TLP:CLEAR

DNS Abuse Techniques

From the DNS Abuse SIG

June 2023 – Jonathan Spring and Peter Lowe, co-chairs

SIG Goals

Accomplished

- Common DNS abuse language for incident response (IR) teams
- Guidance to incident analysts on routing known DNS abuse

Next targets

- Improve situational awareness of DNS abuse for FIRST community
- Document triage or detection practices
- Improve common language based on your feedback

A bit of history

The DNS Abuse SIG

- Formed in 2019 after a BOF
- Kicked off by Carlos Alvarez and Merike Kaeo, chaired by Michael Hausding and Jonathan Matkowsky
- Representatives from all over the industry
- CERTs, Threat intelligence, Protective DNS services, Law Enforcement, app / device makers, ICANN, Registries, …

What we published in https://www.first.org/global/sigs/dns/DNS-Abuse-Techniques-Matrix_v1.1.pdf

The Document: A Matrix

Covering

- 21 DNS Abuse Techniques
- 15 Stakeholders
- 3 Activities - Detection, Mitigation, Prevention
- 9 Pages in landscape of the matrix itself

IR activities × DNS abuse types × Stakeholders

For each **activity** in:

- Detect
- Mitigate
- Prevent

  For each **abuse type** in:

  - Domain name compromise
  - …
  - Local recursive resolver hijacking

    For each **stakeholder** in

    - Registrars
    - …
    - End users

We answer the question:

Can the **stakeholder** successfully do the **activity** for the **abuse type**?

We published this matrix as a series of tables

Detection

✅ : The entity has the capability to detect
❌ : The entity lacks the capability to detect

	Registrars	Registries	Authoritative Operators	Domain name resellers	Recursive Operators	Network Operators	Application Service Provider	Hosting Provider	Threat Intelligence Provider	Device, OS, & Application Software Developers	Domain Registrants	End User	Law Enforcement and Public Safety Authorities	CSIRTs / ISACs	Incident responder (internal)
DGAs	✅ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✅ (eSLDs only)	✅ (eSLDs only, w/ analysis of customer domains)	✅ (eSLDs only)	✅ (Logs/ Passive DNS logging & analysis)	❌	✅	❌	✅	❌	N/A (Registrant is Threat Actor Itself)	❌	✅ (Can engage registries and/or PSWG GAC)	❌	✅ (if outgoing queries logged)
Domain name compromise	✅	✅	❌	✅	✅ (DNS RPZ + threat intelligence feeds)	❌	❌	❌	✅	❌	✅ (w/ proactive monitoring)	❌	✅	❌	❌ (Assuming external domain)
Lame delegations	❌	✅	❌	❌	✅	❌	❌	❌	✅	❌	✅ (w/ proactive monitoring)	❌	❌	❌	❌ (without historical delegation info)
DNS cache poisoning	❌	❌	❌	❌	✅ (Validating DNSSEC at the recursive and enabling extended errors - RFC 8914)	✅ (Flow analysis - NetFlow, Zeek)	❌	❌	✅	❌	✅ (w/ proactive monitoring)	❌	❌	❌	❌ (Assuming external resolver is poisoned)
DNS rebinding	❌	❌	❌	❌	✅ (pDNS analysis - DNS responses varying from public to RFC 1918)	✅ (Flow analysis - NetFlow, Zeek)	❌	❌	✅	❌	✅ (w/ proactive monitoring)	❌	❌	❌	✅
DNS server compromise	❌	❌	✅ (if the compromise is of the authoritative server)	❌	✅ (if the recursive resolver is itself compromised)	❌	✅	❌	✅	❌	❌	❌	❌	❌	❌ (If no passive DNS logs from before the compromise)

Where to access

Read the PDF here:

- https://www.first.org/global/sigs/dns/DNS-Abuse-Techniques-Matrix_v1.1.pdf

Also available as MISP galaxy:

- https://github.com/MISP/misp-galaxy/blob/main/clusters/first-dns.json

Join the SIG:

- https://portal.first.org/g/DNS%20Abuse%20SIG

Questions?

Peter Lowe

- peter.lowe@first.org
- https://twitter.com/pgl - https://infosec.exchange/@pgl

Jono

- Actual first name . Last name @cisa, we're also on the FIRST Slack.

Resources

- dns-abuse-sig@first.org
- https://www.first.org/global/sigs/dns/
- https://www.first.org/global/sigs/dns/DNS-Abuse-Techniques-Matrix_v1.1.pdf