Mapping and Analyzing exposed devices

By Brutal Panda

Whoami

- Cyber security enthusiastic
- CTF and emulations
- Gamer

TOC

Intro

As Security Researchers we are curious about everything happening around us starting from devices we use daily to new technology booming around us any tech gadget that .

Why?

Mapping and analyzing exposed devices is a critical part of cybersecurity research because it allows researchers to identify and understand the attack surface of the internet. This information can be used to develop new security controls and techniques, and to prioritize remediation efforts.

(OSINT , Malware , Threat Intel & Hunt)

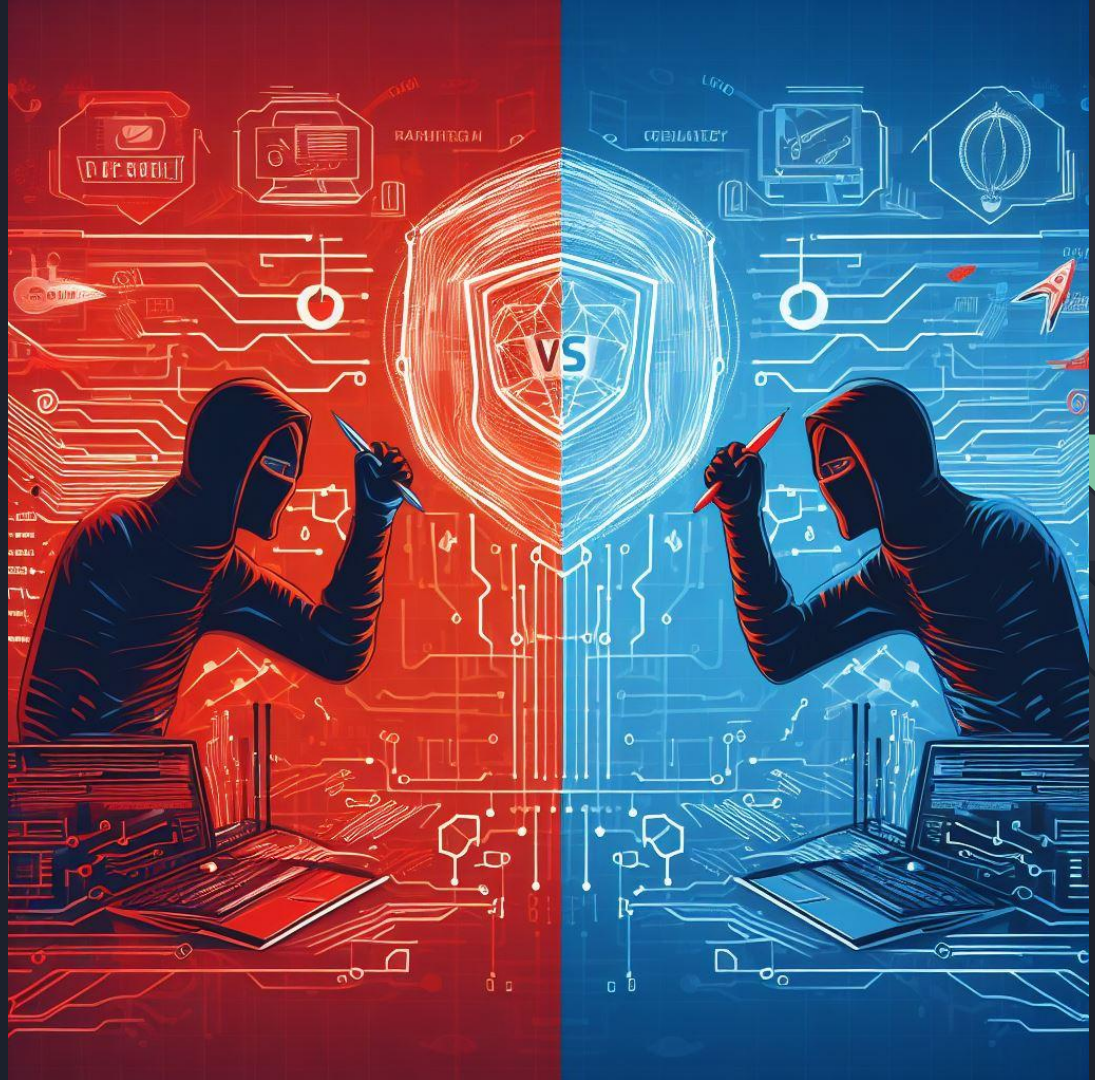
Methodology

Internet Based (TCP/IP)

- Shodan io
- Censys.com
- FOFA.info

Other devices

- Wigle


VS

- Shodan
- Censys

Red Team

- Searching domain names
- Searching vulnerability
- OSINT

Malicious Actors

- Cyber Attack Campaigns
- C2 servers hosting

As a red teamer, you can passively scan for open ports and vulnerabilities on a target host and its subdomains without interacting with the host itself.

// TAGS: cloud self-signed

// LAST SEEN: 2023-11-13

General Information

Cloud Provider [redacted]

Country [redacted]

City [redacted]

Organization [redacted]

ISP [redacted]

ASN [redacted]

Open Ports

22 53 80 443 2083 5005 8443

// 22 / TCP

-1414421435 | 2023-11-13T04:40:09.350903

OpenSSH 8.2p1 Ubuntu-4ubuntu0.8

```
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.8
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDw88vaSHzQuX5Rw3pDFw5Im+AvYeZ7evnwemmXpAihjPcC
FgC9z1MCKaPT1Wp+455+WDE37WrHQlgCB5h/Lf6UaXrcHNIVFHMuz4YyJ/5rafSg3cdOZYOxsJ063
hBgwUY8v+l5zz3AmVVMmcqXDQ3Al04t0ryI1Q/i/zKyFGee6D5ZrY3eNEbjCuk0NK2yXAgWMpk01
ruvwVG3oGzWgXTa8xnBTQFHtqTHmXEGiHN3mZYfQYIa/OUMaV7jycxKSJw0VeGHpOnXP90tTe2ge
eg93YDvtyqOYNDee65hMqX2mlVXPLfN2y3AtfOPQk/GXkpm4tn18+mlV79uchvny26SNMWe2BcxI
kaL7t/gYBHaQQIxj7q79bRHnEwHUAcZhDitX4jygk3hOHHIvB1BYswehxTX35JLpVh/EYR7fGvz4
7bK3THuh425Rypjiee5EEHuZhYwrdUq1d9w1Sgd5dpIO8N6D07IBWR1VXCdQg5OHHqWl9rDTw95n
YoJ290d65ec=
Fingerprint: 2a:60:47:28:95:64:0d:16:4e:d0:bb:3f:a9:55:4e:00

Kex Algorithms:
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group14-sha256
```

Web Technologies

JavaScript Libraries

jQuery 3.5.1

UI Frameworks

Bootstrap 4.5.0

Vulnerabilities

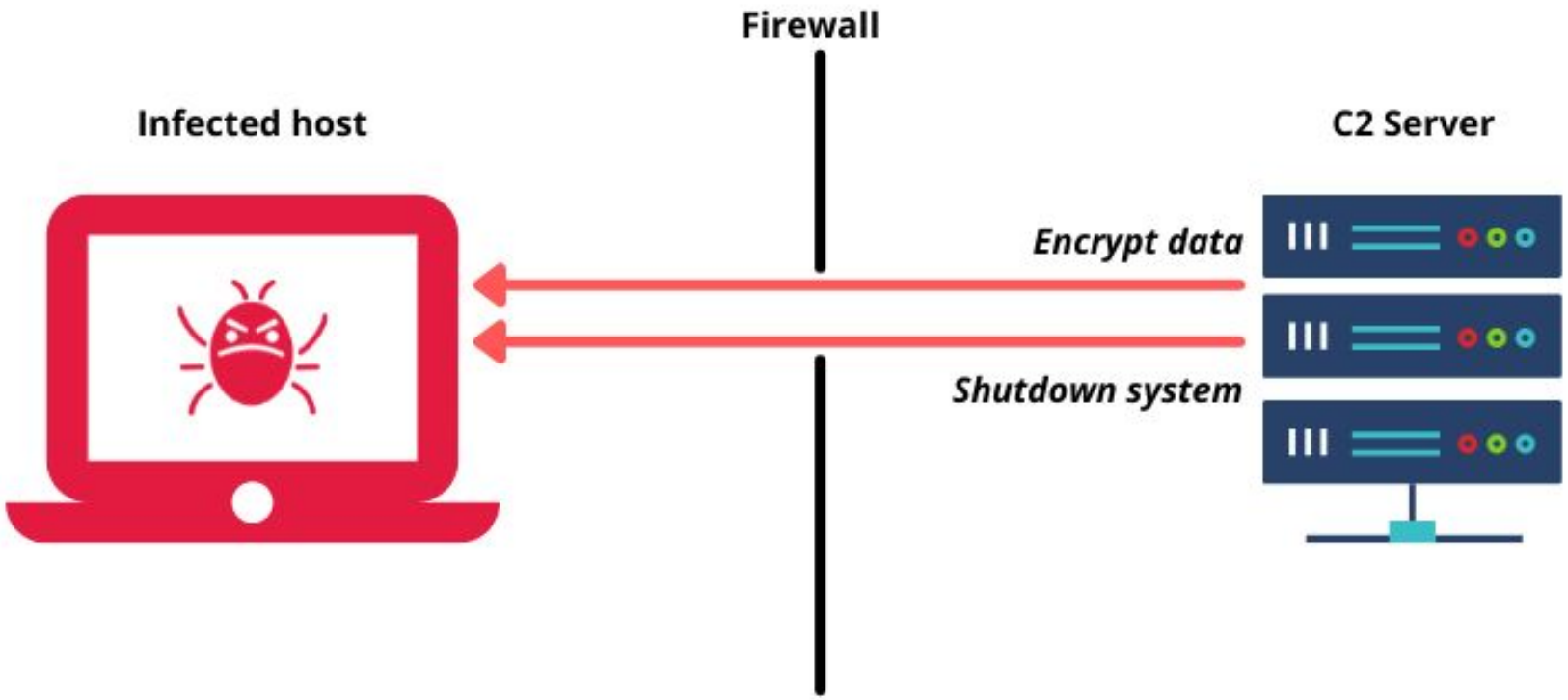
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-25690 Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; |P| ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

CVE-2022-37436 Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

Hunting C2 servers

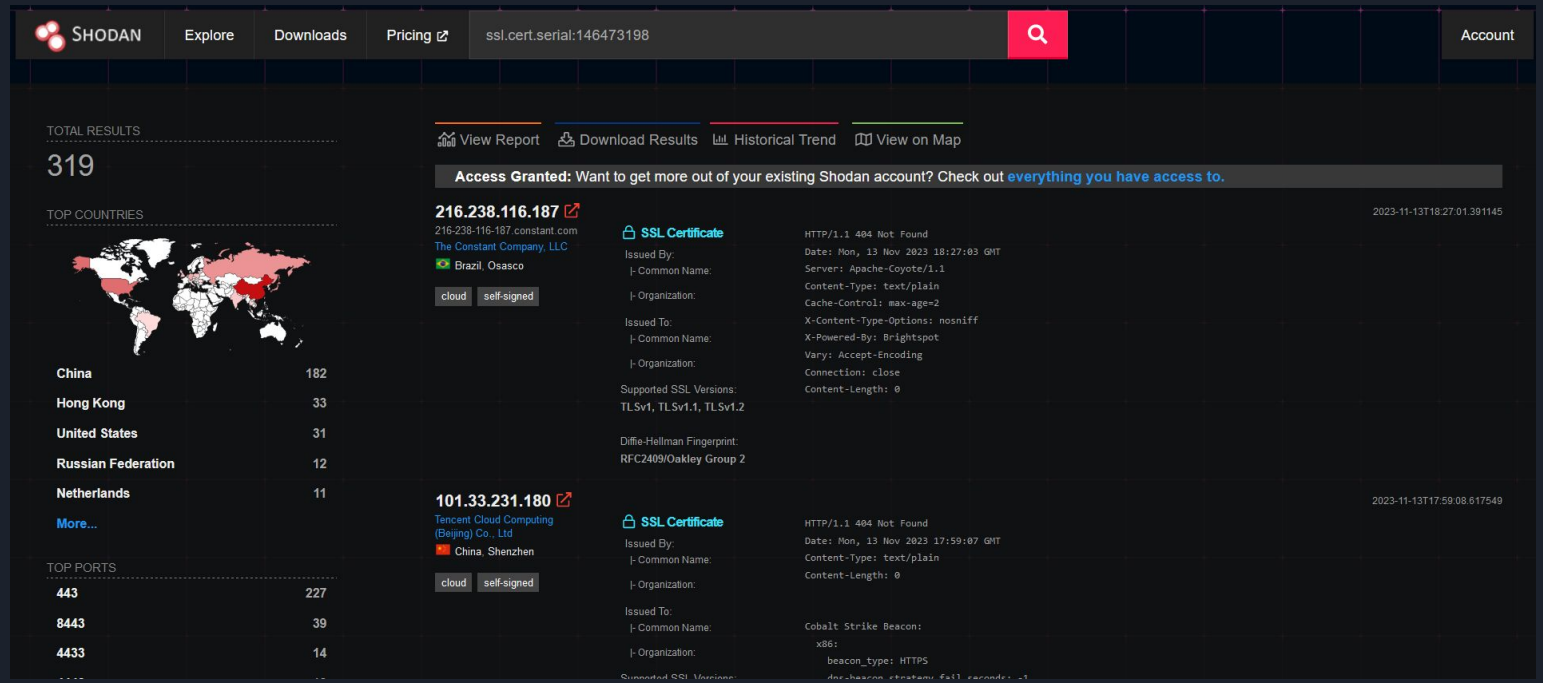
C2 is a command-and-control server that allows malware to communicate and receive commands. We can use tools like Shodan to hunt down malware.


Firewall
Infected host
C2 Server
Encrypt data
Shutdown system

- Threat Hunting
- Threat Intel
- Hunting APT (Advanced Threat groups)


NEXT GEN C2
IMPOSSIBLE TO DETECT
BEHIND PROXY
OPENDIR
BODY HASH

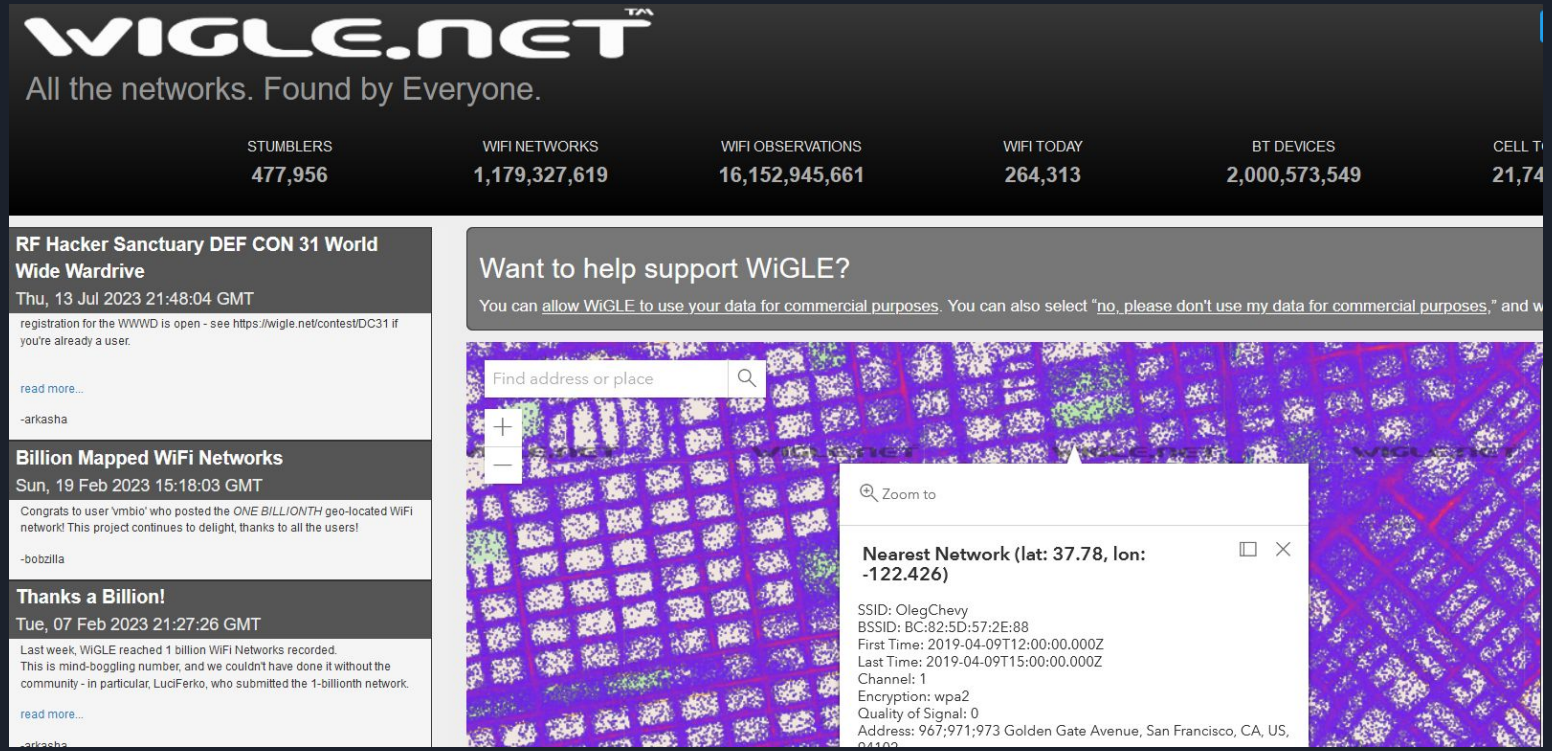
We can use shodan to hunt C2 servers such as cobalt strike framework through different mechanisms we can see one method as following for more u can read [this](). You can see how powerful shodan can used for threat hunting process.

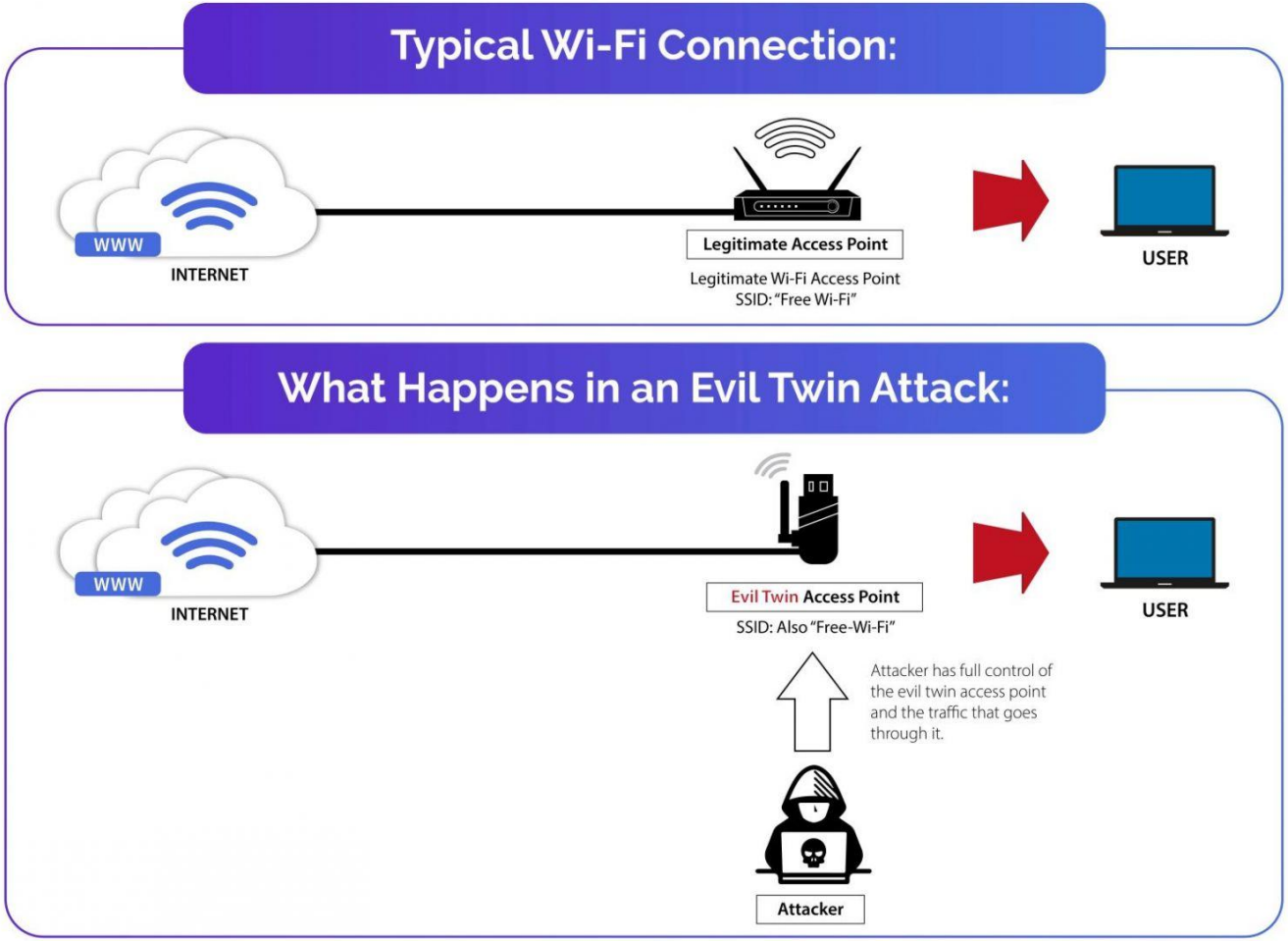


Wigle

- Android
- Bluetooth
- Cars (BUS)
- War driving

An attacker can use Wigle to impersonate a Wi-Fi network in order to trick a user into connecting to it and launching an evil twin attack or similar attacks.




Typical Wi-Fi Connection:
WWW
INTERNET
Legitimate Access Point
Legitimate Wi-Fi Access Point
SSID: "Free Wi-Fi"
USER
What Happens in an Evil Twin Attack:
WWW
INTERNET
Evil Twin Access Point
SSID: Also "Free-Wi-Fi"
USER
Attacker has full control of the evil twin access point and the traffic that goes through it.
Attacker