

Wash your hands! This is bot country!

Nate Warfield

Security Researcher | @n0x08



Why is this interesting?

- Network security is more important now than ever
- Disclosed vulns being used within days or *hours*
- Actors preferring targeted attacks
 - Travelex (Pulse VPN)
 - Healthcare & Hospitals
- Lives are at stake w/COVID-19
- Your perimeter got big. Real big.



WannaCry
NotPetya

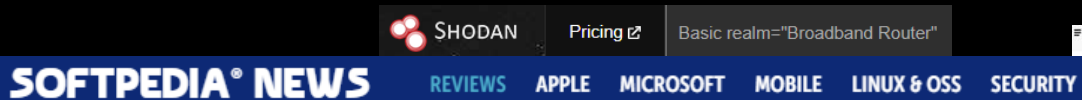


Targeted
Ransomware



The New Normal: Your network perimeter

- Old Routers
- Home appliances
- Home media
- Basic commo



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.

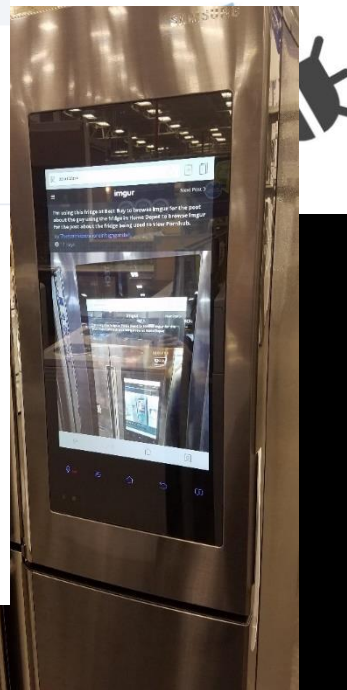


Smart refrigerators are becoming more and ...

85.207.47.46

ip@ipinfo.io
Raisko NET s.r.o.
Added on: 2019-11-15 10:14:32 GMT

Ubiquiti Networks Device
IP: 85.207.47.46



Risk at Enterprise Scale

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



Facet Analysis

vuln:cve-2020-0796

// TOTAL: 126,788

HiNet
NTT
Softbank BB
Rostelecom
Biglobe
Digital United
Fujitsu
Telmex
So-net
Telecom Italia
K-Opticom Corporation
Orange
Telefonica de Espana

932



Tools of the trade

- Censys
- BinaryEdge
- BGPView
- Shodan
- Greynoise

The collage features several tool interfaces:

- Censys:** A search bar at the top with the text "Q IPv4 Hosts" and a filter "80.http.get.title: citrix OR 80.http.get.title: netscaler".
- BinaryEdge:** A search bar containing "product:elasticsearch" with "Search" and "Clear" buttons. Below it is a table with columns "Ports", "Entries", and "Versions".

Ports	Entries	Versions
200/tcp	41,615	Elasticsearch RI API/7.4.2
501/tcp	7,884	Elasticsearch RI API/7.3.1
0/tcp	792	Elasticsearch RI API/6.5.4
306/tcp	154	Elasticsearch RI API/6.3.2
- BGPView:** A dark overlay with the BGPView logo and a "Countries Report" link.
- Shodan:** A search result for "Microsoft Corporation" (AS8075) showing "IPv4 Addresses: 34,407,936" and "Number of Peers: 449". It also lists "IPv4 Prefixes", "Peers", "Upstreams", "Downstreams", "Graphs", "World Map", "Raw Whois", and "IX".
- Greynoise:** A "Summary" section showing "REGIONAL REGISTRY: IANA" and "ALLOCATION STATUS: Assigned". Below it is a "Network" section with "IPv4 PREFIXES: 180", "IPv4 PEERS: 274", and "IPv4 UPSTREAMS: 13".



Malicious traffic is a global problem

- ~6 million 'malicious' IP addresses
- Every country is affected
- ~9 million 'malicious' IP addresses

> Malicious

ISP

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.

CVE-2017-7269 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.

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, 21 Dec 2018 15:42:06 GMT
Accept-Ranges: bytes
ETag: "0cbd7f8f2d9c213-1542067"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 04 Dec 2019 10:58:40 GMT

classification: unknown

results



1,542,067

1,056,874

876,452

558,130

493,375

103724

80272

79933

76967

70091

62820

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

Wallis and Futuna
Antarctica
Nauru
Norfolk Island
Palau
São Tomé and Príncipe
Åndland Islands

2

1

1

1

1

1

1



Forensics & Threat Intel

- greynoise analyze - analyze unstructured log data
 - Feed your VPN logs through it
 - Find out if your remote workforce networks have been compromised
- greynoise pcap – packet capture time machine
- Augment threat intel data



The image displays two overlapping screenshots. The top screenshot is a FireEye research report titled 'Solutions'. It discusses an open-sourced project titled 'bmfdec' and mentions that during the research period, they found an open-sourced project titled 'bmfdec' files. The report is titled 'Uncovering the Exploit' and describes the attackers' activity on September 22, analyzing FireEye Endpoint Security ring buffer events. It mentions that the analysis of the system did not uncover an initial exploit within the same timeframe, but the HTTP logs did uncover the initial payload. The report includes an example HTTP log entry, which is highlighted with a red box: `-` 2886000` 10.10.10.10` -` -` "[23/Sep/2019:10:10:10 +0800]"` "POST /weaver/bsh.servlet.BshServlet/ HTTP/1.1" -` -``. The bottom screenshot is a Greynoise search result for the IP address 49.234.29.65. It shows the IP is associated with the organization 'Shenzhen Tencent Computer Systems Company Limited'. The search results include a world map showing the location of the IP in China, with a bar chart indicating the top countries. The search results also list various scanners and tags, including 'HTTP Alt Scanner', 'Joomla RCE CVE-2015-8562', and 'Tomcat Manager Scanner'.

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

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



CTX267027

TRIPWIRE®

ty in VAN

GreyNoise Intelligence
@GreyNoiseIO

GreyNoise is

Additionally, CVE.

Use the follow opportunistic

Malicious Business

193.187.174.104

Organisation: IT Outsourcing LLC
Actor: Unknown

This IP address has been opportunistically scanning the Internet

First Seen: 2019-12-22 Last Seen: 2020-01-20
OS: Linux 3.11+ ASN: AS94439
Country: Turkmenistan City: Ashgabat
DNS: null

Citrix NetScaler LFI DockerD Scanner Redis Scanner Web Crawl Web Scanner

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

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
```


Shodan hunting 101

- Port
- Product
- Tags
- Enterprise features
 - Corp/Ent. Data License only
 - vuln:CVE-YYYY-NNNN
 - tag:self-signed

SHODAN Pricing [port:2375 product:"Docker"](#)

Top 19 Results for Facet: tag

cloud	38,485,486
self-signed	24,322,245
starttls	15,899,404
vpn	9,199,265
database	6,116,099
scanner	1,056,575
iot	332,385
videogame	247,598
ics	130,056
compromised	14,673
cryptocurrency	12,197
devops	12,146
tor	8,393
honeypot	8,261
medical	2,730
doublepulsar	643
malware	529
onion	50
c2	45

Amazon Data Services France	136
Tencent cloud computing	73
Amazon Data Services Ireland Limited	73

SHODAN Pricing [vuln:CVE-2019-0708](#)

TOTAL RESULTS

470,839

TOP COUNTRIES



China	194,973
United States	53,789
Korea, Republic of	23,891
Brazil	19,704
Russian Federation	18,285

TOP PORTS

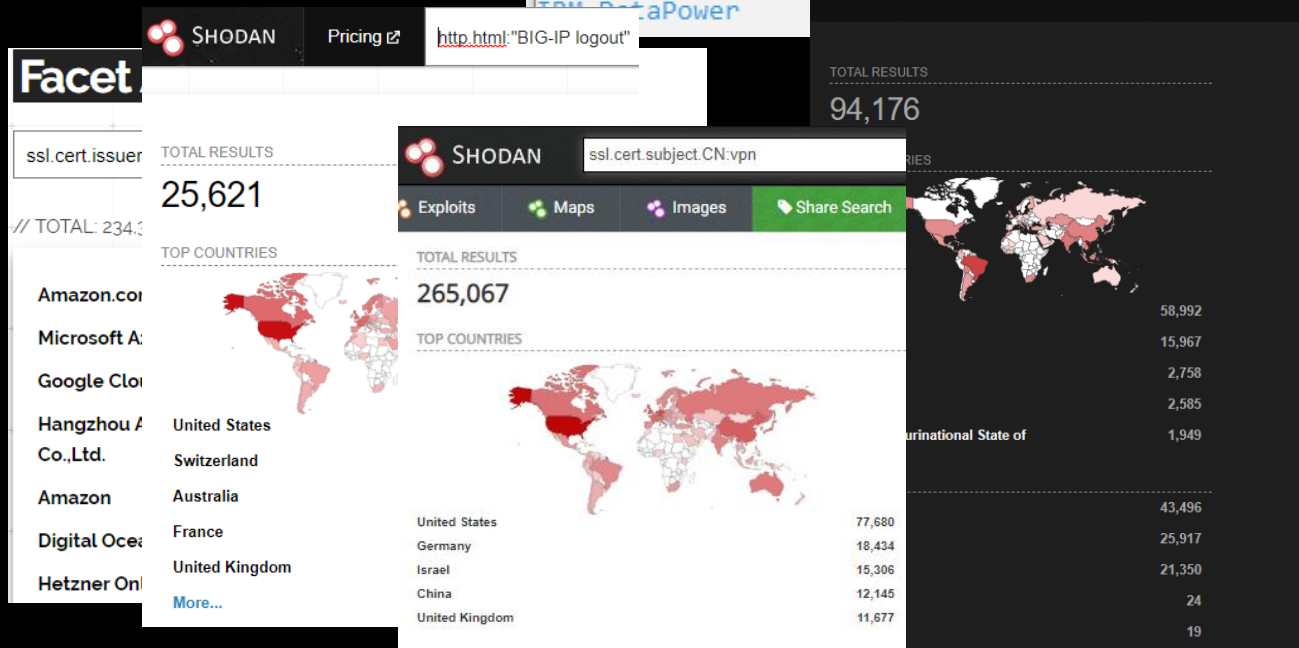
3389	465,269
3388	5,570



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 49,888
Incapsula WAF 49,888
TomcatPower 49,888
```



Advanced fingerprinting techniques

- Find a sample system
- Shodan IP Details → Raw Data
 - Vendor-specific strings
 - Hard-coded landing pages
 - Path redirects
 - HTTP Headers
- Download results for deeper hunting

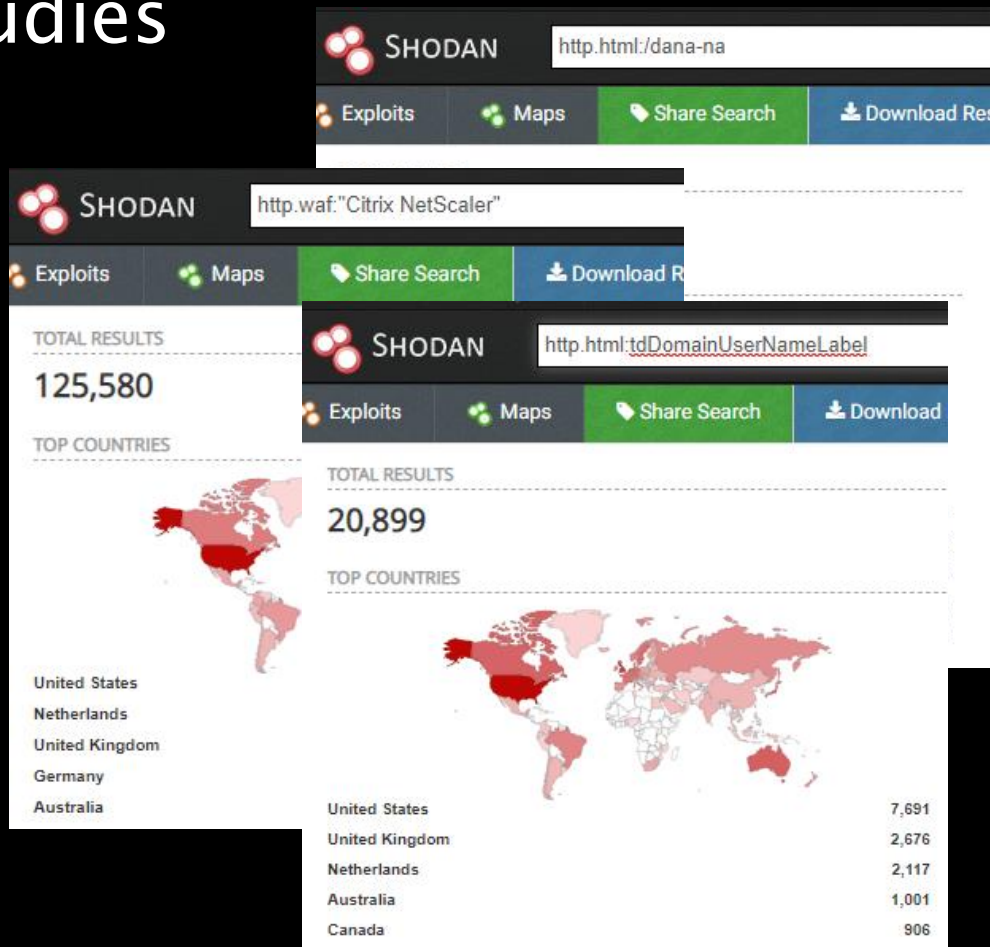
The screenshot displays the Shodan search interface. At the top, the IP address 202.129.58.131 is shown with a 'View Raw Data' link and a 'self-signed' status. Below this, a search bar contains the query 'product:"Pulse Secure"'. The interface includes tabs for 'Exploits', 'Maps', 'Like 2', and 'Download Results'. The search results section shows a total of 24,625 results. A world map highlights the top countries, with a table below it listing the top five countries by result count.

Country	Count
United States	9,790
United Kingdom	1,404
Japan	1,335
Germany	1,246
China	888



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)
 - `http.html:tdDomainUserNameLabel`
 - **port:3391 + manual correlation**



Closing Thoughts



- Attackers thrive on chaos
- Your perimeter has drastically expanded
- Assess your network regularly
 - Use alerting features (Greynoise & Shodan)
 - <https://github.com/n0x08/ShodanTools>
 - <https://github.com/jakejarvis/awesome-shodan-queries>
- Zero days are expensive
- Mistakes are free



#SASatHome | #TheSAS2020

Stay Safe!

#Quarantunities

- Cook dinner every night
- Co-founded CTI League
 - (cti-league.com | @ctileague)

Nate Warfield

Security Researcher | @n0x08

