DNS Abuse Techniques Matrix

FIRST DNS Abuse Special Interest Group

https://www.first.org/global/sigs/dns/

Introduction

This report from the DNS Abuse Special Interest Group (SIG) at FIRST provides advice for incident response teams responding to incidents involving DNS abuse. Crisply defining the edges of what is and is not DNS abuse is a challenge. Many organizations have weighed in on defining DNS abuse as relating to some combination of phishing, malware, unsolicited email, botnets, fraud, or a combination of some or all of these abuse types. The FIRST DNS Abuse SIG has recognized a gap in this conversation, which is that these categories do not give actionable advice to incident responders. This report therefore aims to complement existing efforts in DNS abuse studies by providing common examples of techniques used in incidents that responders and security teams see, and providing a stakeholder list for who might be able to help the incident responders detect, mitigate, or prevent specific techniques used for abuse.

The advice currently takes the form of a matrix indicating whether a specific stakeholder can directly help with a specific technique. By “help”, we mean whether the stakeholder is in a position to detect, mitigate, or prevent the abuse technique. We have organized this information under three spreadsheets covering these incident response actions. For example, during an incident involving DNS cache poisoning, the team can go to the mitigation tab and look at the row for DNS cache poisoning, to find which stakeholders they might be able to contact to help mitigate the incident.

The DNS ecosystem is complex, with many stakeholders and operating models. Some of the techniques listed may have benign uses, so it's not as simple as “these techniques should never be allowed”. However, in the context of incident response, the assumption is that an incident is occurring, so therefore whatever techniques the adversary used to initiate or maintain that incident are malicious or are against the security policy of the organization, or both. Incident responders should adhere to responsible collection within their jurisdictional boundaries. The DNS Abuse SIG is agnostic as to whether any of the listed techniques are abusive of the DNS in general. This report is composed from the point of view of assuming that a technique is used maliciously in the particular incident, and therefore bringing light as to who can take action by detecting, mitigating, or preventing.

Some techniques may be used in parallel with attacks involving the DNS;for example, BGP hijacking or TLS certificate impersonation. Such techniques are out of scope, this document focuses just on DNS abuse techniques.

It could be useful to note that there are other policy-related, governmental, and judicial avenues that can be contacted in response to an incident, which as of this version of the document haven't been included. For example, The Budapest Convention and other international instruments provide a mechanism for both evidence retrieval and suspension of infrastructure across country borders. The first step for a foreign law enforcement investigator will often be an informal preservation request, to ensure that data is not lost pending a formal legal request (that is, an MLAT).

Terms

The three dimensions of the matrix (action, technique, and stakeholder) use the following definitions of terms.

Actions

The definitions are linked to the FIRST CSIRT services framework v2.1, for services that a CSIRT might provide.

- **Detect** – identify potential incidents. Services: Monitoring and Detection; Incident Report Acceptance. Note: The phase of incident management where the IR team wants to confirm and gather additional detection tools and signatures is part of the Mitigation phase, not Detection. The Detection action focuses only on initial detection of the incident.
- **Mitigate** – contain an incident and restore secure operations. Services: Mitigation and Recovery.
- **Prevent** – using DNS-specific steps, make it less likely incidents of this type will occur in the future. Services: Knowledge transfer (including to internal IT teams); Vulnerability Response; also relates to detection (possibly updating the signatures and detection rules) and recovery (during recovery, should the system be reconfigured to prevent recurrence). Note that broad anti-malware prevention is out of scope. Of course everyone should do the broad anti-malware practices, see for example Best Practices | M3AAWG.

Techniques

1. DGAs (Domain Generation Algorithms) – https://attack.mitre.org/techniques/T1568/002/
2. Domain name compromise – The wrongfully taking control of a domain name from the rightful name holder. Compromised domains can be used for different kinds of malicious activity like sending spam or phishing, for distributing malware or as botnet command and control - https://www.icann.org/groups/ssac/documents/sac-007-en.
3. Lame delegations – Lame delegations occur as a result of expired nameserver domains allowing attackers to take control of the domain resolution by re-registering this expired nameserver domain - https://blog.apnic.net/2021/03/16/the-prevalence-persistence-perils-of-lame-nameservers/.

4. DNS cache poisoning – also known as DNS spoofing, is a type of cyber attack in which an attacker corrupts a DNS resolver's cache by injecting false DNS records, causing the resolver to records controlled by the attacker - https://capec.mitre.org/data/definitions/142.html
5. DNS rebinding – a type of attack where a malicious website directs a client to a local network address, allowing the attacker to bypass the same-origin policy and gain access to the victim's local resources - https://capec.mitre.org/data/definitions/275.html
6. DNS server compromise – Attacker gains administrative privileges on an open recursive DNS server, authoritative DNS server, organizational recursive DNS server, or ISP-operated recursive DNS server.
7. Stub resolver hijacking – The attacker compromises the Operating System of a computer or a phone with malicious code that intercepts and responds to DNS queries with rogue or malicious responses
8. Local recursive resolver hijacking – Consumer Premise Equipment (CPE), such as home routers, often provide DNS recursion on the local network. If the CPE device is compromised, the attacker can change the recursive resolver behavior; for example, by changing responses.
9. On-path DNS attack – “Attackers intercept communication between a user and a DNS server and provide different destination IP addresses pointing to malicious sites.” (https://www.imperva.com/learn/application-security/dns-hijacking-redirection/)
10. DoS against the DNS – Multiple systems sending malicious traffic to a target at the same time.
11. DNS as a vector for DoS – "Adversaries may attempt to cause a denial of service by reflecting a high-volume of network traffic to a target. This type of Network DoS takes advantage of a third-party server intermediary that hosts and will respond to a given spoofed source IP address. This third-party server is commonly termed a reflector. An adversary accomplishes a reflection attack by sending packets to reflectors with the spoofed address of the victim. Two prominent protocols that have enabled Reflection Amplification Floods are DNS and NTP through the use of several others in the wild have been documented." These Reflection and Amplification Floods can be directed against components of the DNS, like authoritative nameservers, rendering them unresponsive.” (https://attack.mitre.org/techniques/T1498/002/)
12. Dynamic DNS resolution (as obfuscation technique) – Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name IP address or port number the malware uses for command and control. (https://attack.mitre.org/techniques/T1568/)
13. Dynamic DNS resolution: Fast flux (as obfuscation technique) – “Adversaries may use Fast Flux DNS to hide a command and control channel behind an array of rapidly changing IP addresses linked to a single domain resolution. This technique uses a fully qualified domain name with multiple IP addresses assigned to it which are swapped with high frequency using a combination of round robin IP addressing and short Time-To-Live (TTL) for a DNS resource record.” (https://attack.mitre.org/techniques/T1568/001/)

14. Infiltration and exfiltration via the DNS – Exfiltration via the DNS requires a delegated domain or, if the domain does not exist in the public DNS, the operation of a resolver preloaded with that domain's zone file information and configured to receive and respond to the queries sent by the compromised devices.
15. Malicious registration of (effective) second level domains – For example, before attacking a victim, adversaries purchase or register domains from an ICANN-accredited registrar that can be used during targeting. See also CAPEC-630.
16. Creation of malicious subdomains under dynamic DNS providers – Before attacking a victim, adversaries purchase or create domains from an entity other than a registrar or registry that provides subdomains under domains they own and control. See also https://en.wikipedia.org/wiki/Dynamic_DNS.
17. Compromise of a non-DNS server to conduct abuse – Internet attack infrastructure is a broad category, and this covers any non-DNS server. Many compromised servers, such as web servers or mail servers, interact with the DNS or may be instrumental in conducting DNS abuse. For example, compromised mail servers are one technique that may be used to send phishing emails.
18. Spoofing or otherwise using unregistered domain names – In a context where a domain name is expected (such as the From header in mail or a URL in a web page or message body), supplying a domain name not controlled by the attacker and that **is not** controlled by or registered to a legitimate registrant.
19. Spoofing of a registered domain – In a context where a domain name is expected (such as the From header in mail or a URL in a web page or message body), supplying a domain name not controlled by the attacker and that **is in fact** controlled by or registered to a legitimate registrant.
20. DNS tunneling - tunneling another protocol over DNS – The DNS protocol serves an administrative function in computer networking and thus may be very common in environments. DNS traffic may also be allowed even before network authentication is completed. DNS packets contain many fields and headers in which data can be concealed. Often known as DNS tunneling, adversaries may abuse DNS to communicate with systems under their control within a victim network while also mimicking normal expected traffic. (https://attack.mitre.org/techniques/T1071/004/)
21. DNS beacons - C2 communication – Successive or periodic DNS queries to a command & control server, either to exfiltrate data or await further commands from the C2.

Stakeholders

Many organizations may act in different stakeholder roles at different times. At small and midsize organizations, the same individual may act in different roles at different times. However, these different stakeholders have distinct capabilities and so we have organized them as separate. Even if one organization has different teams that act as different stakeholder roles, it may be helpful to attempt to contact the relevant team that performs a stakeholder capability.

It is important for incident responders to be mindful that not every stakeholder will have their best interests at heart. Contacted stakeholders may be distracted, immature, or at worst intentionally operating infrastructure to support abuse. Organizations doing the latter will be

unreceptive at best and deceptive at worst. If you are unsure about whether to proceed with contacting a stakeholder, check with your peers.

1. Registrars – an organization that allows registration of domains under a TLD - https://www.icann.org/en/icann-acronyms-and-terms/registrar-en
2. Registries – organizations responsible for maintaining the database of domains for a TLD - https://www.icann.org/en/icann-acronyms-and-terms/registry-en
3. Authoritative Operators – https://www.icann.org/en/icann-acronyms-and-terms/authoritative-name-server-en
4. Domain name resellers – https://www.icann.org/resources/pages/reseller-2013-05-03-en
5. Recursive Operators – Organizations operating either a private or public recursive resolver
6. Network Operators – Organizations operating an autonomous system (AS). We assume an organization with this capability is not running a recursive DNS server. This column means netflow and BGP data, and excludes (as a matter of a clarity choice here) passive DNS.
7. Application Service Provider – Software as a Service provider (like Google Docs), see https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en for SaaS definition.
8. Hosting Provider – https://en.wikipedia.org/wiki/Web_hosting_service. If the hosting provider is a bulletproof hosting provider or otherwise complicit in providing attack infrastructure, then at best there is no good that will come from contacting them and at worst it will expose the team to reprisals.
9. Threat Intelligence Provider – Threat intelligence providers aggregate, transform, analyze, interpret, or enrich intelligence to provide the necessary context for decision-making processes. CTI is considered as sharing and analysis only.
10. Device, OS, & Application Software Developers – Software developers who write the code or develop DNS resolver software or are responsible for updating an imported DNS resolver version in their software project.
11. Domain Registrants – "an individual or entity who registers a domain name" https://www.icann.org/en/icann-acronyms-and-terms/registrant-en. In the case of the malicious registration rows, this stakeholder is modeled as the actual human who made the malicious registration.
12. End User – Everyone who uses the Internet (who is not performing one of the other stakeholder capabilities listed).
13. Law Enforcement and Public Safety Authorities – Government organizations with authority to enforce laws or act in the public interest. Such organizations typically become aware of an issue because of:

    a. Ongoing investigation in which LE technique gives unique insight.

    b. Victim complaints provide information indicating the abuse, often relying upon collaboration with technical SMEs to help the organization understand the evidence.

14. CSIRTs / ISACs – Computer Security Incident Response Teams / Information Sharing and Analysis Centers. This column models exclusively the capability of the team or center. Each CSIRT and ISAC also is an end user of services, a registrant, may be a threat intel provider, etc.

When the CSIRT or ISAC (organization) is performing those stakeholder capability, use those columns.

15. Incident responder – The Computer Security Incident Response Team that is internal to the impacted organization.

Examples of Techniques

The SIG has collected examples of various techniques and made the available via the FIRST.org website under the DNS Abuse SIG homepage:

- https://www.first.org/global/sigs/dns/dns-abuse-examples

This list of examples will continue to be updated as more are curated.

JPCERT/CC has published a list of phishing URLs that demonstrate examples of techniques including domain generation algorithms (DGAs) and malicious registrations of effective SLDs.

Nominet published an explanation of how dangling DNS entries can lead to vulnerability to the lame delegation and on-path DNS attack techniques.

The IRS published a warning against SMS scams making use of malicious registration as well as spoofing the target organization.

Advice for Incident Responders

The following spreadsheets represent our advice on what kind of organizations might be productively contacted at different incident response phases for different DNS abuse techniques.The Budapest Convention and other networks provide a mechanism for both evidence retrieval and suspension of infrastructure across country borders. The Convention sets expectations, for example “the first step for an investigator will often be an informal preservation request, to ensure that data is not lost pending a formal legal request (MLAT)”.

Abuse Matrices

Key

✅ : The entity has the capability to **detect** / **mitigate** / **prevent the threat**
❌ : The entity lacks the capability to **detect** / **mitigate** / **prevent the threat**

- DGA : domain generation algorithm
- eSLD : effective second-level domain
- pDNS : passive DNS traffic analysis

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)

	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)
Stub resolver hijacking	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓ (Maybe depends on Anti-virus Software)	✗	✗	✓
Local recursive resolver hijacking	✗	✗	✗	✗	✗	✓ (NetFlow, Zeek + threat intelligence)	✗	✗	✓	✓	✗	✓ (Built-in security features on home routers)	✗	✗	✓
On-path DNS attack	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓ (Only if passive DNS logs and if resolution path can be checked)
DoS against the DNS	✗	✗	✓ (if the attack is against authoritative servers)	✗	✓ (if attack targets the recursive or authoritative - logs, NetFlow, Zeek)	✓ (Flow analysis - NetFlow, Zeek)	✗	✗	✗	✗	✗	✗	✓	✗	✓
DNS as a vector for DoS	✗	✗	✓ (if attack leverages authoritative responses)	✗	✓ (if attack targets the recursive or authoritative - logs, NetFlow, Zeek)	✓ (Flow analysis - NetFlow, Zeek)	✗	✗	✗	✓	✗	✗	✓	✗	✓
Dynamic DNS resolution (as obfuscation technique)	✗	✓ (eSLDs only)	✗	✗	✓	✗	✗	✗	✓	✗	N/A (Registrant is Threat Actor Itself)	✓ (Anti-virus Software)	✓	✗	✓ (assuming pDNS logs, or active resolutions if ongoing)
Dynamic DNS resolution: Fast flux (as obfuscation technique)	✗	✓ (eSLDs only)	✓ (eSLDs only,flagging short TTLs for further analysis)	✗	✓ (Flow analysis using NetFlow, Zeek)	✗ (not without Passive DNS)	✗	✗	✓	✗	N/A (Registrant is Threat Actor Itself)	✓ (Anti-virus Software)	✓	✗	✓ (assuming passive DNS logs, or maybe active resolutions if dynamic DNS is ongoing)

	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)
Infiltration and exfiltration via the DNS	✗	✗	✗	✗	✗	✗ (not without analysis of traffic)	✗	✗	✓	✗	N/A (Registrant is Threat Actor Itself)	✗	✓	✗	✓ (assuming pDNS logs)
Malicious registration of (effective) second level domains	✓ (eSLDs only, w/ analysis at point of creation and during the lifetime of the domains)	✓	✓ (depending on the strings)	✓	✓ (pDNS analysis)	✗	✓	✗	✓	✗	N/A (Registrant is Threat Actor Itself)	✗	✓ (Contact registrar, escalate to registry)	✗	✗ (Can't detect the registration)
Creation of malicious subdomains under dynamic DNS providers	✗	✗	✓	✗	✓ (DNS RPZ logging + threat intelligence)	✗	✓	✗	✓	✗	N/A (Registrant is Threat Actor Itself)	✗	✓	✗	✗ (Creation of names not detectable)
Compromise of a non-DNS server to conduct abuse	✗	✗	✗	✗	✗	✗	✗	✓ (not bulletproof)	✓	✗	✗	✗	✓	✗	✓
Spoofing or otherwise using unregistered domain names	✗	✗	✓	✗	✓ (DNS log analysis, Zeek)	✗	✗	✓ (not bulletproof)	✓	✗	✗		✓	✗	✓
Spoofing of a registered domain	✗	✓	✗	✗	✓ (Analysis of DNS responses - RFC 8914)	✗	✓	✓ (not bulletproof)	✓	✗	✗ (unless using DMARC)	✗	✓	✗	✓ (assuming DMARC or maybe pDNS analysis)
DNS tunneling - tunneling another protocol over DNS	✗	✗	✗	✗	✓ (Flow analysis using NetFlow, Zeek)	✗ (not without analysis of traffic)	✗	✗	✓	✗	✗	✗	✗	✗	✗ (passive DNS can hypothetically detect this, but it is hard)
DNS beacons - C2 communication	✗	✓	✗	✗	✓ (Flow analysis using NetFlow, Zeek)	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓ (if aware of machines using the C2 channel, passive DNS)

Mitigation

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

	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	✅ (updating status to onHold or changing name servers)	✅	❌	✅ (updating status to onHold or changing name servers)	✅ (dns rpz)	❌	❌	❌	❌	❌	N/A (Registrant is Threat Actor Itself)	❌	✅ (Defensive registration, generate domains and share with registries)	❌	✅ (blocking)
Domain name compromise	✅ (if compromise at the registrar level)	✅	✅	✅ (if compromise is at the reseller level)	✅	❌	❌	❌	❌	❌	✅ (w/ appropriate clean up)	❌	❌	❌	✅ (blocking)
Lame delegations	❌	❌	❌	❌	❌	❌	❌	❌	❌	❌	✅ (updating name servers)	❌	❌	❌	❌ (contact registrar, etc.)
DNS cache poisoning	❌	❌	✅	❌	✅ (DNSSEC)	✅	❌	❌	❌	❌	❌	❌	❌	❌	❌ (contact authoritative operator, etc.)
DNS rebinding	❌	✅	❌	❌	❌	✅ (BCP38, BGP blackhole attacker's IP netblock)	❌	❌	❌	❌	❌	❌	❌	❌	✅

	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 server compromise	✗	✗	✓	✗	✓ (only if it is their server)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Stub resolver hijacking	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓ (scan PC with Anti-virus software)	✗	✗	✓
Local recursive resolver hijacking	✗	✗	✗	✗	✗	✓ (block egress traffic to malicious DNS server)	✗	✗	✗	✗	✗	✓ (reboot the home router or initialization)	✗	✗	✓
On-path DNS attack	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗ (contact network operator etc.)
DoS against the DNS	✗	✓	✗	✗	✗	✓ (BGP blackhole the attacker's IP)	✗	✗	✗	✗	✗	✗	✗	✗	✓
DNS as a vector for DoS	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
Dynamic DNS resolution (as obfuscation technique)	✗ (only provide registration services of eSLDs)	✗	✗	✗	✓	✗	✗	✗	✗	✗	N/A (Registrant is Threat Actor Itself)	✗	✗	✗	✓ (blocking, if can be identified)
Dynamic DNS resolution: Fast flux (as obfuscation technique)	✓ if they can act fast enough	✓ if they can act fast enough	✗	✓ if they can act fast enough	✓	✓	✗	✗	✗	✗	N/A (Registrant is Threat Actor Itself)	✗	✗	✗	✓
Infiltration and exfiltration via the DNS	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	N/A (Registrant is Threat Actor Itself)	✗	✗	✗	✓

	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)
Malicious registration of (effective) second level domains	✓ (updating status to onHold or changing name servers)	✓	✗	✓ (updating status to onHold or changing name servers)	✓	✗	✗	✗	✗	✗	N/A (Registrant is Threat Actor Itself)	✗	✓ (notify registrar/registry, domain seizure [LEA])	✗	✗ (cannot change registration itself)
Creation of malicious subdomains under dynamic DNS providers	✗ (only provide registration services of eSLDs)	✗	✓	✗	✓	✗	✗	✗	✗	✗	N/A (Registrant is Threat Actor Itself)	✗	✗	✗	✗ (cannot address creation itself)
Compromise of a non-DNS server to conduct abuse	✗	✗	✗	✗	✗	✗	✓	✓ (not bulletproof)	✗	✗	✗	✗	✗	✗	✓ (if it is the team's AOR to fix the server)
Spoofing or otherwise using unregistered domain names	✗	✗	✓	✗	✓	✗	✗	✓ (not bulletproof)	✗	✗	✗	✗	✗	✗	✗
Spoofing of a registered domain	✓ (w/ analysis at point of creation or though the lifetime of the domains)	✗	✗	✓ (w/ analysis at point of creation or though the lifetime of the domains)	✓	✗	✗	✓ (not bulletproof)	✗	✗	✓ (filing report, UDRP, URS as appropriate)	✗	✗	✗	✗ (even if DMARC applies, does not stop the spoofing)
DNS tunneling - tunneling another protocol over DNS	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	N/A (Registrant is Threat Actor Itself)	✗	✗	✗	✓
DNS beacons - C2 communication	✗ (C2 domain infrastructure only)	✗	✗	✓ (C2 domain infrastructure only)	✓	✗	✗	✗	✗	✗	N/A (Registrant is Threat Actor Itself)	✗	✓	✗	✓

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)	✅

	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 server compromise	✗	✗	✓ (if the compromise is at the authoritative server)	✗	✓ (if the recursive itself is compromised)	✗	✗	✗	✗	✗	✗	✗	✓	✓ (contact relevant stakeholders)	✗ (assuming server is external to org)
Stub resolver hijacking	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓ (keep browser and add-on tools etc. up to date)	✓	✓ (making alerts to End Users)	✓
Local recursive resolver hijacking	✗	✗	✗	✗	✗	✓ (Flow analysis using NetFlow, Zeek + Threat Intelligence)	✗	✗	✗	✓	✗	✓ (Keep software up to date, set strong password, etc.)	✓	✓ (making alerts to End Users)	✓
On-path DNS attack	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓	✓ (share info for awareness)	✓ (DNSSEC validation)
DoS against the DNS	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓ (Coordination for open resolvers and infected machines)	✗ (Assuming BCP 38 is not in IR's purview)
DNS as a vector for DoS	✗	✗	✓ (if the attack weaponizes the authoritative responses)	✗	✓ (ACL, rate-limiting etc)	✗	✗	✗	✗	✓	✗	✓ (keep firmware up to date and proper configuration, etc)	✓ (engage national-level CERT to identity DNS amplifiers)	✓ (Coordination for open resolvers and infected machines)	✓ (clean up infected machines)
Dynamic DNS resolution (as obfuscation technique)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓ (contact relevant stakeholders)	✗
Dynamic DNS resolution: Fast flux (as obfuscation technique)	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓ (contact relevant 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)
Infiltration and exfiltration via the DNS	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓ (share info for awareness)	✓
Malicious registration of (effective) second level domains	✓ (eSLDs only, analysis at point of creation)	✓	✗	✓ (eSLDs only, analysis at point of creation)	✗	✗	✗	✗	✗	✓	N/A (registrant is threat actor itself)	✗	✓ (notify registrar, escalate to registry)	✓ (contact relevant stakeholders)	✗
Creation of malicious subdomains under dynamic DNS providers	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	N/A (registrant is threat actor itself)	✗	✓	✓ (contact relevant stakeholders)	✗
Compromise of a non-DNS server to conduct abuse	✗	✗	✗	✗	✗	✗	✓	✓ (not bulletproof)	✗	✗	✗	✗	✓	✓ (share info for awareness)	✓ (patch management, etc.)
Spoofing or otherwise using unregistered domain names	✗	✓	✗	✗	✗	✗	✗	✓ (not bulletproof)	✗	✗	✗	✗	✓	✓ (share info for awareness)	✗
Spoofing of a registered domain (for abuse)	✓ (eSLDs only, analysis at point of creation)	✗	✓ (preventing resolution for the spoofing domains serviced)	✓ (eSLDs only, analysis at point of creation)	✗	✗	✗	✓ (not bulletproof)	✗	✓	N/A (registrant is threat actor itself)	✗	✓	✓ (share info for awareness)	✗
DNS tunneling - tunneling another protocol over DNS	✗	✗	✗	✗	✓ (TLS Fingerprinting with JA3 and JA3S, Flow analysis, Zeek)	✓ (Flow analysis using NetFlow, Zeek + Threat Intelligence)	✗	✗	✗	✗	✗	✗	✓	✓ (cleaning up infected machines and analyzing the malware)	✗ (assuming firewall rule management and such are not AOR of IR)
DNS beacons - C2 communication	✗	✗	✗	✗	✓ (Flow analysis using NetFlow, Zeek)	✓ (Flow analysis using NetFlow, Zeek + Threat Intelligence)	✗	✗	✗	✗	✗	✗	✓	✓ (cleaning up infected machines and analyzing the malware)	✗

Acknowledgements

SIG members

Andrey Meshkov (AdGuard)

Ángel González (INCIBE-CERT)

Angela Matlapeng (bwCSIRT)

Benedict Addis (Shadowserver)

Brett Carr (Nominet)

Carlos Alvarez (ICANN; founding member)

David Ruefenacht (Infoguard)

Gabriel Andrews (FBI)

John Todd (Quad9; current co-chair of DNS Abuse SIG)

Jonathan Matkowsky (RiskIQ / Microsoft; former co-chair)

Jonathan Spring (CISA; current co-chair of DNS Abuse SIG)

Mark Henderson (IRS)

Mark Svancarek (Microsoft)

Merike Kaeo (Double Shot Security)

Michael Hausding (SWITCH-CERT; former co-chair, current FIRST board member)

Peter Lowe (DNSFilter; current co-chair of DNS Abuse SIG)

Shoko Nakai (JPCERT/CC)

Swapneel Patnekar (Shreshta IT)

Trey Darley (FIRST board; founding member)

SIG chairs

Current: Jonathan Spring, John Todd, Peter Lowe

Former: Michael Hausding, Jonathan Matkowsky

Special Thanks

To Carlos Alvarez (ICANN) for an initial start on the abuse technique types matrix.