



# We can't stop here! This is Bot Country!

NATE WARFIELD | MICROSOFT | @N0X08

# Why is this interesting?

- Network security is important yet often overlooked
- Disclosed vulns being used within days (sometimes hours)
- Attacks are becoming more precise
  - Travelex (Pulse VPN)
  - Lateral Movement
- Holes in your network exist
- Imperative that you find them first



# FBI: Don't Forget to Change Your Fridge Password

FBI provides security recommendations for IoT users

Dec 6, 2019 11:10 GMT · By Bogdan Popa · Comment · Share: [Twitter](#) [Reddit](#) [Facebook](#) [Google+](#) [Print](#)

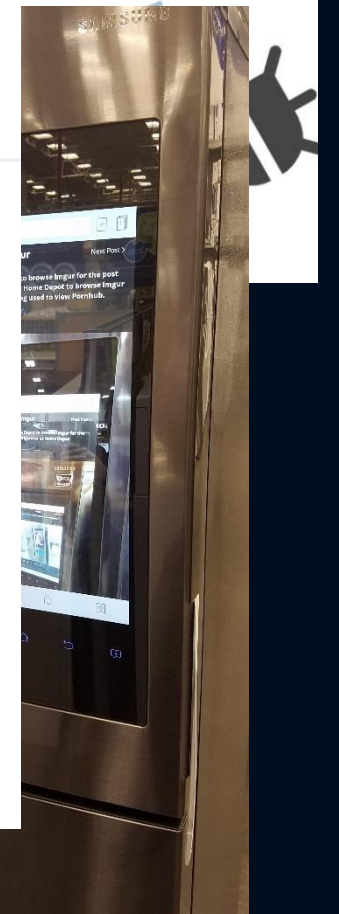
After discussing a series of security measures for smart TVs, the FBI is back with more tips on how to prevent breaches, this time focusing on the Internet of Things (IoT).

The FBI says these recommendations should come in handy as the IoT device market is growing and more customers purchase smart devices during the holiday season, including smartwatches, fitness trackers, home security devices, refrigerators, robots, and pretty much anything else that falls into the IoT group.



Smart refrigerators are becoming more and ...

Buggy Router Models to



SHODAN product:"San

Exploits Maps Sh

TOTAL RESULTS

10,978

TOP COUNTRIES

Korea, Republic of  
United States  
Sweden  
Russian Federation  
Finland

VIEWED

Spain  
Russian Federation

1,072  
852

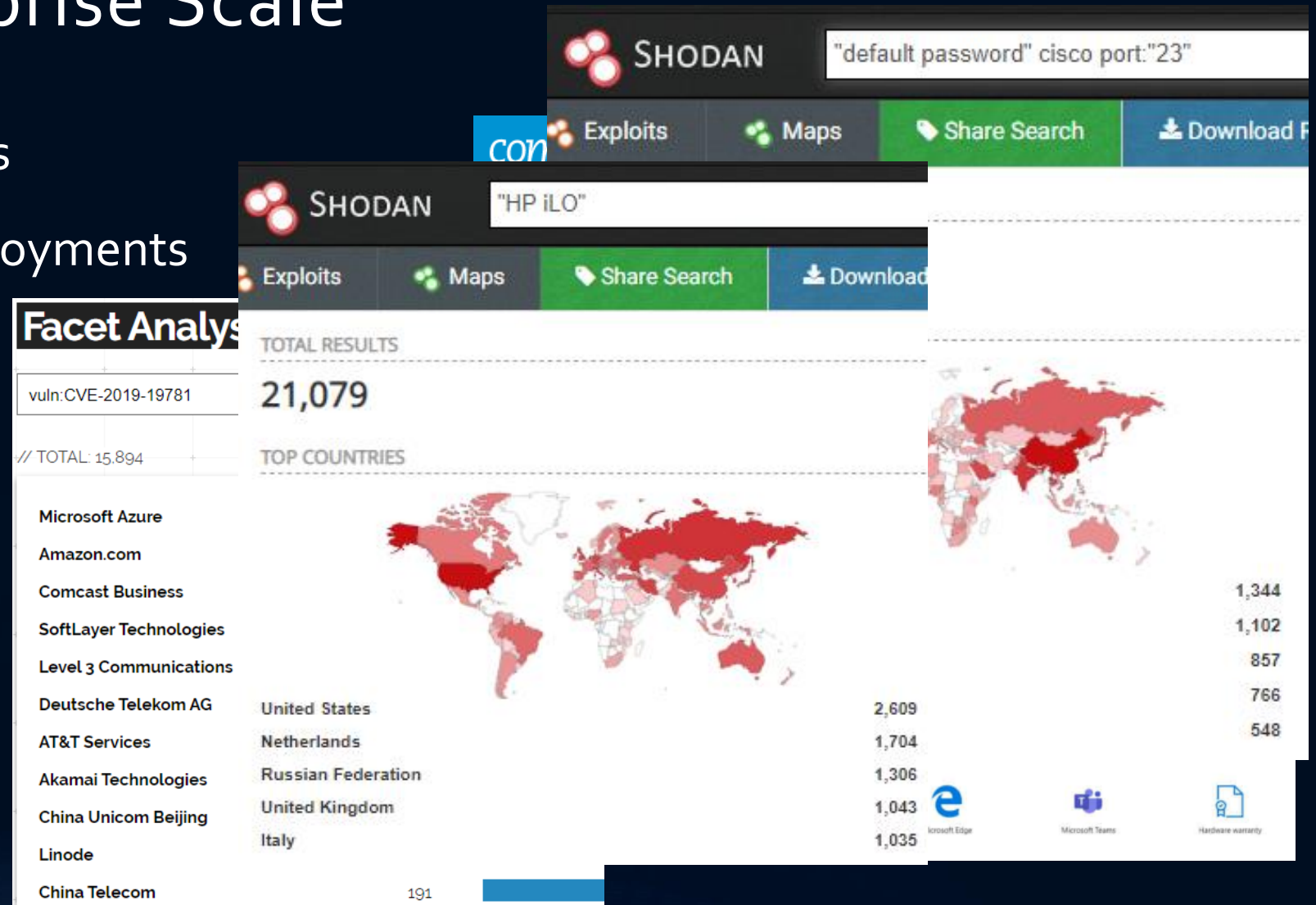
ppoe.ralsko.net.cz  
Ralsko NET s.r.o.  
Added on 2019-11-21 19:14:32 GMT

Ubiquiti Networks Device  
IP: 85.207.47.46



# Risk at Enterprise Scale

- Unpatched systems
- Insecure cloud deployments
- Network hardware
- Server iLO



# Tools of the trade

- Censys
- BinaryEdge
- BGPView
- (many others)
- **Shodan**
- **Greynoise**

The screenshot displays the Censys search interface. At the top, the Censys logo is on the left, and a search bar contains the query '80.http.get.title: citrix OR 80.http.get.title: netscaler'. Below the search bar, the results are filtered by 'product:elasticsearch'. A table lists search results with columns for 'Ports', 'Entries', and 'Versions'. The first result shows '200/tcp' with 41,615 entries and 'Elasticsearch R API/7.4.2'. Other results show '501/tcp' (7,884 entries), '0/tcp' (792 entries), and '806/tcp' (154 entries). To the right, a detailed view for 'Microsoft Corporation' (AS8075) is shown, including its IPv4 addresses (34,407,936), number of peers (449), and a summary of regional registry (IANA) and allocation status (Assigned). The network summary also lists 180 IPv4 prefixes, 274 IPv4 peers, and 13 IPv4 upstreams.

**Censys**

SEARCH THE DATA GATHERED BY BINARYEDGE

Ports	Entries	Versions
200/tcp	41,615	Elasticsearch R API/7.4.2
501/tcp	7,884	Elasticsearch R API/7.3.1
0/tcp	792	Elasticsearch R API/6.5.4
806/tcp	154	Elasticsearch R API/6.3.2

**BGPVIEW** Countries Report

**Microsoft Corporation**  
AS8075 ~ MICROSOFT-CORP-MSN-AS-BLOCK

IPv4 Addresses: 34,407,936 Number of Peers: 449

**Summary**

REGIONAL REGISTRY: IANA  
ALLOCATION STATUS: Assigned

**Network**

IPV4 PREFIXES: 180  
IPV4 PEERS: 274  
IPV4 UPSTREAMS: 13

# Malicious traffic is a global problem

- ~6 million 'malicious' IPs
- Every country
- ~9mil 'malicious' IPs

Countries:

- China
- Vietnam
- Brazil
- Egypt
- Indonesia
- Russia
- India
- Taiwan
- Thailand
- Venezuela
- Greece
- United States
- Turkey
- Iran
- Mexico
- Argentina
- Italy
- Ukraine
- Hong Kong
- South Korea
- Viet Nam

**194.177.239.81** tms.video.gl View Raw Data

Internet Scanner

City	Nuuk
Country	Greenland
Organization	Tele Greenland
ISP	Tele Greenland
Last Update	2019-12-04T10:58:40.940932
Hostnames	tms.video.gl
ASN	AS8818

**Vulnerabilities**

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

<b>CVE-2017-7269</b>	Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (IIS) 6.0 in Microsoft Windows Server 2003 R2 allows remote attackers to execute arbitrary code via a long header beginning with "If: <http://" in a PROPFIND request, as exploited in the wild in July or August 2016.
----------------------	---

79933  
76967  
70091  
62820

- Ping Scanner
- DVR/IP Camera Bruteforcer
- VStarcam C7824WIP Hardcoded Telnet Attempt
- Looks Like Conficker
- Mikrotik CVE-2018-14847 Worm
- Mirai Variant

26764

**Ports**

80

**Services**

80  
tcp  
http

**Microsoft IIS h**

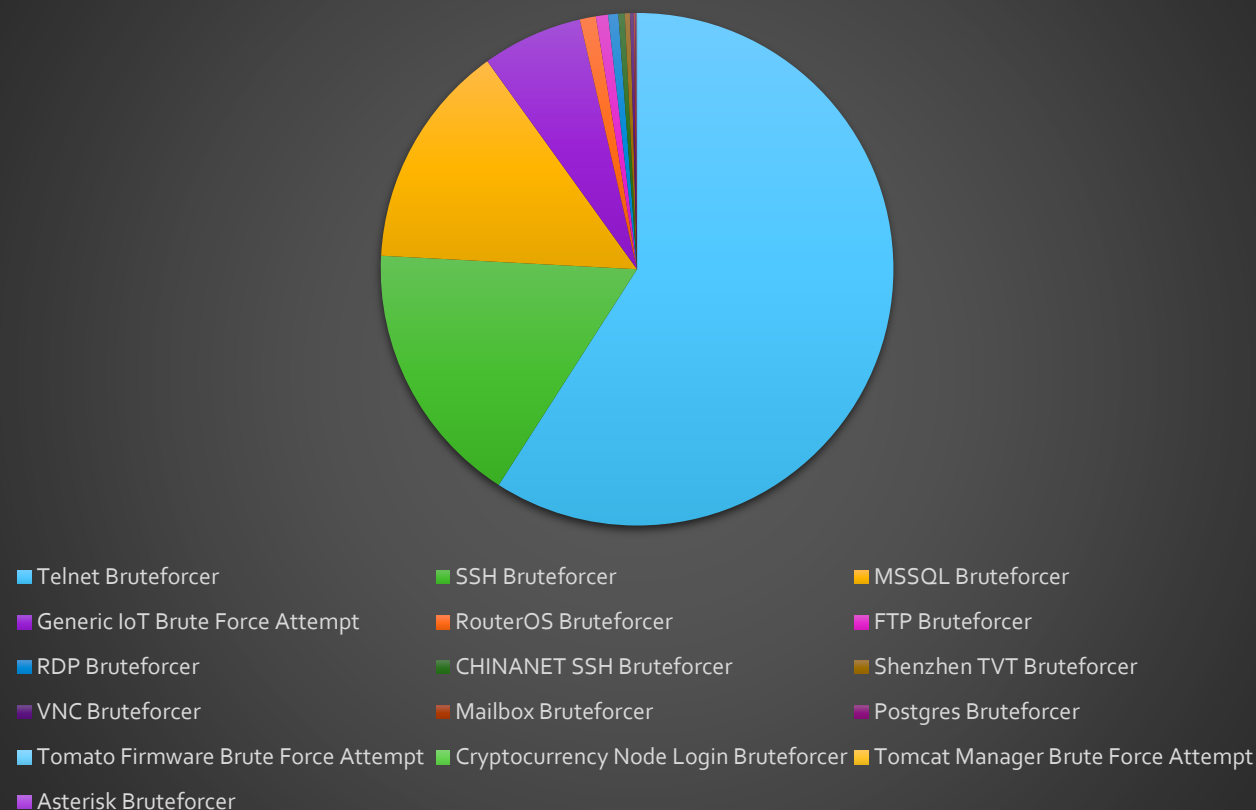
HTTP/1.1 200 OK  
Content-Length: 1433  
Content-Type: text/html  
Content-Location: http://tms.video.gl/  
Last-Modified: Fri, 20 Dec 2019 10:58:40 GMT  
Accept-Ranges: bytes  
ETag: "0cbd7f8f2d9c21111111111111111111"  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET  
Date: Wed, 04 Dec 2019 10:58:40 GMT

India 558,130  
Vietnam 493,375

# 12 months of bad traffic

- 139 different worm heuristics
- 3,922,904 IPs total
- **68.6%** of malicious traffic
- 16 brute force techniques
- 1,465,406 IPs total
- **26%** of malicious traffic

Brute Force Attempts (source: Greynoise)





# Malicious traffic coming from Israel

## 1. Organizations

## 2. Tags

## 3. OS's

## 4. ASNs

### Organizations:

- Bezeq International-Ltd	3544
- Partner Communications Ltd.	1822
- Cellcom Fixed Line Communication L.P.	1608
- Hot-Net internet services Ltd.	661
- XFone 018 Ltd	428
- 013 Netvision	390
- Please Send Abuse/SPAM complaints To Abuse@012.net.il	292
- *SE4-DRP*	159
- Triple C Cloud Computing Ltd.	113

### ASNs:

- AS8551	4551
- AS1680	2301
- AS9116	2200
- AS12849	904
- AS47956	536
- AS12400	462
- AS50463	169
- AS16116	115

### Tags:

- Mirai	8335
- Telnet Scanner	5754
- Telnet Bruteforcer	3510
- HTTP Alt Scanner	3091
- SMB Scanner	2469
- Looks Like EternalBlue	1242
- Eternalblue	1054
- EquationGroup Eternal/MS17-010	954
- Eternal MS17-010	954
- Web Scanner	878
- Generic IoT Brute Force Attempt	784
- Web Crawler	415
- Telnet Worm	378
- MSSQL Scanner	309
- MSSQL Bruteforcer	284
- SSH Scanner	275
- SSH Bruteforcer	217
- Open Proxy Scanner	207
- ADB Worm	187
- Mirai Variant	141
- DVR/IP Camera Bruteforcer	136
- Ping Scanner	134
- VStarcam C7824WIP Hardcoded Telnet Attempt	105

### Operating systems:

- Linux 2.2.x-3.x (Embedded)	3611
- Linux 2.2-3.x	2373
- Windows 7/8	2261
- unknown	1333
- Linux 3.1-3.10	400
- Windows 2000	258
- Linux 2.4.x	248
- Linux 3.x	181
- Linux 3.11+	119
- Windows XP	48
- Linux 2.4-2.6	35
- Linux 2.6	11
- Windows NT kernel 6.x	11
- Mac OS X 10.x	3
- FreeBSD	2



# Forensics & Threat Intel

- greynoise analyze - analyze unstructured log data
- greynoise pcap – packet capture time machine (still in beta)
- Augment threat intel data
- Find & block known bad actors

The screenshot displays the Greynoise web interface. At the top, a browser window shows a packet capture file: 3bd6f15f-8989-4082-ba0b-b71fa105198f.pcap. The Greynoise logo is visible on the left. A search bar on the right contains the query: `raw_data.web.paths: "/weaver/bsh.servlet.BshServlet"`. Below the search bar, it indicates "208 results". A world map on the left shows the top countries, with China highlighted at 144. On the right, a detailed view of a specific IP address is shown, including its organization (Shenzhen Tencent Computer Systems Company Limited) and various tags like "Malicious", "Hosting", "HTTP Alt Scanner", "Joomla RCE CVE-2015-8562", and "Tomcat Manager Scanner".

log entries, process creation, registry entries, etc. While reviewing the memory image instances of `mshta.exe` spawned under `javaw.exe`, the creation date for these processes pivoted our investigative focus to that date.

App name (tds.7login.appname), 20 bytes

# Attack timeline: Citrix LFI (CVE-2019-19781)

- Vendor disclosed: Dec. 17<sup>th</sup>, 2019
- Tripwire article: Jan 8<sup>th</sup>, 2020
- Greynoise signature: Jan 9<sup>th</sup>, 2020
- Exploitation attempts: **Jan 10<sup>th</sup>, 2020**
- Evasion attempts: Jan 17<sup>th</sup>, 2020

2020-01-10 00:35:29.000 UTC	82.102.16.220	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-10 02:02:23.000 UTC	82.102.16.220	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 01:25:56.000 UTC	54.200.158.6	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 01:29:57.000 UTC	54.200.158.6	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 01:32:43.000 UTC	54.200.158.6	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 12:07:40.000 UTC	5.101.0.209	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 12:10:47.000 UTC	5.101.0.209	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 12:13:33.000 UTC	5.101.0.209	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 12:17:38.000 UTC	5.101.0.209	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1
2020-01-12 12:18:42.000 UTC	5.101.0.209	GET /vpn/./vpns/cfg/smb.conf HTTP/1.1

		Malicious Business		First Seen: 2019-12-22 Last Seen: 2020-01-29	
		193.187.174.104		OS: Linux 3.11+ ASN: AS64499	
2020-01-17 21:24:35.000 UTC	179.43.149.12	GET /vpn/js/%2E./%2E/%76pns/cfg/smb.conf HTTP/1.1			
2020-01-19 18:16:45.000 UTC	91.207.175.198	GET /vpn/js/%2e./%2e/%76pns/cfg/smb.conf HTTP/1.1			
2020-01-25 06:55:56.000 UTC	179.43.149.12	GET /vpn/js/%2E./%2E/%76pns/cfg/smb.conf HTTP/1.1			
2020-01-28 10:24:53.000 UTC	94.177.123.109	GET /vpn/./vpns/portal/scripts/picktheme.pl?f=3e2e41bd			
2020-01-30 13:38:16.000 UTC	175.139.71.8	GET /vpn/js/%2e./%2e/%76pns/cfg/smb.conf HTTP/1.1			

6379 / TCP  
8063 / TCP

Web

Paths  
/vpn/./vpns/cfg/smb.conf  
/vpn/./vpns/portal/scripts/newbm.pl

User-Agent

This IP address has been observed attempting CVE-2019-19781, a local file inclusion vulnerability in Citrix NetScaler products that could enable enumeration of system data, modification of user accounts, and arbitrary code execution.

References:  
<https://www.tripwire.com/state-of-security>  
<https://www.cisecurity.org/advisory/vulnerability>

 SERVICES

### January 12, 2020 Compromise

The first compromise came from IP address 193.187.174.104 and started with the attacker accessing the **smb.conf** file using the directory traversal attack. This is a good litmus test for the attackers to see if a system is vulnerable and was often seen before an attack occurred.


```
193.187.174.104 - - [12/Jan/2020:11:26:02 +0000] "GET /vpn/./vpns/cfg/smb.conf HTTP/1.1" 200
```

6:12 PM · Jan 10, 2020 · Twitter Web App

# Attack surface & anomalies

- ASN is a good starting point
  - Caveat: Cloud deployments
- BGPView
- ASN search in Shodan
- Scanning hosts from Greynoise

**BGPVIEW** Countries Report

 **Iran Cell Service and Communication**  
AS44244 ~ IRANCELL-AS

IPv4 Addresses: 1,314,816      Number of Peers: 4


---

**SHODAN**

Exploits   Maps   Images   Share Search

TOTAL RESULTS  
**2,910**


TOP COUNTRIES




Iran, Islamic Republic of      2,910

TOP SERVICES

Modem Web Interface	357
HTTP	304
NTP	160
554	116
SNMP	106

 **GREYNOISE**      metadata.asn:AS44244

396,834 results



Top Countries

Iran	384,222
Iran, Islamic Republic of	12,610
Turkey	2



# It's always (in) DNS

- 'shodan domain'

- 'shodan

- whois -h  
+short d

```
nate@0dayAllday:~$ shodan domain clearview.ai -D
CLEARVIEW.AI
```

```
A      104.31.79.155 Ports: 80, 443
A      104.31.78.155 Ports: 80, 443
AAAA   2606:4700:3033::681f:4e9b
AAAA   2606:4700:3034::681f:4f9b
```


```
nate@0dayAllday:~$ shodan domain aeroclub.org.il -D
AEROCLUB.ORG.IL
```

```
A      213.8.139.134 Ports: 80, 443
MX     mail.netprotek.com
MX     mail.aeroclub.org.il
NS     ns2.media4u.co.il
NS     ns1.media4u.co.il
SOA    ns1.media4u.co.il
TXT    v=spf1 a mx include:mail.netprotek.com ip4:213.8.195.61 ~all
mail   A      213.8.195.60 Ports: 25, 80, 110, 143, 3389, 8889
```

```
nate@0dayAllday:~$ whois -h whois.cymru.com $(dig +short aeroclub.org.il)
```

AS	IP	AS Name
9116	213.8.139.134	GOLDENLINES-ASN Partner Communications Main Autonomous System, IL

```
config A      104.31.78.155
config A      104.31.79.155
```

**Luke Stephens (hakluke)**  
@hakluke

Follow

Want to do some lazy bug bounty hunting today?

Get the ASN of a company by using this (in this case, Tesla):

whois -h [whois.cymru.com](#) \$(dig +short

the ASN filter in Shodan to  
through their IP space.

[search?query=a...](#)

2086, 2087, 2096, 8080, 8443, 8880  
2083, 2086, 2095, 8080, 8443, 8880

86, 2087, 8880

```
AAAA   2606:4700:3033::681f:4e9b Ports: 80, 443, 2083, 2086, 2087, 8080, 8443, 8880
A      104.31.79.155 Ports: 80, 443, 2052, 2082, 2083, 2086, 2095, 8080, 8443, 8880
A      104.31.78.155 Ports: 80, 443, 2082, 2083, 2086, 2087, 2096, 8080, 8443, 8880
AAAA   2606:4700:3034::681f:4f9b Ports: 443
AAAA   2606:4700:3033::681f:4e9b Ports: 443
```

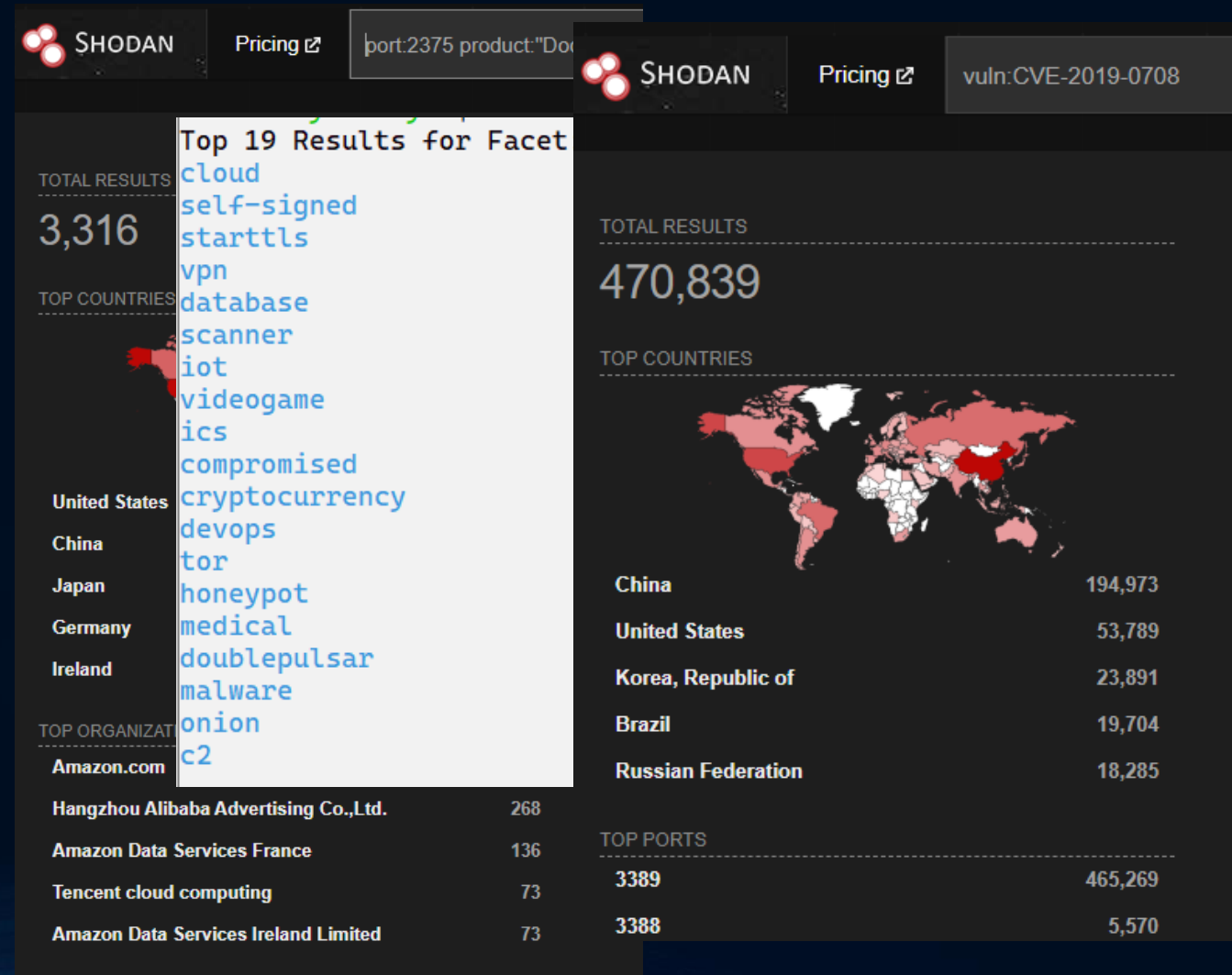
0, 8443, 8880

080, 8443, 8880

080, 8443, 8880

# Shodan hunting 101

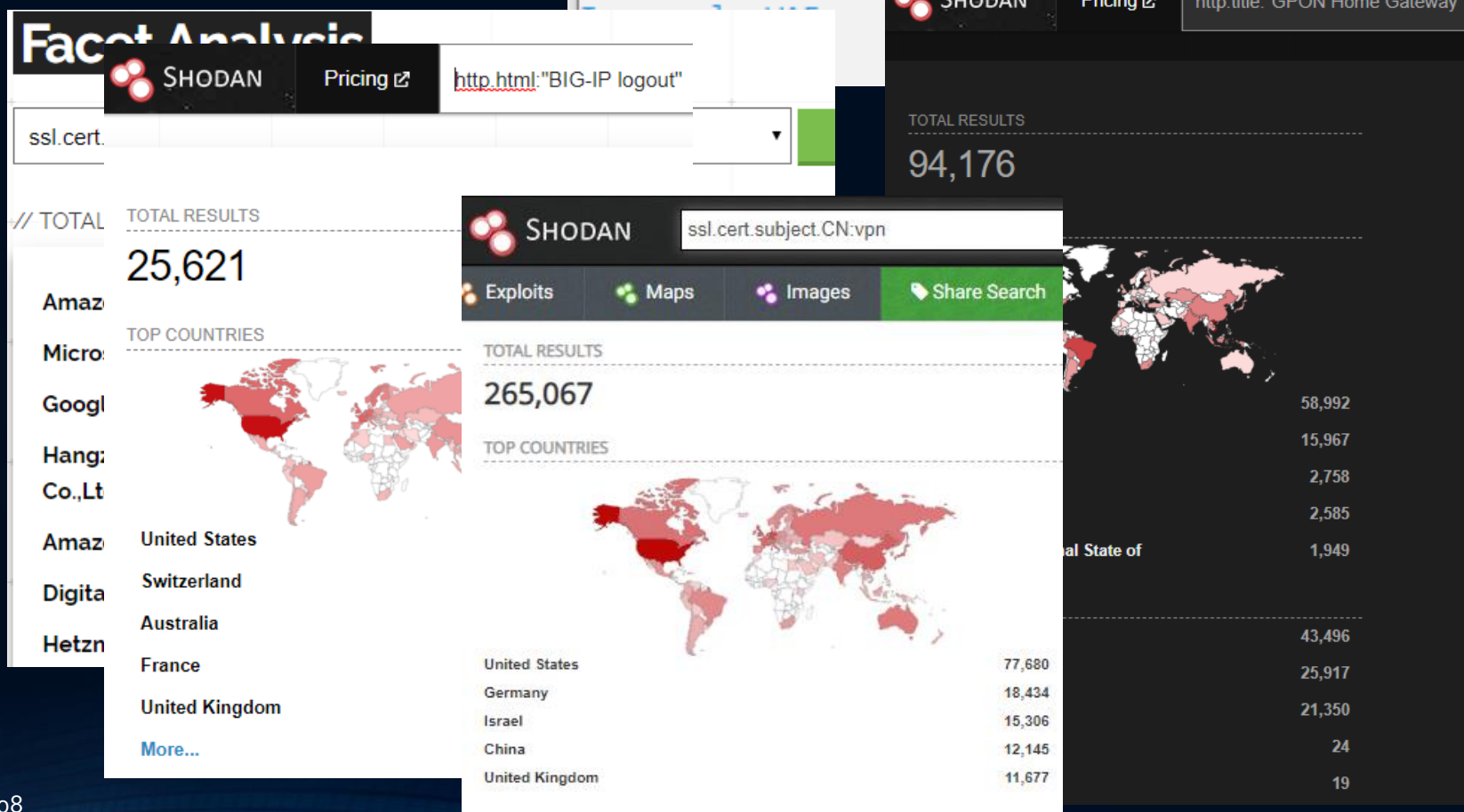
- Port
- Product
- Organization
- tag:self-signed
- Enterprise feature
  - \$10k/year license
- vuln:CVE-YYYY-NNNN



# Down the rabbit hole

- 'shodan stats --facet <metadata> net:0/0'
- ssl.cert.issuer.CN
- http.html
- http.title
- ssl.cert.subject.CN

```
Top 10 Results for Facet: http.waf
CloudFlare          3,135,328
AWS WAF             1,147,577
F5 BIG-IP APM       547,306
F5 BIG-IP LTM       152,062
Citrix NetScaler    130,131
Safedog              96,521
F5 BIG-IP ASM       78,119
Edgecast / Verizon
```





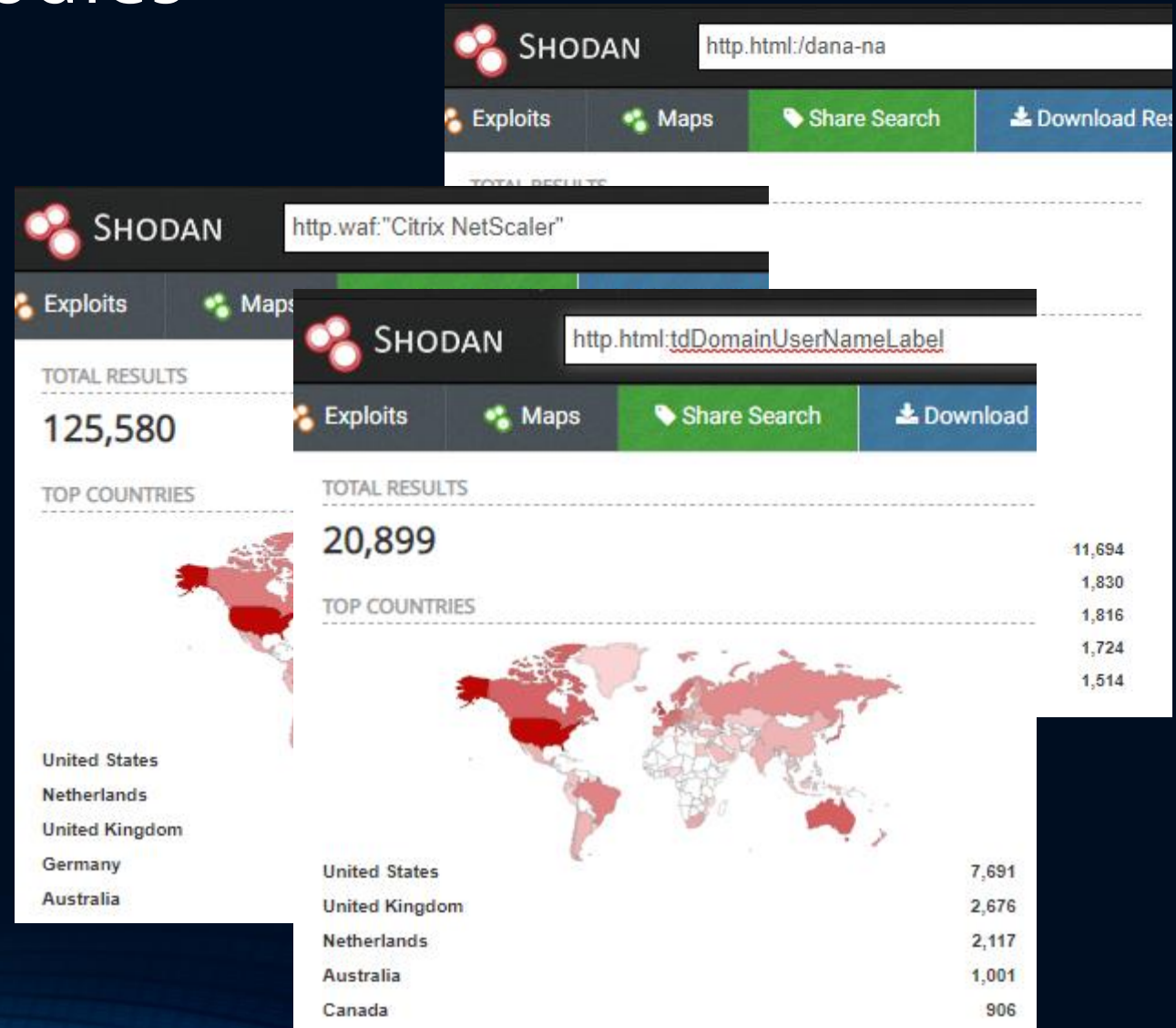
# Advanced fingerprinting techniques

- Find a sample system
- Shodan IP Details → Raw Data
- Find a unique attribute
  - Vendor-specific strings
  - Hard-coded landing pages
  - Path redirects
  - HTTP Headers
  - Shodan metadata
- Download results for deep digging



# Fingerprinting case studies

- Pulse VPN (CVE-2019-11510)
  - `http.html:/dana-na`
  - **`vuln:CVE-2019-11510`**
- Citrix LFI (CVE-2019-19781)
  - `http.waf:"Citrix NetScaler"`
  - **`vuln:CVE-2019-19781`**
- RD Gateway (CVE-2020-0609/0610)
  - `http.html:tdDomainUserNameLabel`
  - **`port:3391` + manual correlation**



# Closing Thoughts

- The go's called; they want their attacks back
- Zero days are expensive
- Mistakes are free
- Assess your network regularly
  - Weekly/Monthly
  - Exploit disclosure
  - Anytime something changes





# Thank you BlueHat IL!

SPECIAL THANKS: ANDREW MORRIS, @ACKMAGE & THE ENTIRE  
GREYNOISE TEAM