Definition of Domain Name System Abuse

May 16, 2023

SPONSORING COMMITTEE: Internet Committee

RESOLUTION:

WHEREAS, Domain Name System Abuse ("DNS Abuse") poses a significant and present threat to global enterprises, their business partners and consumers and often involves the misuse of brands, trademarks, and related intellectual property;

WHEREAS, the definition of DNS Abuse remains unclear within the private sector, governmental bodies, and academia;

WHEREAS, certain definitions do not sufficiently protect consumers and brand owners from deceptive and illegal activity, while other definitions provide unduly vague standards that may not sufficiently protect lawful speech;

WHEREAS, certain definitions do not account for emerging technologies;

AND WHEREAS, the International Trademark Association ("INTA"), on behalf of its members, can advance a standard definition of DNS Abuse that will allow brand owners to protect their brands when they are targeted;

BE IT RESOLVED, that it is the position of INTA that "DNS Abuse" should be understood and defined as "***any activity that makes, or intends to make, use of domain names, the Domain Name System protocol, or any digital identifiers that are similar in form or function to domain names to carry out deceptive, malicious, or illegal activity."***

BACKGROUND:

DNS Abuse is a significant threat to global enterprises, their business partners and consumers and often involves the misuse of trademarks to perpetuate fraud, theft, and intellectual property infringement. DNS Abuse allows bad actors to perpetuate scams and steal from consumers while infringing trademark owners' valuable brands. DNS Abuse refers to the malicious or inappropriate use of domain names or the DNS for nefarious purposes, including phishing, spamming, distributing malware, or conducting fraudulent activities. DNS Abuse can take many forms, not limited to cybersquatting, typosquatting, DNS/domain hijacking, domain shadowing (when malicious subdomains are used under compromised domains), and domain spoofing (domain names that appear familiar but are not originating from the legitimate intellectual property rights holder).

Perpetrators of DNS Abuse know that domain names often represent the digital “front door” that customers and business partners associate with a company’s products, email communications, and corporate persona.[1] These bad actors register malicious domains by using names that are similar to legitimate domain names or trademarks, or by compromising or hijacking legitimate domains.

In 2022, the EU Commission published the EU Study on DNS Abuse.[2] The study examined the causes and mitigation steps that should be taken to help curb the threat of DNS Abuse. The Commission has been clear in public meetings that if the proposed suggestions on mitigation are not voluntarily adopted by the private sector, they may consider new legislation. Therefore, a comprehensive, concise, and workable definition will become critical to potential new regulations and enforcement.

In March of 2023, the U.S. announced an affirmative National Cybersecurity Strategy commitment to secure critical infrastructure, such as cloud services, domain registrars, email, hosting providers, other digital services, and the DNS.[3] Both are encouraging developments for proponents of online consumer safety and brand owners because phishing attacks, business email compromise, wire transfer fraud and other related scams often involve DNS Abuse containing “trusted” brand names. US policy development will also require a comprehensive, concise, and workable definition of DNS Abuse.

Other Definitions of DNS Abuse

Other organizations have acknowledged that DNS Abuse is a problem, but their definitions could exclude intellectual property issues such as infringement and piracy or are vague and impractical. These include the following:

- EU Commission Study (published 1/31/22)[2]:

  > “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.”

- Internet Corporation for Assigned Names and Numbers (ICANN) Specification 11 of Registry Agreement [4:]

  > “…Malware, botnets, phishing, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law… “

- DNS Abuse Voluntary Framework[5] (definition adopted by the Domain Name System Abuse Institute, which is funded by operator of .org):

> Malware, Botnets, Phishing, Pharming, or SPAM that delivers Malware, Botnets, Phishing, or Pharming.

> The Voluntary Framework has also been signed by various members of the domain name industry and the private sector. Private sector signatories include INTA members who consider this definition to serve as a “floor” not a “ceiling” for combatting DNS Abuse.

Why INTA Needs Its Own Definition

While other definitions capture much of what the technical community acknowledges as abuse (potentially more than half), they do not capture all the abuses that affect and harm consumers and our members. For example, limiting DNS Abuse to “technical violations” does not extend to pirated material unless and until it is proven to contain a “technical violation,” such as malware, even though (a) it is illegal, (b) harms intellectual property owners, and (c) is likely also to contain technical violations.

On the other hand, while the EU Commission’s definition for addressing harm is understandable, its use of overly broad “harmful” language does not provide sufficient concrete guidance.

As a leading voice for brand owners, INTA believes that it is imperative to formally adopt a definition of DNS Abuse. This will shed much needed light on the harm of DNS Abuse within the legal and domain name communities to ensure that they and relevant domain name governance organizations take steps to provide relief for brand owners and the consuming public, which all forms of DNS Abuse harm. In this effort, INTA supports global policy makers and thought leaders who highlight the global systemic risks associated with the manipulation of the DNS especially when this activity weaponizes “trusted” brand names.

INTA recognizes that the risk for abusive practices extends to alternative identifiers that are similar in form or function to domain names. The providers of alternative identifiers such as Web3 Domains are not bound by rights protection mechanisms like the Uniform Dispute Resolution Policy (UDRP). In anticipation of IP rights being extended to new and emerging technologies, INTA supports a forward-thinking definition of DNS Abuse that anticipates new technologies.

Further, INTA is concerned that DNS Abuse is likely to increase significantly following the ICANN’s planned second round of new gTLDs. And non-traditional domain names, such as those on the blockchain, have virtually no rights protection mechanisms, which makes defining and fighting DNS Abuse for these new domain names critical for protecting brand owners.

One of the most prevalent forms of DNS Abuse is phishing. In the second quarter of 2022, the Anti-Phishing Working Group (APWG) observed 1,097,811 total phishing attacks, a record at the time. In the third quarter of 2022, APWG observed 1,270,883 total phishing attacks, a new record and the worst quarter for phishing that APWG has ever observed.[6]

According to a Palo Alto Networks' Unit42 report, in 2021, one in five aged domain names was malicious, risky, or unsafe.[7]

Another 2021 study reported that more than 7 out of 10 organizations have experienced a DNS attack within the last 12 months.[8] In 2022 phishing attacks rose by 61%, and furthermore phishing associated with cryptocurrencies dramatically increased by 257%.[9]

A CSC report, *Threatening Domains of the Top 10 Most Valuable Brands*, found that 99% of the identified domain names that closely matched legitimate brand names were owned by third parties.[10] This followed up on a report that shows that more than 7 out of 10 domain names that contain brand names on the internet are not owned by the actual brand owners.[11] This resulting chronic abuse of domain names adds a layer of significant risk that can harm the security, consumer safety, intellectual property, and revenue of victim companies.

CSC's *Domain Security Report* also shows that most organizations overlook preventive domain security protections that safeguard against takeover of domains, phishing, and related attacks. Nearly 75% of the Forbes Global 2000 have implemented less than half of the domain security measures CSC analyzed, such as DMARC, DNSSEC and Domain Registry Lock.[12]

As DNS Abuse and cyber risks continue to increase, organizations and cyber insurers face greater challenges in quantifying them and addressing their capacity for harm. By some estimates, ransomware alone costs companies billions annually.[(1 and 13)]

It is imperative that INTA and its members be prepared to fight and help prevent DNS Abuse. We therefore believe it is essential for INTA to adopt and socialize a workable definition that effectively protects end-users, including consumers, and the brands they trust.

ENDNOTES

1. https://www.rmmagazine.com/articles/article/2022/09/29/how-to-reduce-the-risk-of-web-domain-attacks
2. https://data.europa.eu/doi/10.2759/616244
3. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
4. https://www.icann.org/resources/pages/advisory-registry-agreement-spec-11-3b-2017-06-08-en
5. https://dnsabuseframework.org/media/files/2020-05-29_DNSAbuseFramework.pdf
6. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf?_ga=2.260996110.2054624729.1678125575-191591588.1678125575&_gl=1*1wgs7p*_ga*MTkxNTkxNTg4LjE2NzgxMjU1NzU.*_ga_55RF0RHXSR*MTY3ODEyNTU3NS4xLjEuMTY3ODEyNTYwNi4wLjAuMA
7. https://www.bleepingcomputer.com/news/security/silent-danger-one-in-five-aged-domains-is-malicious-risky-or-unsafe/#:~:text=A%20report%20from%20Palo%20Alto,are%20unsafe%20for%20work%20environments.
8. https://neustarsecurityservices.com/resources/whitepapers/cybercrime-economy-threats-trends-report
9. https://interisle.net/PhishingLandscape2022.pdf
10. https://www.cscdbs.com/assets/pdfs/Threatening-Domains-Targeting-the-Top-10-Most-Valuable-Brands.pdf

11. https://www.cscdbs.com/blog/domain-security-zero-trust-model/
12. https://www.cscdbs.com/assets/pdfs/Domain-Security-Report-2022.pdf
13. https://www.securityinfowatch.com/cybersecurity/article/21250614/the-realities-of-domain-security