UNIT 42 BY PALO ALTO NETWORKS   Paul | Weiss

What does your organization look like to a bad guy?

An opportunity.

John Carlin | Partner, Paul Weiss

Ross Worden | Senior Consulting Director, Palo Alto Networks Unit 42

paloalto NETWORKS

Speaker Introductions

John Carlin
Partner
Paul, Weiss, Rifkind,
Wharton & Garrison LLP
jcarlin@paulweiss.com

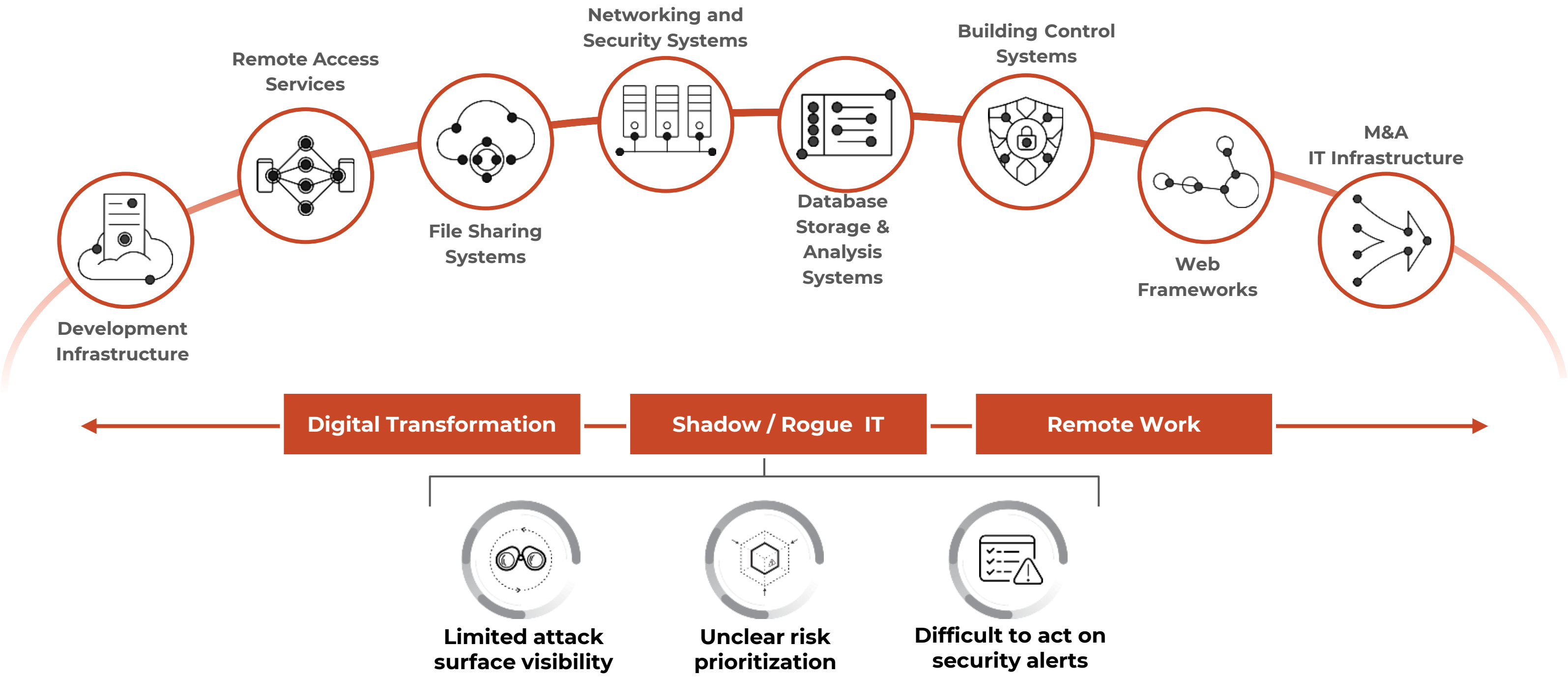
Ross Worden
Senior Consulting Director
Palo Alto Networks Unit 42
rworden@paloaltonetworks.com

Agenda

- Why is Attack Surface Management (ASM) Important?
- Tools & Use Cases
- Read the 2022 Attack Surface Threat Report

Why is Attack Surface Management Important?

Your IT infrastructure is Responsible for Generating Billions of Dollars in Revenue - Do your IT people know what they have? Process, Tech failures. Conscious risk acceptance vs unknown unknowns



Development Infrastructure

Remote Access Services

File Sharing Systems

Networking and Security Systems

Database Storage & Analysis Systems

Building Control Systems

Web Frameworks

M&A IT Infrastructure

Digital Transformation

Shadow / Rogue IT

Remote Work

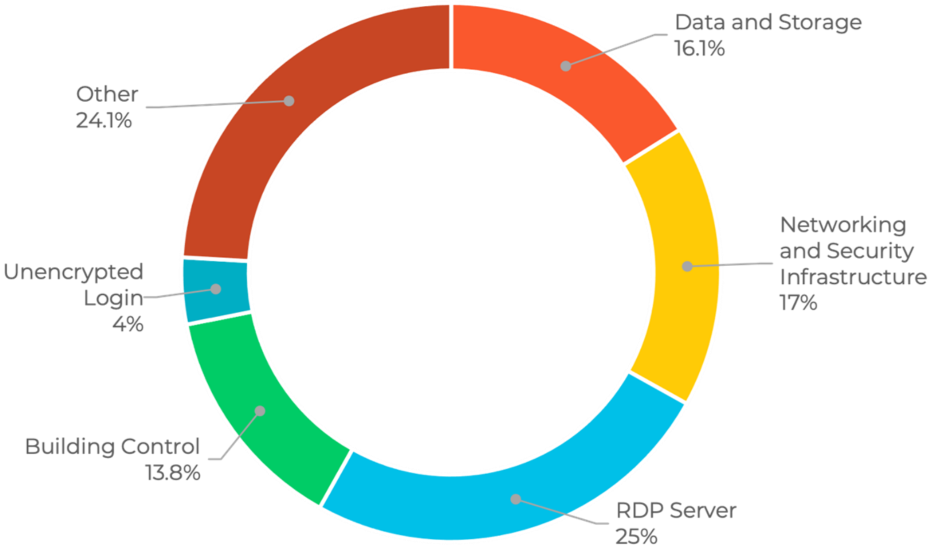
Limited attack surface visibility

Unclear risk prioritization

Difficult to act on security alerts

Modern Attack Surface Is Fragmented and Growing

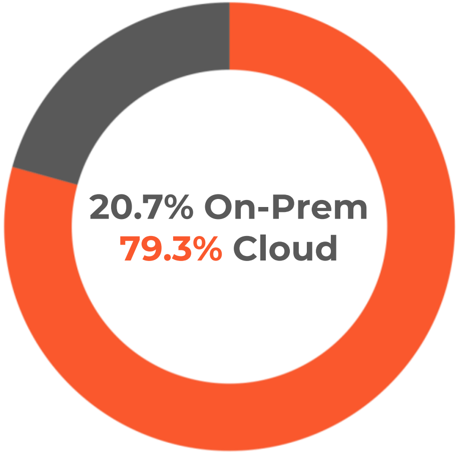
- Nearly **1 out of 4** issues found on the attack surface was related to RDP servers
- **Networking equipment** related vulnerabilities were the second largest type of issues found on the attack surface.
- Exposed Data Storage and Analysis systems are also prevalent and could **lead to data leaks** and **exfiltration**.

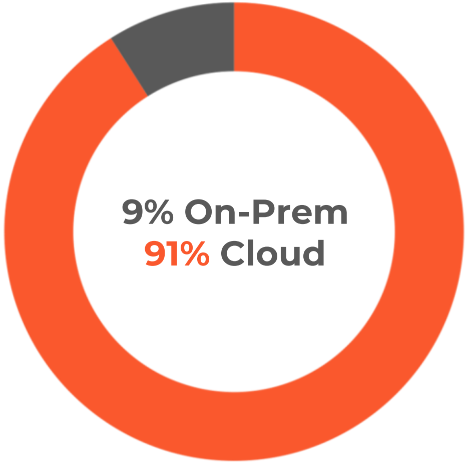


Distribution of risks across the global attack surface

Source - 2022 Cortex Xpanse Attack Surface Threat Report

Cloud Continues To Be a Target





Per data from mid-2021, nearly 80% of new issues discovered were in the cloud (left), but that number jumped to 91% in the first half of 2022 (right)

Source - 2022 Cortex Xpanse Attack Surface Threat Report

End-of-Life and Unpatched Software Risk

ASM findings provide environmental context and and visibility into security program gaps

Apache Web Server	Microsoft Exchange Server
~32% of scanned organizations were running EOL versions	**29%** of scanned organizations were running EOL/unsupported versions

Attack surface scans showed organizations across industries are:

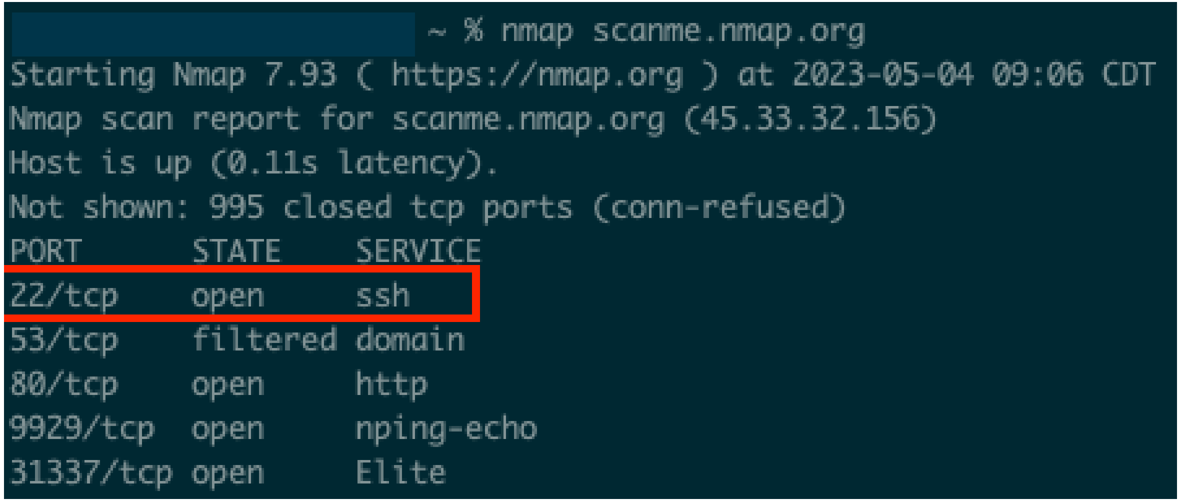
- **Running end-of-life versions of software**
- **Running unpatched software with known exploits, even when patches are available**

Source - 2022 Cortex Xpanse Attack Surface Threat Report

Tools & Use Cases

Nmap: Free network utility

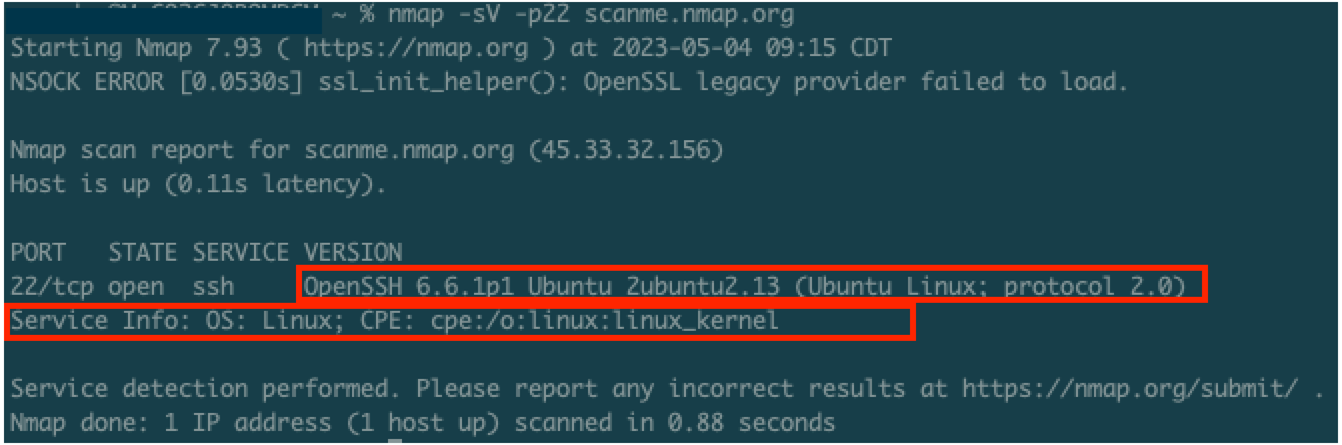
- That can also be used to perform reconnaissance against your network
- Here, we see that a sensitive service (SSH) is exposed to the internet
  - This is not good, but how bad is it?
  - To answer this, we need to know what version of SSH is running and other information



```
[redacted] ~ % nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 09:06 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
53/tcp    filtered domain
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
```

Nmap can provide this information with another command

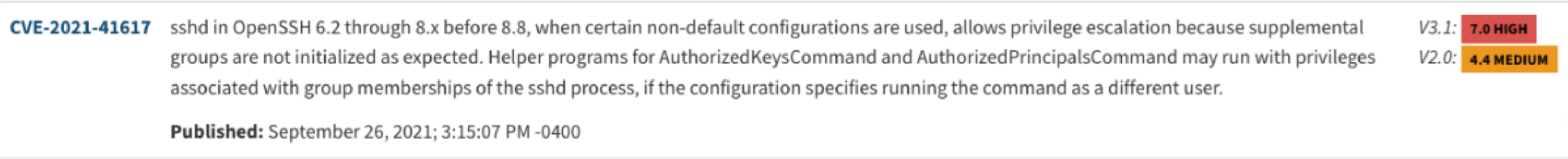
- One command tells us that OpenSSH version 6.6.1p1 is running on Ubuntu - the current version is 9.1
- Is this older version of OpenSSH vulnerable to exploits?



```
[redacted] ~ % nmap -sV -p22 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 09:15 CDT
NSOCK ERROR [0.0530s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.11s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
```

Nmap + National Vulnerability Database (NVD)

- NVD is run by NIST and provides a searchable database of vulnerabilities by software, version, and other variables.
- It also provides severity scores that can help with triage
- In this case, OpenSSH 6.6.1p has a high risk vulnerability associated with it
- The next step would be to find or develop an exploit and deploy it
    - Many of these exploits are freely available online or available for purchase on the dark web



CVE-2021-41617 sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

V3.1: **7.0 HIGH**

V2.0: **4.4 MEDIUM**

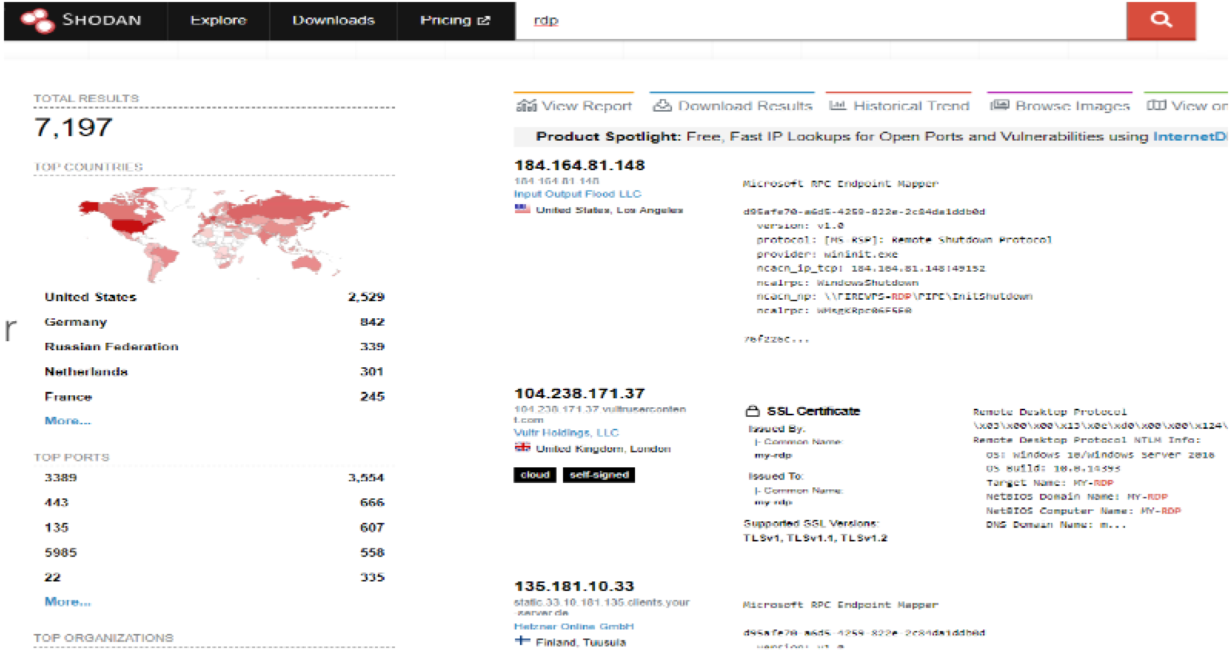
Published: September 26, 2021; 3:15:07 PM -0400

Shodan - internet scanner

- Shodan is free (upgrades paid) and scans the internet for interesting ports, infrastructure, etc.
- It only identifies internet-accessible resources
- Frequently used by threat actors to identify vulnerable systems en masse

Shodan - easily find exploitable servers

- RDP exposures on the internet
- RDP is commonly attacked by threat actors
- You can see RDP versions, IP addresses, their locations, even “handshake” information



TOTAL RESULTS

7,197

TOP COUNTRIES

United States	2,529
Germany	842
Russian Federation	339
Netherlands	301
France	245

More...

TOP PORTS

3389	3,554
443	666
135	607
5985	558
22	335

More...

TOP ORGANIZATIONS

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetD

184.164.81.148
184.164.81.148
Input Output Flood LLC
United States, Los Angeles

```
Microsoft RPC Endpoint Mapper

d95afe70-a6d5-4259-822e-2c84da1ddb0d
  version: v1.0
  protocol: [MS-RSP]: Remote Shutdown Protocol
  provider: wininit.exe
  ncacn_ip_tcp: 184.164.81.148:49152
  ncalrpc: WindowsShutdown
  ncacn_np: \\FIREVPS-RDP\PIPE\InitShutdown
  ncalrpc: WMsgKRpc06F5E0

76f226c...
```

104.238.171.37
104.238.171.37.vultrusercontent.com
Vultr Holdings, LLC
United Kingdom, London

cloud | self-signed

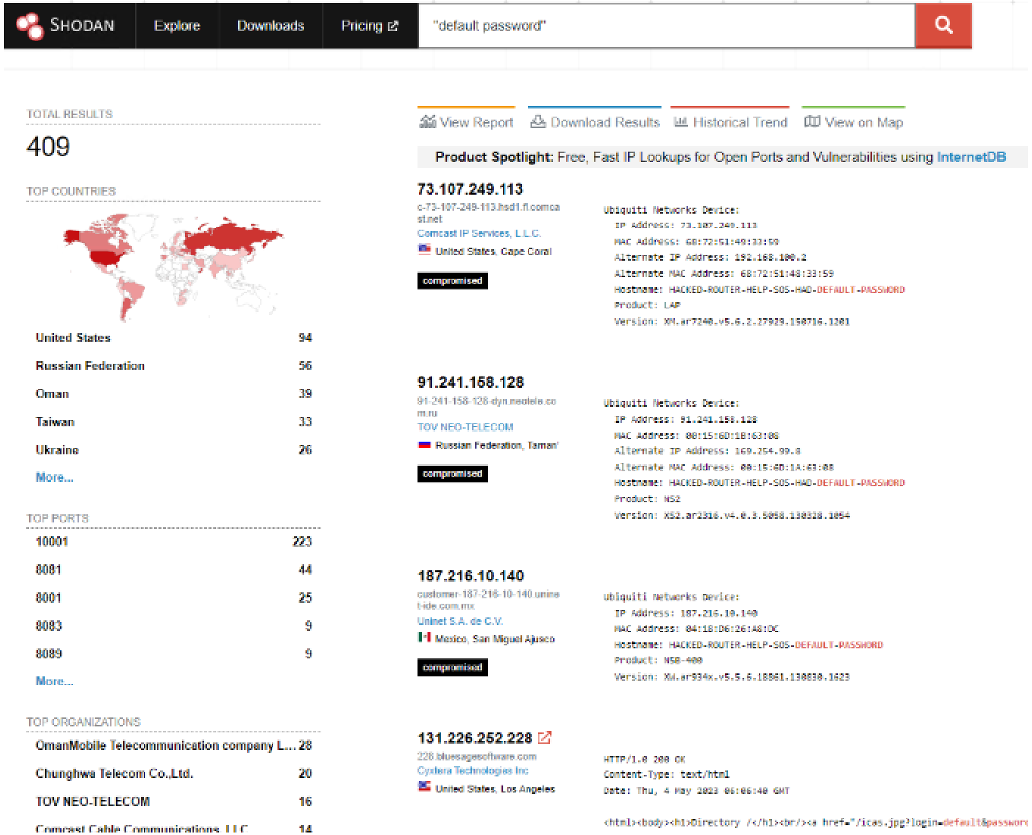
SSL Certificate
Issued By:
|- Common Name:
my-rdp
Issued To:
|- Common Name:
my-rdp
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\
Remote Desktop Protocol NTLM Info:
  OS: Windows 10/Windows Server 2016
  OS Build: 10.0.14393
  Target Name: MY-RDP
  NetBIOS Domain Name: MY-RDP
  NetBIOS Computer Name: MY-RDP
  DNS Domain Name: m...
```

135.181.10.33
static.33.10.181.135.clients.your-server.de
Hetzner Online GmbH
Finland, Tuusula

```
Microsoft RPC Endpoint Mapper

d95afe70-a6d5-4259-822e-2c84da1ddb0d
  version: v1.0
```

Shodan - what about servers possibly using default passwords? Sure.



"default password"

TOTAL RESULTS

409

TOP COUNTRIES

United States	94
Russian Federation	56
Oman	39
Taiwan	33
Ukraine	26
More...	

TOP PORTS

10001	223
8081	44
8001	25
8083	9
8089	9
More...	

TOP ORGANIZATIONS

OmanMobile Telecommunication company L...	28
Chunghwa Telecom Co.,Ltd.	20
TOV NEO-TELECOM	16
Comcast Cable Communications, LLC	14

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

73.107.249.113
c-73-107-249-113.hsd1.fl.comcast.net
Comcast IP Services, L.L.C.
United States, Cape Coral
compromised

```
Ubiquiti Networks Device:
  IP Address: 73.107.249.113
  MAC Address: 68:72:51:40:33:59
  Alternate IP Address: 192.168.100.2
  Alternate MAC Address: 68:72:51:48:33:59
  Hostname: HACKED-ROUTER-HELP-SOS-HAD-DEFAULT-PASSWORD
  Product: LAP
  Version: XM.ar7240.v5.6.2.27929.150716.1201
```

91.241.158.128
91-241-158-128-dyn.neotele.com.ru
TOV NEO-TELECOM
Russian Federation, Taman'
compromised

```
Ubiquiti Networks Device:
  IP Address: 91.241.158.128
  MAC Address: 00:15:6D:18:63:08
  Alternate IP Address: 169.254.99.8
  Alternate MAC Address: 00:15:6D:1A:63:08
  Hostname: HACKED-ROUTER-HELP-SOS-HAD-DEFAULT-PASSWORD
  Product: NS2
  Version: XS2.ar2316.v4.0.3.5058.130328.1054
```

187.216.10.140
customer-187-216-10-140.uninet-ide.com.mx
Uninet S.A. de C.V.
Mexico, San Miguel Ajusco
compromised

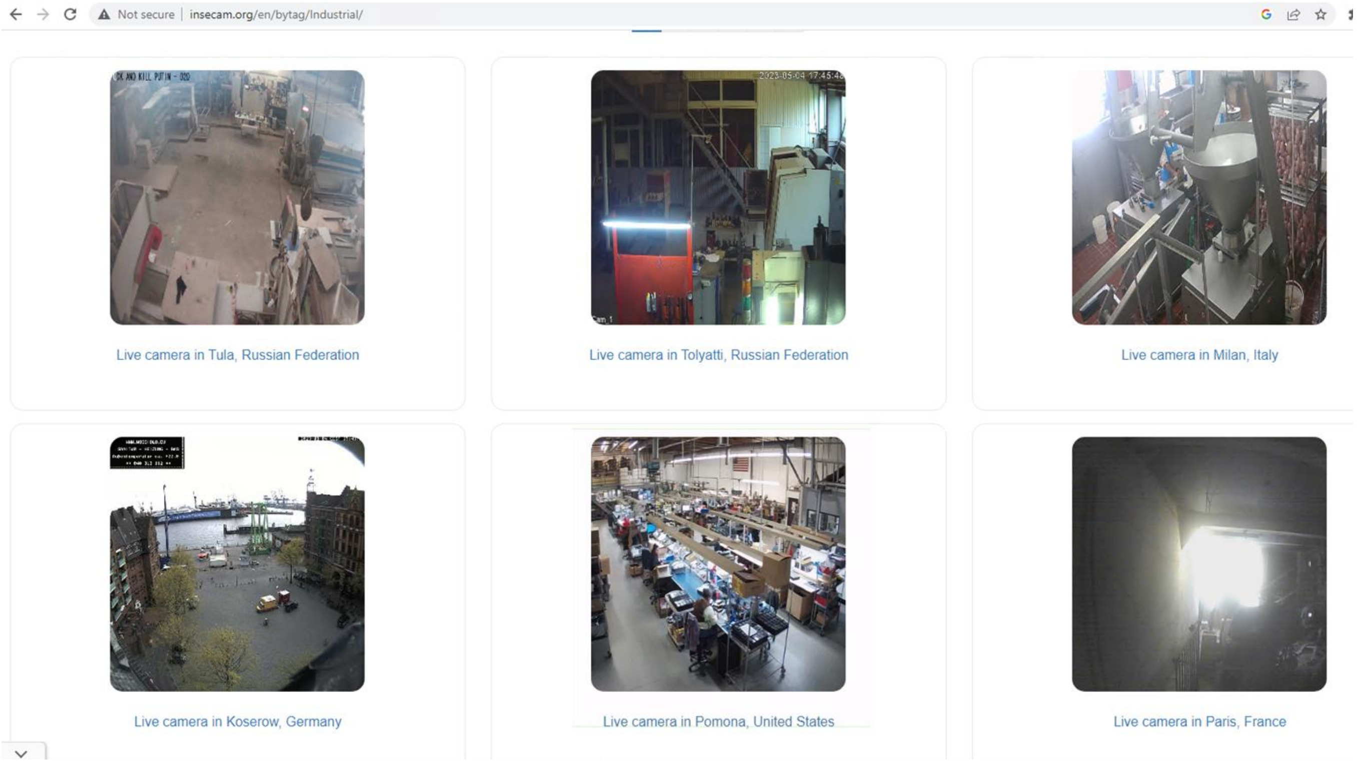
```
Ubiquiti Networks Device:
  IP Address: 187.216.10.140
  MAC Address: 04:18:D6:26:48:DC
  Hostname: HACKED-ROUTER-HELP-SOS-DEFAULT-PASSWORD
  Product: N5B-400
  Version: XW.ar934x.v5.5.6.18861.130830.1623
```

131.226.252.228
228.bluesagesoftware.com
Cyxtera Technologies Inc
United States, Los Angeles

```
HTTP/1.0 200 OK
Content-Type: text/html
Date: Thu, 4 May 2023 06:06:40 GMT

<html><body><h1>Directory /</h1><br/><a href="/icas.jpg?login=default&passwor
```

Shodan and other sites can help you find webcams

- These webcams are related to manufacturing sites



Live camera in Tula, Russian Federation

Live camera in Tolyatti, Russian Federation

Live camera in Milan, Italy

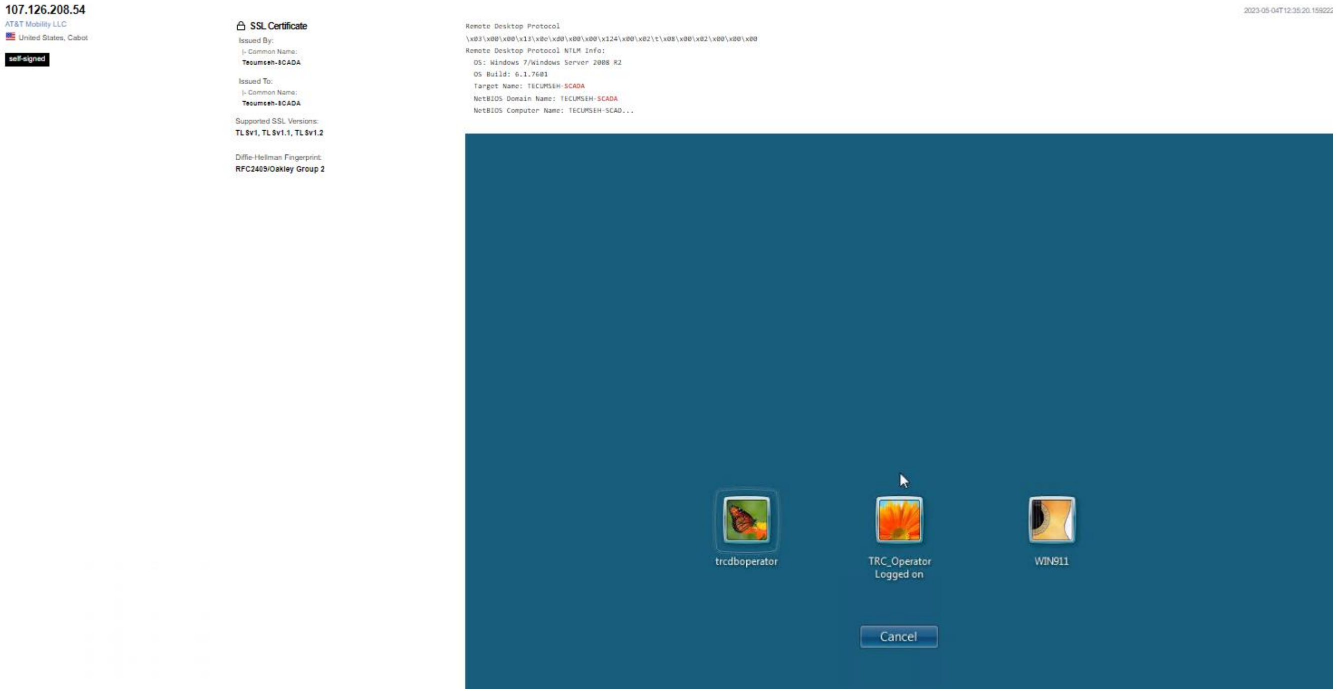
Live camera in Koserow, Germany

Live camera in Pomona, United States

Live camera in Paris, France

Shodan can find SCADA/OT information

- This SCADA site is apparently exposing RDP with usernames, one of which appears to be logged in



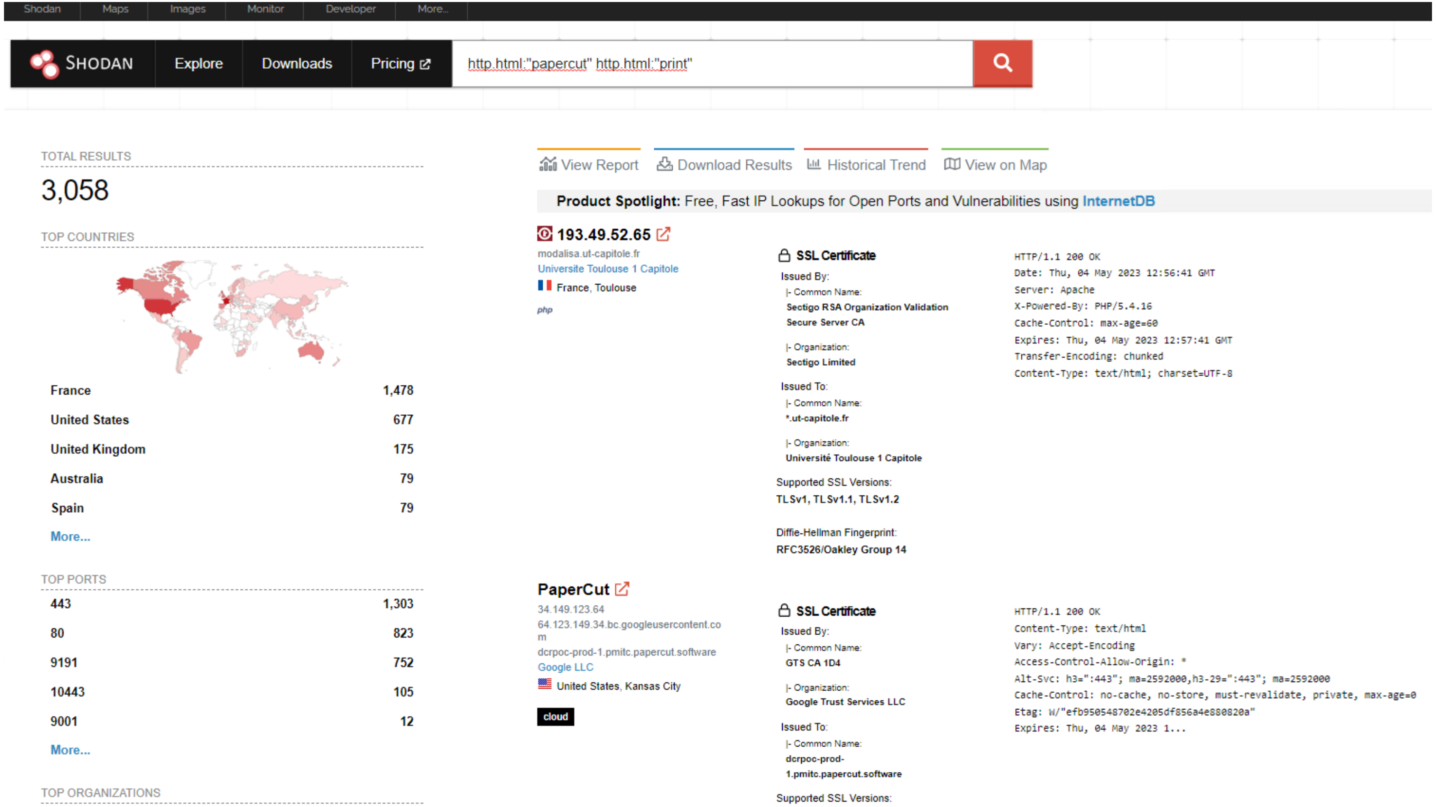
107.126.208.54
AT&T Mobility LLC
United States, Cabot
self-signed

SSL Certificate
Issued By:
|- Common Name:
Teoumseh-SCADA
Issued To:
|- Common Name:
Teoumseh-SCADA
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2

2023-05-04T12:35:20.159222

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\t\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 7/Windows Server 2008 R2
  OS Build: 6.1.7601
  Target Name: TECUMSEH-SCADA
  NetBIOS Domain Name: TECUMSEH-SCADA
  NetBIOS Computer Name: TECUMSEH-SCAD...
```

Shodan can identify systems vulnerable to active exploits (Papercut)



http.html:"papercut" http.html:"print"

TOTAL RESULTS

3,058

TOP COUNTRIES

France	1,478
United States	677
United Kingdom	175
Australia	79
Spain	79

More...

TOP PORTS

443	1,303
80	823
9191	752
10443	105
9001	12

More...

TOP ORGANIZATIONS

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

193.49.52.65

modalisa.ut-capitole.fr
Universite Toulouse 1 Capitole
France, Toulouse
php

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Organization Validation Secure Server CA
|- Organization:
Sectigo Limited

Issued To:
|- Common Name:
*.ut-capitole.fr
|- Organization:
Université Toulouse 1 Capitole

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Thu, 04 May 2023 12:56:41 GMT
Server: Apache
X-Powered-By: PHP/5.4.16
Cache-Control: max-age=60
Expires: Thu, 04 May 2023 12:57:41 GMT
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

PaperCut

34.149.123.64
64.123.149.34.bc.googleusercontent.com
dcrpoc-prod-1.pmitc.papercut.software
Google LLC
United States, Kansas City
cloud

SSL Certificate

Issued By:
|- Common Name:
GTS CA 1D4
|- Organization:
Google Trust Services LLC

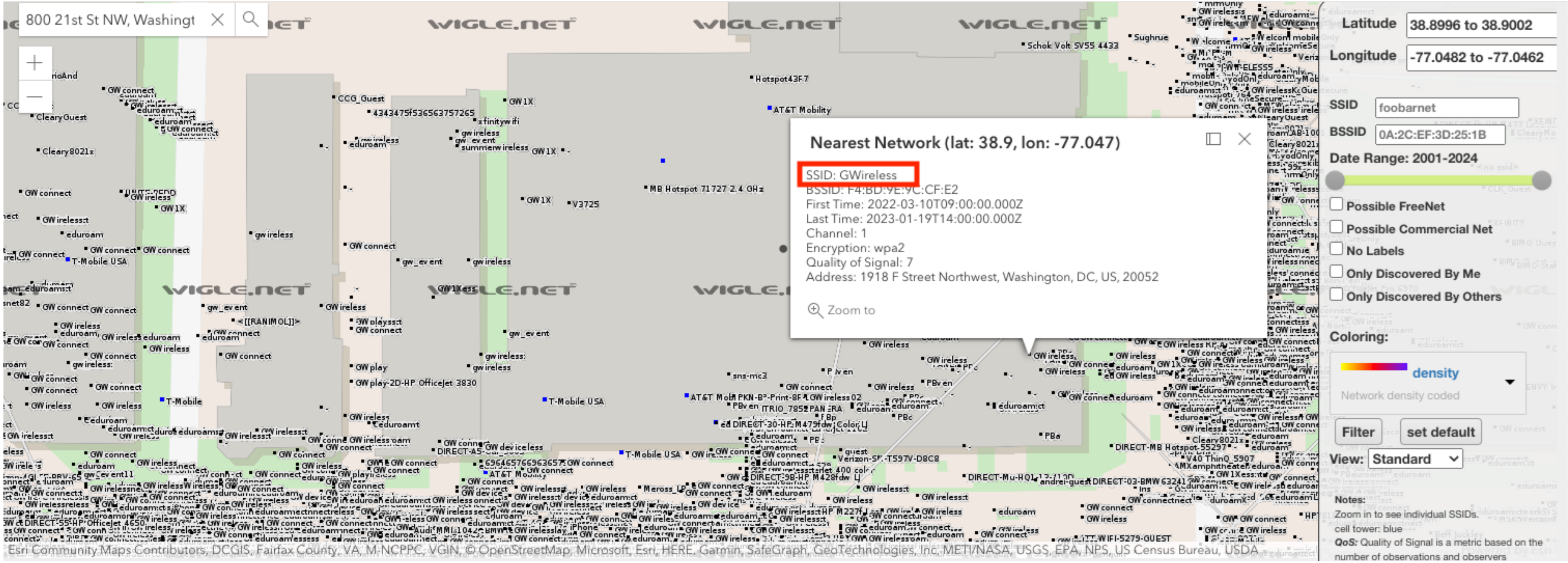
Issued To:
|- Common Name:
dcrpoc-prod-1.pmitc.papercut.software

Supported SSL Versions:

```
HTTP/1.1 200 OK
Content-Type: text/html
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Cache-Control: no-cache, no-store, must-revalidate, private, max-age=0
Etag: W/"efb950548702e4205df856a4e880820a"
Expires: Thu, 04 May 2023 1...
```

Wigle - free data on wifi networks all over the world

- It is only as good as the data entered into it, but can still be useful
- Anybody on GWireless right now?


800 21st St NW, Washingt
WIGLE.NET
Hotspot43F7
AT&T Mobility
CCG_Guest
GW1X
T-Mobile USA
GWireless
gwireless
GWconnect
eduroam
Esri Community Maps Contributors, DCGIS, Fairfax County, VA, M-NCPPC, VGIN, © OpenStreetMap, Microsoft, Esri, HERE, Garmin, SafeGraph, GeoTechnologies, Inc, METI/NASA, USGS, EPA, NPS, US Census Bureau, USDA

Nearest Network (lat: 38.9, lon: -77.047)

SSID: GWireless
BSSID: F4:BD:9E:9C:CF:E2
First Time: 2022-03-10T09:00:00.000Z
Last Time: 2023-01-19T14:00:00.000Z
Channel: 1
Encryption: wpa2
Quality of Signal: 7
Address: 1918 F Street Northwest, Washington, DC, US, 20052

Zoom to

Latitude: 38.8996 to 38.9002
Longitude: -77.0482 to -77.0462
SSID: foobarnet
BSSID: 0A:2C:EF:3D:25:1B
Date Range: 2001-2024

□ Possible FreeNet
□ Possible Commercial Net
□ No Labels
□ Only Discovered By Me
□ Only Discovered By Others

Coloring: density
Network density coded

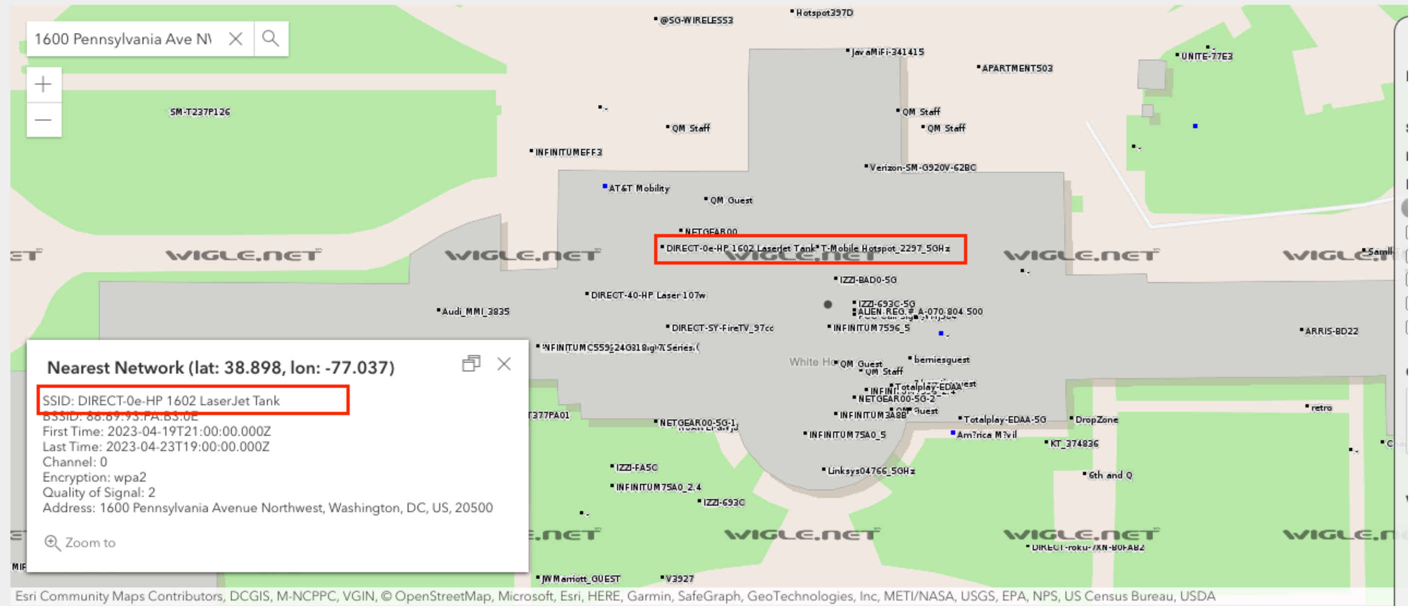
Filter | set default

View: Standard

Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

Wigle - search sensitive sites

- Does the White House use an HP 1602 LaserJet Tank Printer?



1600 Pennsylvania Ave N\

Nearest Network (lat: 38.898, lon: -77.037)

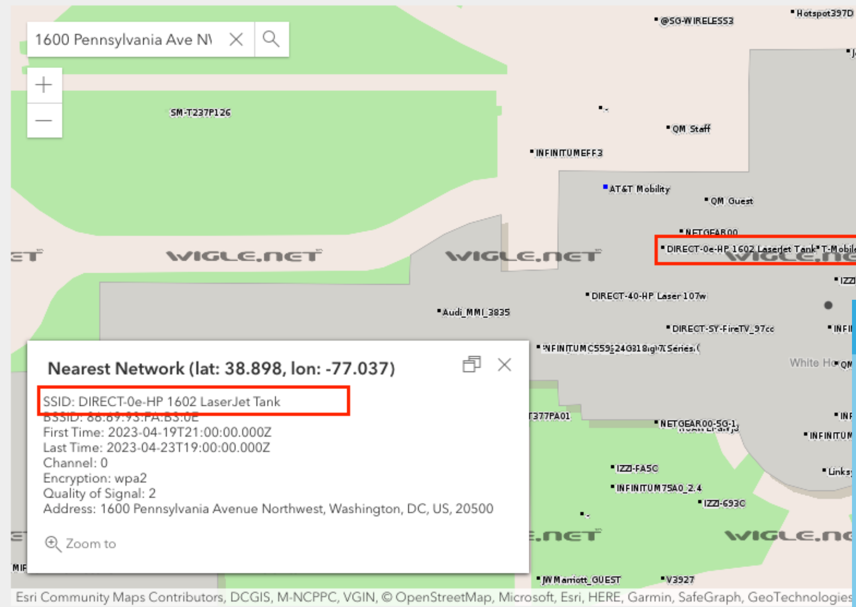
SSID: DIRECT-0e-HP 1602 LaserJet Tank
BSSID: 88:69:93:FA:B3:0E
First Time: 2023-04-19T21:00:00.000Z
Last Time: 2023-04-23T19:00:00.000Z
Channel: 0
Encryption: wpa2
Quality of Signal: 2
Address: 1600 Pennsylvania Avenue Northwest, Washington, DC, US, 20500

Zoom to

Esri Community Maps Contributors, DCGIS, M-NCPPC, VGIN, © OpenStreetMap, Microsoft, Esri, HERE, Garmin, SafeGraph, GeoTechnologies, Inc, METI/NASA, USGS, EPA, NPS, US Census Bureau, USDA

Wigle - search sensitive sites

- Does the White House use an HP 1602 LaserJet Tank Printer?

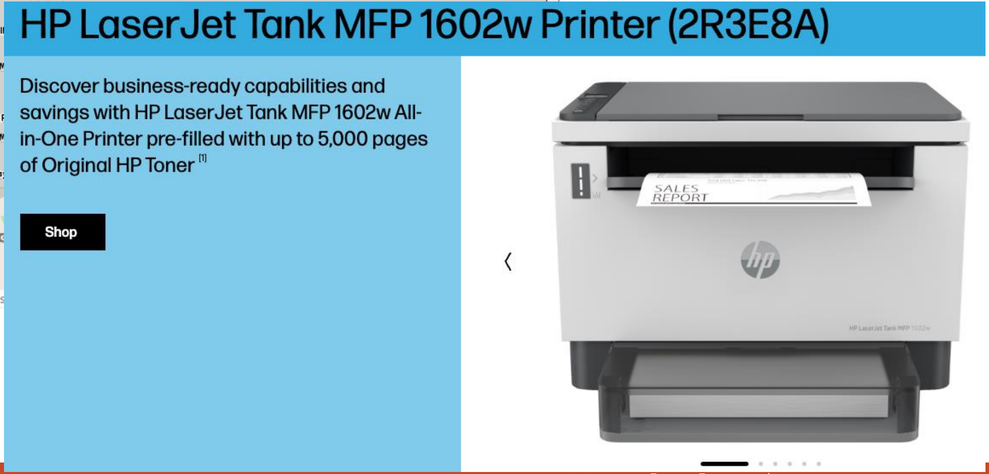


Nearest Network (lat: 38.898, lon: -77.037)

SSID: DIRECT-0e-HP 1602 LaserJet Tank
BSSID: 88:69:93:FA:B3:0E
First Time: 2023-04-19T21:00:00.000Z
Last Time: 2023-04-23T19:00:00.000Z
Channel: 0
Encryption: wpa2
Quality of Signal: 2
Address: 1600 Pennsylvania Avenue Northwest, Washington, DC, US, 20500

Zoom to

Esri Community Maps Contributors, DCGIS, M-NCPPC, VGIN, © OpenStreetMap, Microsoft, Esri, HERE, Garmin, SafeGraph, GeoTechnologies

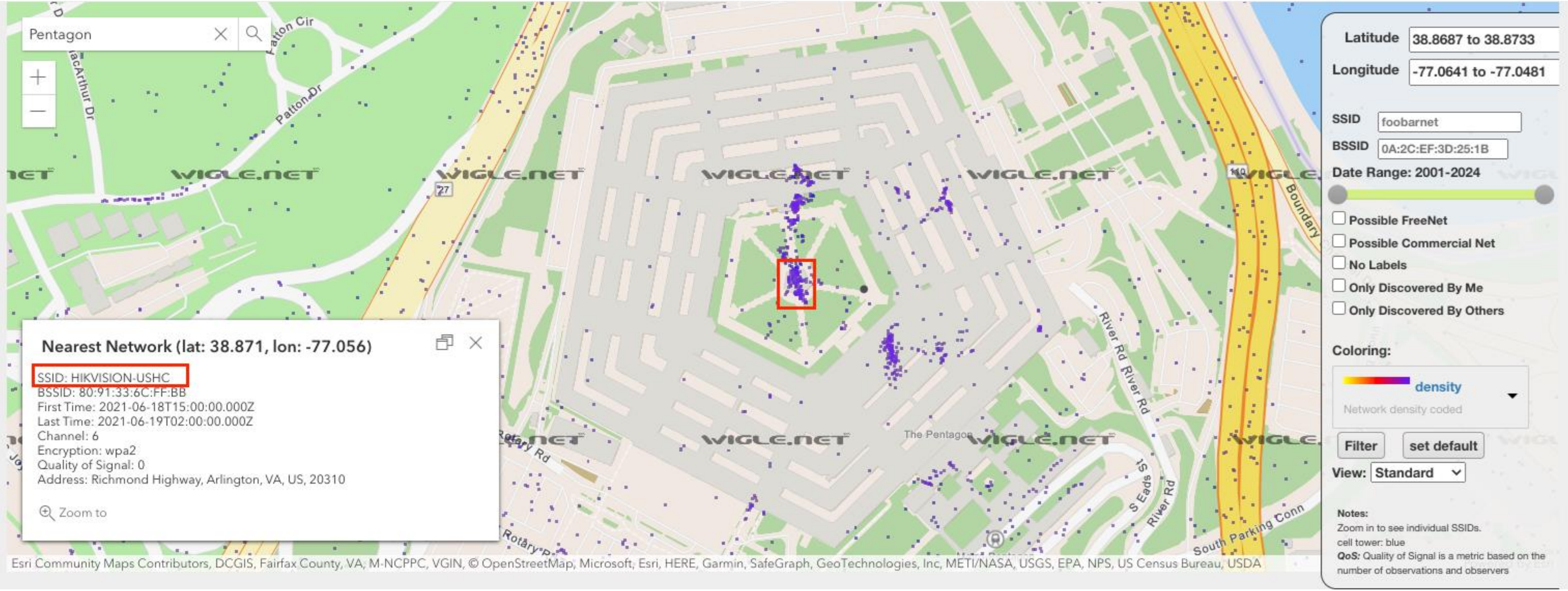


HP LaserJet Tank MFP 1602w Printer (2R3E8A)

Discover business-ready capabilities and savings with HP LaserJet Tank MFP 1602w All-in-One Printer pre-filled with up to 5,000 pages of Original HP Toner [1]

Examples

- Was there a HikVision device at the Pentagon in 2021?



Nearest Network (lat: 38.871, lon: -77.056)

SSID: HIKVISION-USHC
BSSID: 80:91:33:6C:FF:BB
First Time: 2021-06-18T15:00:00.000Z
Last Time: 2021-06-19T02:00:00.000Z
Channel: 6
Encryption: wpa2
Quality of Signal: 0
Address: Richmond Highway, Arlington, VA, US, 20310

Zoom to

Latitude: 38.8687 to 38.8733
Longitude: -77.0641 to -77.0481
SSID: foobarnet
BSSID: 0A:2C:EF:3D:25:1B
Date Range: 2001-2024

□ Possible FreeNet
□ Possible Commercial Net
□ No Labels
□ Only Discovered By Me
□ Only Discovered By Others

Coloring: density
Network density coded

Filter | set default

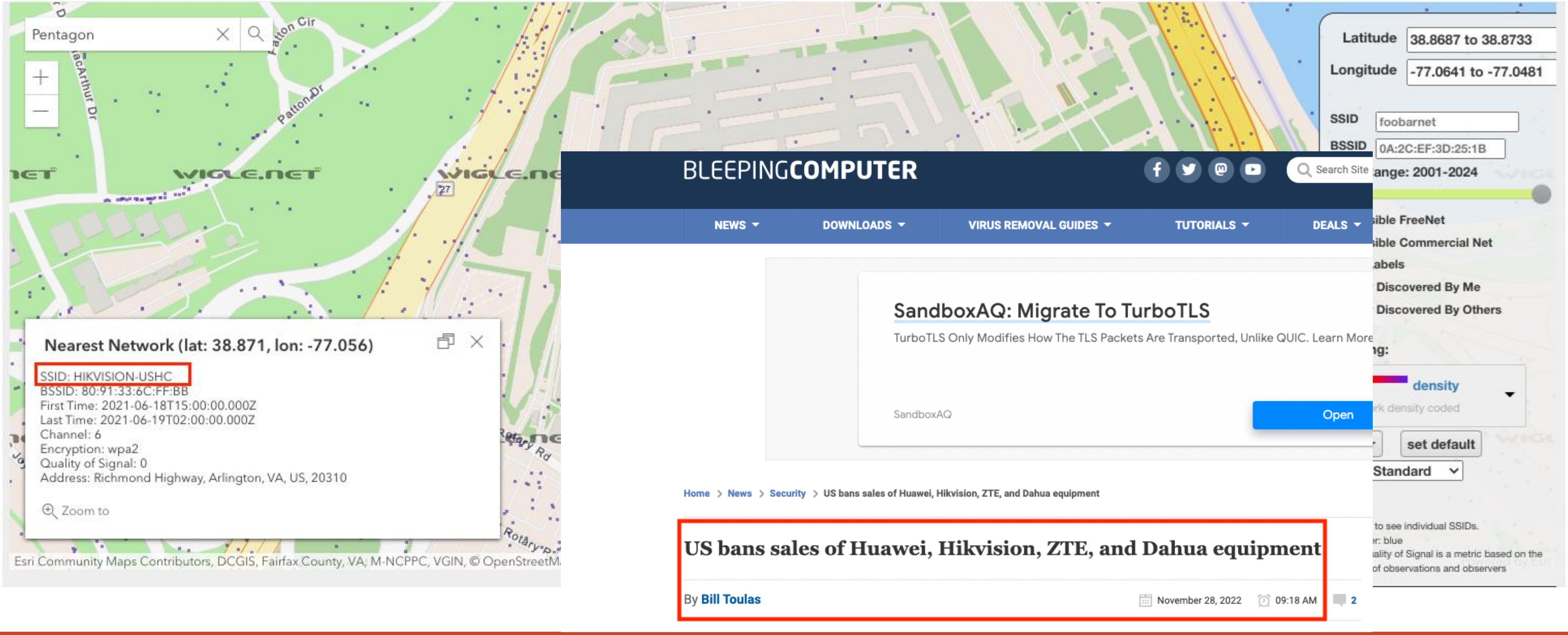
View: Standard

Notes:
Zoom in to see individual SSIDs.
cell tower: blue
QoS: Quality of Signal is a metric based on the number of observations and observers

Esri Community Maps Contributors, DCGIS, Fairfax County, VA, M-NCPPC, VGIN, © OpenStreetMap, Microsoft, Esri, HERE, Garmin, SafeGraph, GeoTechnologies, Inc, METI/NASA, USGS, EPA, NPS, US Census Bureau, USDA

Examples

- Was there a HikVision device at the Pentagon in 2021?


Pentagon
Patton Cir
Patton Dr
MacArthur Dr
WIGLE.NET
27
Rotary Rd
Zoom to
Esri Community Maps Contributors, DCGIS, Fairfax County, VA, M-NCPPC, VGIN, © OpenStreetM
BLEEPINGCOMPUTER
Search Site
NEWS
DOWNLOADS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
SandboxAQ: Migrate To TurboTLS
TurboTLS Only Modifies How The TLS Packets Are Transported, Unlike QUIC. Learn More
SandboxAQ
Open
set default
Standard
density

Nearest Network (lat: 38.871, lon: -77.056)

SSID: HIKVISION-USHC
BSSID: 80:91:33:6C:FF:BB
First Time: 2021-06-18T15:00:00.000Z
Last Time: 2021-06-19T02:00:00.000Z
Channel: 6
Encryption: wpa2
Quality of Signal: 0
Address: Richmond Highway, Arlington, VA, US, 20310

Latitude: 38.8687 to 38.8733
Longitude: -77.0641 to -77.0481
SSID: foobarnet
BSSID: 0A:2C:EF:3D:25:1B
ange: 2001-2024

ible FreeNet
ible Commercial Net
abels
Discovered By Me
Discovered By Others
ng:
k density coded

to see individual SSIDs.
r: blue
ality of Signal is a metric based on the
of observations and observers

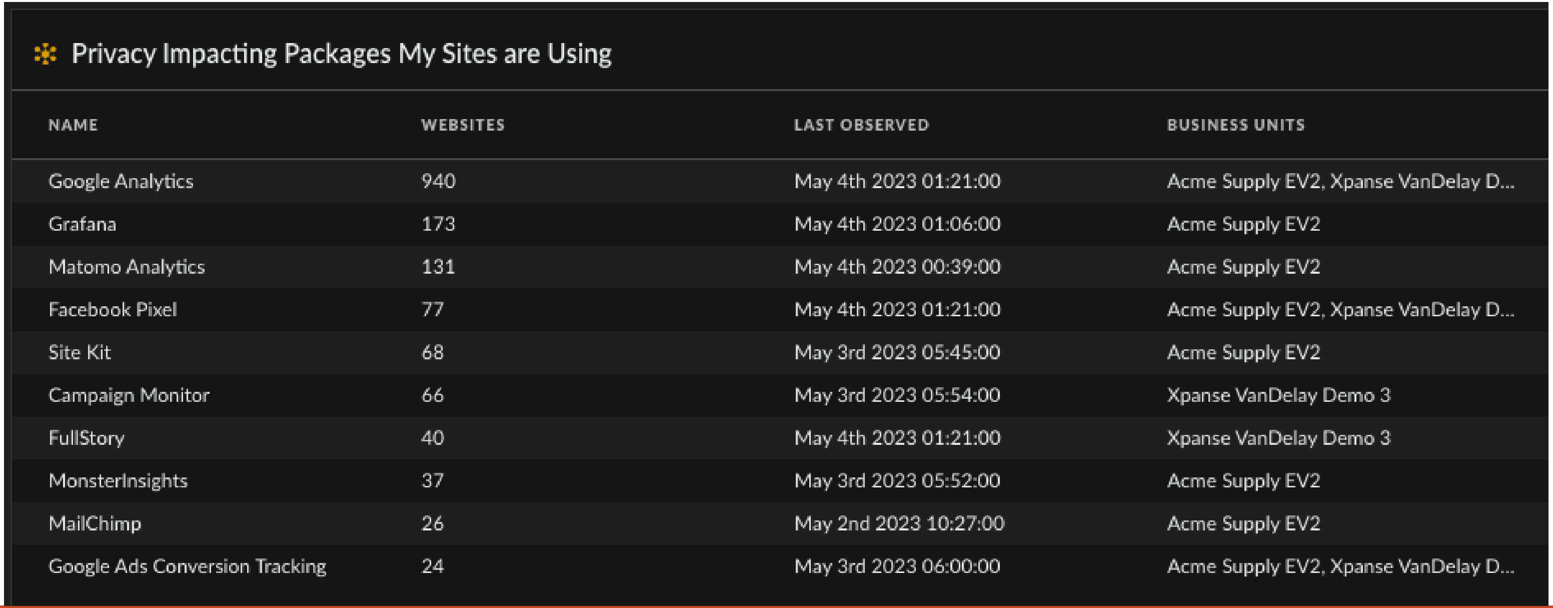
Home > News > Security > US bans sales of Huawei, Hikvision, ZTE, and Dahua equipment

US bans sales of Huawei, Hikvision, ZTE, and Dahua equipment

By Bill Toulas November 28, 2022 09:18 AM 2

Cortex Xpanse - Find potential privacy violations in your environment

- **Security does not guarantee Privacy**
- **Cookies, Trackers, Pixels, and Advertising/Marketing tech are increasingly involved in class action lawsuits when organizations do not deploy them in line with privacy regulations that have changed over time.**



Privacy Impacting Packages My Sites are Using

NAME	WEBSITES	LAST OBSERVED	BUSINESS UNITS
Google Analytics	940	May 4th 2023 01:21:00	Acme Supply EV2, Xpanse VanDelay D...
Grafana	173	May 4th 2023 01:06:00	Acme Supply EV2
Matomo Analytics	131	May 4th 2023 00:39:00	Acme Supply EV2
Facebook Pixel	77	May 4th 2023 01:21:00	Acme Supply EV2, Xpanse VanDelay D...
Site Kit	68	May 3rd 2023 05:45:00	Acme Supply EV2
Campaign Monitor	66	May 3rd 2023 05:54:00	Xpanse VanDelay Demo 3
FullStory	40	May 4th 2023 01:21:00	Xpanse VanDelay Demo 3
MonsterInsights	37	May 3rd 2023 05:52:00	Acme Supply EV2
MailChimp	26	May 2nd 2023 10:27:00	Acme Supply EV2
Google Ads Conversion Tracking	24	May 3rd 2023 06:00:00	Acme Supply EV2, Xpanse VanDelay D...

You need

an updated view of your attack surface to **discover**, **evaluate** and **mitigate** exposure of your internet-connected assets.

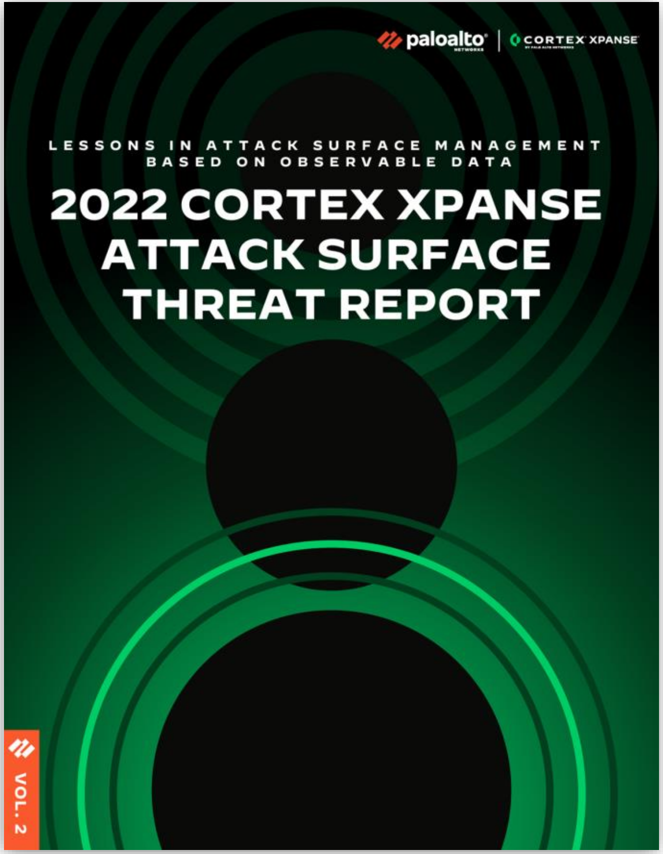
Read the Report

Live asset data discovered via scans.
Not survey data!

Attack surface data observed from January to February 2022

- 100+ firms across NAM, EMEA, JAPAC
- > 1% of global IPv4 space
- New Critical Vulnerabilities and Exposures (CVE) covered

Download the 2022 Cortex Xpanse ASM Threat Report today: tinyurl.com/2022ASMReport


paloalto NETWORKS | CORTEX XPANSE
LESSONS IN ATTACK SURFACE MANAGEMENT BASED ON OBSERVABLE DATA
2022 CORTEX XPANSE ATTACK SURFACE THREAT REPORT
VOL. 2

Thank you

paloaltonetworks.com

paloaltonetworks.com/unit42

paulweiss.com/practices/litigation/cybersecurity-data-protection