TLP:CLEAR

DNS Abuse Techniques Matrix

From the DNS Abuse SIG at FIRST

June 2023 - Peter Lowe, co-chair and DNS Abuse Ambassador

Introduction

Who we are

- **FIRST**: The Forum of Incident Responders and Security Teams
- **DNS Abuse SIG**: cybersecurity and DNS people from all over the industry

Caveats

- Incorporating feedback right now
- SIG is recently back from a break

Introduction

Who I am

- DNS Abuse Ambassador at FIRST
- Co-chair of the DNS Abuse SIG
- Accidental DNS person
- Cybersecurity enthusiast
- Closet privacy evangelist

FIRST
Improving Security Together

Before we start...

TLP:CLEAR

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)

Background

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 are we trying to achieve?

Main objectives

- A tool for incident responders and security teams
- A resource to inform DNS Abuse policy

But also to address…

- Lack of a common language
- Incomplete taxonomies
- Bringing DNS Abuse communities together

A bit of history

The DNS Abuse SIG

- Our #1 stated goal:

  “Initially, provide a common language and a FIRST-definition of what the global incident response community understands as DNS Abuse in an operational context to protect its constituencies, as well as for purposes of global policy recommendations.”

A bit of history

The DNS Abuse SIG

- Our #2 stated goal:

  “Develop a classification scheme for DNS Abuse.”

So what's in it?

The Document: format

- Introduction
- Definitions and examples
- General advice
- **The Matrix… Matrixes… Matrices**

The Document: The Matrix(es)

Covering

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

DNS Abuse Techniques Matrix: Actions

Before: Detection

→ Identify potential problems

During: Mitigation

→ Contain an incident and restore secure operations

After: Prevention

→ Make it less likely incidents of this type will occur in the future

DNS Abuse Techniques Matrix: Stakeholders

- 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)

DNS Abuse Techniques Matrix: Techniques

- DGAs
- Domain name compromise
- Lame delegations
- DNS cache poisoning
- DNS rebinding
- DNS server compromise
- Stub resolver hijacking
- Local recursive resolver hijacking
- On-path DNS attack
- DoS against the DNS
- DNS as a vector for DoS
- Dynamic DNS resolution (as obfuscation technique)
- Dynamic DNS resolution: Fast flux (as obfuscation technique)
- Infiltration and exfiltration via the DNS
- Malicious registration of (effective) second level domains
- Creation of malicious subdomains under dynamic DNS providers
- Compromise of a non-DNS server to conduct abuse
- Spoofing or otherwise using unregistered domain names
- Spoofing of a registered domain
- DNS tunneling - tunneling another protocol over DNS
- DNS beacons - C2 communication

TLP:CLEAR

Prevention

✅ : The entity has the capability to prevent the threat
❌ : The entity lacks the capability to prevent the threat

	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)	✅ (if DG algorithm is known)	✅ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✅ (if DG algorithm is known, DNS RPZ + threat intelligence)	✅ (if DG algorithm is known)	❌	❌	❌	❌	N/A (registrant is threat actor itself)	❌	✅	✅ Investigating DG Algorithm)	❌
Domain name compromise	✅ (measures to prevent compromise of registrant account)	❌	❌	✅ (measures to prevent compromise of registrant account)	❌	❌	❌	❌	❌	❌	✅ (proactive measures to prevent compromise of registrant account)	❌	✅	✅ (contact relevant stakeholders)	❌
Lame delegations	❌	✅	❌	❌	❌	❌	❌	❌	❌	❌	✅ (good practices managing domain portfolio)	❌	✅	✅ (contact relevant stakeholders)	❌
DNS cache poisoning	❌	❌	❌	❌	✅ (DNSSEC validation enabled in the recursive)	❌	❌	❌	❌	❌	❌	❌	✅	✅ (contact recursive operator or network operator clear/refresh cache)	❌ (assuming cache is external to the org)
DNS rebinding	❌	❌	❌	❌	❌	❌	❌	❌	❌	❌	❌	✅ (set a strong password on the home router or rely on browser security features)	✅	✅ (coordinating vulnerable/defaced websites)	✅

Footnotes

A bit of history

- So this maybe took a bit longer than expected
- (3+ years)
- Multiple iterations
- But the same vision and (mostly) the same document (ish)
- Big thanks to former chairs and Carlos Alvarez

Challenges

- Lot of “sometimes” and “maybes” and qualifiers
- Which stakeholders to include? Or exclude?
- Which techniques to include?
- What terminology to use?
- How to incorporate notes and clarifications?
- What do we call it?
- **NB:** Not all these challenges have been entirely solved

Future work

V2

- Incorporating feedback, adjusting for nuances
- UI/UX work
- Solve unsolved challenges

Other work

- Report: What kind of DNS Abuse are you experiencing?
- MISP taxonomy
- Where are abuse reports going?

Questions?

Peter Lowe

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

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
- https://docs.google.com/presentation/d/1GfiorLzaqylxXMHBhTe_scPITnP9o5sfvmyxmQU2Yj0/edit (these slides)