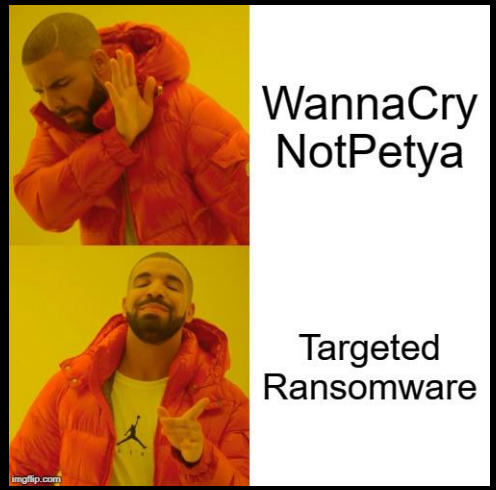
Wash your hands!
This is bot country!

Nate Warfield
Security Researcher | @n0x08

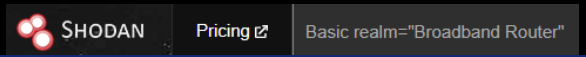
Why is this interesting?

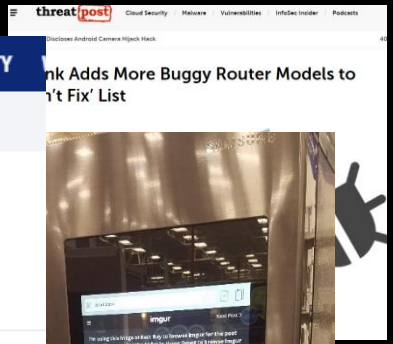
- Network security is more important now than ever
- Disclosed vulns being used within days or *hours*
- Actors preferring targeted attacks
  - Travelex (Pulse VPN)
  - Healthcare & Hospitals
- Lives are at stake w/COVID-19
- Your perimeter got big. Real big.



The New Normal: Your network perimeter

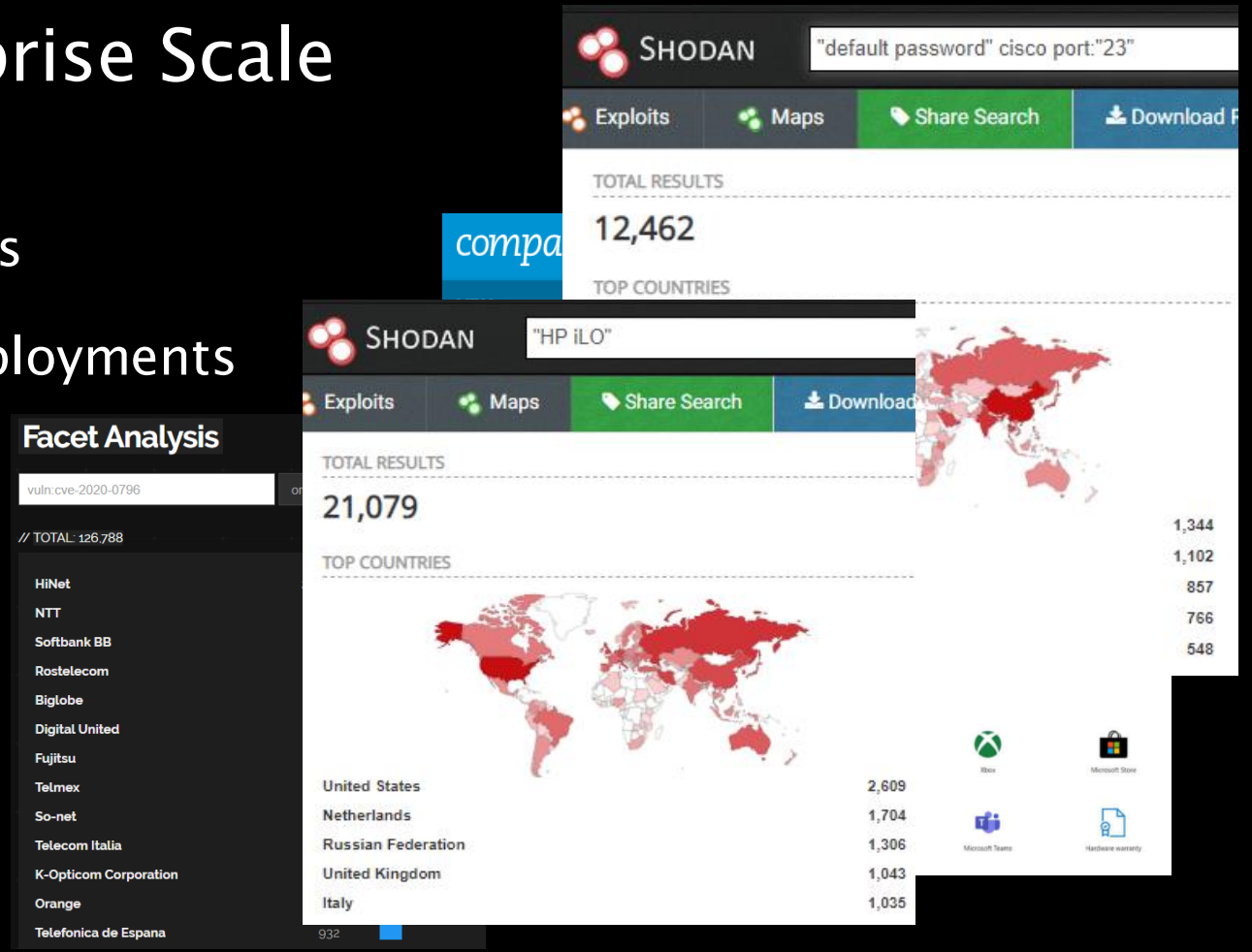
- Old Routers
- Home applia
- Home media
- Basic commo





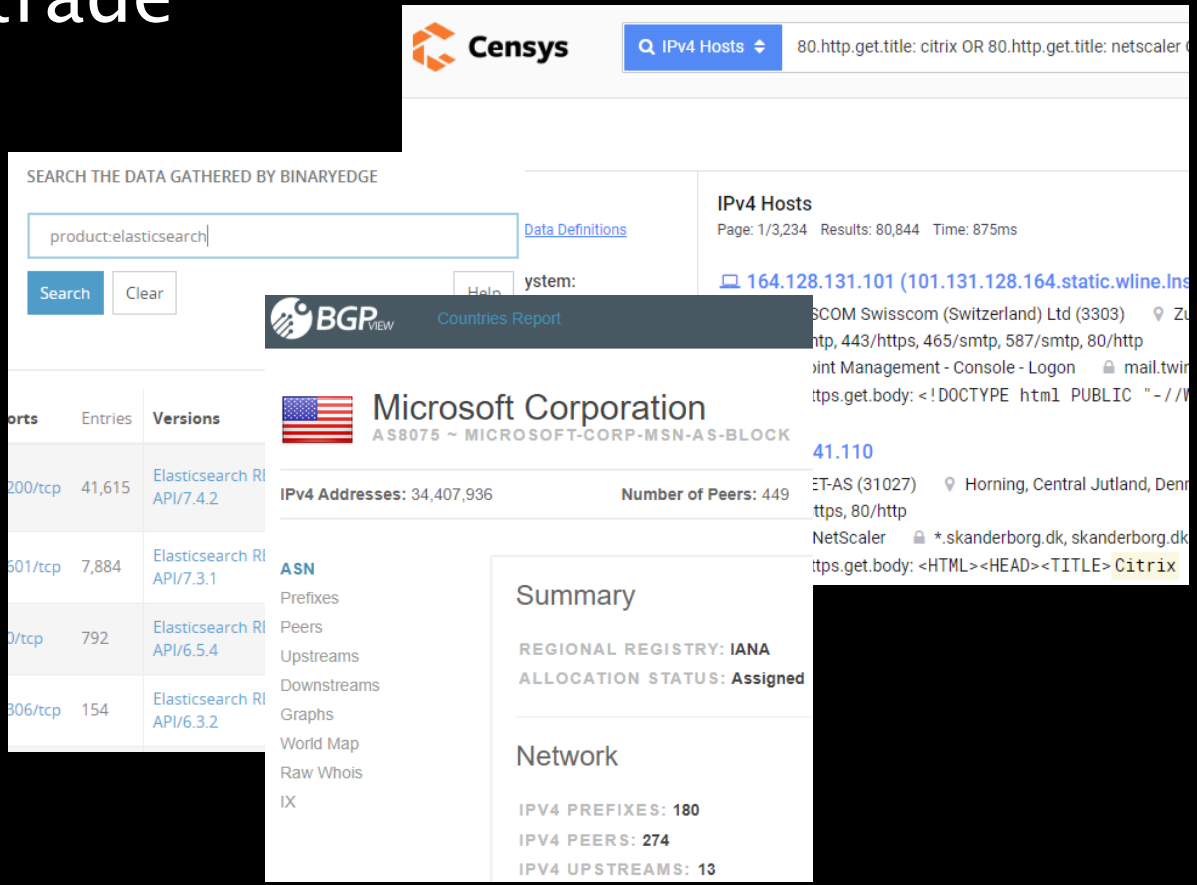
Risk at Enterprise Scale

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



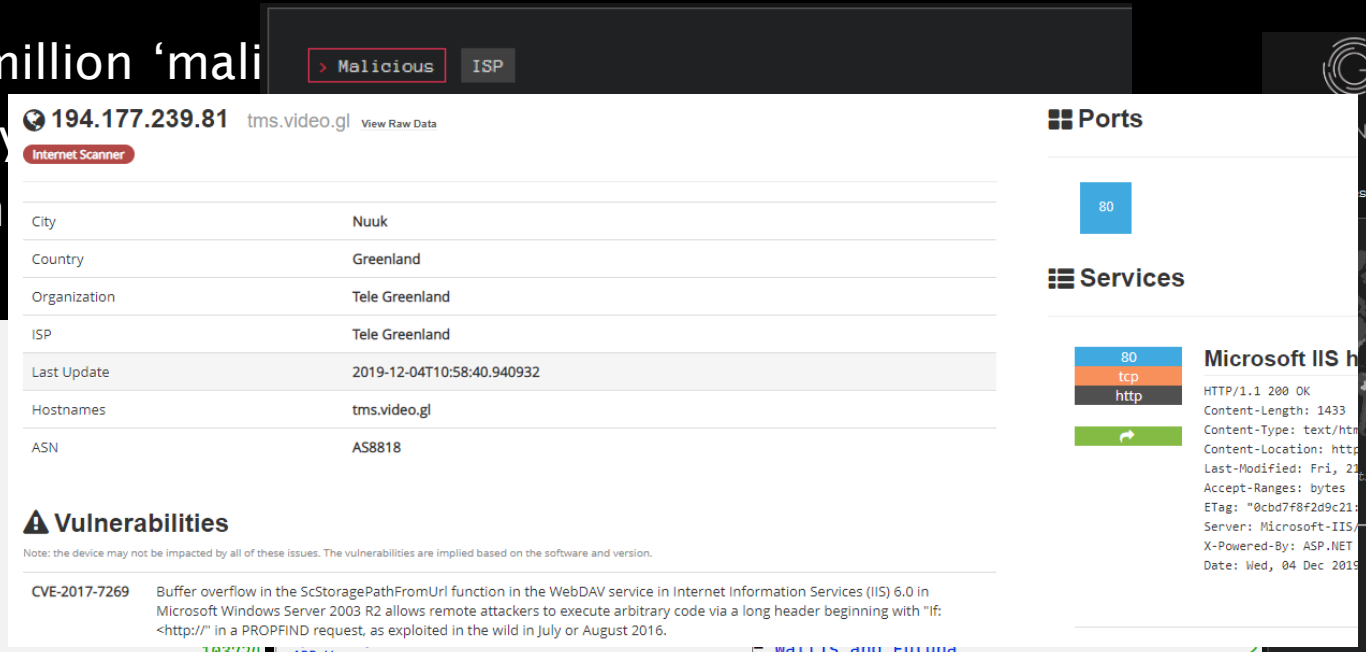
Tools of the trade

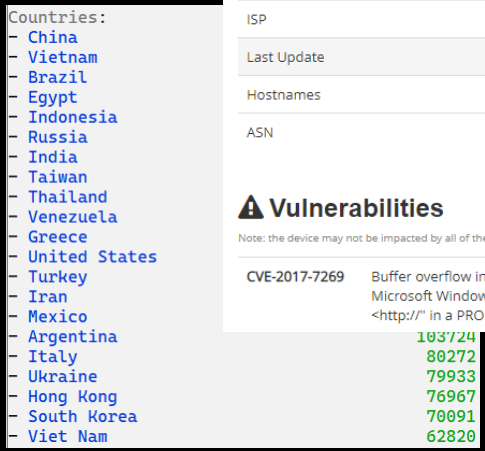
- Censys
- BinaryEdge
- BGPView
- **Shodan**
- **Greynoise**

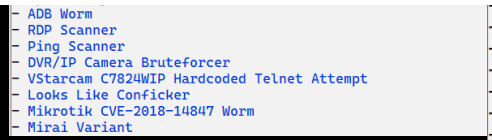


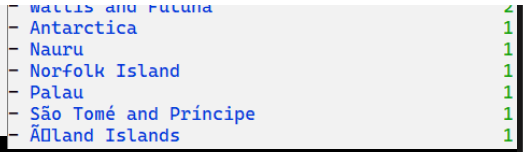
Malicious traffic is a global problem

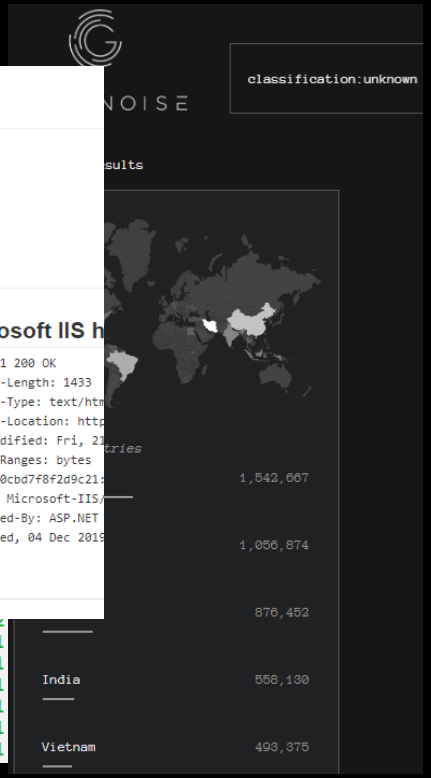
- ~6 million ‘mali
- Every
- ~9m





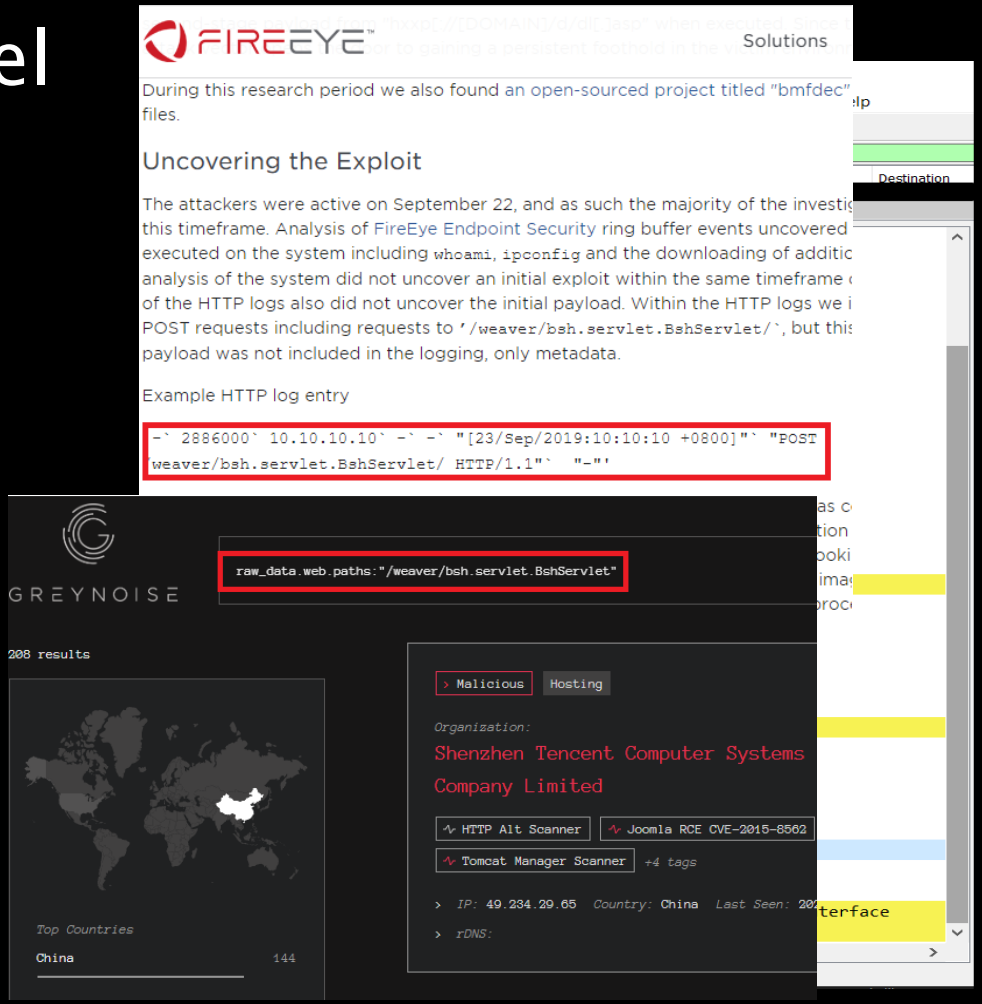






Forensics & Threat Intel

- 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



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

CTX267027

TRIPWIRE VERT

ty in NAN

GreyNoise Intelligence
@GreyNoiseIO

GreyNoise is

Additionally, CVE.

Use the follo opportunistic

Malicious Business

193.187.174.104

Organization: IT Outsourcing LLC

Actor: Unknown

This IP address has been opportunistically scanning the Internet

First Seen: 2019-12-22 Last Seen: 2020-01-29

OS: Linux 3.11+ ASN: AS64439

Country: Turkmenistan City: Ashgabat

rDNS: 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 H
2020-01-19 18:16:45.000 UTC	91.207.175.198	GET /vpn/js/%2e./.%2e/%76pns/cfg/smb.conf HTTP/1.1 Ho
2020-01-25 06:55:56.000 UTC	179.43.149.12	GET /vpn/js/%2E./.%2E/%76pns/cfg/smb.conf HTTP/1.1 H
2020-01-28 10:24:53.000 UTC	94.177.123.109	GET /vpn/../vpns/portal/scripts/picktheme.pl?f=3e2e41bd H
2020-01-30 13:38:16.000 UTC	175.139.71.8	GET /vpn/js/%2e./.%2e/%76pns/cfg/smb.conf HTTP/1.1 Ho

TR

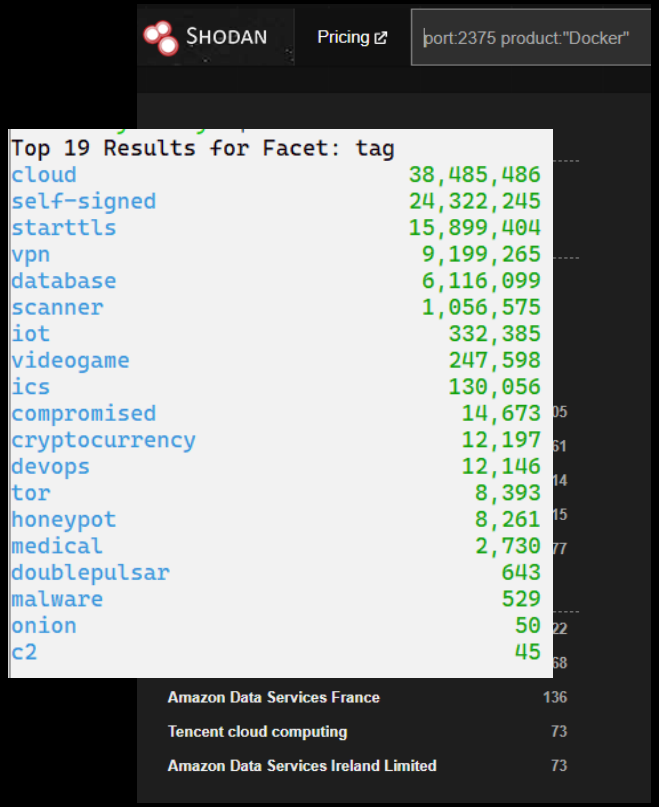
January 12, 2020 Compromise

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
```

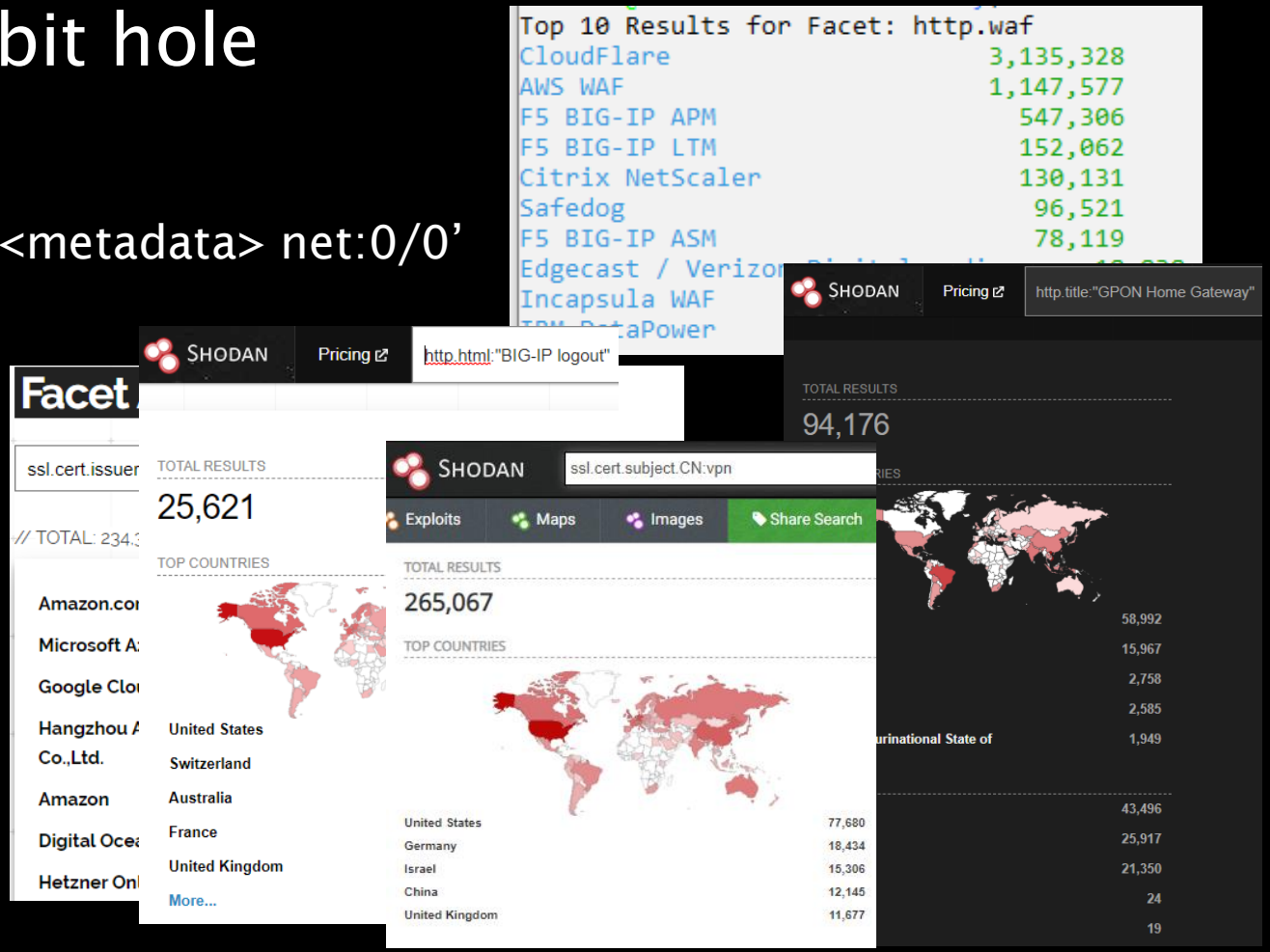
Shodan hunting 101

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



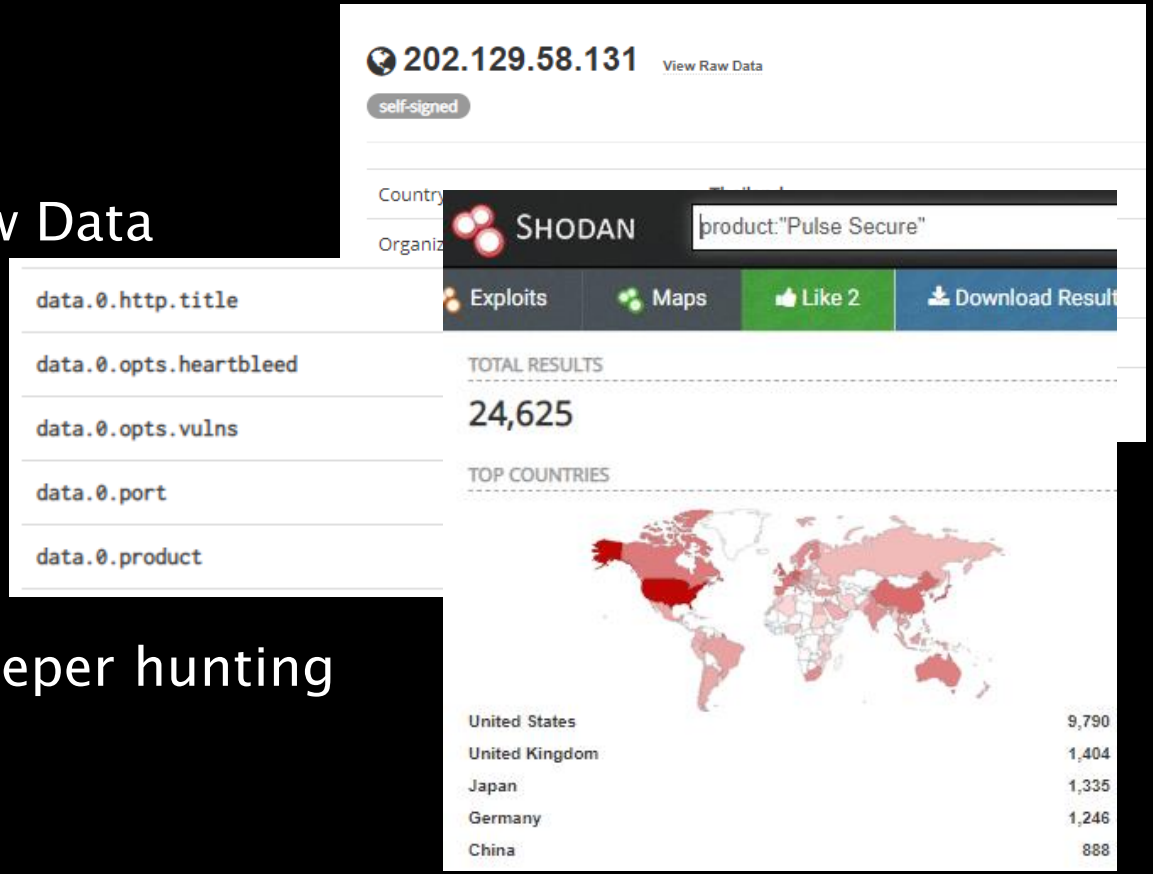
Down the rabbit hole

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



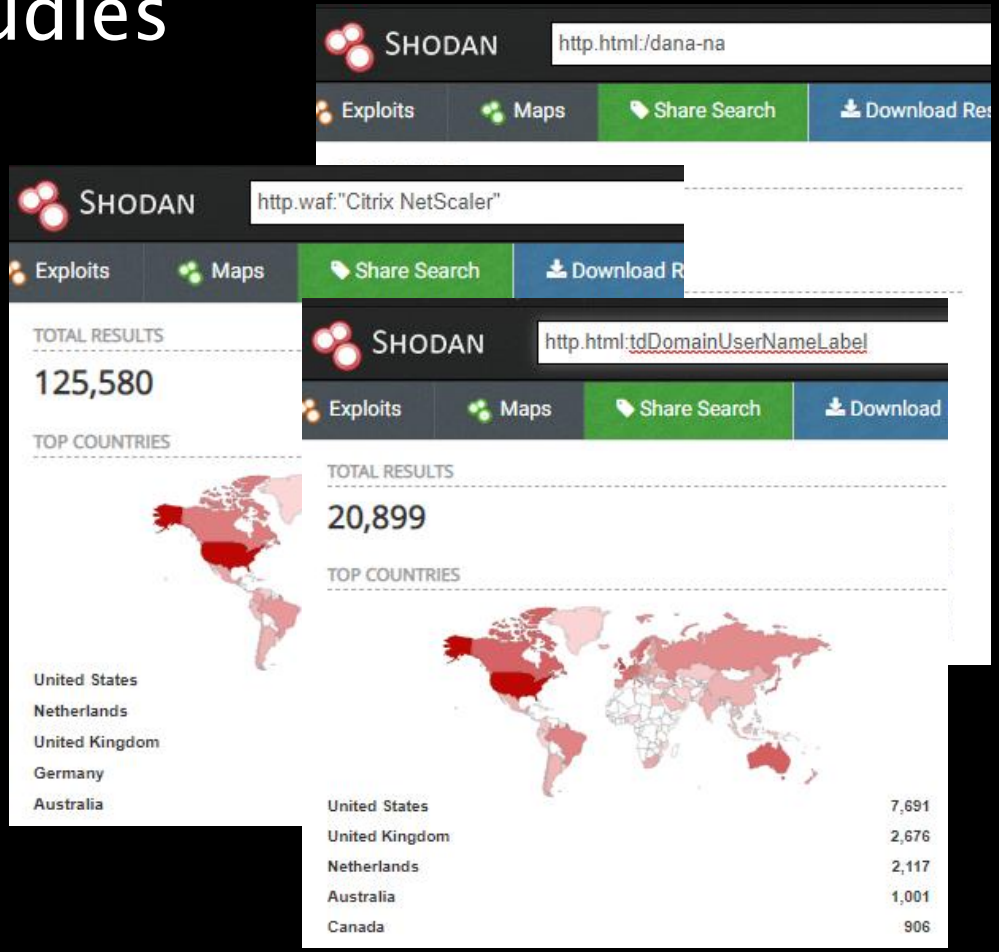
Advanced fingerprinting techniques

- 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



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