

DNS As An Early Warning System

Practical DNS Telemetry For Early Threat Detection and Response

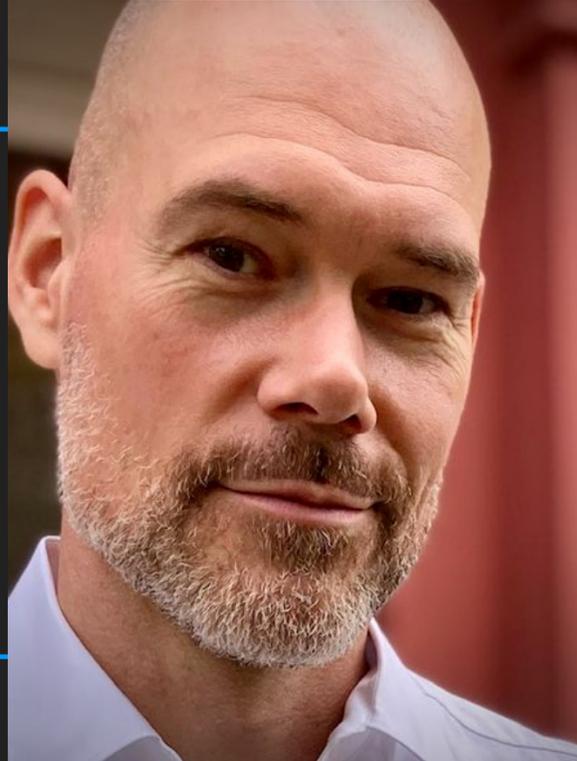


Andreas Taudte
Senior Technical Marketing Manager



March 2026

Speaker



Andreas Taudte

Senior Technical Marketing Manager

- 15+ years in DDI across enterprise and public-sector environments
- Delivered architectures, migrations, workshops, and governance models
- Turning complex DDI topics into clear, decision-ready guidance
- Connecting practitioners through the DDI User Group



ataudte



ataudte



ataudte



ataudte

Agenda



- 1. Where DNS Becomes A Security Signal**
- 2. Real-Life Signals In DNS Traffic**
- 3. From DNS Signals To Detection And Validation**

Where DNS Becomes A Security Signal

DNS – The Ignored Component

- DNS is foundational but rarely monitored
- Most security tools lack DNS specific visibility
- Logs alone do not create visibility



What Hides In DNS Traffic

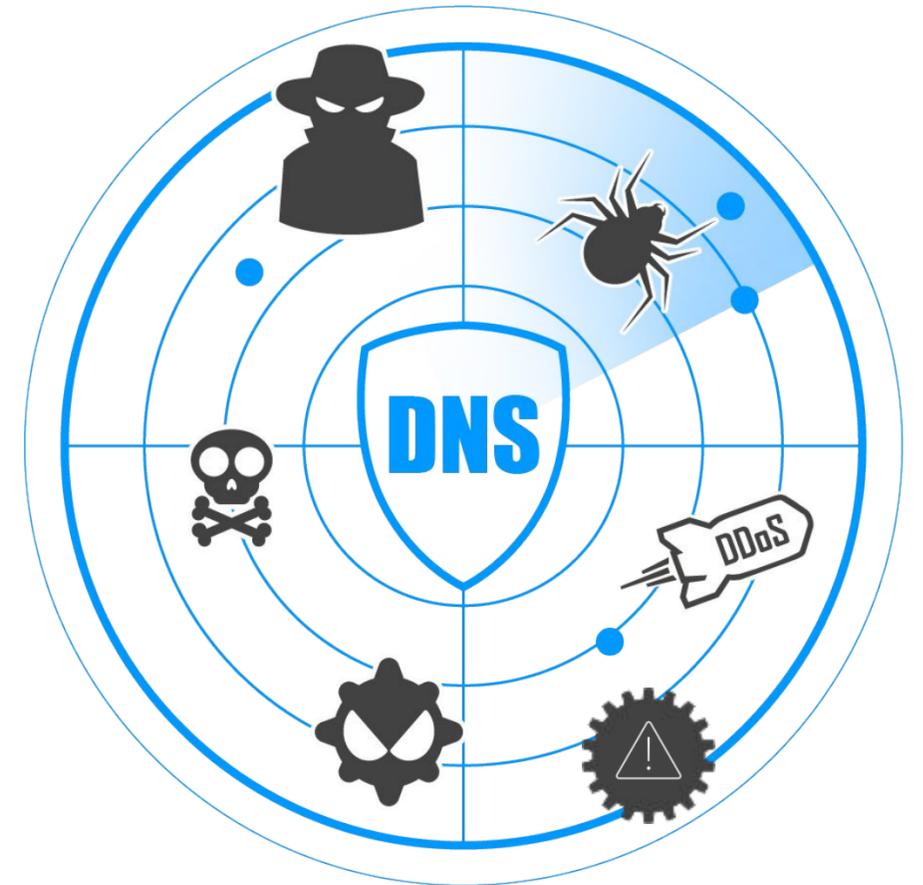
- Active threats (exfiltration, C&C, DGA, tunneling, phishing, etc.)
- Early warning signals (reconnaissance, staging, pre-positioning, DGA ramp-up, etc.)
- Volume attacks and stress patterns (floods, spikes, etc.)
- Operational issues (misconfigurations, malfunctions, abnormality, etc.)
- External dependency issues (routing, peering, cloud outages)



Indicators Of Abuse In DNS

- Algorithmically generated domain names
- Oversized labels and deeply nested subdomains
- Spikes in non-existent domain (`NXDOMAIN*`) responses
- Unusual record types
- Query patterns and query volume

* WPAD, search list, localhost, TTL issues, etc.



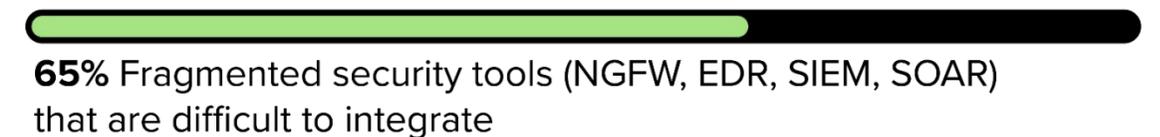
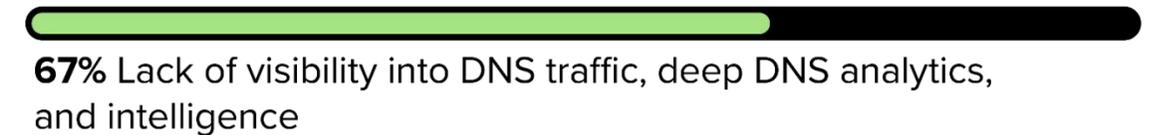
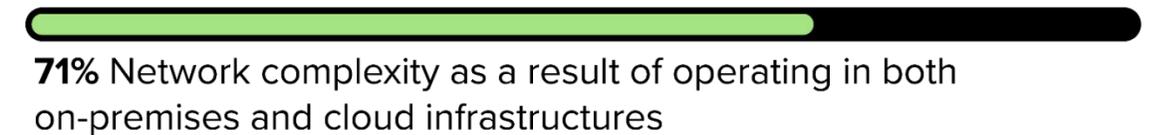
DNS provides early indicators, but not every anomaly is malicious.

The Visibility Gap

- Mixed DNS vendors and servers
- Fragmented visibility
- Inconsistent logs
- Too much DNS data
- Limited skills and staffing

“How challenging are each of the following to your security teams to effectively defend and protect your network?”

(Showing “Highly challenging” and “Challenging”)

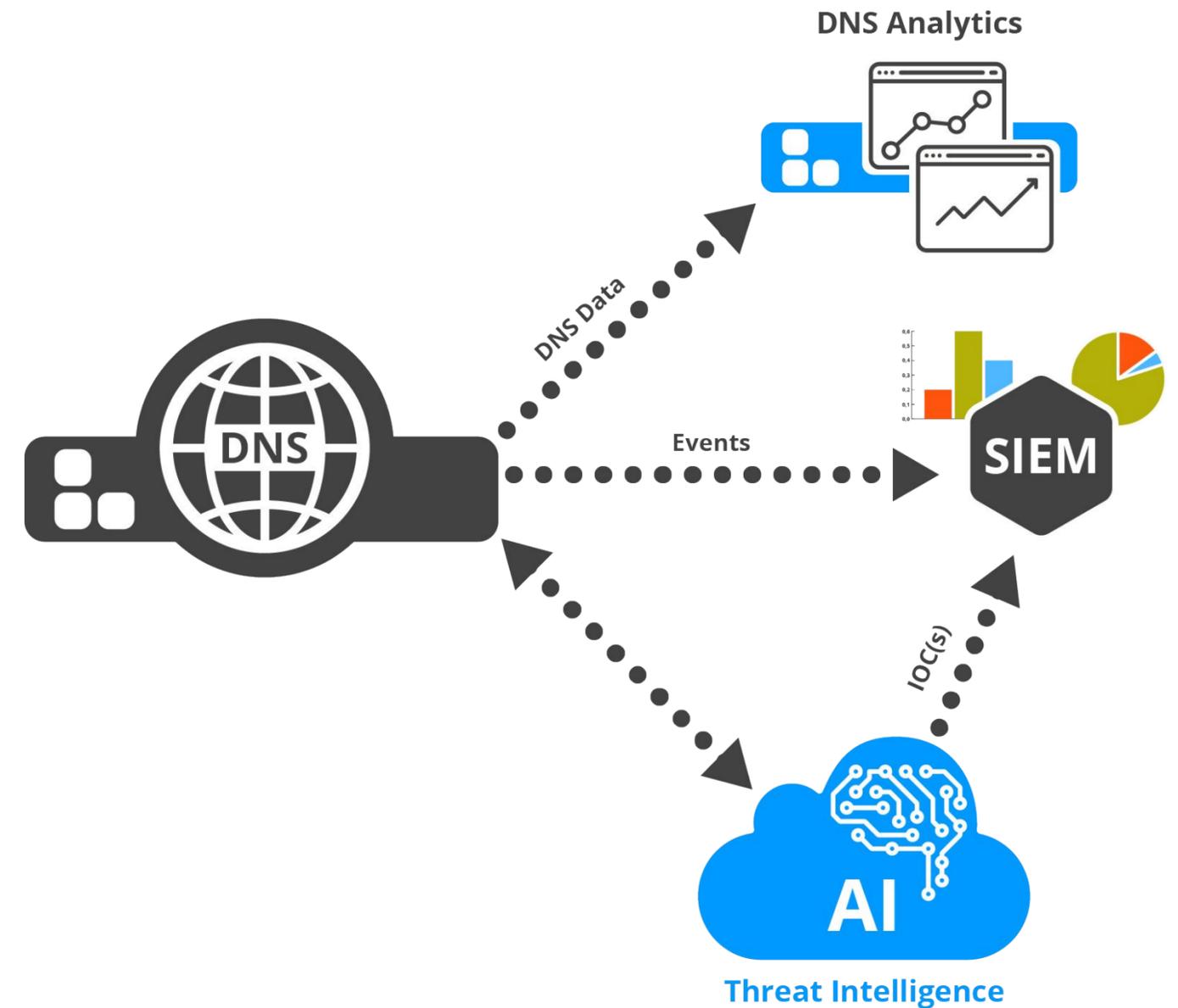


Source: [Forrester 2025 Study on DNS Security in a Cloud Era](#)

Base: 218 decision-makers with responsibility for their organization's security and threat intelligence strategy
Source: Forrester's Q2 2025 DNS Security Survey [E-62853]

From Logging To Response

- Detection ≠ defense
- DNS signals enable visibility for decisions
- Signals must trigger investigation



Real-Life Signals In DNS Traffic

Algorithmic Domain Names

- High entropy labels
- No linguistic structure
- Repetitive querying of non-existent names



Demo: DGA & N-gram



My Guideflow

```
~/ddi-scripts — -sh — 118x31  
[myPro:ddi-scripts andreas$ ./dns_dga-demo.sh ]
```

DGA Demo

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_dga-demo.sh
#
timestamp      domain          status
#
20260225-102903 b2xp9cciihw.net NXDOMAIN
20260225-102903 j1nfd6ltth1q.com REGISTERED
20260225-102903 9uqub38urhdc.com NXDOMAIN
#
20260225-112903 9c868daylc6t.net REGISTERED
20260225-112903 2pmpnda5tbvv.org NXDOMAIN
20260225-112903 c0o22hhnm1hi.org NXDOMAIN
#
20260225-122903 pcksbuavjejz.de NXDOMAIN
20260225-122903 pkb7a5m2do7s.net REGISTERED
20260225-122903 x2sbmgq4z3m5.com NXDOMAIN
#
20260225-132903 a8se4k63k62f.com REGISTERED
20260225-132903 xgc91zc5od60.com NXDOMAIN
20260225-132903 ytdx6vicm4p1.de NXDOMAIN
#
20260225-142903 vmi45940p5cb.org NXDOMAIN
20260225-142903 i62vyc5fc8rb.de NXDOMAIN
20260225-142903 n6n8sekc335p.com REGISTERED
#
myPro:ddi-scripts andreas$
```

inactive

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_dga-demo.sh ]
#
timestamp      domain          status
#
20260225-102903 b2xp9cciijhw.net NXDOMAIN
20260225-102903 j1nfd6ltth1q.com REGISTERED
20260225-102903 9uqub38urhdc.com NXDOMAIN
#
20260225-112903 9c868daylc6t.net REGISTERED
20260225-112903 2pmpnda5tbvv.org NXDOMAIN
20260225-112903 c0o22hhnm1hi.org NXDOMAIN
#
20260225-122903 pcksbuavjejz.de NXDOMAIN
20260225-122903 pkb7a5m2do7s.net REGISTERED
20260225-122903 x2sbmgq4z3m5.com NXDOMAIN
#
20260225-132903 a8se4k63k62f.com REGISTERED
20260225-132903 xgc91zc5od60.com NXDOMAIN
20260225-132903 ytdx6vicm4p1.de NXDOMAIN
#
20260225-142903 vmi45940p5cb.org NXDOMAIN
20260225-142903 i62vyc5fc8rb.de NXDOMAIN
20260225-142903 n6n8sekc335p.com REGISTERED
#
myPro:ddi-scripts andreas$
```

active

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_dga-demo.sh ]
#
timestamp      domain          status
#
20260225-102903 b2xp0ccijhw.net NXDOMAIN
20260225-102903 ojlh1q.com      REGISTERED
20260225-102903 9uqub3arhdc.com NXDOMAIN
#
20260225-112903 9c868daylc6t.net REGISTERED
20260225-112903 2pmpnda5tbvv.org NXDOMAIN
20260225-112903 c0o22hhnm1hi.org NXDOMAIN
#
20260225-122903 pcksbuavjejz.de NXDOMAIN
20260225-122903 pkb7a5m2do7s.net REGISTERED
20260225-122903 x2sbmgq4z3m5.com NXDOMAIN
#
20260225-132903 a8se4k63k62f.com REGISTERED
20260225-132903 xgc91zc5od60.com NXDOMAIN
20260225-132903 ytdx6vicm4p1.de NXDOMAIN
#
20260225-142903 vmi45940p5cb.org NXDOMAIN
20260225-142903 i62vyc5fc8rb.de NXDOMAIN
20260225-142903 n6n8sekc335p.com REGISTERED
#
myPro:ddi-scripts andreas$ █
```

10:29

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_dga-demo.sh ]
#
timestamp      domain          status
#
20260225-102903 b2xp9cciijh.net NXDOMAIN
20260225-102903 j1nfd6ltth1q.com REGISTERED
20260225-102903 9uqub38urhdc.com NXDOMAIN
#
20260225-112903 9c0111:29 c6t.net REGISTERED
20260225-112903 2pmpn0a3cbvv.org NXDOMAIN
20260225-112903 c0o22hhnm1hi.org NXDOMAIN
#
20260225-122903 pcksbuavjejz.de NXDOMAIN
20260225-122903 pkb7a5m2do7s.net REGISTERED
20260225-122903 x2sbmgq4z3m5.com NXDOMAIN
#
20260225-132903 a8se4k63k62f.com REGISTERED
20260225-132903 xgc91zc5od60.com NXDOMAIN
20260225-132903 ytdx6vicm4p1.de NXDOMAIN
#
20260225-142903 vmi45940p5cb.org NXDOMAIN
20260225-142903 i62vyc5fc8rb.de NXDOMAIN
20260225-142903 n6n8sekc335p.com REGISTERED
#
myPro:ddi-scripts andreas$ █
```

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_dga-demo.sh ]
#
timestamp      domain          status
#
20260225-102903 b2xp9cciijh.net NXDOMAIN
20260225-102903 j1nfd6ltth1q.com REGISTERED
20260225-102903 9uqub38urhdc.com NXDOMAIN
#
20260225-112903 9c868daylc6t.net REGISTERED
20260225-112903 2pmpnda5tbvv.org NXDOMAIN
20260225-112903 c0o22hhnm1hi.org NXDOMAIN
#
20260225-122903 pcksbuavjejz.de NXDOMAIN
20260225-122903 pkb7a5m2do7s.net REGISTERED
20260225-122903 x2sbmgq4z3m5.com NXDOMAIN
#
20260225-132903 a8se4k63k62f.com REGISTERED
20260225-132903 xgc91zc5od60.com NXDOMAIN
20260225-132903 ytdx6vicm4p1.de NXDOMAIN
#
20260225-142903 vmi45940p5cb.org NXDOMAIN
20260225-142903 i62vyc5fc8rb.de NXDOMAIN
20260225-142903 n6n8sekc335p.com REGISTERED
#
myPro:ddi-scripts andreas$
```

high entropy

My Guideflow

```
~/ddi-scripts — -sh — 118x31  
[myPro:ddi-scripts andreas$ ./dns_n-gram.sh n6n8sekc335p n-gram ]
```

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_n-gram.sh n6n8sekc335p ]
n6n - not a valid word in English
6n8 - not a valid word in English
n8s - not a valid word in English
8se - not a valid word in English
sek - not a valid word in English
ekc - not a valid word in English
kc3 - not a valid word in English
c33 - not a valid word in English
335 - not a valid word in English
35p - not a valid word in English
n6 - not a valid word in English
6n - not a valid word in English
n8 - not a valid word in English
8s - not a valid word in English
se - valid word in English
ek - not a valid word in English
kc - not a valid word in English
c3 - not a valid word in English
33 - not a valid word in English
35 - not a valid word in English
5p - not a valid word in English
'n6n8sekc335p' is 4.00% an English word (according to /usr/share/dict/words)
myPro:ddi-scripts andreas$
```

4%

My Guideflow

```
~/ddi-scripts — -sh — 118x31  
myPro:ddi-scripts andreas$ ./dns_n-gram.sh firefighter n-gram
```

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_n-gram.sh firefighter ]
fir - valid word in English
ire - valid word in English
ref - valid word in English
efi - not a valid word in English
fig - valid word in English
igh - not a valid word in English
ght - not a valid word in English
hte - not a valid word in English
ter - not a valid word in English
fi - valid word in English
ir - common prefix/suffix in English
re - valid word in English
ef - not a valid word in English
fi - valid word in English
ig - not a valid word in English
gh - not a valid word in English
ht - not a valid word in English
te - valid word in English
er - valid word in English
'firefighter' is 47.00% an English word (according to /usr/share/dict/words)
myPro:ddi-scripts andreas$
```

Deceptive But Valid Domains

- Visually identical names
- Unexpected punycode
- Legitimate resolution



Demo: Look-a-like



My Guideflow

```
~/ddi-scripts — -sh — 118x31  
myPro:ddi-scripts andreas$ ./dns_look-a-like.sh guug.de
```

look-a-like

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_look-a-like.sh guug.de ]
----
original: guug.de
punycode: guug.de
----
modified: guug.de
punycode: guug.xn--d-jtb
----
modified: ġuug̃.de
punycode: xn--uu-wnac.de
----
modified: gùùg.de
punycode: xn--gg-okaa.de
----
myPro:ddi-scripts andreas$
```

original

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_look-a-like.sh guug.de ]
----
original: guug.de
punycode: guug.de
----
modified: guug.de
punycode: guug.xn--d-jv
----
modified: ġuug.de
punycode: xn--uu-wnac.de
----
modified: gùùg.de
punycode: xn--gg-okaa.de
----
myPro:ddi-scripts andreas$
```

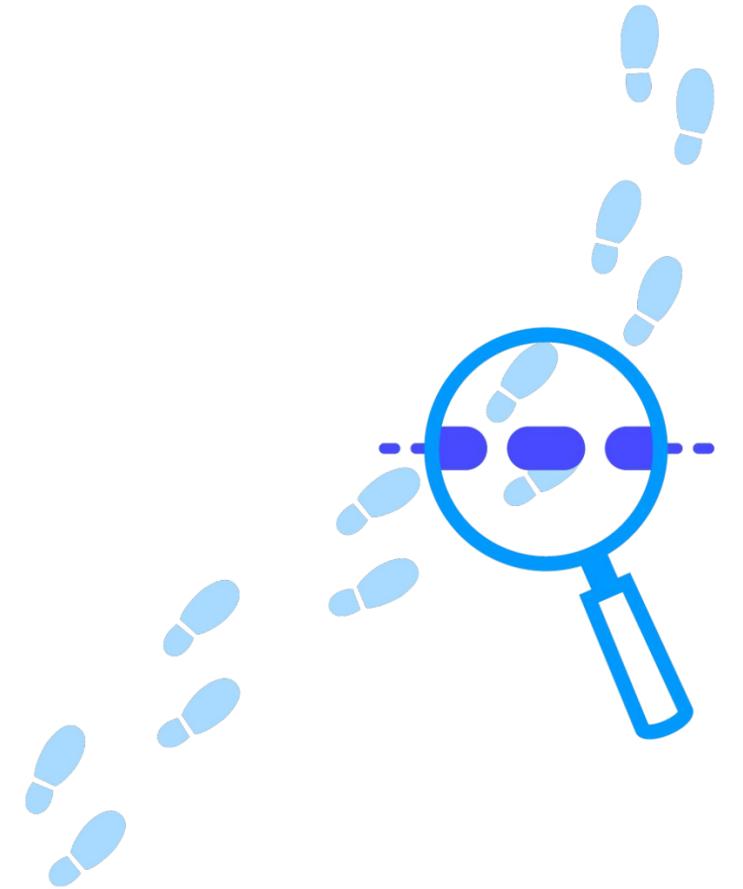
modified

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ ./dns_look-a-like.sh guug.de ]
----
original: guug.de
punycode: guug.de
----
modified: guug.de
punycode: guug.xn--d-jtb
----
modified: ğuug.de
punycode: xn--uu-wnac.de
----
modified: gùùg.de
punycode: xn--gg-okaa.de
----
myPro:ddi-scripts andreas$
```

punycode

Blending Into DNS Noise

- Random-looking hostnames under real zones
- Persistent NXDOMAIN noise
- Deliberately distributed, low-and-slow patterns



Demo: DNS Straying



My Guideflow

```
~/ddi-scripts — -sh — 118x31  
[myPro:ddi-scripts andreas$ ./dns_straying.sh guug.de ]
```

DNS Straying

```
My Guideflow
~/ddi-scripts — dns_straying.sh guug.de — 118x31
[myPro:ddi-scripts andreas$ ./dns_straying.sh guug.de ]
Zone:      guug.de
NS names:  ns2.guug.de ns1.linuxtag.net ns2.dnspartner.de
NS addr:   178.33.39.66 2001:41d0:304:200::c92a 2a01:198:12::a 2a01:410:140:54e4::2 46.4.78.167 91.184.37.10

Generated FQDNs:
 xefve8ucga9i301y.guug.de
 ashe52foa14eui73.guug.de
 jf43tyvohle7et8z.guug.de
 ejyjk51t8wr6doip.guug.de
 6nlt5c7znpc0fd8l.guug.de
 3vraqjdp0gi9236j.guug.de
 d371hxrj07z05axi.guug.de
 918asd7eq6gahrpa.guug.de
 sspmwnn42mru8fe.guug.de
 c5010o5269l1cky0.guug.de
 41i90spgkm4p1a07.guug.de
 7oyxcyv7msanskta.guug.de
 otsra0r9s2dmhyx2.guug.de
 zcrnprcbjhdjt0.guug.de
 cuam0fwh4lzko7tb.guug.de
 7fujgpmmitg6bvm5.guug.de

Send 16 DNS queries to 6 servers? [Y/n]: █
```

servers to use

```
My Guideflow
~/ddi-scripts — dns_straying.sh guug.de — 118x31
[myPro:ddi-scripts andreas$ ./dns_straying.sh guug.de ]
Zone:      guug.de
NS names:  ns2.guug.de ns1.linuxtag.net ns2.dnspartner.de
NS addrs:  178.33.39.66 2001:41d0:304:200::c92a 2a01:198:12::a 2a01:4f8:140:54e4::2 46.4.78.167 91.184.37.10

Generated FQDNs: (data breach)
xefve8ucga9i301y.guug.de
ashe52foa14eui73.guug.de
jf43tyvohle7et8z.guug.de
ejyjk51t8wr6doip.guug.de
6nlt5c7znpc0fd8l.guug.de
3vraqjdp0gi9236j.guug.de
d371hxrj07z05axi.guug.de
918asd7eq6gahrpa.guug.de
sspmwnn42mru8fe.guug.de
c5010o5269l1cky0.guug.de
41i90spgkm4p1a07.guug.de
7oyxcyv7msanskta.guug.de
otsra0r9s2dmhyx2.guug.de
zcrnprcbjhdjt0.guug.de
cuam0fwh4lzko7tb.guug.de
7fujgpmmitg6bvm5.guug.de

Send 16 DNS queries to 6 servers? [Y/n]:
```

```
My Guideflow

~/ddi-scripts — -sh — 118x31

c5010o526911cky0.guug.de
41i90spgkm4p1a07.guug.de
7oyxcyv7msanskta.guug.de
otsra0r9s2dmhyx2.guug.de
zcrnprcbjhdjtt0.guug.de
cuam0fwh4lzko7tb.guug.de
7fujgpmmitg6bvm5.guug.de

Send 16 DNS queries to 6 servers? [Y/n]: Y

Sending queries...
xefve8ucga9i30ly.guug.de with 0.50s delay to 2a01:4f8:140:54e4::2
ashe52foa14eui73.guug.de with 1.25s delay to 91.184.37.10
jf43tyvohle7et8z.guug.de with 1.25s delay to 46.4.78.167
ejyjk51t8wr6doip.guug.de with 2.00s delay to 2a01:4f8:140:54e4::2
6nlt5c7znpc0fd8l.guug.de with 0.50s delay to 91.184.37.10
3vraqjdp0gi9236j.guug.de with 1.25s delay to 46.4.78.167
d371hxrj07z05axi.guug.de with 0.75s delay to 2a01:4f8:140:54e4::2
918asd7eq6gahrpa.guug.de with 0.75s delay to 2001:41d0:304:200::c92a
sspmwnn42mru8fe.guug.de with 1.50s delay to 91.184.37.10
c5010o526911cky0.guug.de with 2.00s delay to 2a01:198:12::a
41i90spgkm4p1a07.guug.de with 0.75s delay to 91.184.37.10
7oyxcyv7msanskta.guug.de with 0.75s delay to 91.184.37.10
otsra0r9s2dmhyx2.guug.de with 1.00s delay to 2001:41d0:304:200::c92a
zcrnprcbjhdjtt0.guug.de with 1.25s delay to 46.4.78.167
cuam0fwh4lzko7tb.guug.de with 1.25s delay to 91.184.37.10
7fujgpmmitg6bvm5.guug.de with 0.50s delay to 2001:41d0:304:200::c92a

Done.

myPro:ddi-scripts andreas$
```

0.50s delay

```
My Guideflow

~/ddi-scripts — -sh — 118x31

c5010o526911cky0.guug.de
41i90spgkm4p1a07.guug.de
7oyxcyv7msanskta.guug.de
otsra0r9s2dmhyx2.guug.de
zcrnprcbjhdjtt0.guug.de
cuam0fwh4lzko7tb.guug.de
7fujgpmmitg6bvm5.guug.de

Send 16 DNS queries to 6 servers? [Y/n]: Y

Sending queries...
xefve8ucga9i30ly.guug.de with 0.50s delay to 2a01:4f8:140:54e4::2
ashe52foa14eui73.guug.de with 1.25s delay to 91.184.37.10
jf43tyvohle7et8z.guug.de with 1.25s delay to 46.4.78.167
ejyjk51t8wr6doip.guug.de with 2.00s delay to 2a01:4f8:140:54e4::2
6nlt5c7znpc0fd8l.guug.de with 0.50s delay to 91.184.37.10
3vraqjdp0gi9236j.guug.de with 1.25s delay to 46.4.78.167
d371hxrj07z05axi.guug.de with 0.75s delay to 2a01:4f8:140:54e4::2
918asd7eq6gahrpa.guug.de with 0.75s delay to 2001:41d0:304:200::c92a
sspmwnn42mru8fe.guug.de with 1.50s delay to 91.184.37.10
c5010o526911cky0.guug.de with 2.00s delay to 2a01:198:12::a
41i90spgkm4p1a07.guug.de with 0.75s delay to 91.184.37.10
7oyxcyv7msanskta.guug.de with 0.75s delay to 91.184.37.10
otsra0r9s2dmhyx2.guug.de with 1.00s delay to 2001:41d0:304:200::c92a
zcrnprcbjhdjtt0.guug.de with 1.25s delay to 46.4.78.167
cuam0fwh4lzko7tb.guug.de with 1.25s delay to 91.184.37.10
7fujgpmmitg6bvm5.guug.de with 0.50s delay to 2001:41d0:304:200::c92a

Done.

myPro:ddi-scripts andreas$
```

first server used

```
My Guideflow

~/ddi-scripts — -sh — 118x31

c5010o526911cky0.guug.de
41i90spgkm4p1a07.guug.de
7oyxcyv7msanskta.guug.de
otsra0r9s2dmhyx2.guug.de
zcrnprcbjhdjtt0.guug.de
cuam0fwh4lzko7tb.guug.de
7fujgpmmitg6bvm5.guug.de

Send 16 DNS queries to 6 servers? [Y/n]: Y

Sending queries...
xefve8ucga9i30ly.guug.de with 0.50s delay to 2a01:4f8:140:54e4::2
ashe52foa14eui73.guug.de with 1.25s delay to 91.184.37.10
jf43tyvohle7et8z.guug.de with 1.25s delay to 46.4.78.167
ejyjk51t8wr6doip.guug.de with 2.00s delay to 2a01:4f8:140:54e4::2
6nlt5c7znp0fd8l.guug.de with 0.50s delay to 91.184.37.10
3vraqjdp0gi9236j.guug.de with 1.25s delay to 46.4.78.167
d371hxrj07z05axi.guug.de with 0.75s delay to 2a01:4f8:140:54e4::2
918asd7eq6gahrpa.guug.de with 0.75s delay to 2001:41d0:304:200::c92a
sspmwnn42mru8fe.guug.de with 1.50s delay to 91.184.37.10
c5010o526911cky0.guug.de with 2.00s delay to 2a01:198:12::a
41i90spgkm4p1a07.guug.de with 0.75s delay to 91.184.37.10
7oyxcyv7msanskta.guug.de with 0.75s delay to 91.184.37.10
otsra0r9s2dmhyx2.guug.de with 1.00s delay to 2001:41d0:304:200::c92a
zcrnprcbjhdjtt0.guug.de with 1.25s delay to 46.4.78.167
cuam0fwh4lzko7tb.guug.de with 1.25s delay to 91.184.37.10
7fujgpmmitg6bvm5.guug.de with 0.50s delay to 2001:41d0:304:200::c92a

Done.

myPro:ddi-scripts andreas$
```

1.25s later

```
My Guideflow
~/ddi-scripts — -sh — 118x31

c5010o526911cky0.guug.de
41i90spgkm4p1a07.guug.de
7oyxcyv7msanskta.guug.de
otsra0r9s2dmhyx2.guug.de
zcrnprcbjhdjtt0.guug.de
cuam0fwh4lzko7tb.guug.de
7fujgpmmitg6bvm5.guug.de

Send 16 DNS queries to 6 servers? [Y/n]: Y

Sending queries...
xefve8ucga9i30ly.guug.de with 0.50s delay to 2a01:4f8:140:54e4::2
ashe52foa14eui73.guug.de with 1.25s delay to 91.184.37.10
jf43tyvohle7et8z.guug.de with 1.25s delay to 46.4.78.167
ejyjk51t8wr6doip.guug.de with 2.00s delay to 2a01:4f8:140:54e4::2
6nlt5c7znpc0fd8l.guug.de with 0.50s delay to 91.184.37.10
3vraqjdp0gi9236j.guug.de with 1.25s delay to 46.4.78.167
d371hxrj07z05axi.guug.de with 0.75s delay to 2a01:4f8:140:54e4::2
918asd7eq6gahrpa.guug.de with 0.75s delay to 2001:41d0:304:200::c92a
sspmwnn42mru8fe.guug.de with 1.50s delay to 91.184.37.10
c5010o526911cky0.guug.de with 2.00s delay to 2a01:198:12::a
41i90spgkm4p1a07.guug.de with 0.75s delay to 91.184.37.10
7oyxcyv7msanskta.guug.de with 0.75s delay to 91.184.37.10
otsra0r9s2dmhyx2.guug.de with 1.00s delay to 2001:41d0:304:200::c92a
zcrnprcbjhdjtt0.guug.de with 1.25s delay to 46.4.78.167
cuam0fwh4lzko7tb.guug.de with 1.25s delay to 91.184.37.10
7fujgpmmitg6bvm5.guug.de with 0.50s delay to 2001:41d0:304:200::c92a

Done.

myPro:ddi-scripts andreas$
```

another server used

DNS As A Covert Signaling Channel

- Data embedded in DNS queries (tunneling)
- Data embedded in DNS metadata (SOA serials)
- RFC-compliant traffic with hidden meaning



Demo: DNS Tunneling & Serial Numbers



```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ cat list_credit-cards.txt
Name;           Number           Expiry; CVC
Roxanne Clagon; 4111 1111 1111 1111; 01/27; 987
Fernande Searight; 5500 0000 0000 0004; 06/29; 654
Hedwig Facer;   3400 0000 0000 0097; 11/31; 321
myPro:ddi-scripts andreas$
```

data breach

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ cat list_credit-cards.txt
Name;          Number          Expiry; CVC
Roxanne Clagon; 4111 1111 1111 1111; 01/27; 987
Fernande Searight; 5500 0000 0000 0004; 06/29; 654
Hedwig Facer; 3400 0000 0000 0097; 11/31; 321
[myPro:ddi-scripts andreas$ ./dns_tunnel.sh client list_credit-cards.txt
File encoded as DNS hostnames and saved to dns_tunnel.log
myPro:ddi-scripts andreas$
```

client's tunnel

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ cat list_credit-cards.txt
Name;           Number           Expiry; CVC
Roxanne Clagon; 4111 1111 1111 1111; 01/27; 987
Fernande Searight; 5500 0000 0000 0004; 06/29; 654
Hedwig Facer;   3400 0000 0000 0097; 11/31; 321
[myPro:ddi-scripts andreas$ ./dns_tunnel.sh client list_credit-cards.txt
File encoded as DNS hostnames and saved to dns_tunnel.log
[myPro:ddi-scripts andreas$ cat dns_tunnel.log
TmFtZTsJCQl0dW1iZXIJCQlFeHBpcnk7CUNWQwpSb3hhbm5lIENsYWdvdjJsJCTQ.ftgijjya.com
xMTEgMTExMSAxMTExIDExMTE7CTAxLzI3Owk5ODcKRmVybmluZGU2Vhcm1naH.ftgijjya.com
Q7CTU1MDAgMDAwMCAwMDAwIDAwMDQ7CTA2LzI5Owk2NTQKSGVkd2lnIEZlY2V5O.ftgijjya.com
wkJMzQwMCAwMDAwIDAwMDAgMDA5NzsjMTEvMzE7CTMyMQo=.ftgijjya.com
myPro:ddi-scripts andreas$
```

data breach in DNS

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ cat list_credit-cards.txt
Name;                Number                Expiry; CVC
Roxanne Clagon;      4111 1111 1111 1111;    01/27; 987
Fernande Searight;    5500 0000 0000 0004;    06/29; 654
Hedwig Facer;        3400 0000 0000 0097;    11/31; 321
[myPro:ddi-scripts andreas$ ./dns_tunnel.sh client list_credit-cards.txt
File encoded as DNS hostnames and saved to dns_tunnel.log
[myPro:ddi-scripts andreas$ cat dns_tunnel.log
TmFtZTsJCQl0dW1iZXIJCQlFeHBpcnk7CUNWQwpSb3hhbm5lIENsYWdvdjJsJCTQ.ftgijjya.com
xMTEgMTExMSAxMTExIDExMTE7CTAxLzI3Owk5ODcKRmVybmlnaH.ftgijjya.com
Q7CTU1MDAgMDAwMCAwMDAwIDAwMDQ7CTA2LzI5Owk2NTQKSGVkd2lnIEZlY2V5O.ftgijjya.com
wkJMzQwMCAwMDAwIDAwMDAgMDA5NzsjMTEvMzE7CTMyMQo=.ftgijjya.com
[myPro:ddi-scripts andreas$ ./dns_tunnel.sh server dns_tunnel.log
File successfully reconstructed and saved to tunnel/reconstructed_file
myPro:ddi-scripts andreas$
```

server's query log

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ cat list_credit-cards.txt
Name;          Number          Expiry; CVC
Roxanne Clagon; 4111 1111 1111 1111; 01/27; 987
Fernande Searight; 5500 0000 0000 0004; 06/29; 654
Hedwig Facer; 3400 0000 0000 0097; 11/31; 321
[myPro:ddi-scripts andreas$ ./dns_tunnel.sh client list_credit-cards.txt
File encoded as DNS hostnames and saved to dns_tunnel.log
[myPro:ddi-scripts andreas$ cat dns_tunnel.log
TmFtZTsJCQl0dW1iZXIJCQlFeHBpcnk7CUNWQwpSb3hhbm5lIENsYWdvbjJsJCTQ.ftgijjya.com
xMTEgMTExMSAxMTExIDExMTE7CTAxLzI30wk5ODcKRmVybmlnaH.ftgijjya.com
Q7CTU1MDAgMDAwMCAwMDAwIDAwMDQ7CTA2LzI50wk2NTQKSGVkd2lnIEZhY2VyO.ftgijjya.com
wkJMzQwMCAwMDAwIDAwMDAgMDA5NzsJMTEvMzE7CTMyMQo=.ftgijjya.com
[myPro:ddi-scripts andreas$ ./dns_tunnel.sh server dns_tunnel.log
File successfully reconstructed and saved to tunnel/reconstructed_file
[myPro:ddi-scripts andreas$ cat tunnel/reconstructed_file
Name;          Number          Expiry; CVC
Roxanne Clagon; 4111 1111 1111 1111; 01/27; 987
Fernande Searight; 5500 0000 0000 0004; 06/29; 654
Hedwig Facer; 3400 0000 0000 0097; 11/31; 321
myPro:ddi-scripts andreas$
```

reconstructed file

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ dig soa guug.de +short
ns1.linuxtag.net. hostmaster.guug.de. 2026012601 3600 7200 1209600 600
myPro:ddi-scripts andreas$ ]
```

serial in SOA

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ dig soa guug.de +short
ns1.linuxtag.net. hostmaster.guug.de. 2026012601 3600 7200 1200600 600
[myPro:ddi-scripts andreas$ ./dns_ip-serial.sh 2026012601 serial to IP
120.194.127.185
myPro:ddi-scripts andreas$
```

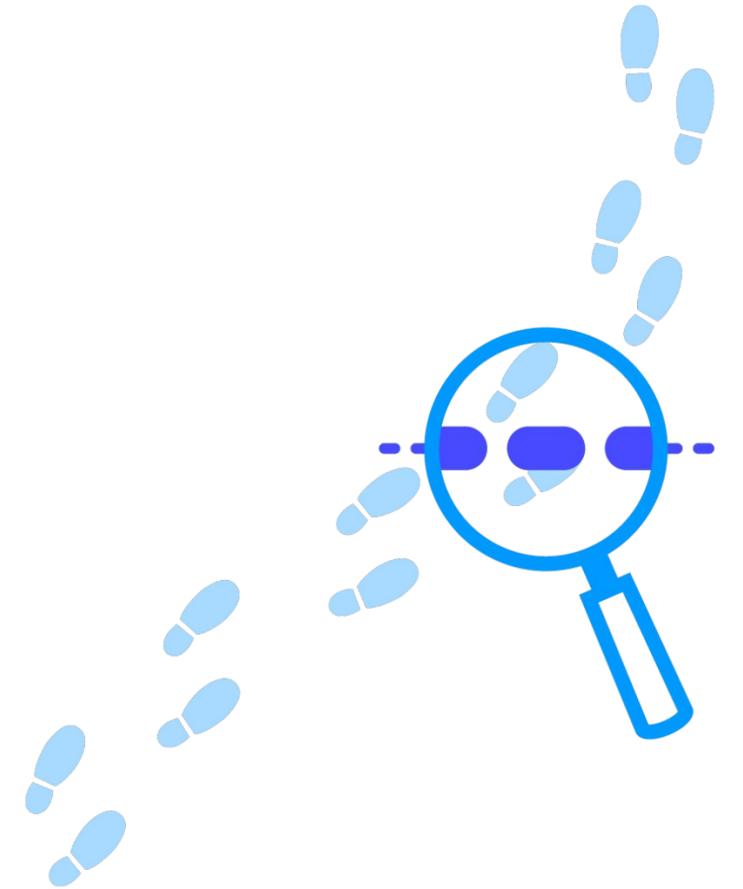
```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ dig soa guug.de +short ]
ns1.linuxtag.net. hostmaster.guug.de. 2026012601 3600 7200 1209600 600 ]
[myPro:ddi-scripts andreas$ ./dns_ip-serial.sh 2026012601 ]
120.194.127.185 ]
[myPro:ddi-scripts andreas$ ./dns_ip-serial.sh 10.0.187.188 ] IP to serial ]
167820220 ]
myPro:ddi-scripts andreas$
```

```
My Guideflow
~/ddi-scripts — -sh — 118x31
[myPro:ddi-scripts andreas$ dig soa guug.de +short
ns1.linuxtag.net. hostmaster.guug.de. 2026012601 3600 7200 1209600 600
[myPro:ddi-scripts andreas$ ./dns_ip-serial.sh 2026012601
120.194.127.185
[myPro:ddi-scripts andreas$ ./dns_ip-serial.sh 10.0.187.188
167820220
[myPro:ddi-scripts andreas$ ping -c 4 167820220 ping to serial
PING 167820220 (10.0.187.188): 56 data bytes
64 bytes from 10.0.187.188: icmp_seq=0 ttl=64 time=1.870 ms
64 bytes from 10.0.187.188: icmp_seq=1 ttl=64 time=2.031 ms
64 bytes from 10.0.187.188: icmp_seq=2 ttl=64 time=1.626 ms
64 bytes from 10.0.187.188: icmp_seq=3 ttl=64 time=1.283 ms

--- 167820220 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.283/1.703/2.031/0.282 ms
myPro:ddi-scripts andreas$
```

All Of This In Your DNS

- Early warning signals are already in DNS telemetry
- Generic tools often miss DNS specific patterns
- DNS specialized security is needed
- DNS data volume is the challenge

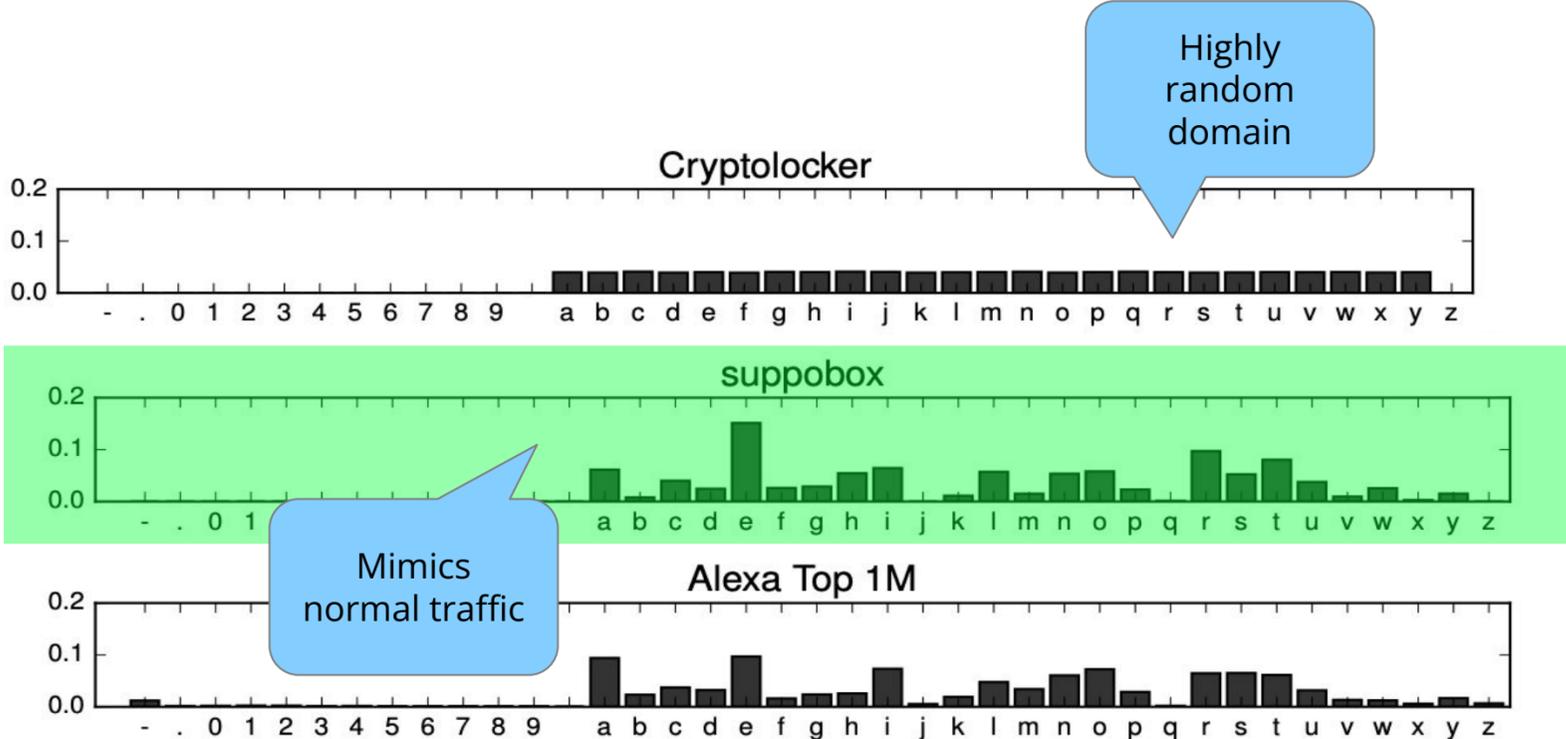


The signals are there. Finding them at scale needs DNS specific detection.

From DNS Signals To Detection And Validation

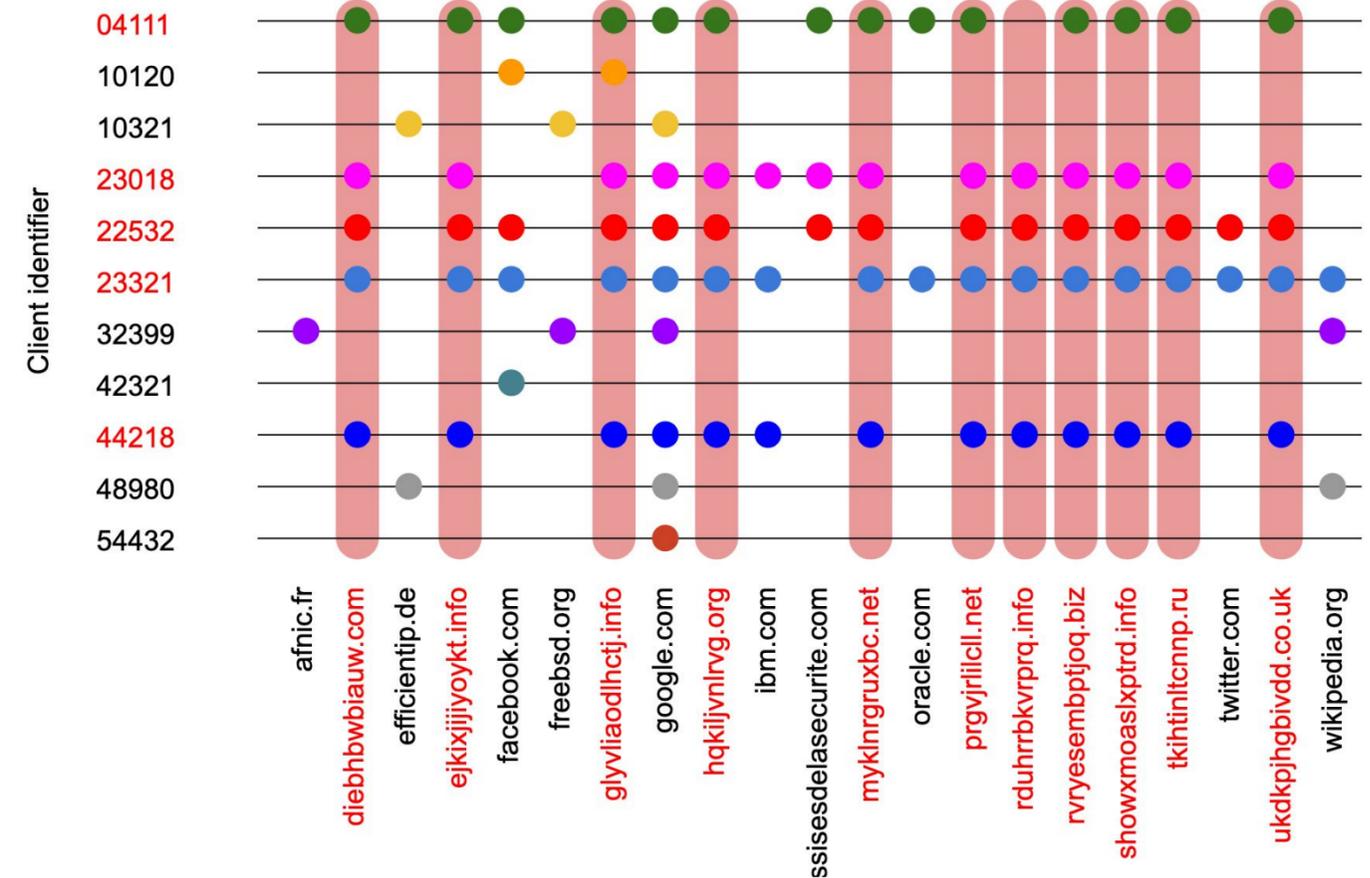
Common DGA Detection

- Analyze domain name syntax only
- Use statistical or ML-based patterns
- High false positives and easy to evade

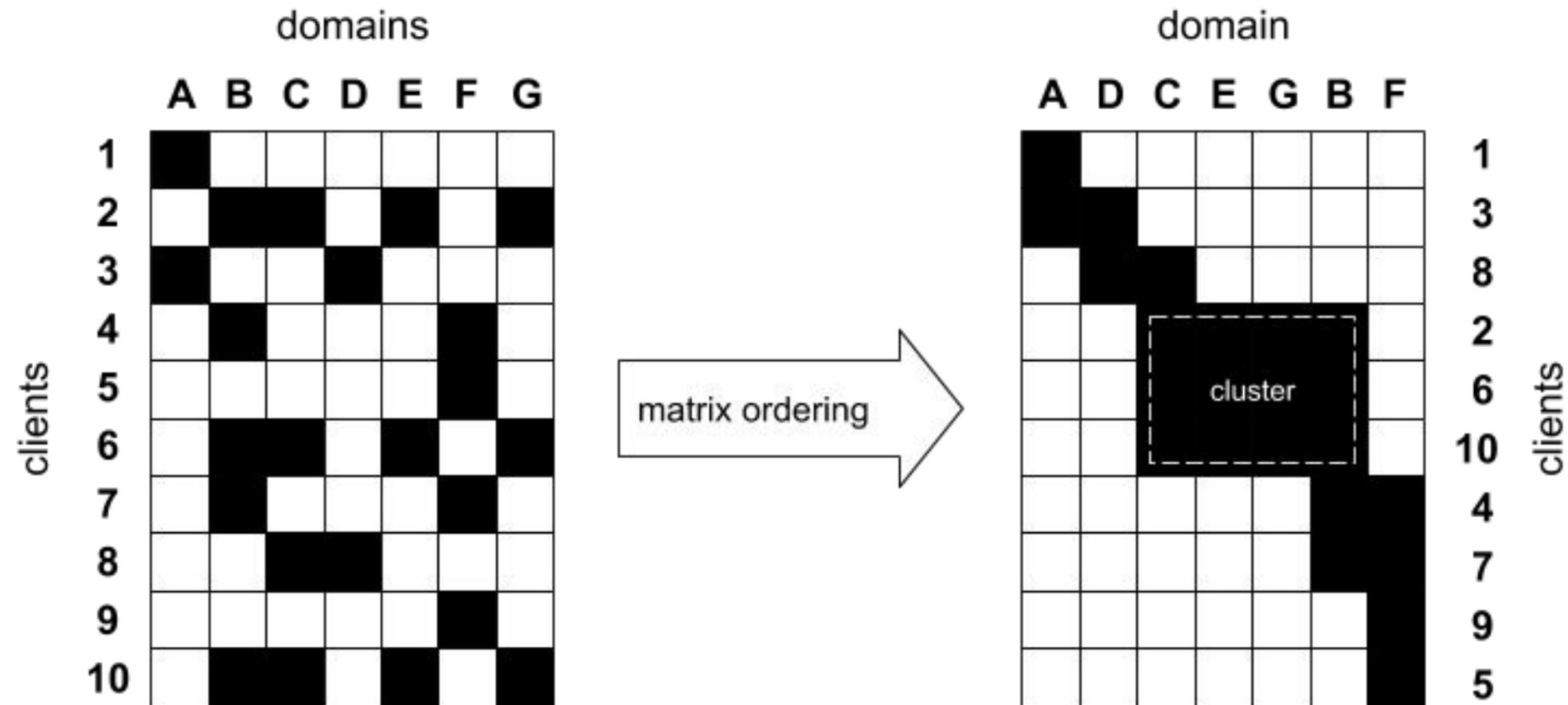


Focus On Clients For DGA Detection

- Analyzes clients instead of domains
- Groups by client and DNS behavior
- Tracks evolution and recruitment dynamics

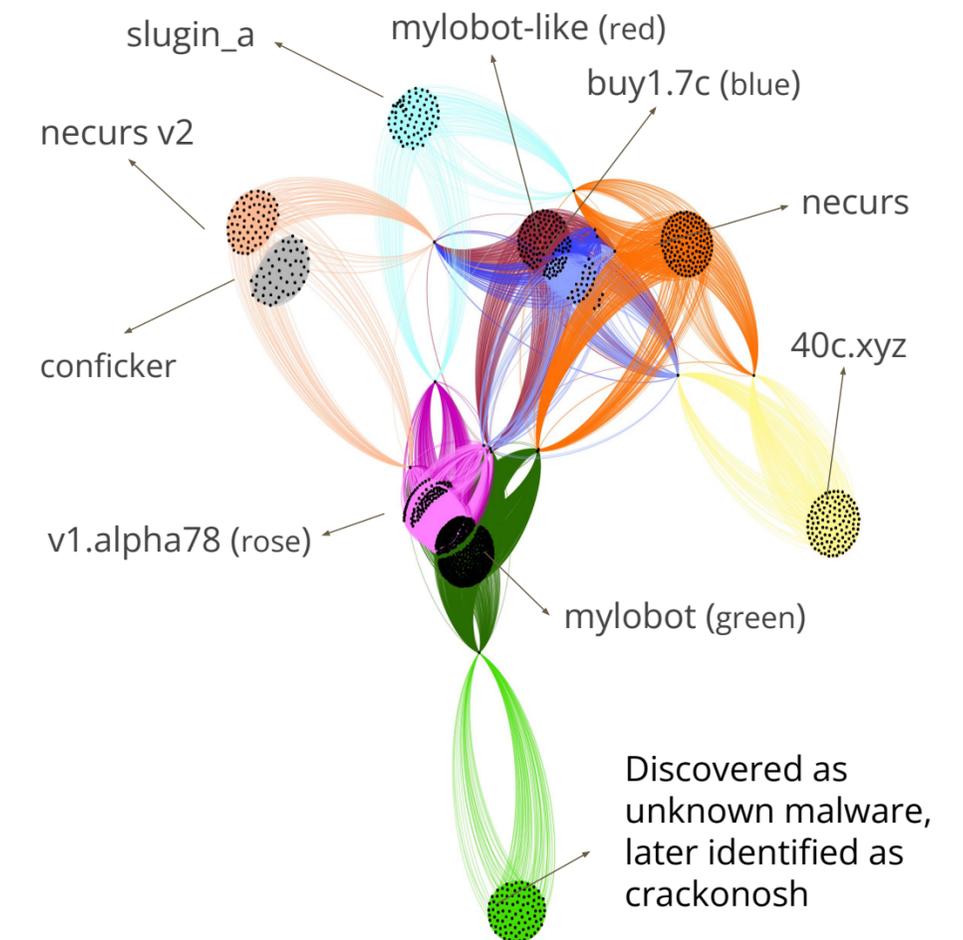


Matrix-Based Validation Of DGA Activity

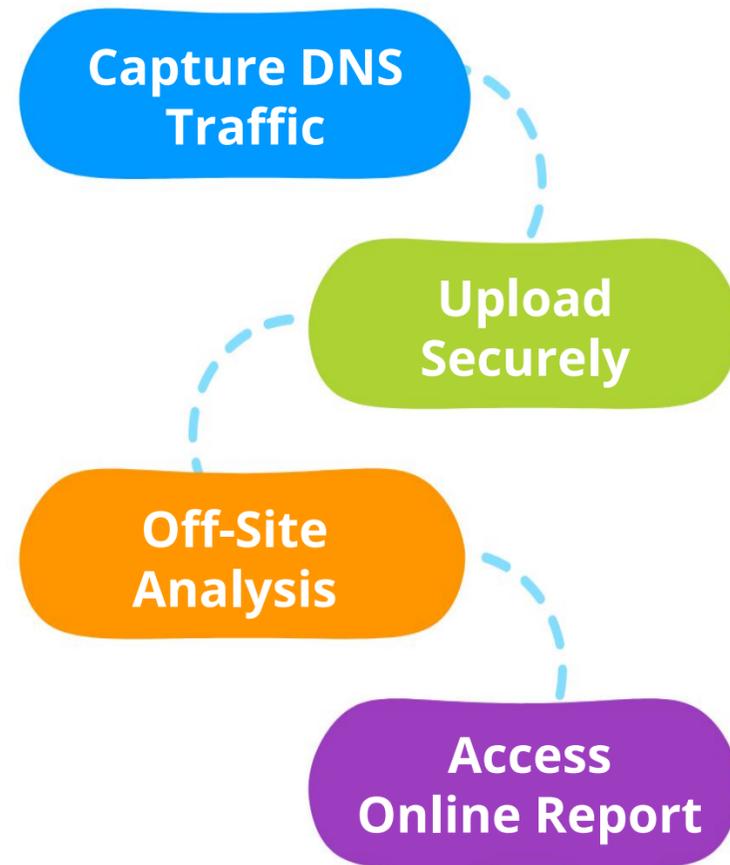


Detecting DGAs Via Tuple Clustering

- Project client–domain tuples into a multidimensional space
- Cluster associations using unsupervised analysis
- Clusters indicate potential DGA activity



DNS Risk Assessment



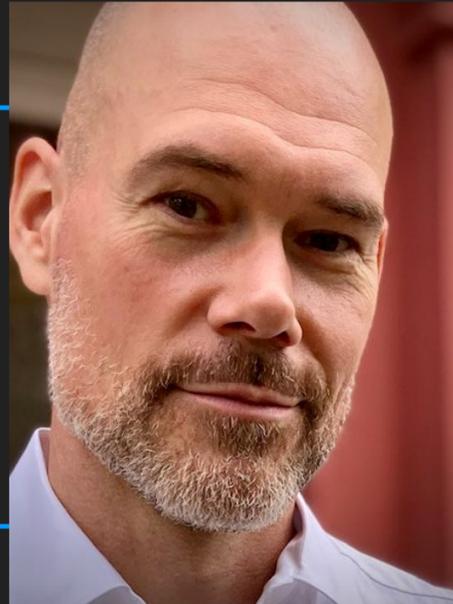
FREE DNS RISK ASSESSMENT

Do you really know what's **hidden in your network?**

Try looking below the surface

efficient iP®

Questions



Andreas Taudte

Senior Technical Marketing Manager

andreas.taudte@efficientip.com

Thank You

A collection of words in various languages and scripts, including: Vinaka, Maake, Dhanyavadagalu, Shukria, Manana Dankon, Kam Sah Hammida, Arakiss, Mauruuru, Biyan, Matondo, Dank Je, Dankscheen, spacybo köszön, Kaitos, Blagodaram, Ngiyabonga, Dziakuje, Juspaxar, Arigato, Chokrane, Grazie, Tack, Mochchakkeram, Graziar, Graciar, Tingki, Gratias Tibi, Ua Tsaug Rau Koj, Bedankt, Dakujem, धन्यवाद, cảm ơn bạn, Obrigado, Gratias Tibi, Suksama, Dėkuji, Nirringrazzjak, Hvala, Welalin, Di Ou Mési, Kia Ora, Kop Khun Khap, Paldies, ありがとう, Misaotra, Rahmat, Matur Nuvun, 谢, xBalla, Danke, Merci, Go Raibh Maith Agat, Djiere Dieuf, Eskerrik Asko, Najis Tuke, and others.