The Challenge of Defining DNS Abuse

Peter Lowe, DNS Abuse Ambassador

September 2022

Who am I?

- Peter Lowe
- DNS Abuse Ambassador for FIRST
- Co-chair of the DNS Abuse SIG
- Worked in DNS security for around 3 years now, 28 years in tech
- Principal Security Researcher for DNSFilter
- Been in the tech industry most of my life

What is FIRST?

- The **F**orum of **I**ncident **R**esponders and **S**ecurity **T**eams
- Founded in 1990
- Great name, but sometimes hard to search for

- We enable incident responders
  - To **engage with their peers**
  - To have a **shared understanding** of security problems
  - By developing **technologies and standards**
  - By fostering an **environment conducive to their work**

DNS Abuse as a term

- Means different things to different people
- For many, it's just malicious domain registrations
- For others, it encompasses using the DNS to effect abuse
- And for others, it's abusing the DNS itself
- This means it's a challenge to define!

DNS Abuse as a term

- From Quora:
  - *"DNS abuse is using some or all parts of a DNS infrastructure to do something it wasn’t designed to do."*
- SIDN:
  - *"When people use our DNS servers, there is less server capacity available for others. Excessive use can therefore create problems for everyone else."*
- DNS Abuse Institute
  - *"DNS Abuse is comprised of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam (when it serves as a delivery mechanism for the other forms of DNS Abuse)."*

DNS Abuse as a term

- An article in dotmagazine on "THE DEBATE AROUND DEFINING, … DNS ABUSE"
  - *"Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity".*
- EU study on Domain Name System (DNS) Abuse:
  - *"Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity."*
- ICANN wiki:
  - *"DNS Abuse is any malicious activity aimed at disrupting the DNS infrastructure or causing the DNS to operate in an unintended manner."*

Abuse *of* the DNS vs. Abuse *via* the DNS

- Not as many types of abuse of the DNS
  - cache poisoning
  - DDoS attacks
  - DGA domains
- Lots of abuse via the DNS
  - C2 domains
  - phishing
  - spam
  - typosquatting

DNS Abuse Organisations

Focused on DNS Abuse

- FIRST DNS Abuse SIG
- DNS Abuse Institute
- Global Cyber Alliance
- ICANN's SSAC
- Shadowserver
- Spamhaus
- SURBL

Related groups

- Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG)'s Names and Numbers Committee
- KINDNS
- IETF dnsop working group
- RIPE DNS working group
- APWG

And more!

DNS Abuse Stakeholders

- Domain registries
- Domain registrars
- Incident response groups
- Threat intelligence organisations
- Governments
- Enterprise risk management
- Resolvers - both firewalls and filtering services
- Policy makers
- Law enforcement
- Rights holders
- … and, of course, every single victim on the internet

What can we do?

- Try to keep perspective that there are others coming from a different angle
- Try to create a common language - goal of the FIRST DNS Abuse SIG
- For myself: facilitate conversations and remind people
- ie: Beat the drum

FIRST's DNS Abuse SIG

- Working on providing that common language
- And developing a classification scheme for DNS Abuse

- Really do have a good representation of different people, orgs, stakeholders:

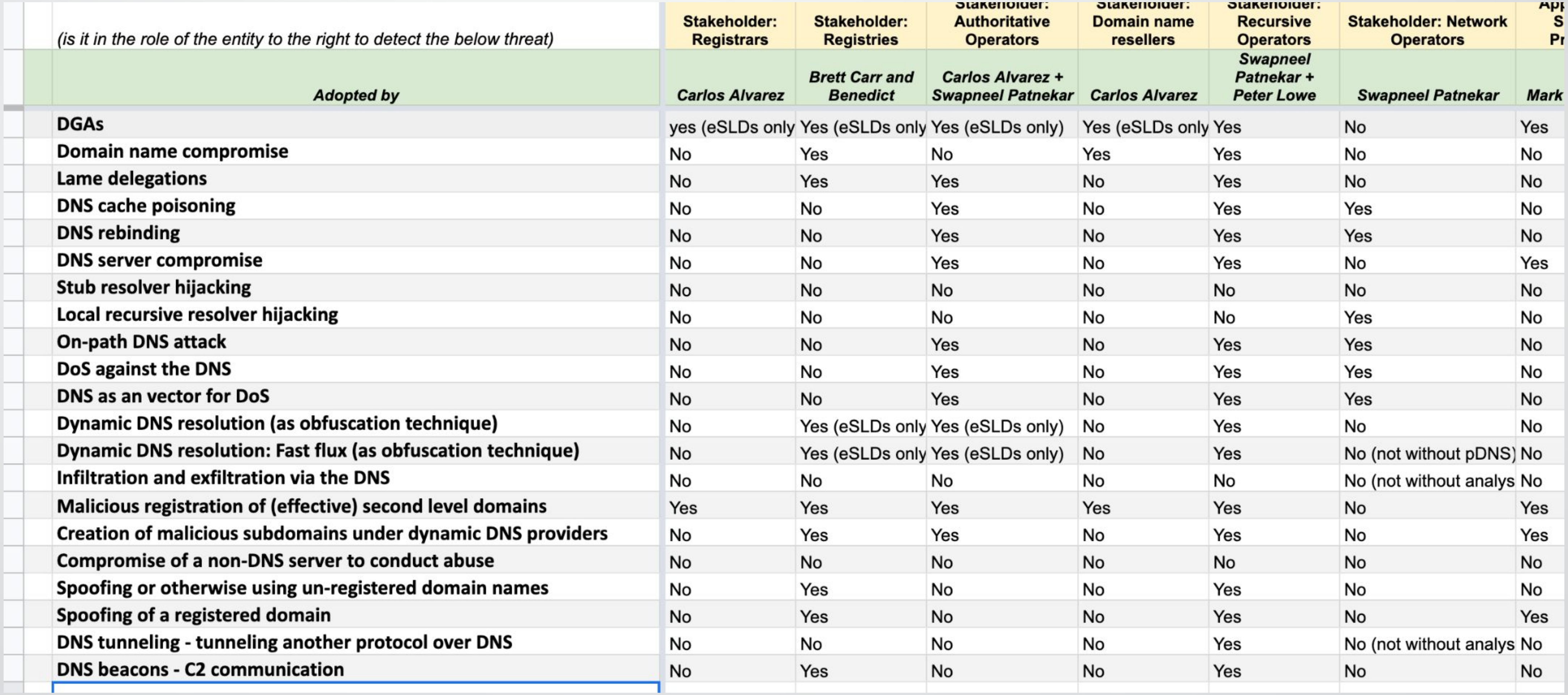
- People from *(deep breath)* CERTs, Internet governance, commercial resolvers, public resolvers, law enforcement registries, registrars, CTI, other governments

- Over 100 countries

- Chairs: Jonathan Spring (US-CERT), John Todd (Quad9), Peter Lowe (DNSFilter)

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

FIRST DNS Abuse SIG: A common language



(is it in the role of the entity to the right to detect the below threat)	Stakeholder: Registrars	Stakeholder: Registries	Stakeholder: Authoritative Operators	Stakeholder: Domain name resellers	Stakeholder: Recursive Operators	Stakeholder: Network Operators	App S Pr
Adopted by	***Carlos Alvarez***	***Brett Carr and Benedict***	***Carlos Alvarez + Swapneel Patnekar***	***Carlos Alvarez***	***Swapneel Patnekar + Peter Lowe***	***Swapneel Patnekar***	***Mark***
DGAs	yes (eSLDs only	Yes (eSLDs only	Yes (eSLDs only)	Yes (eSLDs only	Yes	No	Yes
Domain name compromise	No	Yes	No	Yes	Yes	No	No
Lame delegations	No	Yes	Yes	No	Yes	No	No
DNS cache poisoning	No	No	Yes	No	Yes	Yes	No
DNS rebinding	No	No	Yes	No	Yes	Yes	No
DNS server compromise	No	No	Yes	No	Yes	No	Yes
Stub resolver hijacking	No	No	No	No	No	No	No
Local recursive resolver hijacking	No	No	No	No	No	Yes	No
On-path DNS attack	No	No	Yes	No	Yes	Yes	No
DoS against the DNS	No	No	Yes	No	Yes	Yes	No
DNS as an vector for DoS	No	No	Yes	No	Yes	Yes	No
Dynamic DNS resolution (as obfuscation technique)	No	Yes (eSLDs only	Yes (eSLDs only)	No	Yes	No	No
Dynamic DNS resolution: Fast flux (as obfuscation technique)	No	Yes (eSLDs only	Yes (eSLDs only)	No	Yes	No (not without pDNS)	No
Infiltration and exfiltration via the DNS	No	No	No	No	No	No (not without analys	No
Malicious registration of (effective) second level domains	Yes	Yes	Yes	Yes	Yes	No	Yes
Creation of malicious subdomains under dynamic DNS providers	No	Yes	Yes	No	Yes	No	Yes
Compromise of a non-DNS server to conduct abuse	No	No	No	No	No	No	No
Spoofing or otherwise using un-registered domain names	No	Yes	No	No	Yes	No	No
Spoofing of a registered domain	No	Yes	No	No	Yes	No	Yes
DNS tunneling - tunneling another protocol over DNS	No	No	No	No	Yes	No (not without analys	No
DNS beacons - C2 communication	No	Yes	No	No	Yes	No	No

Questions?

peter.lowe@first.org

https://twitter.com/pgl
https://linkedin.com/in/peterlowe