Perspective on DNS Abuse

Javier Rúa-Jovet

ccTLD News Session

27 May 2021

Quick Intro & Disclaimers

©FreePik

Please install current anti-virus software!

Please delete emails that are to good (or bad) to be true!

What is DNS Abuse?

There is no consensus based, community-wide definition.

One general starting point for conversation & discussion:

"DNS Abuse" could be generally thought of as any "malicious activity aimed at disrupting the DNS infrastructure or causing the DNS to operate in an unintended manner". […] https://www.icann.org/en/icann-acronyms-and-terms/domain-name-system-abuse-en

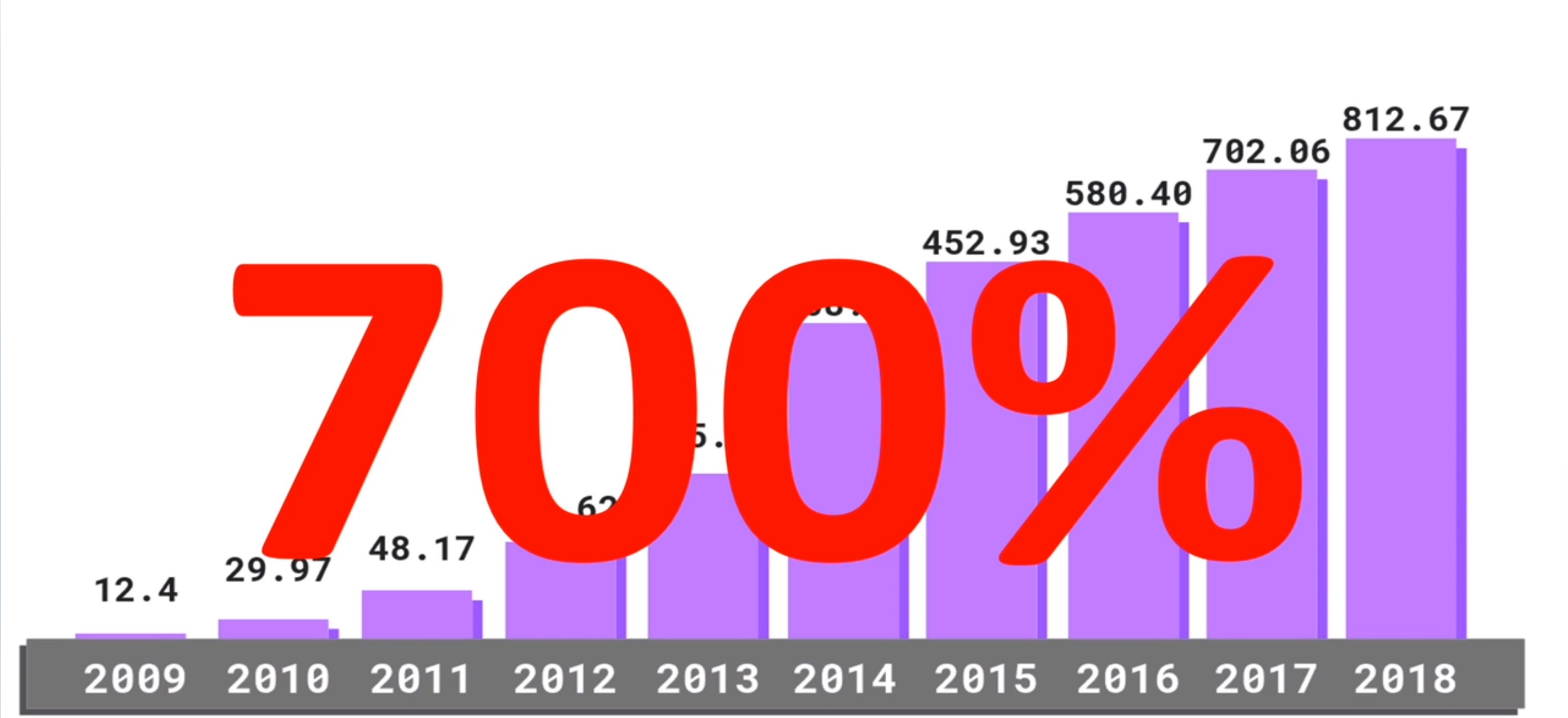
DNS Abuse in ICANN Bylaws?

- “...[E]nsure the *stable and secure operation* of the Internet's unique identifier systems…”
- “…[F]acilitate the openness, interoperability, resilience, *security and/or stability* of the DNS…” Sec. 1.1(a). Mission, ICANN Bylaws (11/28/19)https://www.icann.org/resources/pages/governance/bylaws-en/#article1

- “ICANN shall perform a periodic review of the execution of its commitment to enhance the operational *stability, reliability, resiliency, security*, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet’s system of unique identifiers that ICANN coordinates (“SSR Review”).” ICANN Bylaws, Sec. 4.6(c)

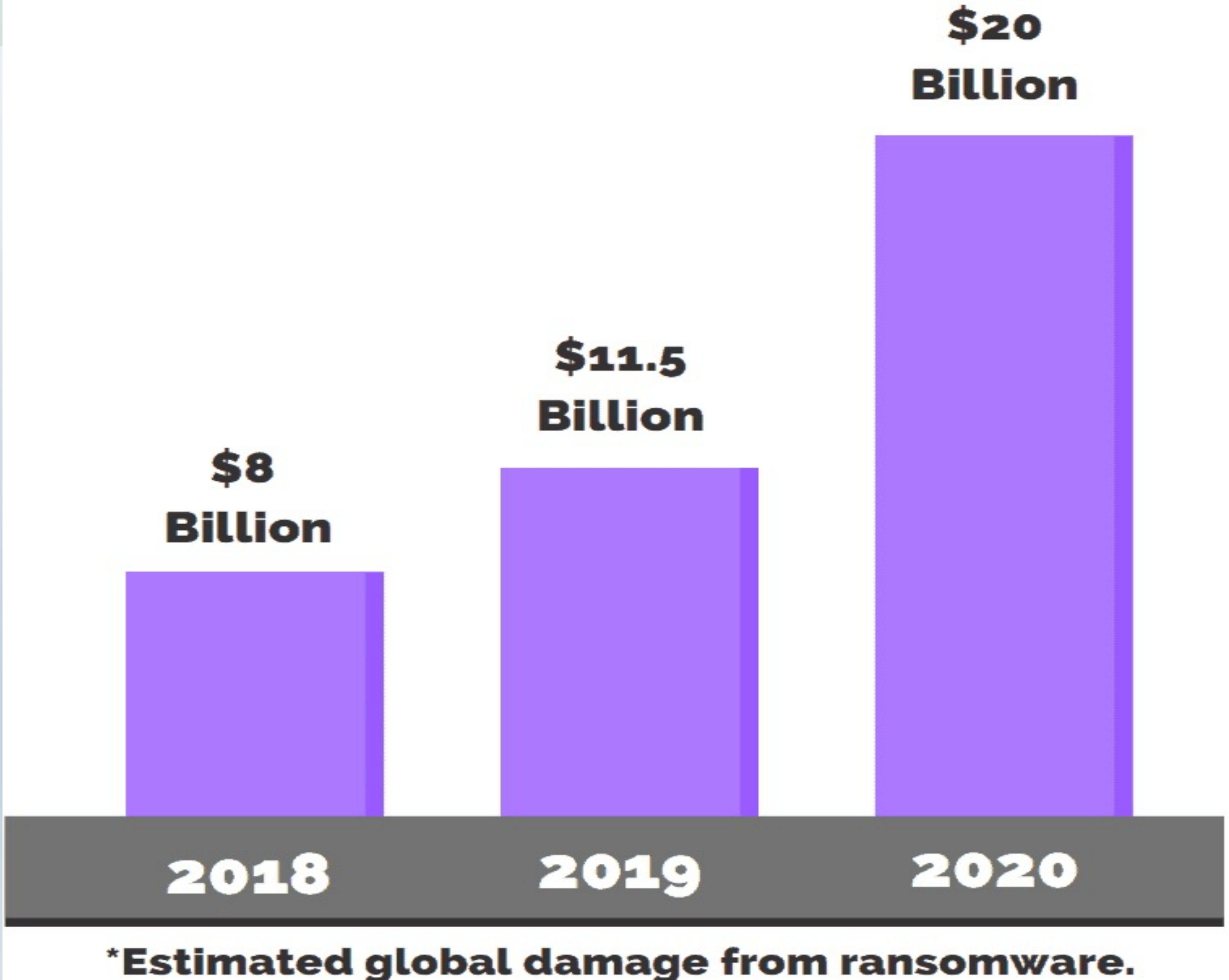
Why care about DNS Abuse?

Its pervasive & growing:



700%

Why care about DNS Abuse?



*Estimated global damage from ransomware.

Source: https://purplesec.us/cyber-security-trends-2021/

Some forms of DNS Abuse

- **Phishing:** Pages that masquerade as a trustworthy (e.g., a bank, known brand, online merchant or government agency) to infect a computer with malware or obtain sensitive information, such as login credentials.
- **Pharming**: When you enter a website, your browser checks DNS cache or a DNS server for the corresponding IP address. Pharmers "plant" malicious code, changing the IP address that corresponds to the domain name, redirecting victims to a fraudulent site designed that can look exactly like the user-intended, legitimate site.
- **Malware**: any software that performs unwanted an/or damaging activity, often for the benefit of a third party. Adware, spyware, and viruses are some well-known forms of malware. Ransomware is a growing threat.
- **Botnets**: A botnet is a collection of malware-infected software/code devices that can act in response to commands from a central attacker. Typically, a botnet central control instructs its botnets to extract information from their host systems or engage in malicious action such as a direct or a distributed denial-of-service (DoS) attack, that overwhelms a targeted system with spurious requests, making the system difficult or impossible for its intended users to reach.
- **Spam**: Generally, the practice of sending unwanted bulk email messages, frequently with commercial content by harvesting identifiers (domain names or addresses).

Combating DNS Abuse: DAAR

- ICANN monitors DNS Abuse across TLD registration activities via its ‘Domain Abuse Activity Reporting System’ (DAAR).
- DAAR continuously collects zone file data and from numerous reputation data feeds, to identify and keep track TLDs employed for “security threat activities”. https://www.icann.org/en/system/files/files/daar-monthly-report-04feb19-en.pdf

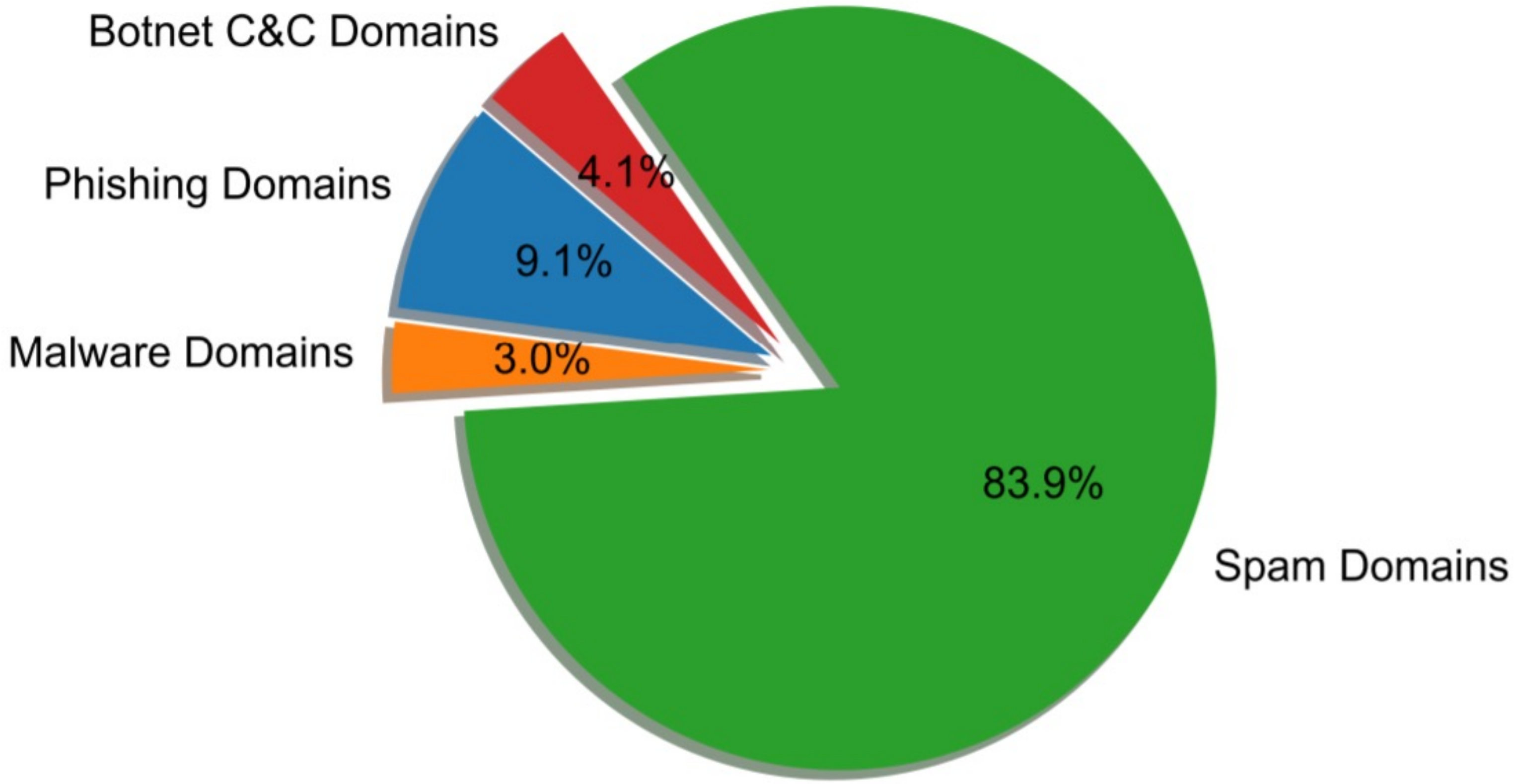
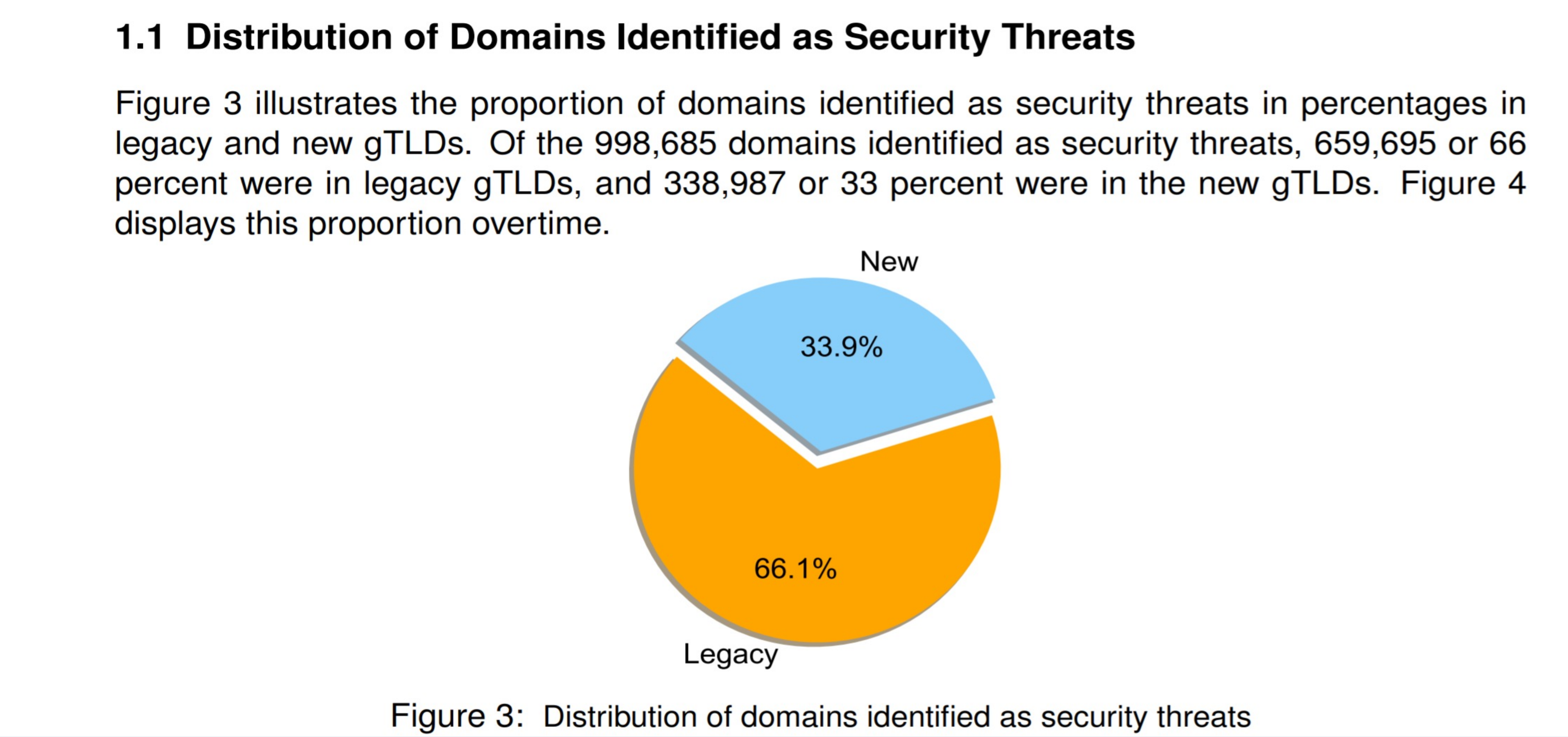


Figure 7: Breakdown of domains identified as security threats across all DAAR threat types



1.1 Distribution of Domains Identified as Security Threats

Figure 3 illustrates the proportion of domains identified as security threats in percentages in legacy and new gTLDs. Of the 998,685 domains identified as security threats, 659,695 or 66 percent were in legacy gTLDs, and 338,987 or 33 percent were in the new gTLDs. Figure 4 displays this proportion overtime.

Figure 3: Distribution of domains identified as security threats

Combating DNS Abuse: gTLDs

- ICANN Contractual Compliance is called to enforce certain contractual obligations set forth in ICANN’s policies and agreements.

- For example, gTLD Registry operators must periodically assess whether their gTLDs are being used to perpetrate security threats such as DNS abuse and report to ICANN, upon request (Base Registry Agreement, specification 11 3(a) &(b).

DNS Abuse & ccTLDs

- ccTLDs can and many do voluntarily adopt pertinent community practices; for example, ccTLDs can participate in DAAR and benefit from daily reports DAAR generates.
- As we all know, ccTLD Operators are self-regulating, bound only by the national and local laws of its territory, so each will have its own approach to dealing with the issues described commonly as DNS Abuse.

We shall all learn from their experiences & practices today!

¡Gracias!

jrj@conecta.pr / javrua@gmail.com