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
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
Route53: Domain Hijacking

Wiz.io

ns-1334.awsdns-38.org
ns-883.awsdns-46.net
ns-457.awsdns-57.com
ns-1611.awsdns-09.co.uk
## Route53: Domain Hijacking

<table>
<thead>
<tr>
<th>Official AWS DNS Server</th>
<th>Customer’s DNS Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns-1334.awsdns-38.org</td>
<td>wiz.io</td>
</tr>
<tr>
<td></td>
<td>company.com</td>
</tr>
<tr>
<td></td>
<td>company2.com</td>
</tr>
<tr>
<td></td>
<td>company3.com</td>
</tr>
<tr>
<td></td>
<td>wiz.io</td>
</tr>
</tbody>
</table>
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?
Different angle:

Illustration

Official AWS DNS Server

Customer's DNS Zones

<table>
<thead>
<tr>
<th>ns-852.awsdns-42.net</th>
<th>alpha.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns-852.awsdns-42.net</td>
<td>beta.com</td>
</tr>
<tr>
<td>ns-852.awsdns-42.net</td>
<td>gamma.com</td>
</tr>
<tr>
<td>ns-852.awsdns-42.net</td>
<td>delta.com</td>
</tr>
</tbody>
</table>

To view the entire diagram, please refer to the full document.
Nameserver Hijacking:
Analyzing the Traffic

- Why are we getting any traffic?
- Most of it is Dynamic DNS
- IP addresses
- Computer Names
- Domain names
Frame 475734: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
Internet Protocol Version 4, Src: 212.113.12.9, 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.example.com: type CNAME, class NONE
  Updates
    Evelyn-PC.example.com: type AAAA, class ANY
    Evelyn-PC.example.com: type A, class ANY
    Evelyn-PC.example.com: type A, class IN, addr 192.168.1.3
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
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
Nameserver Hijacking:
Dynamic DNS

Internal Primary Master server (internal-dns.wiz.io)

SHIR-PC is 10.0.0.4

Update IP: 10.0.0.4

SHIR-PC?

SHIR-PC

AMI-PC
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)

- SOA query for SHIR-PC.corp.wiz.io
- Primary server: internal-dns.wiz.io
- Dynamic update SOA wiz.io
- Dynamic update response SOA wiz.io
- Success!
Dynamic DNS:
Finding the Master (External Network)

SOA query for SHIR-PC.corp.wiz.io
Primary server: ns-1611.awsdns-09.co.uk
Dynamic update SOA wiz.io
A query for ns-1611.awsdns-09.co.uk
A response with 1.3.3.7

External Recursive
DNS Resolver

Amazon's Route53
Nameserver
(ns-1611.awsdns-09.co.uk)

Fail!

Malicious Actor:
1.3.3.7
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.
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
Hyderabad, India: 611 Endpoints
The Risk:

IP based Intelligence

- Companies in violation of OFAC (Office of Foreign Assets Control) sanctions
Abidjan, Ivory Coast: 6 Endpoints
The Risk:

IP based Intelligence

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

Tehran, Iran: 13 Endpoints
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

• Provide information about the Endpoint
• In what segment is it located
• Employees names
The Risk:

Internal IPv6

• Sometime accessible from the internet!
• 6% expose services such as RDP, SMB, HTTP and many more
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
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!)
Disclosure:

Microsoft

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

<table>
<thead>
<tr>
<th>Record name</th>
<th>Type</th>
<th>Value/Route traffic to</th>
</tr>
</thead>
<tbody>
<tr>
<td>wiz.io</td>
<td>NS</td>
<td>ns-1363.awsdns-42.org.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ns-1720.awsdns-23.co.uk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ns-779.awsdns-33.net.</td>
</tr>
<tr>
<td>wiz.io</td>
<td>SOA</td>
<td>invalid.wiz.io</td>
</tr>
</tbody>
</table>
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
Additional records
- 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 Expiration: May 31, 2021 21:30:23.000000000 Jerusalem Daylight Time
  Mode: GSSAPI (3)
  Error: No error (0)
  Key Size: 40
- Key Data: 4e544c4d535350000100000978208e200000000000000000000000000000000a003938...

NTLM Secure Service Provider
- NTLMSSP identifier: NTLMSSP
- NTLM Message Type: NTLMSSP_NEGOTIATE (0x00000001)
- Negotiate Flags: 0xe2088297, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate 256
- 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
The Research:

Q&A

@AmiLuttwak  ami@wiz.io
@ShirTamari  shir@wiz.io