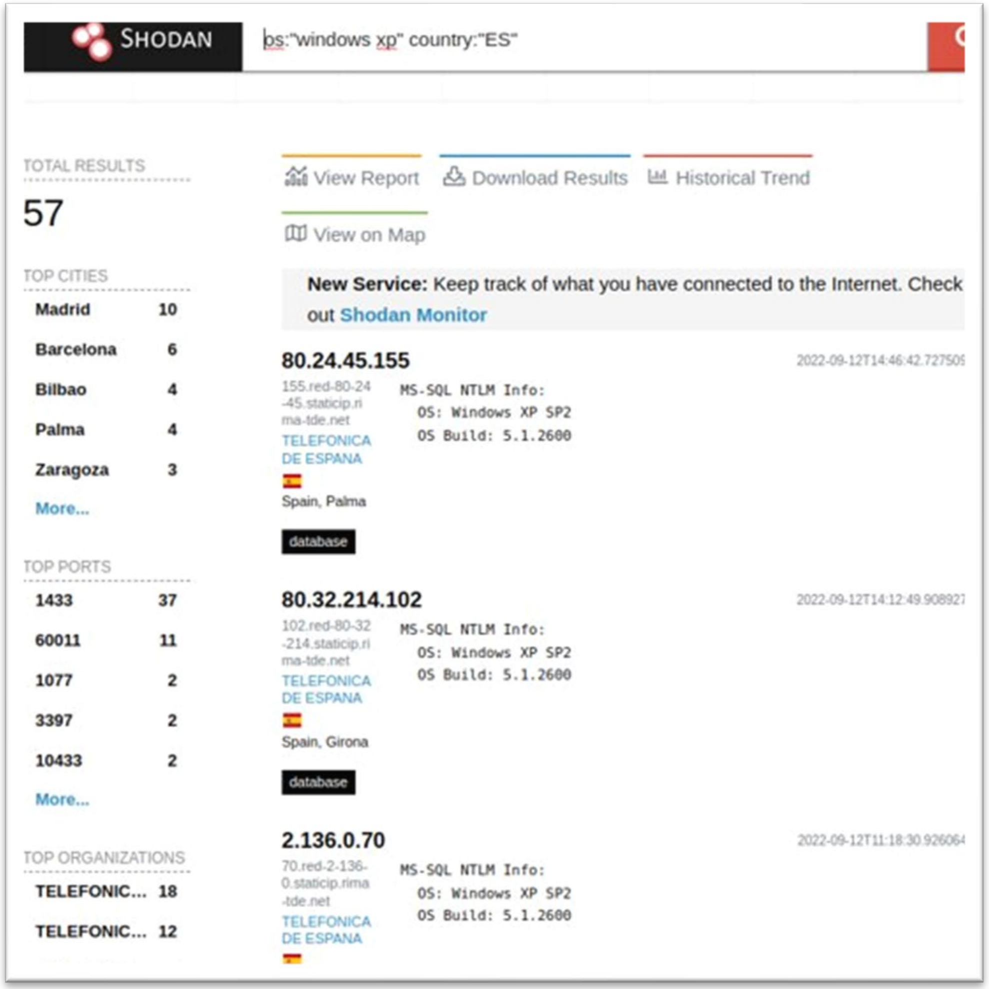
database

218.6.214.238 2022-09-12T17:08:52.13141

238.214.6.218.broad.my.sc.dynamic.163data.com.cn

CHINANET Sichuan province network

```
MS-SQL NTLM Info:
  OS: Windows XP SP2
  OS Build: 5.1.2600
```



os:"windows xp" country:"ES"

TOTAL RESULTS

57

View Report · Download Results · Historical Trend

View on Map

TOP CITIES

Madrid	10
Barcelona	6
Bilbao	4
Palma	4
Zaragoza	3

More...

TOP PORTS

1433	37
60011	11
1077	2
3397	2
10433	2

More...

TOP ORGANIZATIONS

TELEFONIC...	18
TELEFONIC...	12

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

80.24.45.155 2022-09-12T14:46:42.72750

155.red-80-24-45.staticip.rima-tde.net

TELEFONICA DE ESPANA

Spain, Palma

```
MS-SQL NTLM Info:
  OS: Windows XP SP2
  OS Build: 5.1.2600
```

database

80.32.214.102 2022-09-12T14:12:49.908927

102.red-80-32-214.staticip.rima-tde.net

TELEFONICA DE ESPANA

Spain, Girona

```
MS-SQL NTLM Info:
  OS: Windows XP SP2
  OS Build: 5.1.2600
```

database

2.136.0.70 2022-09-12T11:18:30.926064

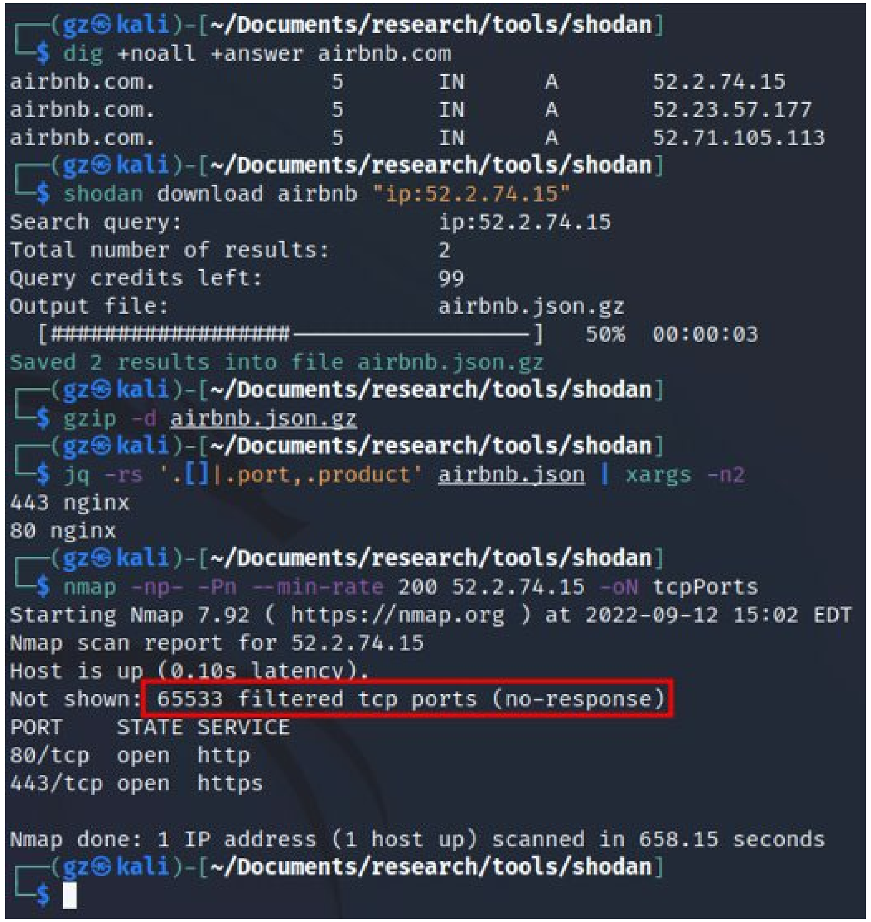
70.red-2-136-0.staticip.rima-tde.net

TELEFONICA DE ESPANA

```
MS-SQL NTLM Info:
  OS: Windows XP SP2
  OS Build: 5.1.2600
```

More than just Web

- Port Scan
  - Passive
    - Shodan
    - Censys
    - ZoomEye
  - Active
    - Nmap
    - Masscan



```
┌──(gz㉿kali)-[~/Documents/research/tools/shodan]
└─$ dig +noall +answer airbnb.com
airbnb.com.             5       IN      A       52.2.74.15
airbnb.com.             5       IN      A       52.23.57.177
airbnb.com.             5       IN      A       52.71.105.113
┌──(gz㉿kali)-[~/Documents/research/tools/shodan]
└─$ shodan download airbnb "ip:52.2.74.15"
Search query:                   ip:52.2.74.15
Total number of results:        2
Query credits left:             99
Output file:                    airbnb.json.gz
  [##################──────────────────]   50%  00:00:03
Saved 2 results into file airbnb.json.gz
┌──(gz㉿kali)-[~/Documents/research/tools/shodan]
└─$ gzip -d airbnb.json.gz
┌──(gz㉿kali)-[~/Documents/research/tools/shodan]
└─$ jq -rs '.[]|.port,.product' airbnb.json | xargs -n2
443 nginx
80 nginx
┌──(gz㉿kali)-[~/Documents/research/tools/shodan]
└─$ nmap -np- -Pn --min-rate 200 52.2.74.15 -oN tcpPorts
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 15:02 EDT
Nmap scan report for 52.2.74.15
Host is up (0.10s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 658.15 seconds
┌──(gz㉿kali)-[~/Documents/research/tools/shodan]
└─$ 
```

People Information Gathering

When there is too much information on the Internet

OSINT (Open-Source Intelligence)

- *Is the practice of collecting and analysing information gathered from open sources to produce actionable intelligence*
  - *Using open data to reveal information that organisations want to keep secret*
- Public information is more than just the Internet
- Open sources that feed into OSINT can be divided up into six categories of information flow:
  - **Public media:** newspaper, magazines, and television.
  - **Internet:** Online publications and blogs, discussion groups, forums, social media websites, etc.
  - **Public government data:** public government reports, budgets, press conferences, hearings, and speeches.
  - **Professional and academic publications:** Journals, conferences, academic papers, and theses.
  - **Commercial data:** Commercial imagery, business and financial assessments, and databases.
  - **Grey literature:** Technical reports, patents, business documents, unpublished works, and newsletters.
- Greatest OSINT sources
  - Clear Net
  - Deep Web
  - Dark Net
- Best tool: Search engines

European Commission

OSINT – Search Engines

- Search Engines: Google, Bing, DuckDuckGo, Yandex, Baidu, CarrotSearch, Ask, etc.
    - Specialised Search Engines: Wolfram, IntelligenceX, Shodan, Censys, ZoomEye, etc.
    - Advanced Search: Dorks (e.g.: GHDB: *Google Hacking Database*).
- Video Search Engine: Youtube (unlisted videos), Vimeo, etc.
- Reverse Image : Yandex, Bing, Google, TinEye, etc.
- Archives: Wayback Machine, etc.
- Source code: GitHub, GitLab, BitBucket, etc.

OSINT – Tools

- Social media accounts: namecheckup.com (also domains)
  - Search tool to check domain name and social media username availability over numerous popular networks/websites to have consistent names across multiple platforms.
- Leaked passwords: Passwords match those found in a list of stolen credentials?
  - HIBP (it does not show the password)
    - Check whether personal data has been compromised by data breaches.
    - Collects and analyzes hundreds of database dumps.
  - Pwndb (it used to be available on the *dark net* **Tor**)
    - Search leaked credentials
  - IntelligenceX (paid service, may offer some free information)
    - Online search tool, which gives a lot of information with a wide range of data sources: open web, deep web and dark web.
    - Used to perform threat analysis, search for security gaps, or analysis and forensics.
- Automated tools: theHarvester, Sherlock, etc.
  - Used during the reconnaissance stage of a red team assessment or penetration test.
  - Performs OSINT gathering to help determine a domain's external threat landscape. The tool gathers names, emails, IPs, subdomains, and URLs by using
  - multiple public resources.
- Password generators
  - CeWL (wordlist out of a webpage)
  - CUPP (wordlist out of a profile)

OSINT – Gathering Emails

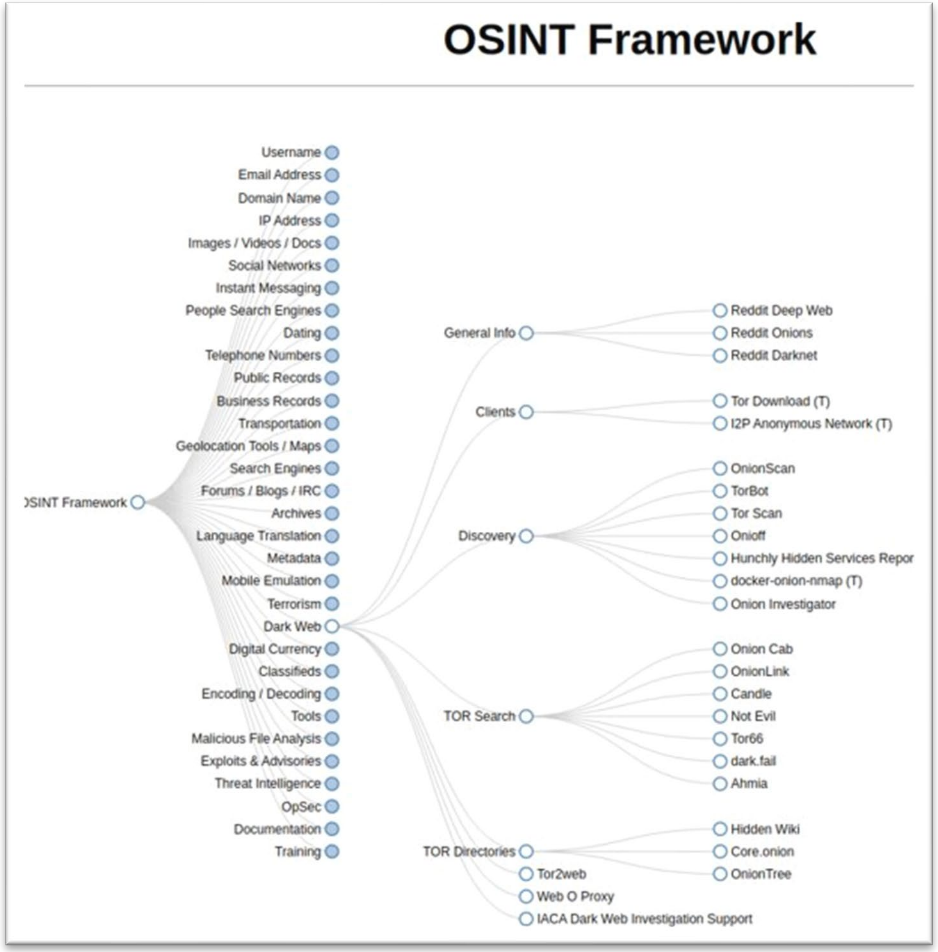
1. What is the domain of the organisation/corporation?
   - https://www.crunchbase.com/, search engines.
     - Provide business information about public and private companies
2. What is the email format they use?
   - https://hunter.io/
3. Create emails with (ex-)employees from LinkedIn:
   - CrossLinked
4. Which of those emails are valid?
   - https://www.verifyemailaddress.org/

- Is there a better/suplementary way? Phonebook.cz (by IntelligenceX)

OSINT - Frameworks

- Many OSINT tools
- Recopilation:
  - OSINTFramework
  - Awesome-OSINT
- OSINT tools integrated: Obtain, visualize and analyze data
  - IKy
  - Lampyre
  - Maltego

Implementation



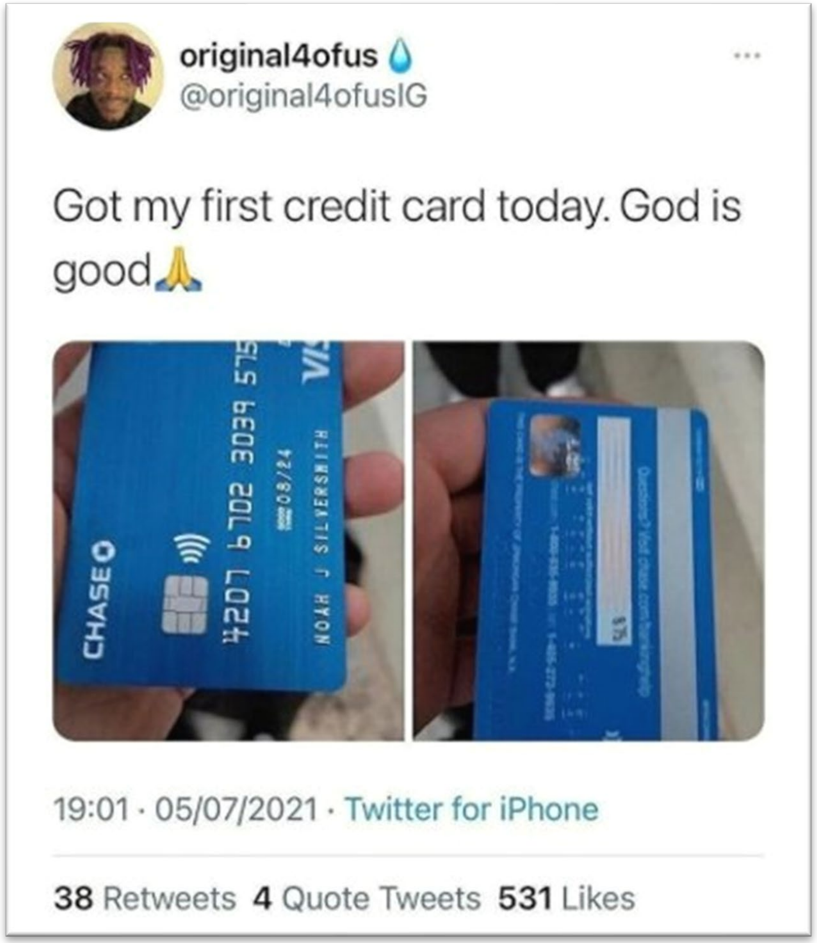
People Hacking

The weakest link

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Social Engineering

- *"An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks."*
- Human Vulnerabilities
  - Intense Emotions
    - Fear
    - Euphoria
    - Curiosity
    - Rage
    - Guilt
  - Urgency
  - Trust


original4ofus 💧
@original4ofusIG

Got my first credit card today. God is good🙏

19:01 · 05/07/2021 · Twitter for iPhone

38 Retweets 4 Quote Tweets 531 Likes

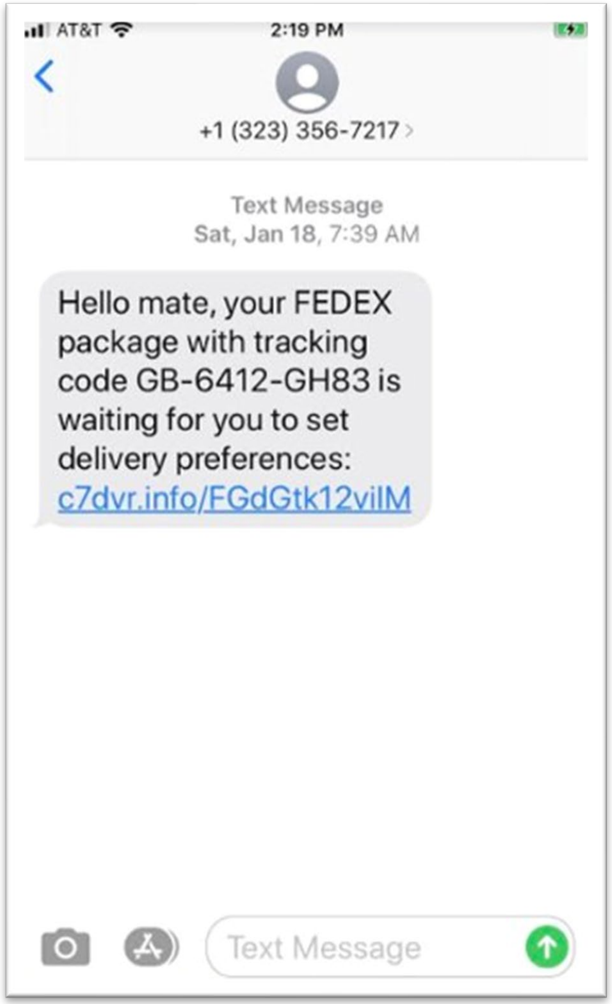
Social Engineering - Phishing

- Spam (*mass phishing*)
    - Smishing (*SMS phishing*)
- Vishing (*Voice phishing*)
- Pharming
    - Redirect users into a fake Web site masquerading as a legitimate one to steal their credentials and personal information.
- Spear Phishing (*targeted phishing attack*)
    - Whaling (*target high-ranking members of organizations*)

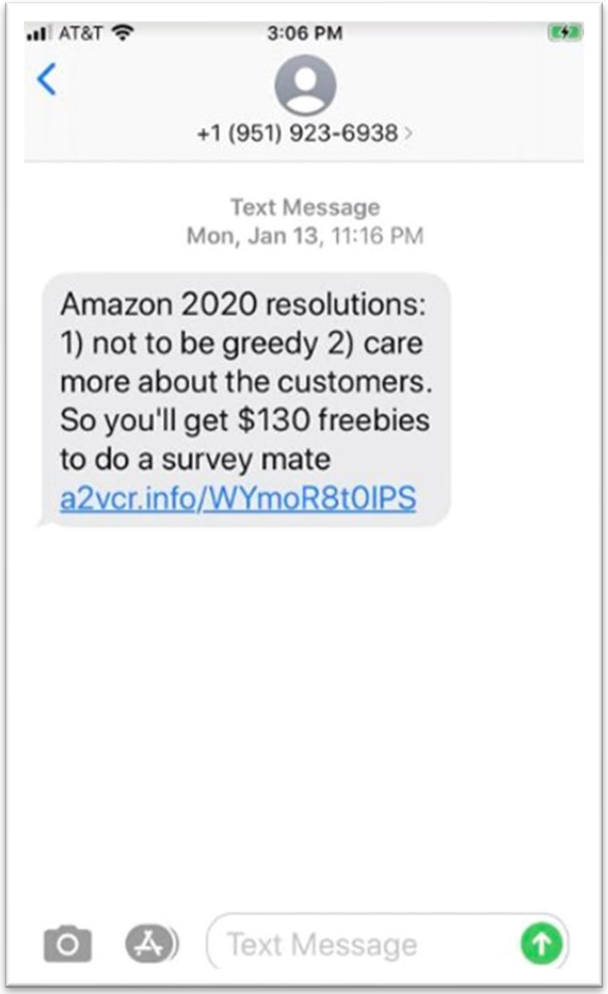
Some Techniques
Spoof sender email
Attach malicious files
Use of malicious links

Some Features of mass phishing
Generic, not personalised
Loads of typos
Unnatural writing
Senseless messages

Social Engineering – Phishing – Smishing



Hello mate, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: c7dvr.info/FGdGtk12vilM



Amazon 2020 resolutions: 1) not to be greedy 2) care more about the customers. So you'll get $130 freebies to do a survey mate a2vcr.info/WYmoR8t0IPS

Social Engineering – Phishing – Vishing

- More effective
  - Immediate response – little or no time to think
  - Victim's feedback – attacker can manipulate them
  - People tend to trust voice call more
- Some common methods
  - Virtual kidnapping (link)
  - Computer technician calling for a virus
  - Romance scam

Techniques
Spoof telephone number
Record your voice
Synthesize someone's voice

Social Engineering – Phishing – Masking URLs

- Masking link with another link
  - Example: `<a href="malicious.site">google.com</a>`
  - Solution: Hover over links
- Triggering a function through an event
  - Example: `<img src="cat.jpg" onhover="fetch('malicious.site')"/>`
  - Solution: Deactivate Scripts on the browser
- Using short links
  - Solution: Use an unshortener, e.g.: unshorten.it.

Social Engineering – Phishing – Typosquatting

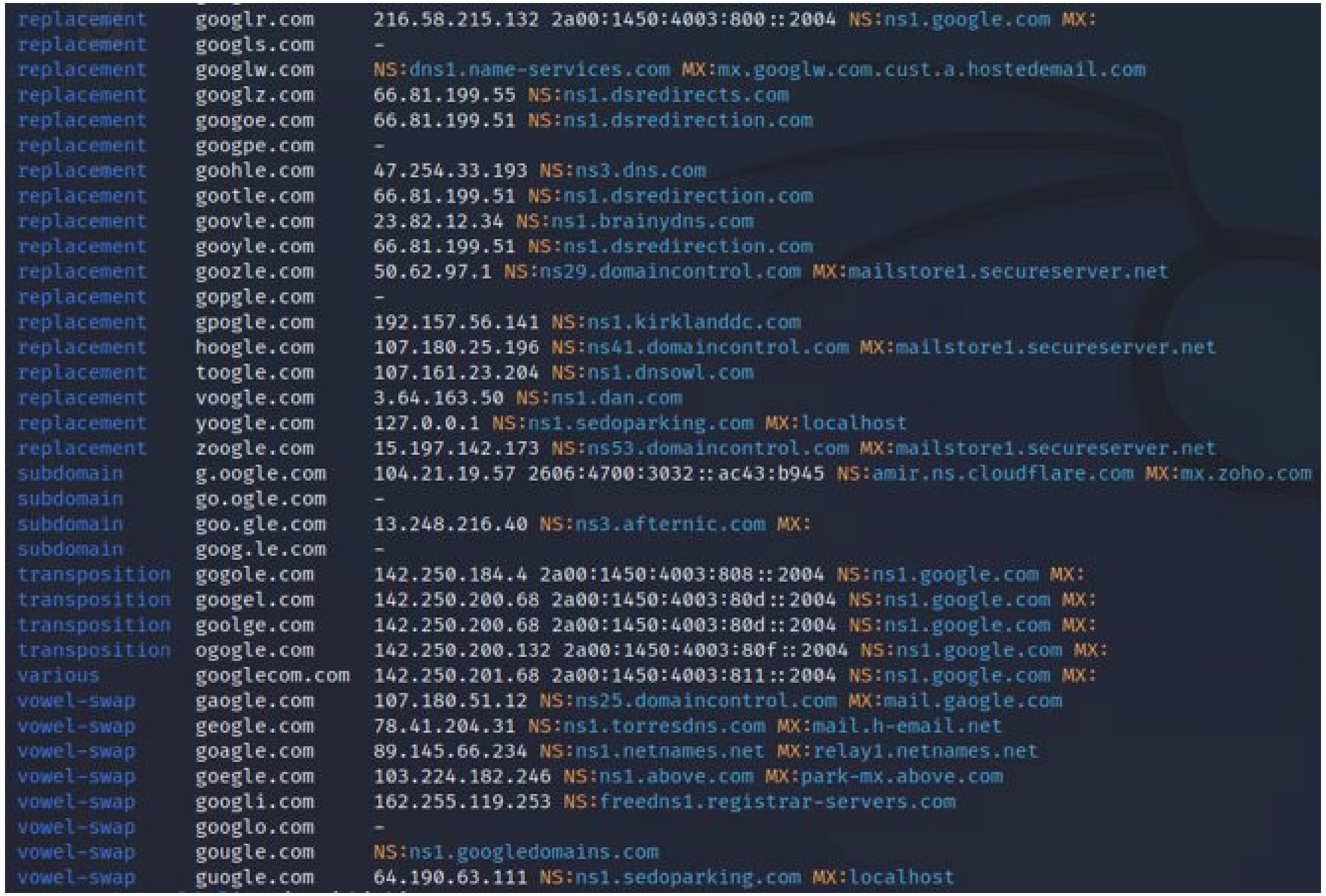
- Registering a misspelled domain

technique	example	technique	example
omission	gogle.com	hyphenation	goo-gle.com
repetition	gooogle.com	subdomain	g.oogle.com
insertion	googl1e.com	homoglyph	goog£e.com
transposition	goolge.com	bitsquatting	coogle.com

- Easy to spot, isn't it?

Social Engineering – Phishing – Typosquatting

- Generation
  - DNSTwist:
    - Generates a list of similarly looking domain names for a given domain name and performs DNS queries for them
    - Web
    - CLI



```
replacement    googlr.com     216.58.215.132 2a00:1450:4003:800::2004 NS:ns1.google.com MX:
replacement    googls.com     -
replacement    googlw.com     NS:dns1.name-services.com MX:mx.googlw.com.cust.a.hostedemail.com
replacement    googlz.com     66.81.199.55 NS:ns1.dsredirects.com
replacement    googoe.com     66.81.199.51 NS:ns1.dsredirection.com
replacement    googpe.com     -
replacement    goohle.com     47.254.33.193 NS:ns3.dns.com
replacement    gootle.com     66.81.199.51 NS:ns1.dsredirection.com
replacement    goovle.com     23.82.12.34 NS:ns1.brainydns.com
replacement    gooyle.com     66.81.199.51 NS:ns1.dsredirection.com
replacement    goozle.com     50.62.97.1 NS:ns29.domaincontrol.com MX:mailstore1.secureserver.net
replacement    gopgle.com     -
replacement    gpogle.com     192.157.56.141 NS:ns1.kirklanddc.com
replacement    hoogle.com     107.180.25.196 NS:ns41.domaincontrol.com MX:mailstore1.secureserver.net
replacement    toogle.com     107.161.23.204 NS:ns1.dnsowl.com
replacement    voogle.com     3.64.163.50 NS:ns1.dan.com
replacement    yoogle.com     127.0.0.1 NS:ns1.sedoparking.com MX:localhost
replacement    zoogle.com     15.197.142.173 NS:ns53.domaincontrol.com MX:mailstore1.secureserver.net
subdomain      g.oogle.com    104.21.19.57 2606:4700:3032::ac43:b945 NS:amir.ns.cloudflare.com MX:mx.zoho.com
subdomain      go.ogle.com    -
subdomain      goo.gle.com    13.248.216.40 NS:ns3.afternic.com MX:
subdomain      goog.le.com    -
transposition  gogole.com     142.250.184.4 2a00:1450:4003:808::2004 NS:ns1.google.com MX:
transposition  googel.com     142.250.200.68 2a00:1450:4003:80d::2004 NS:ns1.google.com MX:
transposition  goolge.com     142.250.200.68 2a00:1450:4003:80d::2004 NS:ns1.google.com MX:
transposition  ogogle.com     142.250.200.132 2a00:1450:4003:80f::2004 NS:ns1.google.com MX:
various        googlecom.com  142.250.201.68 2a00:1450:4003:811::2004 NS:ns1.google.com MX:
vowel-swap     gaogle.com     107.180.51.12 NS:ns25.domaincontrol.com MX:mail.gaogle.com
vowel-swap     geogle.com     78.41.204.31 NS:ns1.torresdns.com MX:mail.h-email.net
vowel-swap     goagle.com     89.145.66.234 NS:ns1.netnames.net MX:relay1.netnames.net
vowel-swap     goegle.com     103.224.182.246 NS:ns1.above.com MX:park-mx.above.com
vowel-swap     googli.com     162.255.119.253 NS:freedns1.registrar-servers.com
vowel-swap     googlo.com     -
vowel-swap     gougle.com     NS:ns1.googledomains.com
vowel-swap     guogle.com     64.190.63.111 NS:ns1.sedoparking.com MX:localhost
```

Social Engineering – Quizzes

- Phishingbox: https://www.phishingbox.com/phishing-iq-test
- Complete-it (context): https://www.complete-it.co.uk/cyber-security-phishing-quiz/
- Security Inside (actions taken): https://phishingquiz.securityinside.com/quiz/start?id=1
- Google Phishing Quiz (interactive): https://phishingquiz.withgoogle.com/

InfoSec culture:

- CybSafe (interactive): https://www.cybsafe.com/quizzes/

Social Engineering – USB – USB Drop

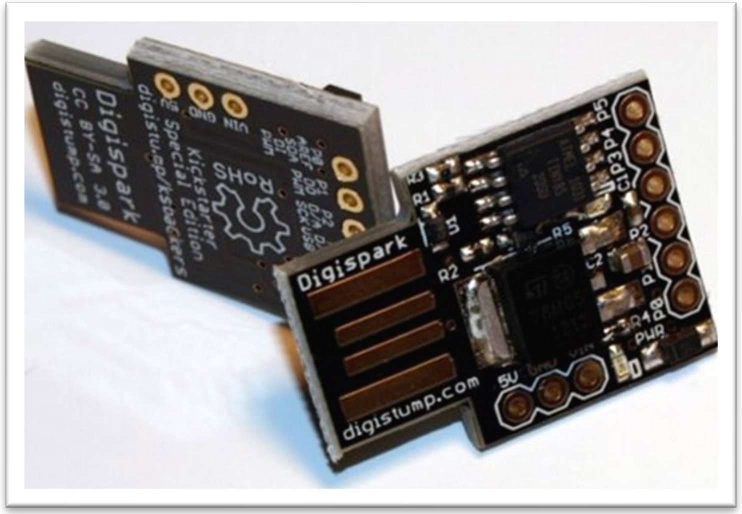
I have just found a thumb drive, lucky me!

- Attack vectors
  - Social Engineering
    - Vulnerability: curiosity
    - Bait (appealing): salary, XXX, etc.
  - HID Spoofing (e.g.: Rubber Ducky)
  - 0-day (e.g.: *Stuxnet*)

Does dropping USB drives really work? BlackHat USA (2006)

Social Engineering – USB – Rubber Ducky

- HID (Human Interface Device)
  - It behaves as a keyboard
  - It bypasses USB block policies
- It looks similar to a USB Pen drive.
- It is used to hack a system, steal victims essential an credential data



Social Engineering – USB – Juice Jacking

The dangers of public USB charging stations

Malware installed through a corrupted USB port can lock a device or export personal data and passwords

- Solution
  - Carry your own portable charger
  - Use a Datablocker

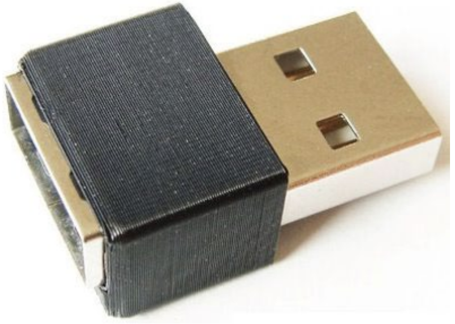
Malware

Malware (***Mal**icious Soft**ware***)

- Some examples
    - Virus
        - Ransomware
    - Worm
    - Trojan
    - Backdoor
    - Spyware
        - Keylogger
        - Screenlogger
    - Logic/Time bomb

Malware – Spyware – Keylogger

- Target information: credentials, cryptowallets, PINs, etc.
- Types
  - Hardware
  - Software
    - Local
    - Remote



[O.MG cable](#)

Malware – Spyware – Screenlogger

- Target information: credentials, cryptowallets, PINs, etc.
- Types
  - Hardware
  - Software
- There is a context, unlike with a keylogger
- Content from protected fields not seen
  - Example: <input type="password" name="pwd">
  - Solution: use along with keylogger

Extra Resources

There is more...

Documentaries, presentations, CTFs and more

- From email address to telephone number. A new OSINT approach, by Martin Vigo (BSides 2019) [31:05].
- Live recon and automation on Shopify's Bug Bounty Program with @TomNomNom (NahamSecCon 2021) [1:17:17].
- The Bug Hunter's methodology v4 – Recon edition by @jhaddix (NahamSecCon 2020) [1:39:42].
- Anatomy of a Killing – BBC [11:06].
- Hackers Find Missing People for Fun [6:06].
- CTF (Capture The Flag): cybersecurity challenges.
  - Contests: https://ctftime.org/
  - Set of CTF pages: https://ctfsites.github.io/
  - OSINT CTFs: OsintDojo, OsintGames, Trace Labs (searching for missing people).
  - DFIR CTFs: CyberDefenders.
  - Web3 CTFs: Ethernaut (Smart Contracts).
- Bug bounty platforms: websites where companies' security can be assessed and "pay" for bugs hunted.
  - BugCrowd, HackerOne, Intigriti.
- More (useful?) links: IsItHacked, IsItUp, PanoptiClick.

References

Links

- *https://domaineye.com/reverse-whois/*
- *https://github.com/OWASP/Amass*
- *https://github.com/fwaeytens/dnsenum*
- *https://github.com/darkoperator/dnsrecon*
- *https://github.com/aboul3la/Sublist3r*
- *zonetransfer.me*
- *https://github.com/ffuf/ffuf*
- *https://github.com/tomnomnom/assetfinder*
- *https://github.com/tomnomnom/httprobe*
- *https://github.com/tomnomnom/waybackurls*
- *https://github.com/tomnomnom/anew*
- *https://github.com/wappalyzer/wappalyzer*
- *https://github.com/urbanadventurer/WhatWeb*
- *https://github.com/zaproxy/zaproxy*
- *https://portswigger.net/burp/communitydownload*

Links

- https://cheatsheet.haax.fr/open-source-intelligence-osint/dorks/github_dorks/
- https://github.com/random-robbie/keywords/blob/master/keywords.txt
- https://github.com/obheda12/GitDorker
- https://github.com/ROCXYROCK/CTF_Beginners_Git_Challenge
- https://www.shodan.io/search/filters (Shodan dorks)
- https://github.com/achillean/shodan-python
- https://censys.io/
- https://search.censys.io/search/examples?resource=hosts (Censys dorks)
- https://nmap.org/
- http://advangle.com/ (Dorks)
- https://www.exploit-db.com/google-hacking-database (GHDB)
- https://unlistedvideos.com/ (unlisted Youtube videos)
- https://archive.org/search.php (WaybackMachine)
- https://github.com/laramies/theHarvester (theHarvester)
- https://github.com/sherlock-project/sherlock (Sherlock)

Links

- https://www.namecheck.com/
- https://haveibeenpwned.com/ (HIBP)
- https://intelx.io/ (IntelligenceX)
- https://github.com/martintjj/BreachCompilation
- https://pwdquery.xyz/
- https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- https://github.com/digininja/cewl
- https://github.com/Mebus/cupp
- https://www.crunchbase.com/
- https://hunter.io/
- https://github.com/m8sec/CrossLinked
- https://www.verifyemailaddress.org/
- https://phonebook.cz/
- https://gchq.github.io/CyberChef/
- https://crackstation.net/

Links

- https://howsecureismypassword.net/
- https://en.wikipedia.org/wiki/List_of_the_most_common_passwords
- https://whatsmyname.app/
- https://osintframework.com/
- https://www.maltego.com/
- https://kennbroorg.gitlab.io/ikyweb/
- https://lampyre.io/
- https://github.com/jivoi/awesome-osint
- https://github.com/smicallef/spiderfoot
- https://www.fakenamegenerator.com/
- https://thispersondoesnotexist.com/
- https://hushed.com/ (Virtual phone number service)
- https://www.voicemod.net/
- https://www.youtube.com/watch?v=qTgPSKKjfVg (DALL-E 2)
- https://onemilliontweetmap.com/

Links

- https://iknowwhereyourcatlives.com/
- https://iknowwhatyoudownload.com
- https://www.canarytokens.org/
- https://www.youtube.com/watch?v=opRMrEfAIiI (What is your password?)
- https://cybernews.com/editorial/fake-kidnap-scams-from-a-prison-cell-in-mexico-to-the-boardroom-of-a-top-firm/
- https://www.which.co.uk/consumer-rights/advice/microsoft-phone-scam-aYceu8o7aO4c
- https://www.truecaller.com/
- https://www.listarobinson.es/
- https://dnstwist.it/ (DNSTwist web)
- https://github.com/elceef/dnstwist.git (DNSTwist CLI)
- https://www.punycoder.com/
- https://www.lexilogos.com/keyboard/russian.htm
- https://www.irongeek.com/homoglyph-attack-generator.php
- https://urlvoid.com/
- https://urlscan.io/

Links

- https://dnsdumpster.com
- https://talosintelligence.com/
- https://www.virustotal.com/
- https://www.phishingbox.com/phishing-iq-test (phishing quiz)
- https://www.complete-it.co.uk/cyber-security-phishing-quiz/ (phishing quiz)
- https://phishingquiz.securityinside.com/quiz/start?id=1 (phishing quiz)
- https://phishingquiz.withgoogle.com/ (phishing quiz)
- https://www.cybsafe.com/quizzes/ (quiz)
- https://www.youtube.com/watch?v=ZI5fvU5QKwQ (USB drop - BlackHat USA 2016)
- https://juicejacking.org/product/datablock/
- https://usbkill.com/
- https://www.youtube.com/c/UsbKill (Testing the USBKill)
- https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers
- https://www.youtube.com/watch?v=-jL_Xz-BKBM (O.MG Keylogger cable)
- https://www.keydemon.com/ (Spyware)