topDNS

An initiative by eco

	DNS Abuse?			Mitigation															
	Abuse of the DNS	Abuse via the DNS	No Abuse of DNS	User	Access Provider	CDN	Host / Cloud	Mailbox Provider	ESP	Platform	Registrar	Reseller	Privacy / Proxy	Registry	Registrant	Law Enforcement	Authoritative DNS Operator	DNS-Resolver Operator	DNS-Zone Operator
Content Harms																			
Abusive Content																			
CSAM*			x				x			x	x	x				x			
Child Safety			x				x			x	x	x				x			
Opioids*			x				x			x	x	x				x			
Human Trafficking*			x				x			x	x	x				x			
Hate Speech			x				x			x	x	x				x			
Extreme Violence*			x				x			x	x	x				x			
Dis-/Misinformation			x				x			x	x	x				x			
Criminal Organization			x				x			x	x	x				x			
Harassment			x				x			x	x	x				x			
Fraud / Intellectual Property Infringement																			
Intentional Trademark Infringement or Counterfeiting			x				x			x	x			x		x			
Intentional Unauthorised Use of Resources			x				x			x	x					x			
Intentional Copyright Infringement			x				x			x	x			x		x			
Masquerade			x				x			x	x					x			
Financial / Commercial Harms			x				x			x	x					x			
Infrastructure Harms																			
Botnet*/ Command & Control		x															x	x	
Malware*																			
Malicious Code			x					x	x	x							x	x	
Virus / Worm			x					x	x	x							x	x	
Trojan / Spyware			x					x	x	x							x	x	
Rootkit			x					x	x	x							x	x	
Ransomware			x					x	x	x							x	x	
Availability																			
DoS	x	x			x														
DDoS	x	x			x														
Sabotage	x	x															x	x	
Outage																			
DNS Cache Poisoning	x																x	x	
DNS Rebinding	x																x	x	

* The topDNS Initiative endorses the Framework to Address Abuse. According to the framework, DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam. While spam alone is not considered as DNS Abuse, the framework includes it in the five key forms of DNS Abuse when it is used as a delivery mechanism for the other four forms of DNS Abuse.

The technical community adopts a more restrictive approach on the definition of different types of abuse. The column "DNS Abuse?" reflects this approach, which only considers specific types of abuse that solely target DNS infrastructure. The Framework to Address Abuse is more inclusive.

Specifically, even without a court order, the signatories of the framework believe a registry or registrar should act to disrupt the following forms of Website Content Abuse: (1) child sexual abuse materials ("CSAM"); (2) illegal distribution of opioids online; (3) human trafficking; and (4) specific and credible incitements to violence.

topDNS

An initiative by eco

	DNS Abuse?			Mitigation															
	Abuse of the DNS	Abuse via the DNS	No Abuse of DNS	User	Access Provider	CDN	Host / Cloud	Mailbox Provider	ESP	Platform	Registrar	Reseller	Privacy / Proxy	Registry	Registrant	Law Enforcement	Authoritative DNS Operator	DNS-Resolver Operator	DNS-Zone Operator
Infrastructure Harms																			
Intrusions																			
Private / Unprivate Account Compromise		x		x															
Application Compromise		x		x															
Drive By Infections		x		x															
Rogue DNS Resolver Configuration		x		x															
BGP Hijacking of Authoritative / Recursive DNS Server			x		x	x	x										x		
Illegal Access to Other Computers or Networks			x	x			x	x		x									
Hybrid Harms																			
Phishing*/ Pharming*			x	x				x	x										
Spam*			x	x				x	x										
(Malicious) Information Gathering																			
Scanning		x																x	
Sniffing			x	x															
Social Engineering			x	x															
Information Content Security																			
Unauthorised Access to Information			x	x															
Unauthorised Modification of Information			x	x															
Unauthorised Disclosure			x	x															
Other																			
Abusive Domain Name Registrations			x								x			x					
Illegal Domain Registration			x								x			x					
Compromised Domain (legitimate domains pointing at compromised hosting)			x				x								x				
Fast Flux Hosting			x								x			x					
Domain Hijacking			x								x			x					
Typosquatting			x								x			x					
Exfiltration via the DNS		x															x	x	
DNS Reflection Attack	x				x												x	x	x
Email Configuration Identity Theft via DNS		x																	
Cache Poisoning	x				x		x										x	x	x
Men-in-the-Middle-Attacks	x	x															x	x	x
Downgrade Attacks (e.g. leverage DANE)		x															x	x	x

* The topDNS Initiative endorses the Framework to Address Abuse. According to the framework, DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS: malware, botnets, phishing, pharming, and spam. While spam alone is not considered as DNS Abuse, the framework includes it in the five key forms of DNS Abuse when it is used as a delivery mechanism for the other four forms of DNS Abuse.

The technical community adopts a more restrictive approach on the definition of different types of abuse. The column "DNS Abuse?" reflects this approach, which only considers specific types of abuse that solely target DNS infrastructure. The Framework to Address Abuse is more inclusive.

Specifically, even without a court order, the signatories of the framework believe a registry or registrar should act to disrupt the following forms of Website Content Abuse: (1) child sexual abuse materials ("CSAM"); (2) illegal distribution of opioids online; (3) human trafficking; and (4) specific and credible incitements to violence.