New Class of DNS Vulnerabilities Affecting Many DNSaaS Platforms

Shir Tamari & Ami Luttwak

Wiz.io

Background:

The Wiz Research Team

- Experienced security researchers
- Microsoft Cloud Security Group veterans
- Groundbreaking cloud research

The Beginning:

Why DNS-as-a-Service?

- DNS is the lifeblood of the internet
- Potentially huge impact
- Impacts cloud & on-prem assets
- DNS is incredibly complex

WIZ

Target:

Route53

- DNS-as-a-Service from AWS
- Highly popular

Route53:

Domain Hijacking

- ~2000 **Shared** DNS servers
- Each domain has 4 Name Servers
- Target: wiz.io

WIZ

Route53:

Domain Hijacking

WIZ

ns-1334.awsdns-38.org

ns-883.awsdns-46.net

ns-457.awsdns-57.com

ns-1611.awsdns-09.co.uk

Route53:

Domain Hijacking

Official AWS DNS Server	Customer's DNS Zones
ns-1334.awsdns-38.org	wiz.io
	company.com
	company2.com
	company3.com
	wiz.io

WIZ

Record name	Type	Value/Route traffic to
wiz.io	NS	ns-736.awsdns-28.net. ns-249.awsdns-31.com. ns-1805.awsdns-33.co.uk. ns-1373.awsdns-43.org.
wiz.io	SOA	ns-736.awsdns-28.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

Wiz.io

ns-1334.awsdns-38.org

ns-883.awsdns-46.net

ns-457.awsdns-57.com

ns-1611.awsdns-09.co.uk

WIZ

Domain Hijacking:

Different angle

- What domain can We possibly register?
- Should not exist on the nameservers
- DNS clients must query for it

Domain Hijacking:

Different angle

- Register an AWS official nameserver: What would happen?
- ns-852.awsdns-42.net?

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protoc	Length	Info
4493	28.968953	192.168.1.1	192.168.1.4	DNS	158	Standard query response 0x922c No such name SOA CABe8SkvDYjJXSIRSKRQk.com SOA a.gtld-server
4494	28.974562	192.168.1.4	192.168.1.1	DNS	71	Standard query 0xc17a SOA CV5eY1n.com
4495	28.990418	192.168.1.4	192.168.1.1	DNS	69	Standard query 0x3da2 SOA FaE01.com
4496	28.997007	192.168.1.1	192.168.1.4	DNS	143	Standard query response 0xd06a No such name SOA U7Ncif.com SOA a.gtld-servers.net
4497	29.012801	192.168.1.1	192.168.1.4	DNS	154	Standard query response 0xad4a No such name SOA vON80G1U2qkXeHppp.com SOA a.gtld-servers.ne
4499	29.022270	192.168.1.4	192.168.1.1	DNS	68	Standard query 0x3022 SOA Bj6B.com
4500	29.036688	192.168.1.4	192.168.1.1	DNS	82	Standard query 0x5dcb SOA dEVFXsR4WTXbJXVDrk.com
4501	29.060790	192.168.1.1	192.168.1.4	DNS	144	Standard query response 0xc17a No such name SOA CV5eY1n.com SOA a.gtld-servers.net
4502	29.060790	192.168.1.1	192.168.1.4	DNS	142	Standard query response 0x3da2 No such name SOA FaE01.com SOA a.gtld-servers.net
4503	29.060886	192.168.1.4	192.168.1.1	DNS	65	Standard query 0x3f0e SOA c.com
4504	29.076690	192.168.1.4	192.168.1.1	DNS	74	Standard query 0xf6bd SOA Mi5cLf1lFs.com
4505	29.091660	192.168.1.4	192.168.1.1	DNS	76	Standard query 0x4f50 SOA seoME1C2E9I7.com
4506	29.094018	192.168.1.1	192.168.1.4	DNS	141	Standard query response 0x3022 No such name SOA Bj6B.com SOA a.gtld-servers.net
4507	29.104629	192.168.1.4	192.168.1.1	DNS	92	Standard query 0x8bf9 SOA r4LCBFUZUIpP6RAj8Rd4HjSD0UAb.com
4508	29.107152	192.168.1.1	192.168.1.4	DNS	155	Standard query response 0x5dcb No such name SOA dEVFXsR4WTXbJXVDrk.com SOA a.gtld-servers.n
4509	29.124285	192.168.1.4	192.168.1.1	DNS	72	Standard query 0x1f2a SOA EtVEMmBj.com
4511	29.133000	192.168.1.1	192.168.1.4	DNS	138	Standard query response 0x3f0e No such name SOA c.com SOA a.gtld-servers.net
4517	29.145311	192.168.1.1	192.168.1.4	DNS	147	Standard query response 0xf6bd No such name SOA Mi5cLf1lFs.com SOA a.gtld-servers.net
4518	29.151421	192.168.1.4	192.168.1.1	DNS	91	Standard query 0x3371 SOA JjS8xZxqOcP0iyTOuXyZmsZt47s.com
4519	29.151749	192.168.1.4	192.168.1.1	DNS	88	Standard query 0xc71c SOA G3FnU879bSN3O9fPmfUV57ws.com
4520	29.160175	192.168.1.4	192.168.1.1	DNS	89	Standard query 0x124e SOA KHSc82IrpYYvmA9FljhFljtiy.com
4521	29.163878	192.168.1.1	192.168.1.4	DNS	149	Standard query response 0x4f50 No such name SOA seoME1C2E9I7.com SOA a.gtld-servers.net
4524	29.173077	192.168.1.1	192.168.1.4	DNS	162	Standard query response 0x124e No such name SOA KHSc82IrpYYvmA9FljhFljtiy.com SOA a.gtld-se
4527	29.175459	192.168.1.4	192.168.1.1	DNS	93	Standard query 0x5a78 SOA EElSmQkeL9quROinX1vrfPCzVvvNV.com
4528	29.176434	192.168.1.1	192.168.1.4	DNS	165	Standard query response 0x8bf9 No such name SOA r4LCBFUZUIpP6RAj8Rd4HjSD0UAb.com SOA a.gtld
4529	29.191143	192.168.1.1	192.168.1.4	DNS	166	Standard query response 0x5a78 No such name SOA EElSmQkeL9quROinX1vrfPCzVvvNV.com SOA a.gtl
4530	29.191328	192.168.1.4	192.168.1.1	DNS	88	Standard query 0x5c9c SOA Fa7ze5eWyeKBFsl0Zet4QaPP.com
4531	29.193624	192.168.1.1	192.168.1.4	DNS	145	Standard query response 0x1f2a No such name SOA EtVEMmBj.com SOA a.gtld-servers.net
4532	29.203001	192.168.1.1	192.168.1.4	DNS	161	Standard query response 0x5c9c No such name SOA Fa7ze5eWyeKBFsl0Zet4QaPP.com SOA a.gtld-ser
4534	29.208813	192.168.1.4	192.168.1.1	DNS	71	Standard query 0x57df SOA Bbpvlwn.com
4535	29.220730	192.168.1.1	192.168.1.4	DNS	144	Standard query response 0x57df No such name SOA Bbpvlwn.com SOA a.gtld-servers.net
4536	29.222248	192.168.1.1	192.168.1.4	DNS	161	Standard query response 0xc71c No such name SOA G3FnU879bSN3O9fPmfUV57ws.com SOA a.gtld-ser
4537	29.222534	192.168.1.1	192.168.1.4	DNS	164	Standard query response 0x3371 No such name SOA JjS8xZxqOcP0iyTOuXyZmsZt47s.com SOA a.gtld-
4557	29.325680	192.168.1.4	192.168.1.1	DNS	81	Standard query 0xd958 SOA hsZbbkfGoguTAKE2y.com
4558	29.325934	192.168.1.4	192.168.1.1	DNS	88	Standard query 0x3a7c SOA KBIxGnN0ThFqxqEyVWxo3jl9.com
4559	29.341778	192.168.1.4	192.168.1.1	DNS	93	Standard query 0x7dea SOA 5cEzA2NpK87Fg3svKd3uY98snu67y.com
4562	29.400938	192.168.1.1	192.168.1.4	DNS	161	Standard query response 0x3a7c No such name SOA KBIxGnN0ThFqxqEyVWxo3jl9.com SOA a.gtld-ser
4563	29.402760	192.168.1.4	192.168.1.1	DNS	87	Standard query 0x3bd5 SOA LoYaC2iL4Er4MPOIivaeGjH.com
4564	29.409330	192.168.1.1	192.168.1.4	DNS	154	Standard query response 0xd958 No such name SOA hsZbbkfGoguTAKE2y.com SOA a.gtld-servers.ne
4565	29.417562	192.168.1.1	192.168.1.4	DNS	166	Standard query response 0x7dea No such name SOA 5cEzA2NpK87Fg3svKd3uY98snu67y.com SOA a.gtl
4569	29.475282	192.168.1.1	192.168.1.4	DNS	160	Standard query response 0x3bd5 No such name SOA LoYaC2iL4Er4MPOIivaeGjH.com SOA a.gtld-serv
4574	29.508816	192.168.1.4	192.168.1.1	DNS	86	Standard query 0x471c SOA hmllPewnXuxnCzMdWczvYh.com
4575	29.523604	192.168.1.4	192.168.1.1	DNS	65	Standard query 0xd26b SOA A.com
4581	29.579948	192.168.1.1	192.168.1.4	DNS	159	Standard query response 0x471c No such name SOA hmllPewnXuxnCzMdWczvYh.com SOA a.gtld-serve
4586	29.607871	192.168.1.1	192.168.1.4	DNS	138	Standard query response 0xd26b No such name SOA A.com SOA a.gtld-servers.net

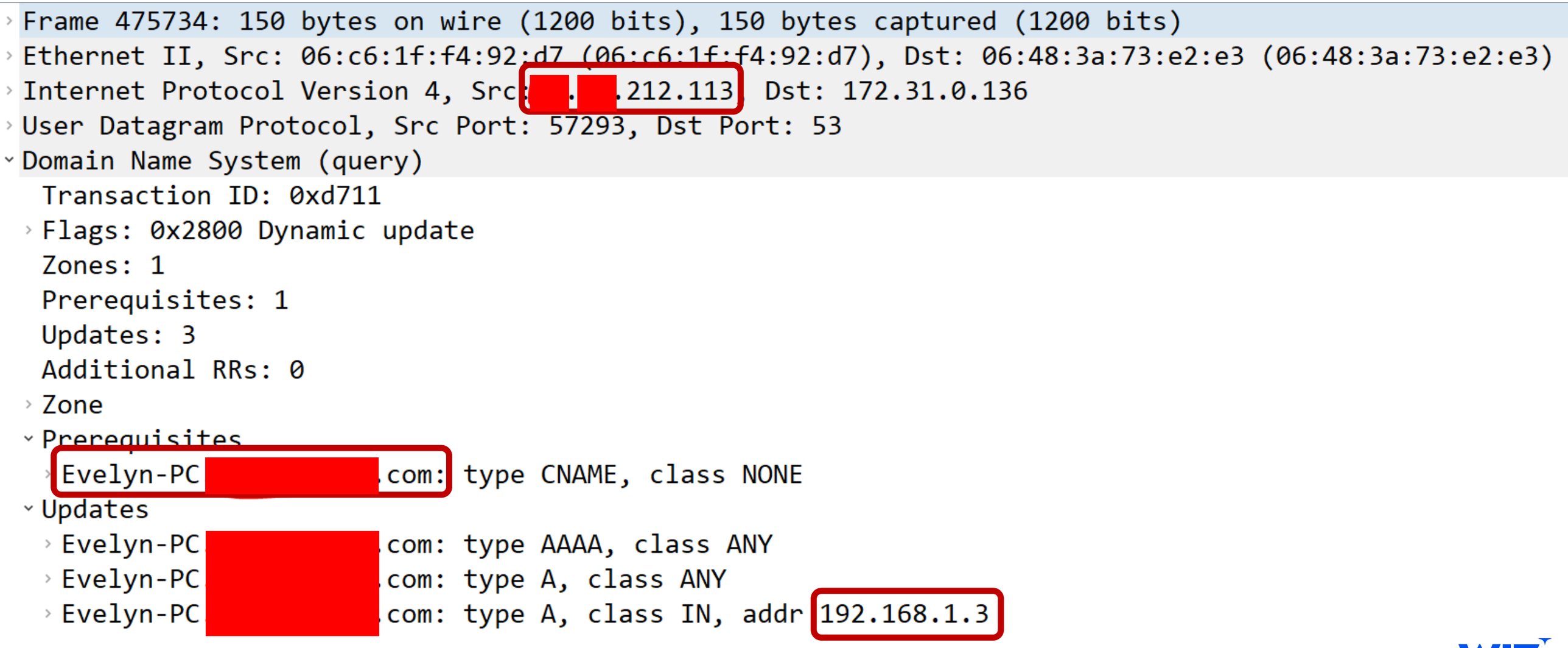
WIZ

Nameserver Hijacking:

Analyzing the Traffic

- Why are we getting any traffic?
- Most of it is Dynamic DNS
- IP addresses
- Computer Names
- Domain names

WIZ


Frame 475734: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
Ethernet II, Src: 06:c6:1f:f4:92:d7 (06:c6:1f:f4:92:d7), Dst: 06:48:3a:73:e2:e3 (06:48:3a:73:e2:e3)
Internet Protocol Version 4, Src: [redacted].212.113, Dst: 172.31.0.136
User Datagram Protocol, Src Port: 57293, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xd711
Flags: 0x2800 Dynamic update
Zones: 1
Prerequisites: 1
Updates: 3
Additional RRs: 0
Zone
Prerequisites
Evelyn-PC [redacted].com: type CNAME, class NONE
Updates
Evelyn-PC [redacted].com: type AAAA, class ANY
Evelyn-PC [redacted].com: type A, class ANY
Evelyn-PC [redacted].com: type A, class IN, addr 192.168.1.3

WIZ

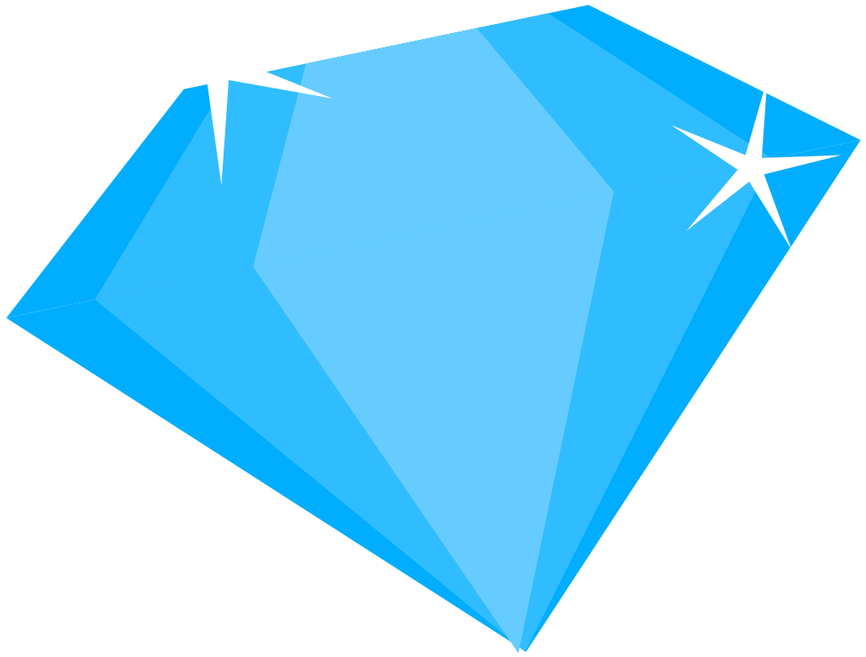
Nameserver Hijacking:

Analyzing the Traffic

- More than one million unique endpoints
- More than 15,000 organizations (Unique FQDN)
- All are AWS Customers

Nameserver Hijacking:

High value targets



- Big companies (Fortune 500)
- 130 government agencies

WIZ

Nameserver Hijacking:

What do we know so far?

- We registered a nameserver domain
- Millions of endpoints started sending dynamic DNS queries to us.

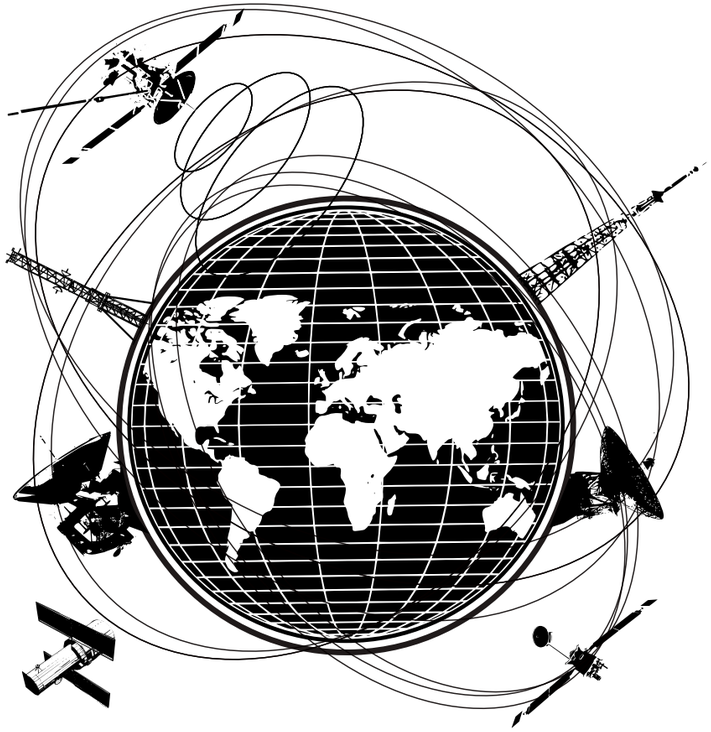
But .. Why?

- Our next step was to dive into the world of Dynamic DNS

Nameserver Hijacking:

Dynamic DNS

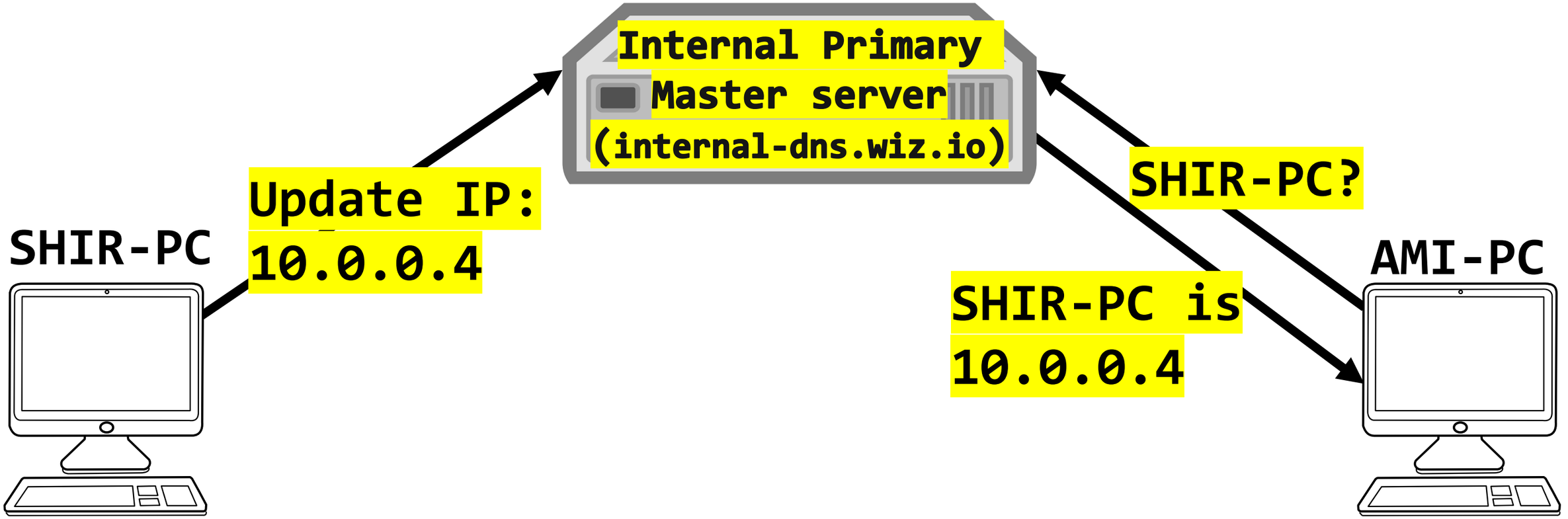
- RFC 2136
- Dynamically updating DNS records
- Common use: Simple way to find IPs in a managed network



WIZ

Nameserver Hijacking:

Dynamic DNS



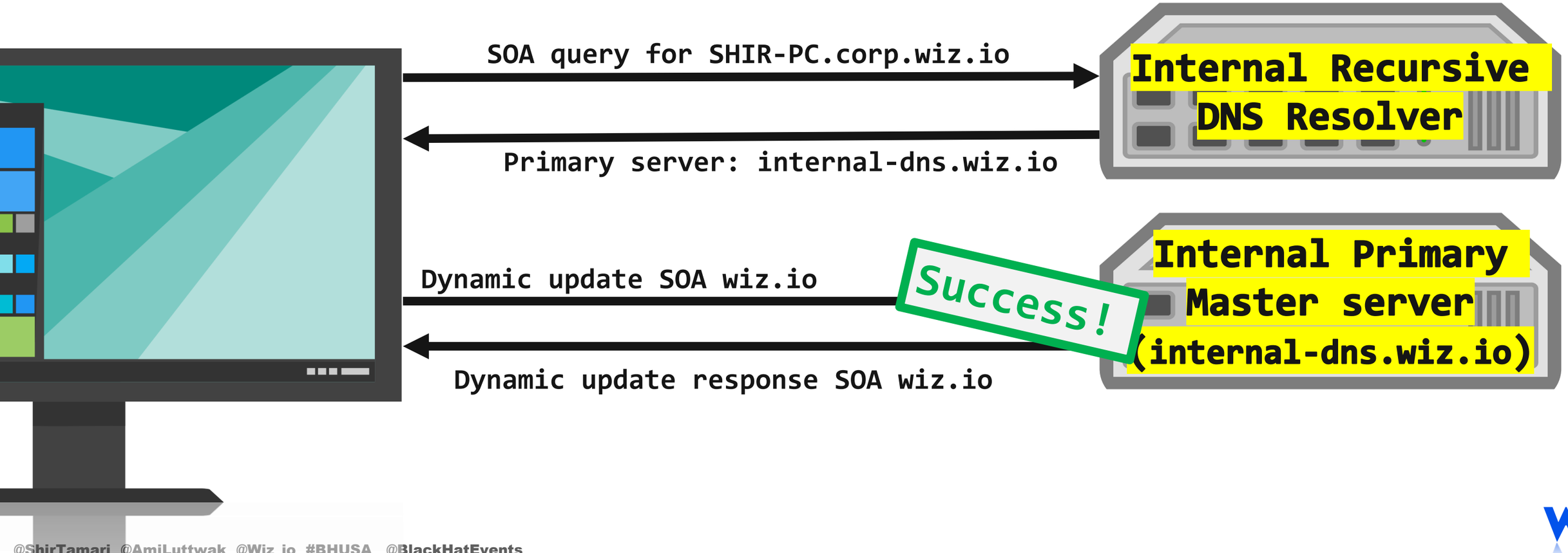
Dynamic DNS:

Finding the Master

- Microsoft has its own algorithm
- It does not work exactly as the RFC defines

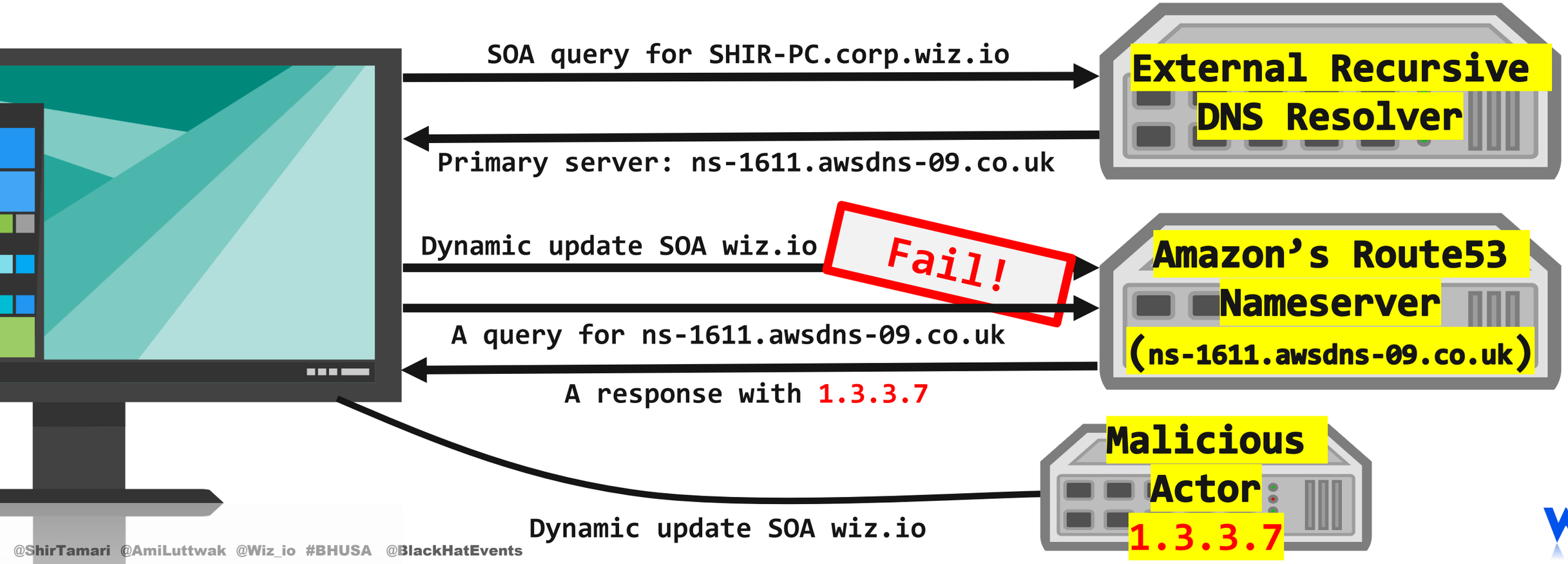
Dynamic DNS:

Finding the Master (Private network)



Dynamic DNS:

Finding the Master (External Network)



WIZ

Dynamic DNS:

So what did we learn so far?

- Windows endpoints use a custom algorithm to find the master DNS
- The algorithm queries the nameserver for its own address
- **The result:** Our malicious DNS server receives Dynamic DNS traffic from millions of endpoints

WIZ

The Risk:

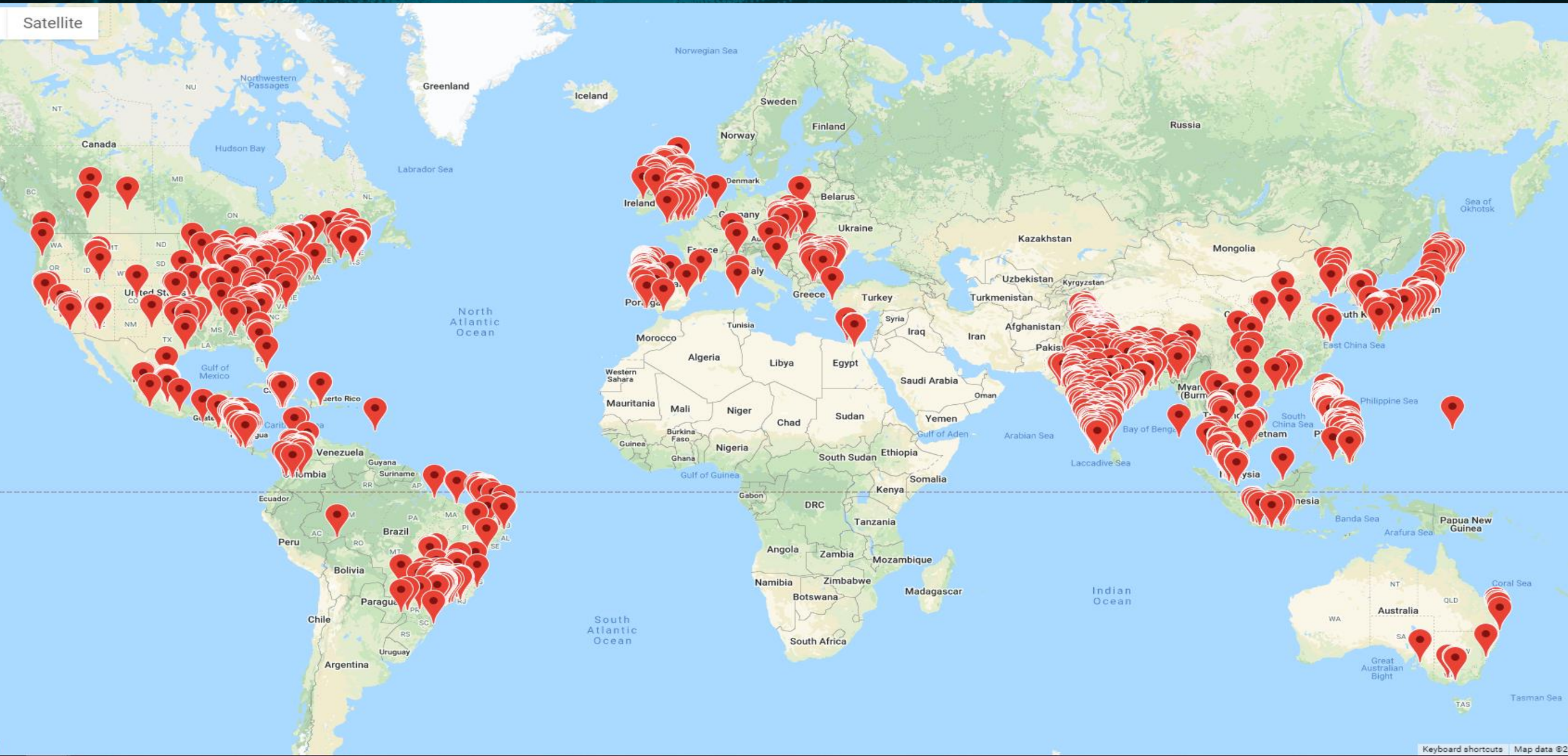
Nation-state intelligence capability

- External IP
- Internal IPs
- Computer names
- **From 15,000 organizations**

The Risk:

IP based Intelligence

- Map companies' sites across the globe


Satellite
Norwegian Sea
Greenland
Iceland
Northwestern Passages
Canada
Hudson Bay
Labrador Sea
Sweden
Finland
Norway
Russia
Ireland
Denmark
Belarus
Ukraine
Kazakhstan
Mongolia
Sea of Okhotsk
Uzbekistan
Kyrgyzstan
Turkmenistan
Greece
Turkey
Syria
Iraq
Iran
Afghanistan
Pakistan
East China Sea
Philippine Sea
South China Sea
Vietnam
Myanmar (Burma)
Bay of Bengal
Arabian Sea
Laccadive Sea
Gulf of Aden
Saudi Arabia
Oman
Yemen
Tunisia
Morocco
Algeria
Libya
Egypt
Western Sahara
Mauritania
Mali
Niger
Chad
Sudan
Burkina Faso
Guinea
Nigeria
Ghana
Gulf of Guinea
South Sudan
Ethiopia
Somalia
Kenya
Gabon
DRC
Tanzania
Angola
Zambia
Mozambique
Namibia
Zimbabwe
Botswana
Madagascar
South Africa
Indian Ocean
North Atlantic Ocean
South Atlantic Ocean
Gulf of Mexico
Puerto Rico
Venezuela
Guyana
Suriname
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Uruguay
Argentina
Banda Sea
Arafura Sea
Papua New Guinea
Coral Sea
Australia
Great Australian Bight
Tasman Sea
Keyboard shortcuts
Map data ©2

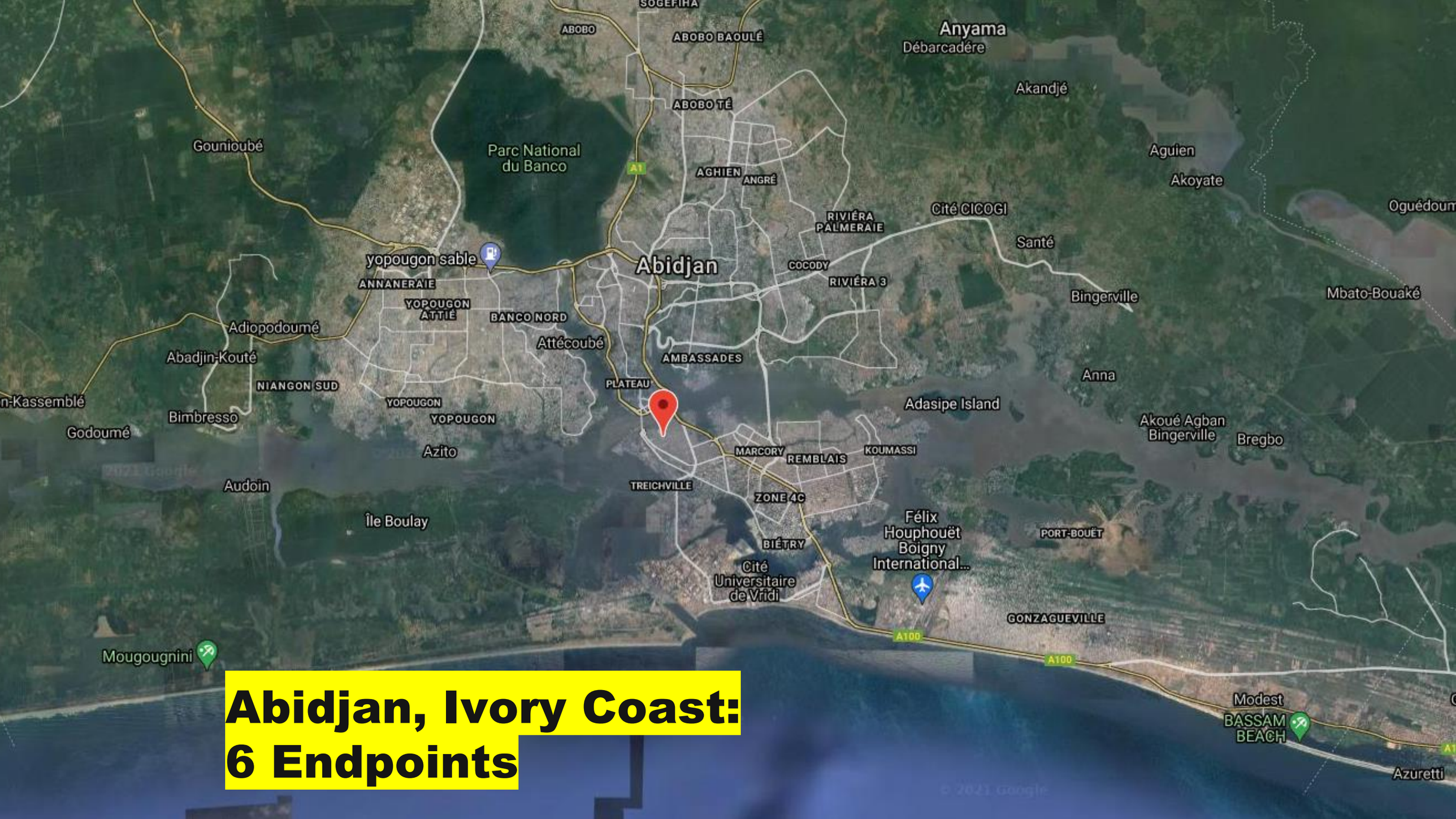
Hyderabad, India: 611 Endpoints

The Risk:

IP based Intelligence

- Companies in violation of OFAC (Office of Foreign Assets Control) sanctions

WIZ



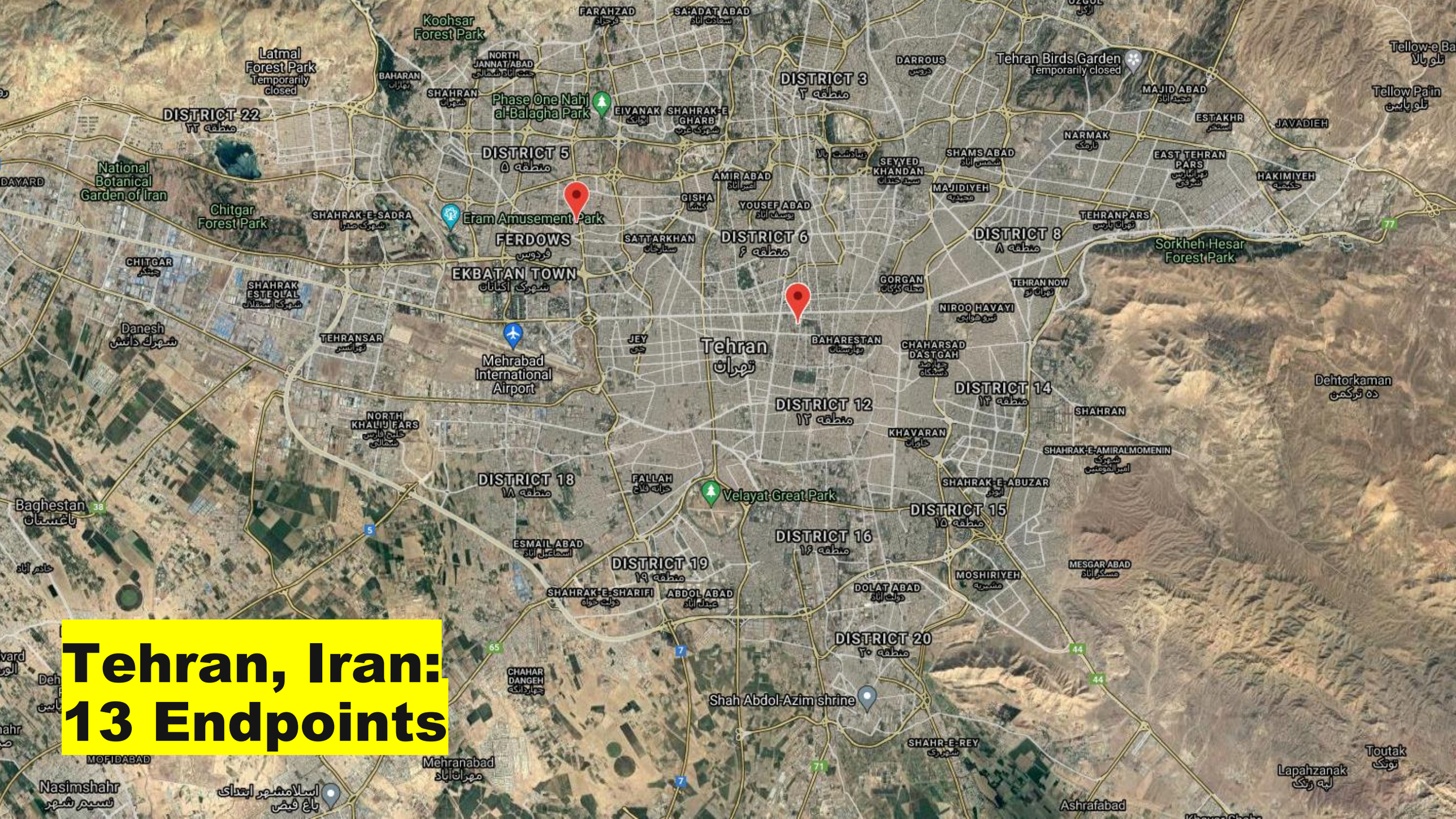
Abidjan, Ivory Coast: 6 Endpoints

The Risk:

IP based Intelligence

- A subsidiary of a large credit union with a branch in Iran

WIZ


Tehran, Iran:
13 Endpoints
Eram Amusement Park
Mehrabad International Airport
Velayat Great Park
Shah Abdol-Azim shrine
Tehran
تهران
DISTRICT 3
DISTRICT 5
DISTRICT 6
DISTRICT 8
DISTRICT 12
DISTRICT 14
DISTRICT 15
DISTRICT 16
DISTRICT 18
DISTRICT 19
DISTRICT 20
DISTRICT 22
FERDOWS
EKBATAN TOWN
Tehran Birds Garden
Temporarily closed
Latmal Forest Park
Temporarily closed
Phase One Nahj al-Balagha Park
Koohsar Forest Park
National Botanical Garden of Iran
Chitgar Forest Park
Sorkheh Hesar Forest Park
Dehtorkaman
Baqhestan
Mehranabad
Nasimshahr
Ashrafabad
Lapahzanak
Toutak

The Risk:

Internal IPs

- Indicate network segments

10.10.*.* - Employee's network

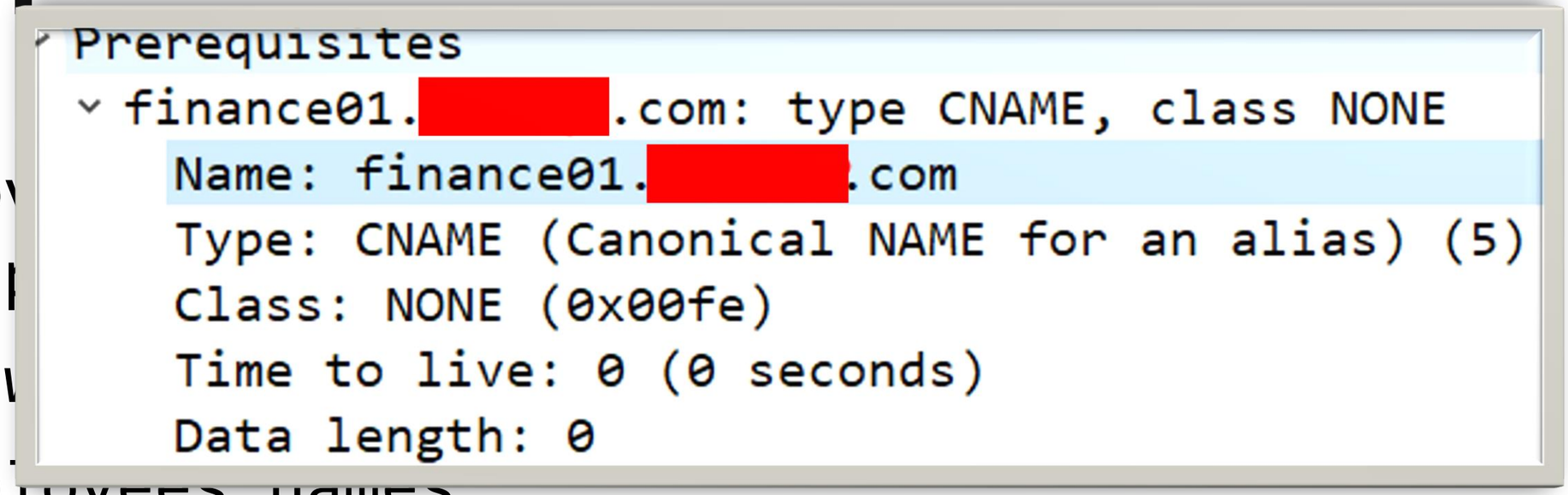
10.10.33.* - CI/CD network

10.100.*.* – Operational network

The Risk:

Computer Names

- Prov
  Endp
- In v
- Employees' names



WIZ

The Risk:

Internal IPv6

- Sometime accessible from the internet!
- 6% expose services such as RDP, SMB, HTTP and many more

```
Updates
> [redacted]35G6.[redacted].com: type AAAA, class ANY
> [redacted]35G6.[redacted].com: type A, class ANY
> [redacted]35G6.[redacted].com: type AAAA, class IN, addr 2601[redacted]be56:3cf6
> [redacted]35G6.[redacted].com: type A, class IN, addr 192.168.0.16
```

The Risk:

Huge Scope

- Cloud providers
- DNS-as-a-Service providers
- Shared hosting
- Domain registrars
- All could be vulnerable to nameserver hijacking

Nameserver Hijacking:

Disclosure

- Amazon AWS – Fixed by 16/02/2021
- Two more cloud providers

  in disclosure process

WIZ

The Fix:

Amazon

- Domain name validation

Error occurred

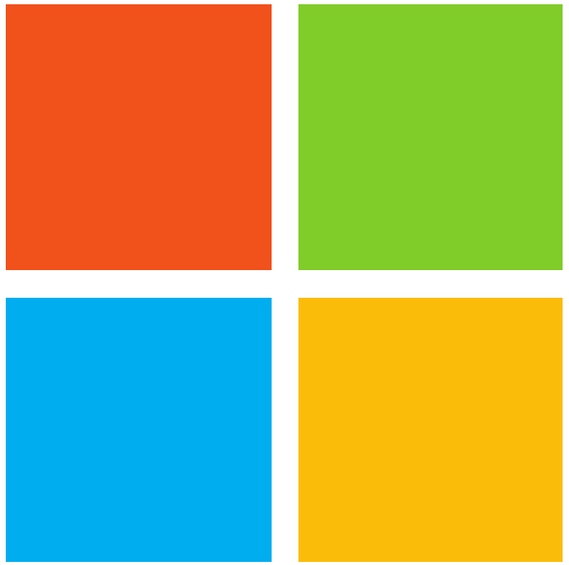
Domain Name contains invalid characters or is in an invalid format.

(InvalidDomainName 400: ns-27.awsdns-03.com is reserved by AWS!)

WIZ

Disclosure:

Microsoft



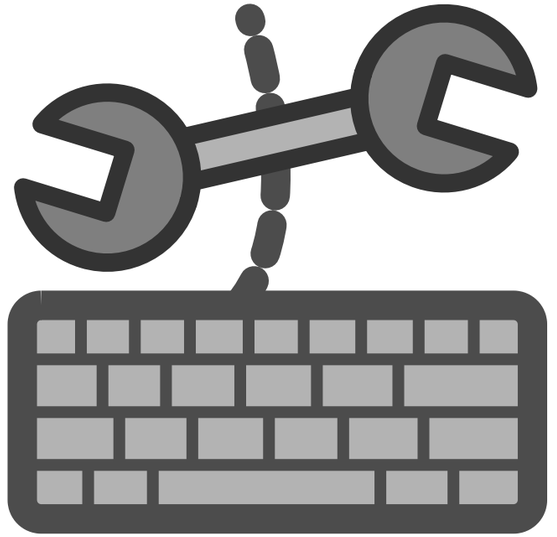
- Not considered a vulnerability
- A known misconfiguration when using external DNS providers

WIZ

Nameserver Hijacking:

Fix it Yourself (Platform)

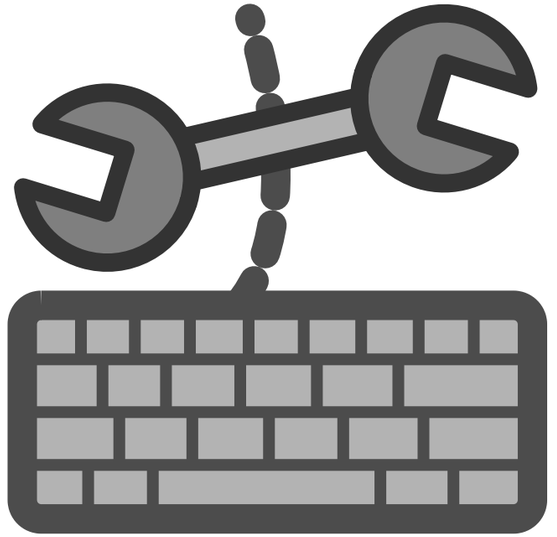
- Domain validation
- Ownership verification
- Follow RFC’s “reserved names”



Dynamic DNS:

Fix it Yourself (Organization)

- Modify the default SOA record

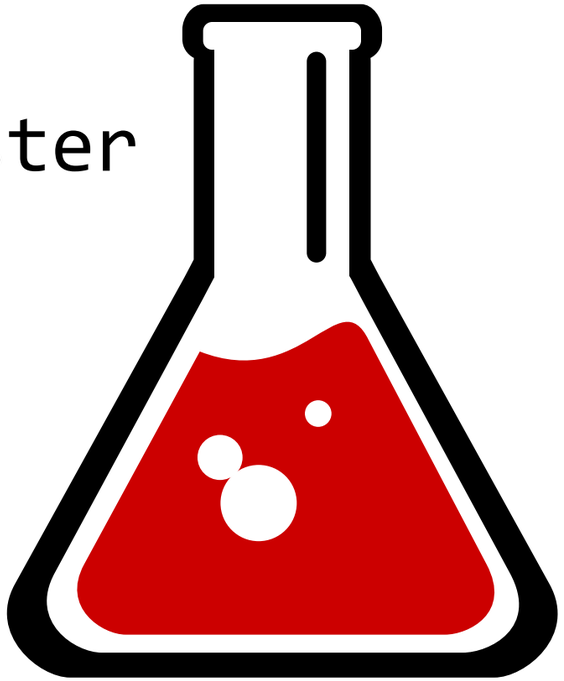


Record name	Type	Value/Route traffic to
wiz.io	NS	ns-1363.awsdns-42.org. ns-1720.awsdns-23.co.uk. ns-779.awsdns-33.net. ns-133.awsdns-16.com.
wiz.io	SOA	invalid.wiz.io. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

Further Research:

Further research

- Many more interesting domains to register
- Dynamically update DNS servers in the wild
- NTLM authentication



Windows 10 (Build 14393) NTLM Negotiation

```
> Queries
v Additional records
  v 3404-ms-7.534-4b4cd65c.7038fa95-b5f7-11eb-5c91-0050569566ec: type TKEY, class ANY
      Name: 3404-ms-7.534-4b4cd65c.7038fa95-b5f7-11eb-5c91-0050569566ec
      Type: TKEY (Transaction Key) (249)
      Class: ANY (0x00ff)
      Time to live: 0 (0 seconds)
      Data length: 66
      Algorithm name: gss-tsig
      Signature Inception: May 30, 2021 21:30:23.000000000 Jerusalem Daylight Time
      Signature Expiration: May 31, 2021 21:30:23.000000000 Jerusalem Daylight Time
      Mode: GSSAPI (3)
      Error: No error (0)
      Key Size: 40
    v Key Data: 4e544c4d535350000100000978208e2000000000000000000000000000000a003938…
      v NTLM Secure Service Provider
          NTLMSSP identifier: NTLMSSP
          NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
        > Negotiate Flags: 0xe2088297, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotia
          Calling workstation domain: NULL
          Calling workstation name: NULL
        > Version 10.0 (Build 14393); NTLM Current Revision 15
```

The Research:

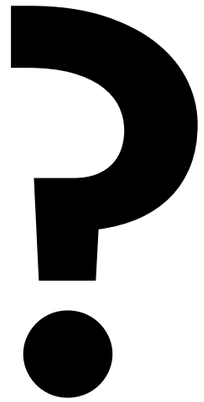
Summary & Takeaways

- We got to nation-state intelligence capabilities from a simple domain registration
- New class of DNS vulnerabilities in DNS-as-a-service
- Huge scope

WIZ

The Research:

Q&A



@AmiLuttwak ami@wiz.io

@ShirTamari shir@wiz.io

WIZ