

Visibility beyond perimeters: C₂ detection

NATE WARFIELD | CHIEF TECHNOLOGY OFFICER | PREVAILION

/whoami (@n0x08)

- Former Defender ATP researcher
 - Former-former: vulnerability herder for MSRC (Patch Tuesday)
- Network hacker / researcher
- Conference speaker
 - BruCON OxOA
 - Kaspersky SAS
 - BSides Las Vegas
 - BlueHat & BlueHat Israel
- WIRED25 – 2020
 - CTI League co-founder



Why is this important?

- We continue to lose the fight against ransomware
- Supply chain attacks are becoming the new normal
- Security solutions have vulnerabilities
- Nearly impossible to know partner security posture
- Your perimeter is now your remote workforce

A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

April 16, 2021 · 10:05 AM ET
Heard on All Things Considered

DINA TEMPLE-RASTON

12-Minute Listen

+ PLAYLIST



An NPR investigation into the SolarWinds attack reveals a hack unlike any other, launched by a sophisticated adversary intent on exploiting the soft underbelly of our digital lives.
Zoe van Dijk for NPR

19 Sep, [REDACTED]

Your website says you do not attack critical infrastructure. We are critical infrastructure - we intertwined with the food supply chain in the US. If we are not able to recover very shortly, there is going to be very very public disruption to the grain, pork and chicken supply chain. About 40% of grain production runs on our software, and 11 million animals feed schedules rely on us. This will break the supply chain very shortly, and we will have to report this to our regulators and likely the public if this disruption continues. I assume you have thought that through? CISA is going to be demanding answers from us within the next 12 hours or so and we are going to have to tell them exactly what has happened and why the food supply chain is disrupted.

19 Sep, [REDACTED]

Support

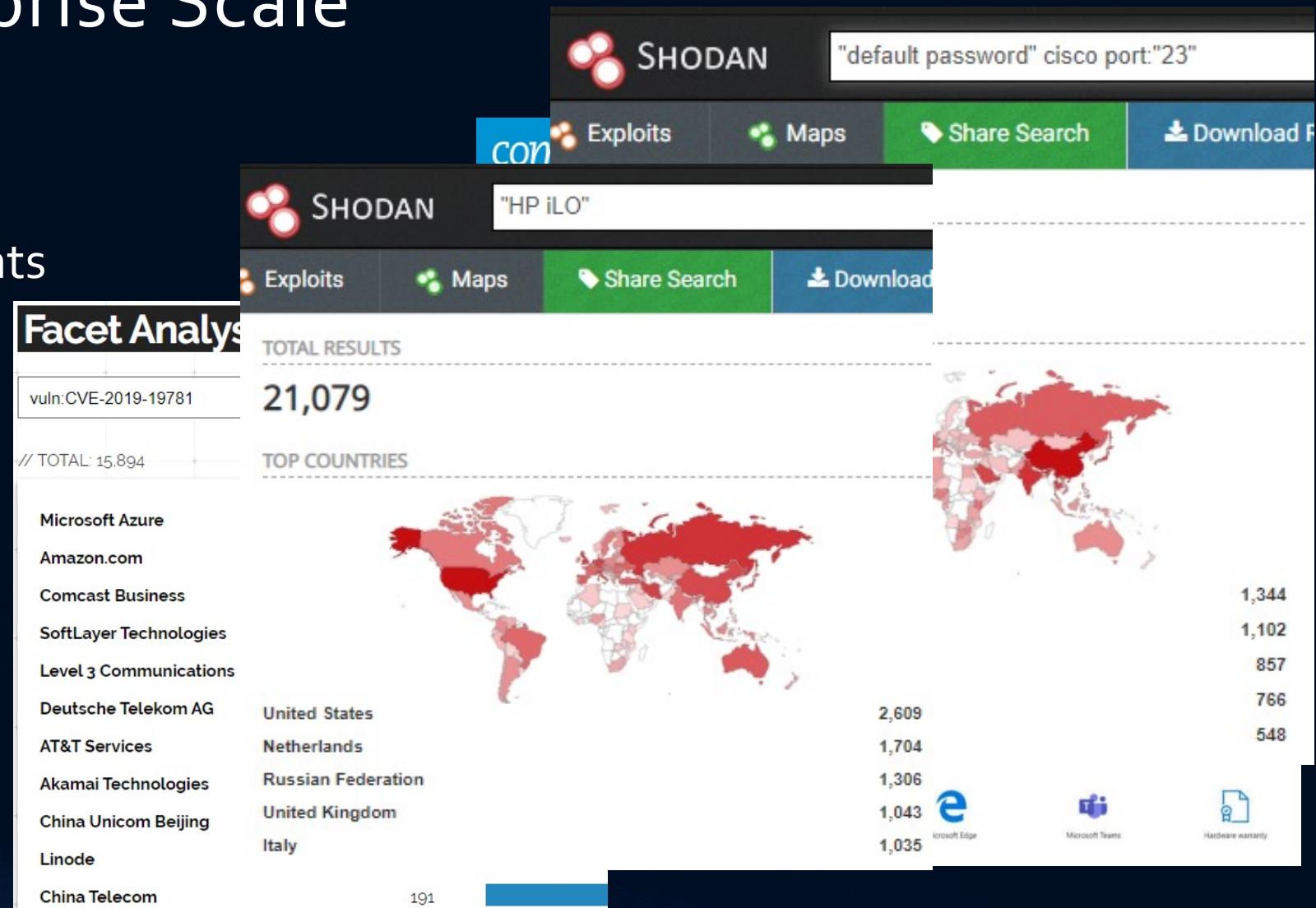
You do not fall under the rules, everyone will only incur losses, everything is tied to the commerce, the critical ones mean the vital needs of a person, and you earn money. Since everything is so serious with you, let's come to an agreement quickly and solve everything quickly.

19 Sep, [REDACTED]

Its not that simple. And it does not sound like you actually have rules. Maybe you just say these things to sound like you care. Supply of food is

Risk at Enterprise Scale

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



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

193.187.174.104		
2020-01-17 21:24:35.000 UTC	179.43.149.12	GET /vpn/js/%2E./%2E/%76pns/cfg/smb.conf
2020-01-19 18:16:45.000 UTC	91.207.175.198	GET /vpn/js/%2e./%2e/%76pns/cfg/smb.conf
2020-01-25 06:55:56.000 UTC	179.43.149.12	GET /vpn/js/%2E./%2E/%76pns/cfg/smb.conf
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

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/vuln...>

TRUSTEDSEC 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
```

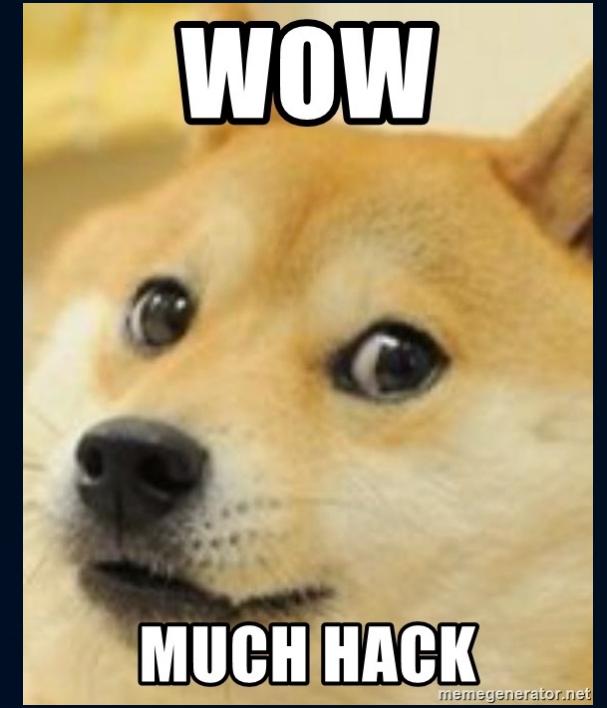
6:12 PM · Jan 10, 2020 · Twitter Web App

CVE-2020-5902 – Security reviews are hard

- *The Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages (K52145254)*
- TL;DR – this is a path traversal vulnerability against the management GUI
- [https://\\$IP/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=ANYTHING](https://$IP/tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?command=ANYTHING)
- F5 does advise against exposing this to the internet
- 10k people didn't follow that advice



BruCON OxOD - October 7th, 2021



CVE-2020-5902 – Two Exploits, One CVE

- tmshCmd.jsp - the “second” exploit was the first seen ITW
- Hsqldb – the POC was Java based; this is the “first” exploit
 - ITW exploits seen 2 days AFTER tmshCmd.jsp variant
- Indiscriminate/automated attacks seen in error messages
 - The requested user (bigipuser3) already exists in partition Common.] cmd_data=create auth user bigipuser3 password **** shell bash partition-access add { all-partitions { role admin }}'; tmsh -c 'list auth' > /var/tmp/auth;t execuq ~ vq ~ ,sq ~ sr java.lang.Integer8 I valuerx java.lang.Number... .. xp sr java.util.HashMap ... ` F loadFactorI thresholdxp?@ w xxx
- IOCs hunting via grep string (seriously!):
 - zgrep -riE '(hsqldb%3b|login.jsp/..%3b/hsqldb|..;|..%3b/|hsqldb|bigipuser3|systems|run util bash|base64|f5.sh|f5mkul)' /var/log/*

Those who do not learn history are doomed to repeat it

- <https://swarm.ptsecurity.com/rce-in-f5-big-ip/>
- Mikhail Klyuchnikov also found CVE-2019-19781 (Citrix RCE)!
- "...take a look at the research "Breaking Parser Logic" by Orange Tsai" (BlackHat 2018)
- The method he used was disclosed 20 months before he found the F5 bug
- CVE-2019-19781 was disclosed 5 months prior
- He didn't find the tmshCmd.jsp POC
- So who did?

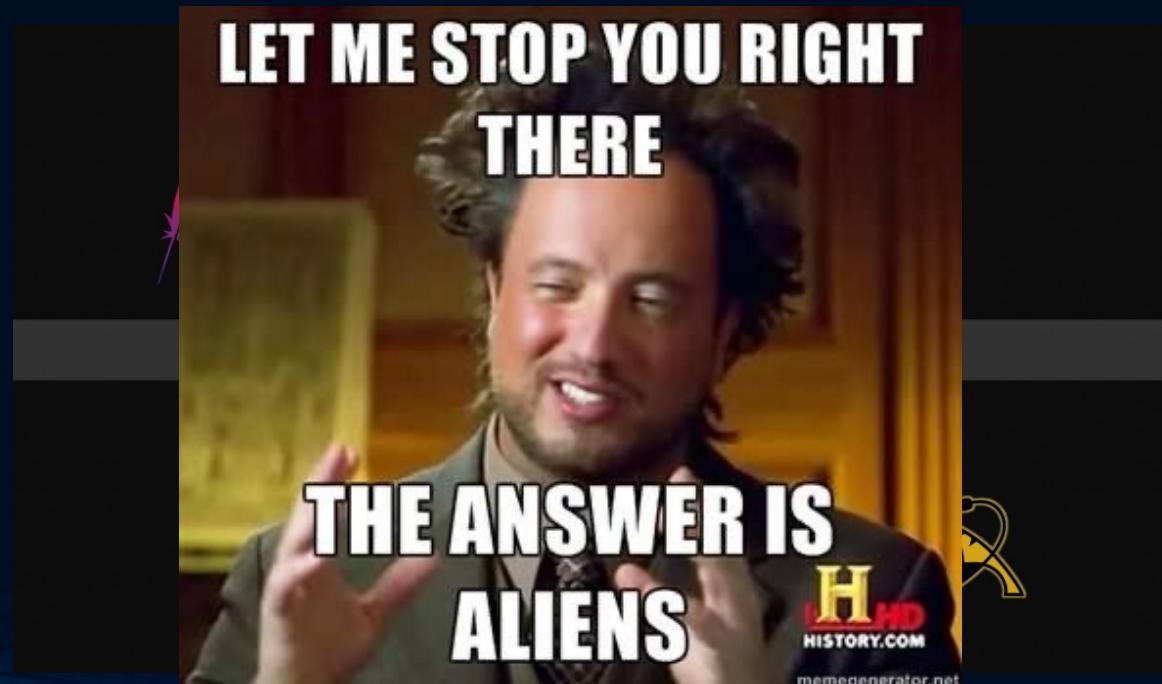
Conclusion

We were able to get Remote Command Execution on the F5 Big-IP appliance via the next three easy steps:

1. Discovering a misconfiguration of the Apache HTTP Server and Apache Tomcat
2. Discovering the use of default credentials for HSQLDB
3. Discovering questionable static methods in the F5 Big-IP TMUI libraries

The timeline:

- 1 April, 2020 – Reported to F5 Networks
- 3 April, 2020 – Vulnerability reproduced by F5
- 1 July , 2020 – Security Advisory and Fixes have been released



What we found in the rubble

- Web Shells, XMR Miners, PupyRAT & more
- Python port scanners/lateral movement tools
- Indications of advanced knowledge:
 - mount -o {rw|ro},remount /usr; (filesystem workaround)
 - cat /config/bigip/kstore/master (SecureVault device key)
- REST API abused post-compromise once attacker account created
 - Mitigations don't apply to REST; functionality is 'by design' when authenticated
- <https://research.nccgroup.com/2020/07/05/rift-f5-networks-k52145254-tmui-rce-vulnerability-cve-2020-5902-intelligence/> - the definitive IOC list



Tools of the trade

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

The screenshot shows the Censys search interface. At the top, there's a search bar with the query "IPv4 Hosts" and a result count of "80.http.get.title: citrix OR 80.http.get.title: netscaler". Below the search bar, the page title is "IPv4 Hosts" with a subtitle "Page: 1/3,234 Results: 80,844 Time: 875ms". The main content area is divided into two columns. The left column displays "Top Tags" with counts: Web Scanner (34), SSH Scanner (18), Telnet Scanner (13), FTP Scanner (7), and DNS Scanner (5). The right column displays "Top OS" with counts: Unknown (92) and Windows 7/8 (1). Below these sections are two detailed host entries for "Air Force Systems Networking". Each entry includes a "Web Scanner" tag, IP address (140.175.191.15 and 140.175.19.21), country (United States), last seen date (2020-05-08), and rDNS information (spoofable addresses like stat-019021.scott.af.mil). At the bottom of the page, there are statistics: "IPV4 PEERS: 274" and "IPV4 UPSTREAMS: 13".

Malicious traffic is a global problem

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

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.

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.

79933 76967 70091 62820

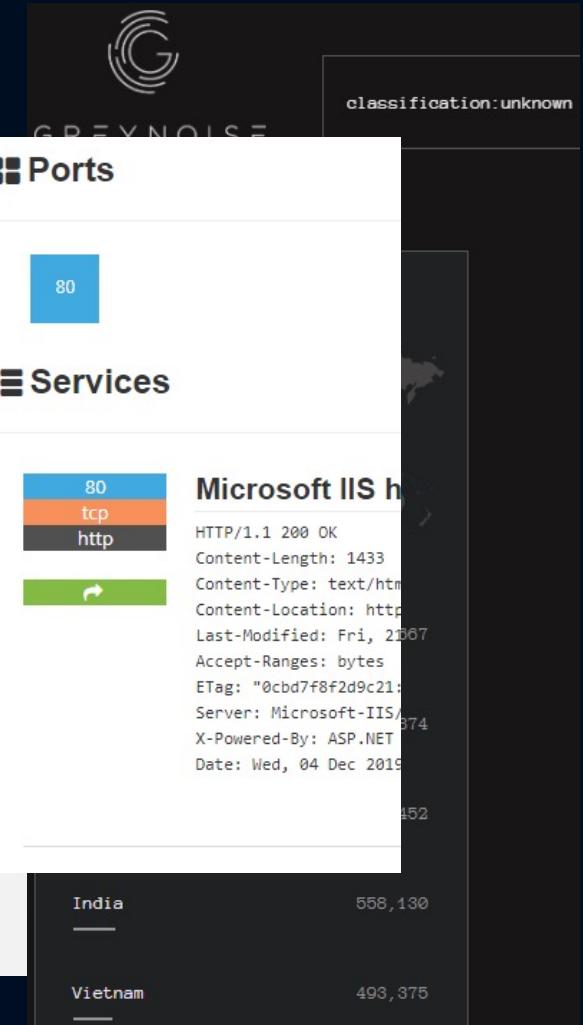
Ping Scanner

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

NOTIFICATION ISLAND

- Palau
- São Tomé and Príncipe
- Åland Islands

26764



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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==1433

FIREYE™ Threat Grid Solutions

GREYNOISE

raw_data.web.paths: "/weaver/bsh.servlet.BshServlet"

208 results

Top Countries

China 144

> Malicious Hosting

Organization:
Shenzhen Tencent Computer Systems
Company Limited

> IP: 49.234.29.65 Country: China Last Seen: 2015-08-11 10:45:00

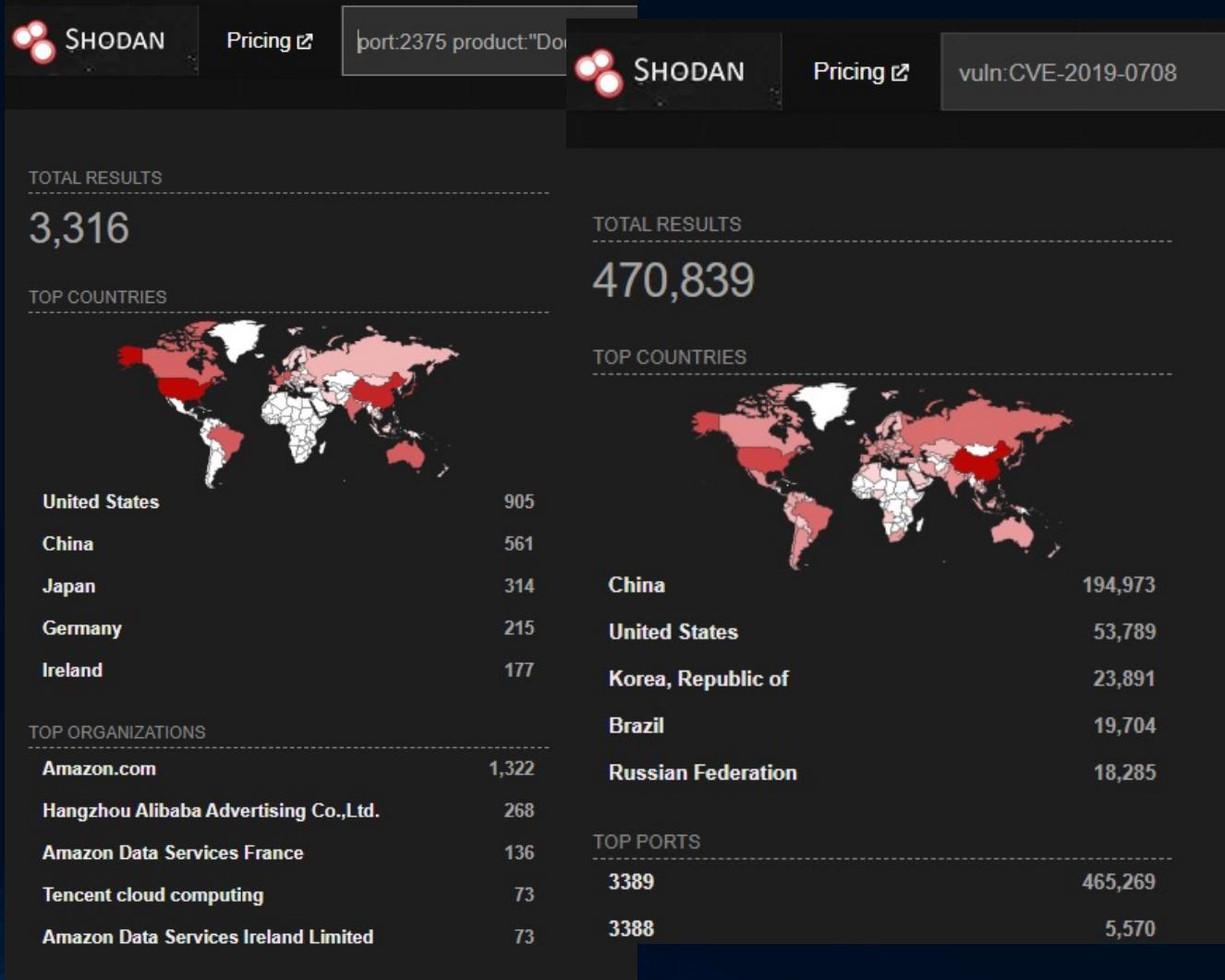
> rDNS:

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 pivoted our investigative focus to that date.

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

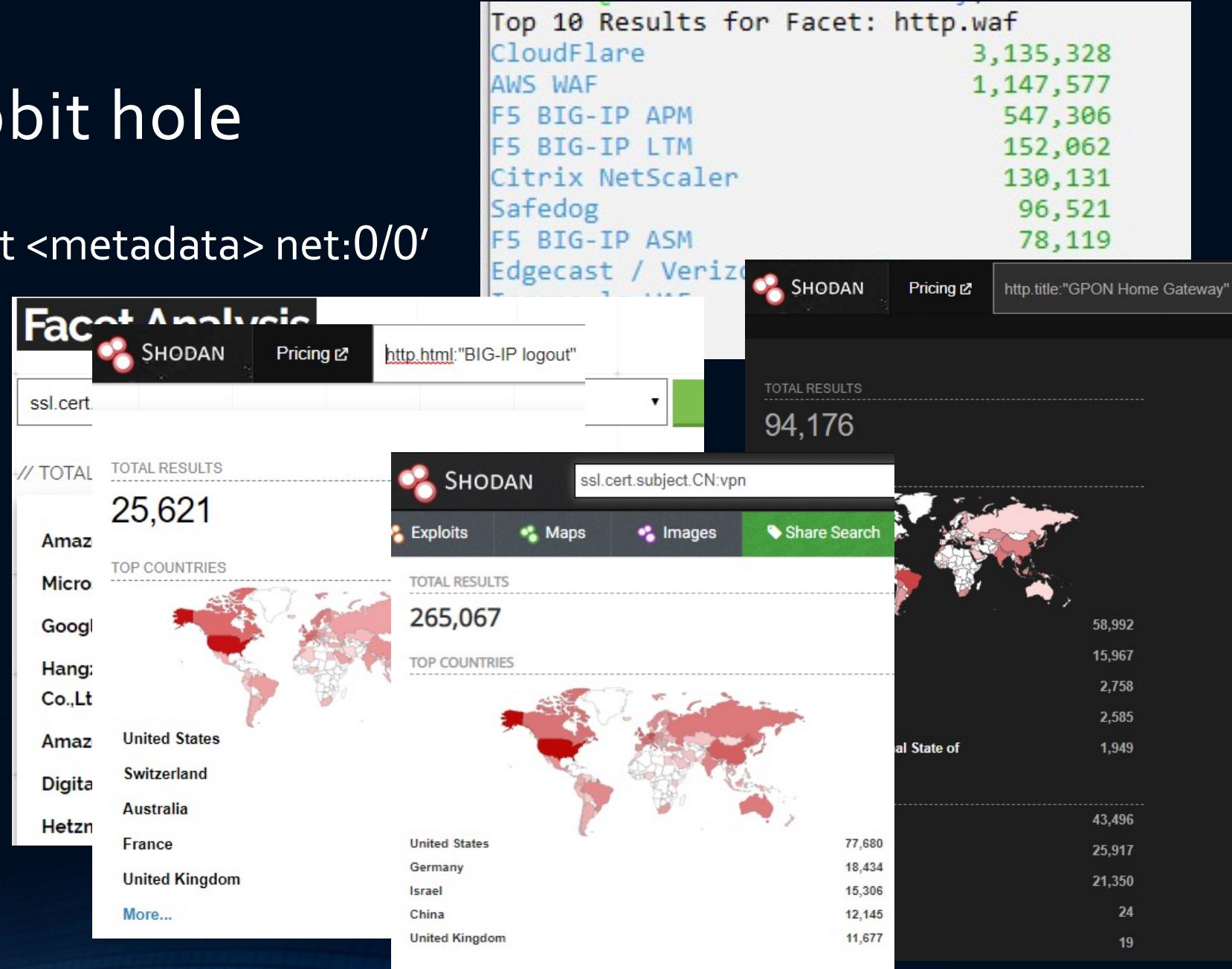
Shodan hunting 101

- Port
- Product
- Organization
- Enterprise features
 - \$10k/year license
- tag:self-signed
- 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



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 deeper digging

 202.129.58.131	View Raw Data
self-signed	
Country	Thailand
Organization	CAT Telecom
ISP	Communication Authority of Thailand,CAT
Last Update	2020-01-28T22:48:36.371616
ASN	AS9931

data.0.http.title	Pulse Connect Secure
data.0.opts.heartbleed	2020/01/28 23:48:45 202.129.58.131:443
data.0.opts.vulns	['CVE-2019-11510']
data.0.port	443
data.0.product	Pulse Secure

Org search is your friend

- Ingram Micro is a huge company
- Many acquisitions
- Hard to find by ASN
- Org:"Ingram Micro"
- Serbian office is interesting...

The screenshot displays a search interface for network assets, specifically focusing on Ingram Micro d.o.o. Beograd. The results are presented in a grid format across four panels:

- Panel 1 (Top Left):** IP address 185.130.127.177. Shows DCE/RPC Endpoint Mapper details: Max Count: 500, Actual Count: 500, Number of Entries: 500. Mapped services listed include d95afe70-a6d5-4259-822e-2c84da1ddb0d (ncalrpc: WindowsShutdown) and d95afe70-a6d5-4259-822e-2c84da1ddb0... (ncalrpc: WindowsShutdown).
- Panel 2 (Top Right):** IP address 185.130.124.112. Shows Minecraft Server details: Online Players: 0, Maximum Players: 2, Version: 1.15.2 (Protocol 578), and Description: A Minecraft Server.
- Panel 3 (Bottom Left):** IP address 185.130.127.162. Shows SSL Certificate details: Issued By: CP-00, Issued To: CP-00; Administrator SES. Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2.
- Panel 4 (Bottom Right):** IP address 185.130.127.177. Shows SMB Status: Authentication: enabled, SMB Version: 1. OS: Windows Server 2016 Datacenter 14393, Software: Windows Server 2016 Datacenter 6.3, Capabilities: extended-security, infolevel-pas.

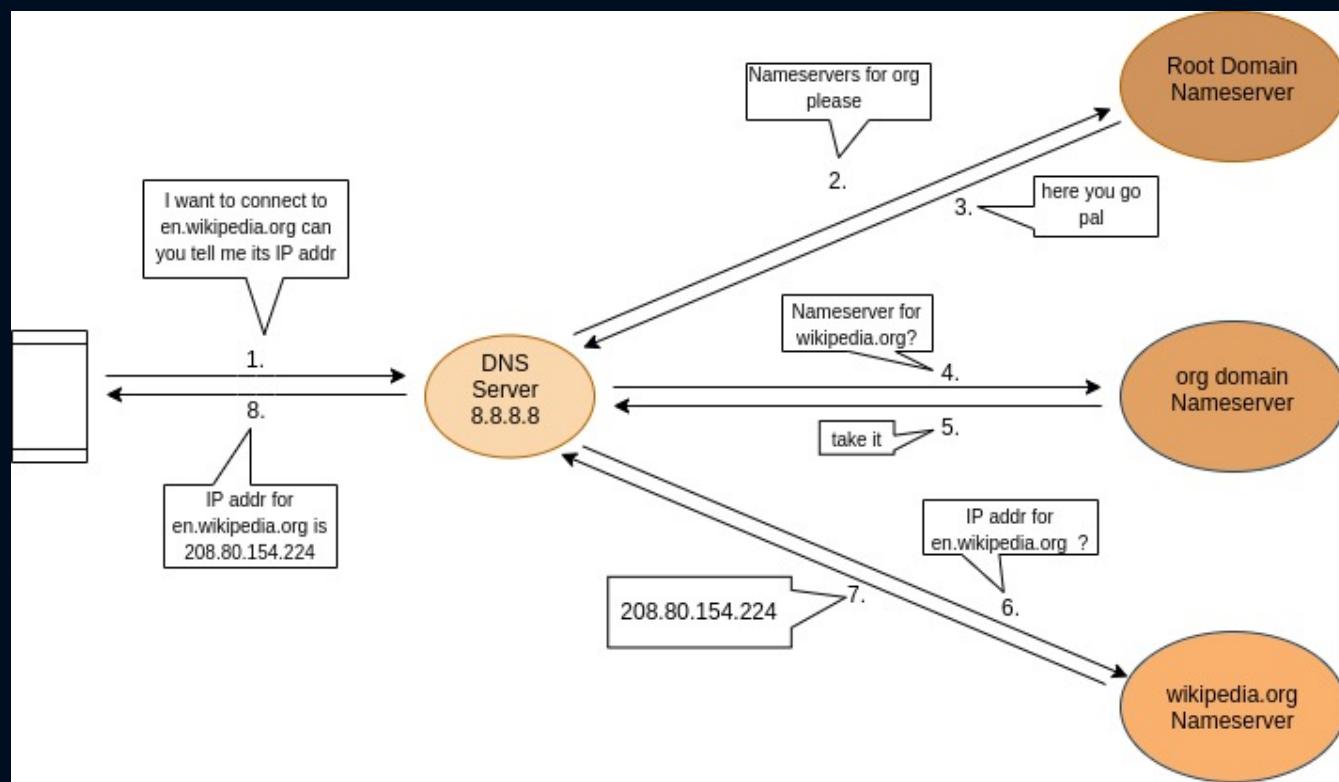
The interface includes a sidebar with a user icon labeled "Administrator" and a password input field.

Command & Control based malware 101

- Bespoke (actor developed & maintained)
- Professional tooling (Metasploit, Cobalt Strike, etc.)
- Commodity tooling (NanoCore, AgentTesla)
- Most common attack vector: email
- Small, usually obfuscated payload
- On execution, attempts to find C2 via DNS or direct IP
- DNS is more resilient & preferred for indiscriminate attacks

It's (almost) always DNS

- DNS means we can infiltrate
- Partial coverage is good enough
- We get signal globally
- Mischief is possible



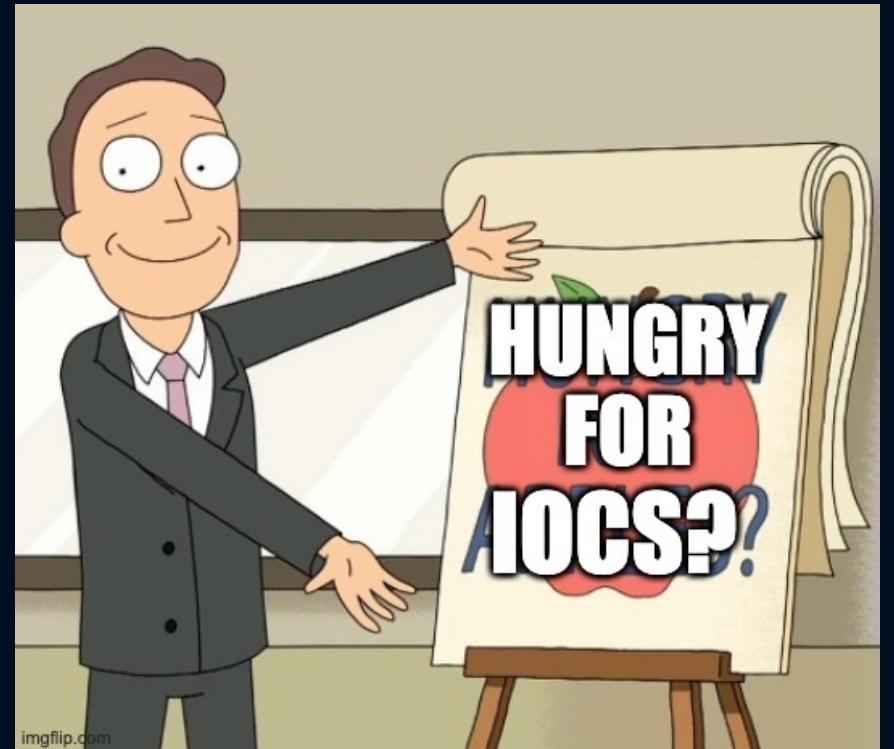
A different approach: C₂ network infiltration

- Bad guys don't notice (attrition is expected)
- Doesn't require endpoint clients / appliances
- Provides instantaneous signals intelligence
- Neuters part of the C₂ infrastructure
- Two flavors: DNS only & full L7
- It's just plain cool



DNS-only infiltration & its limitations

- False positives
 - Security companies
 - Attachment detonation services
 - URL expanders
- Open resolvers (Google, Cloudflare)
- APTs are nearly invisible (bespoke infrastructure)



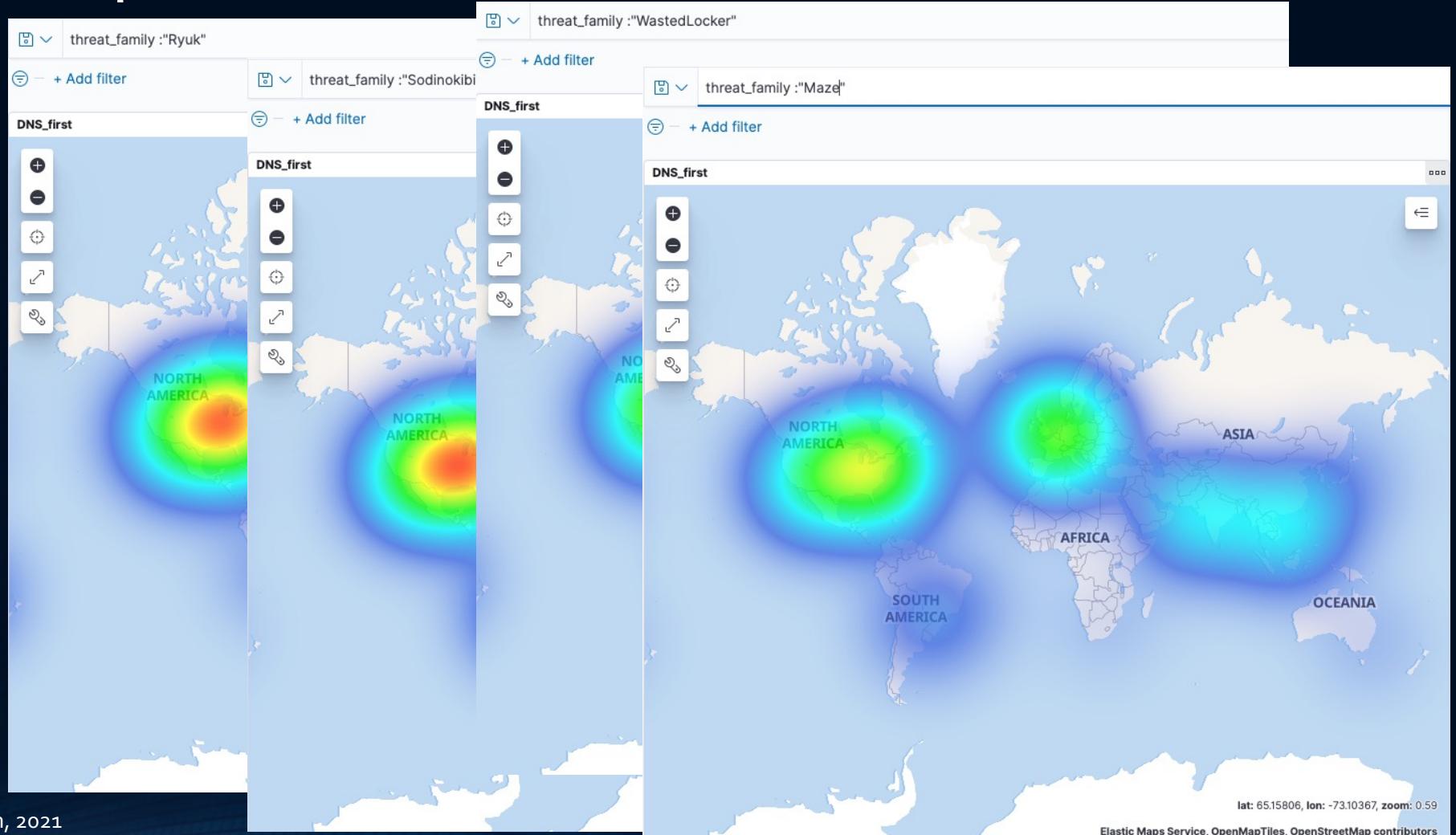
DNS-only visibility is still useful

- Shows how bad we are at utilizing DNS IOCs
- Provides signal “something” happened
- Can be stage 1 of a larger problem
- Groundwork to infiltrate at L7
- Good for assessing geographic trends
- Better context than traditional sinkhole



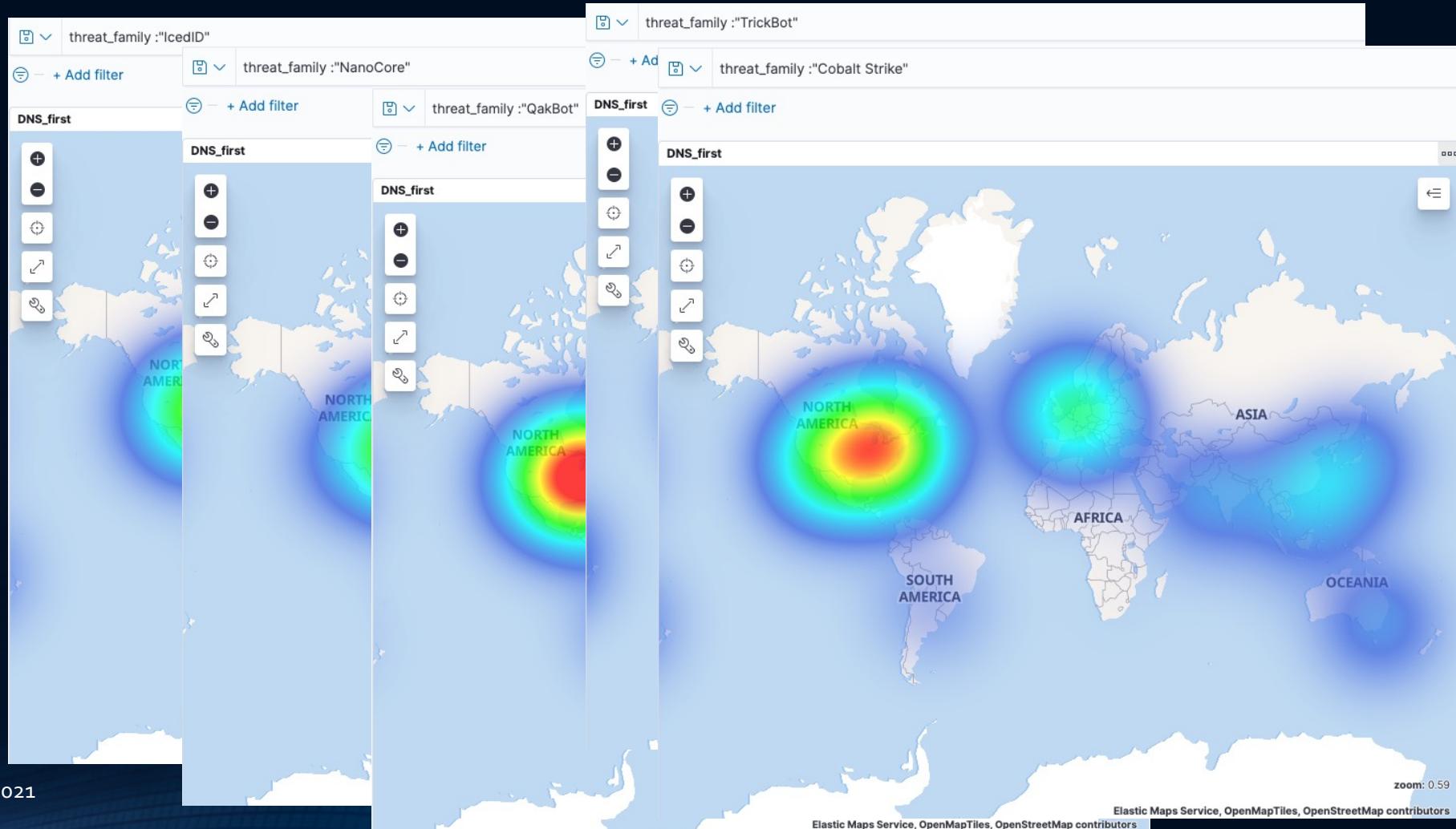
Pathogen Spread: Ransomware

- Ryuk
- Sodinokibi
- WastedLocker
- Maze



Pathogen Spread: RATs

- IcedID
- NanoCore
- QakBot
- TrickBot
- Cobalt Strike



CTI League use of DNS visibility

- Healthcare organizations != security companies
- Signals are more likely to be true positives
- Hospitals were huge targets in 2020
- My boss gave away access for free
- Coordinated with H-ISAC
- Multiple hospitals avoided ransomware

Companies/Organizations

- ↗ [King Faisal Specialist Hospital](#)
 - ↗ [Centre Hospitalier Universitaire De Toulouse](#)
 - ↗ [Azul Hospitality Group](#)
 - ↘ [Soc Benefic De Senhoras Hospital Sirio Libanes](#)
 - ↘ [Apollo Hospitals Enterprise Limited](#)
 - ↘ [Security Forces Hospital](#)
 - ↘ [Mata Chanan Devi Hospital](#)
 - ↘ [Centre Hospitalier Universitaire Vaudois Chuv](#)
 - ↘ [Helsinki University Central Hospital](#)
-
- ## Companies/Organizations
- ↗ [Nalc Health Benefit Plan](#)
 - ↗ [Tsi Fuer Alliance Healthcare Deutschland Ag](#)
 - ↗ [Novant Health Inc](#)
 - ↘ [Intermountain Health Care](#)
 - ↘ [New Era In Healthcare](#)
 - ↘ [Adventist Health Systems](#)
 - ↘ [Personal Home Health Fvs](#)
 - ↘ [Parkland Health & Hospital System](#)

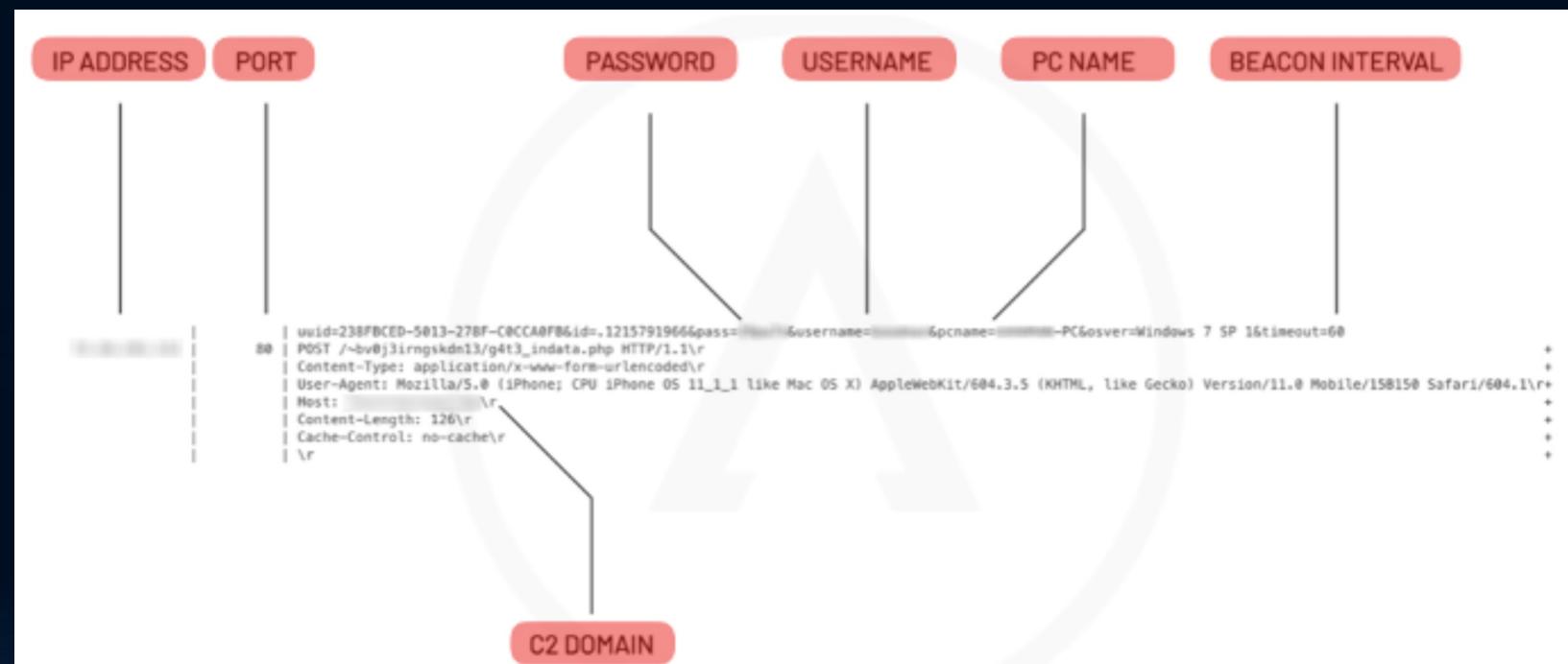
Full infiltration: The better way

- Continue to host malicious C2 zones
- Respond with sensor IP we control
- Allow malware to connect (any port/proto)
- Record what it sends
- Correlation against SSL Cert data
- Spread rate, geographic distribution, etc.

Origin (Infected) IP Address: [REDACTED].149
Beacon Count: 9
First Seen Date & Time: 2021-02-27 10:29:22
Last Seen Date & Time: 2021-03-03 18:45:40
Port & Protocol: 443
Certificate Hash: fb2f577adfe6d9836d00a21a1016e [REDACTED]
Certificate Name: *.amstel.dox.pub
Region: north america
Country: united states
ISP/Cloud Provider: digitalocean llc
Destination (Sensor) IP Address: [REDACTED].132

Visibility provided by full-infiltration

- Actual affected user IPs
- No longer masked by recursive DNS providers
- Usernames & passwords
- Machine names
- OS Versions
- Weird payloads

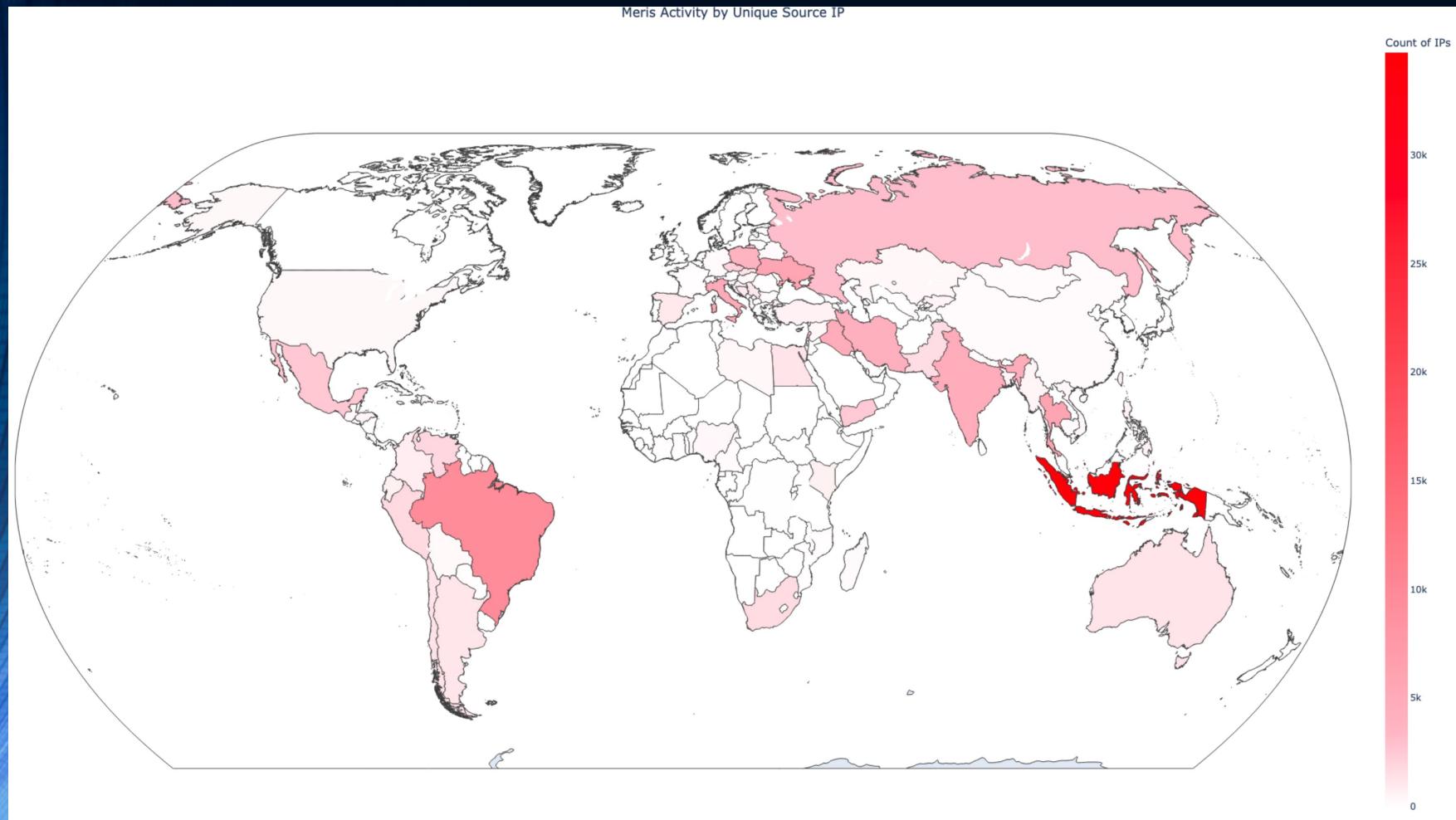


With great power comes....evil ideas

- BGP hijacking attacker C2
- MITM malware traffic
- Insert tracking payloads during exfiltration
- Replace exfiltrated data with ransomware
- Remotely delete malicious payloads
- Patch botnets



Meris Botnet



Closing Thoughts

- The 90'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
- <https://github.com/n0x08>



Thank you!

NATE WARFIELD | CHIEF TECHNOLOGY OFFICER | PREVAILION