FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

European Commission's Study on Domain Name System (DNS) Abuse

Ivett Paulovics *Maciej Korczynski*

8 March 2022 – GAC PSWG Update/DNS Abuse session and Discussions on Subsequent Rounds

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

Agenda

1. Objectives
2. Methodology
3. Timeline
4. Definition
5. Magnitude
6. Good practices
7. Recommendations

1. Objectives

- **DNS abuse phenomenon** (definition, categories, role of actors, magnitude)
- **Policies, laws, industry practices**
- **Measures** (technical and policy) needed to address it

2. Methodology

- **Primary research**: real-time measurements, surveys, in-depth interviews, workshops
    - Real-time measurements: analysis of **2.7 million incidents** and **1.68 million abused domain names** using reputed domain and URL blacklists
- **Secondary research**: review of third-party reports

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

3. Timeline

4. Definition of DNS abuse

- Limit of the (many) terminologies used so far: **technical vs content-related threats** – often overlap (e.g., phishing, malware)

- **Our definition**:

> **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.**

- **Our approach**: bottom-up and distinction between
  - **maliciously registered domain names**
  - **compromised domain names**

4. Definition of DNS abuse

How do we categorize DNS abuse?

- **Type 1**: abuse related to **maliciously registered** domain names
- **Type 2**: abuse related to the operation of the DNS and other infrastructures
- **Type 3**: abuse related to domain names **distributing malicious content** (N.B. may take advantage of maliciously registered or compromised domain names!)

4. Definition of DNS abuse

Who should take action to mitigate DNS abuse?

1. Abuse related **maliciously registered domain names** (e.g., AGD used for C&C communication) (**Type 1**)

Remediation at **DNS level**: **Domain reseller (if any) → registrar → TLD registry**

2. **Malicious content**

   2.1 Malicious content distributed using a maliciously registered domain name (e.g., typosquatted domain serving phishing content) (**Type 1 & 3**)

Remediation at **hosting level**: **Hosting reseller (if any) → hosting provider** **AND** at **DNS level**: **Domain reseller (if any) → registrar → TLD registry**

   2.2 Malicious content distributed using compromised domain names (e.g., compromised domain serving phishing content) (**Type 3**)

Remediation at **hosting level**: **Site operator (if any) → registrant → hosting reseller (if any) → hosting provider**

3. Abuse related to **DNS operations** (e.g., DDoS attack against a DNS server) (**Type 2**) to be addressed **at DNS level**.

5. Magnitude of DNS abuse

Overall health of TLDs:

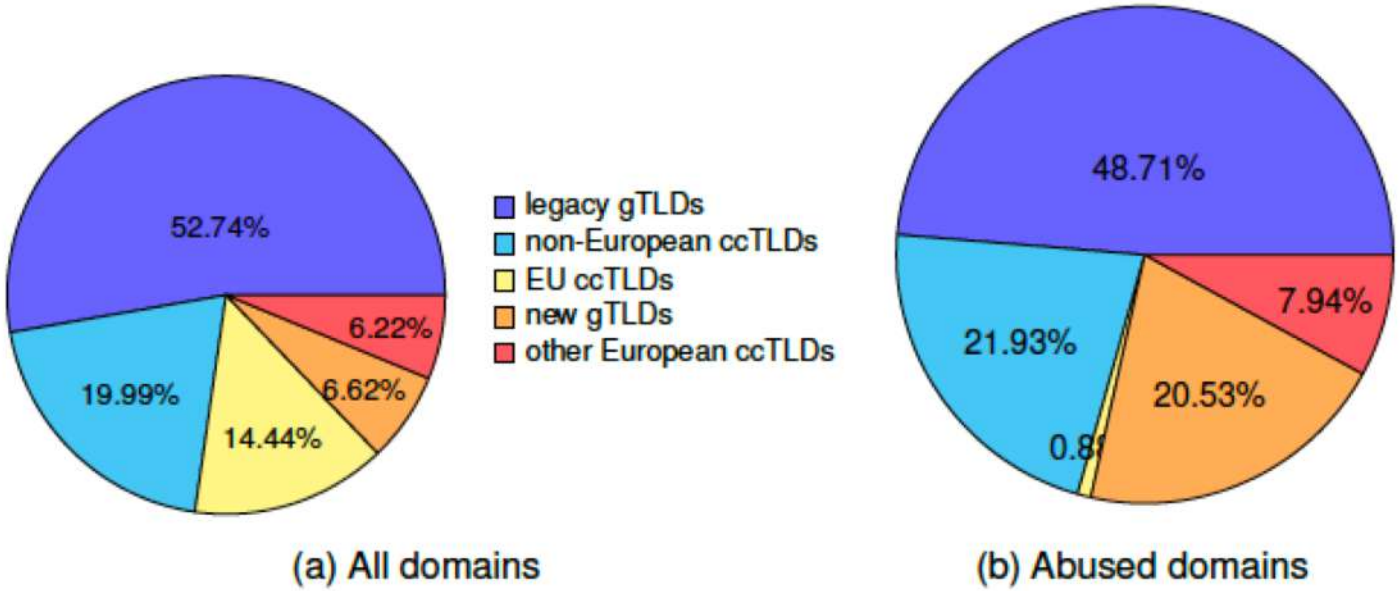

Figure 1: Divison of the domain namespace per TLD type

5. Magnitude of DNS abuse

Malicious vs. compromised domain names: where does the abuse occur?

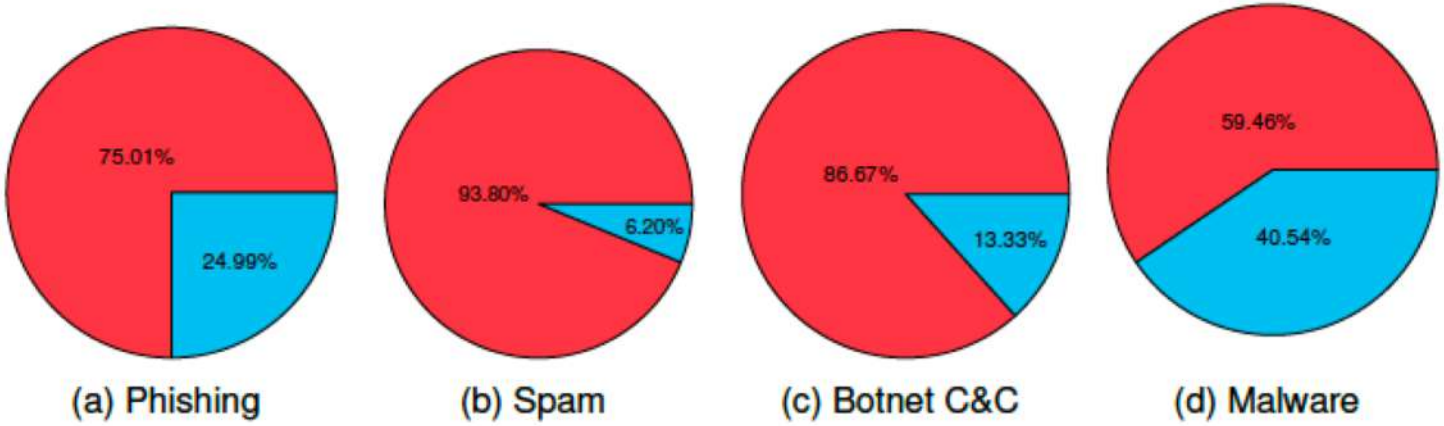

Figure 6: Distribution of compromised (blue) and maliciously registered (red) domain names per abuse type.

- About 25% of phishing domain names and 41% of malware distribution domain names are presumably registered by legitimate users, but compromised at the hosting level.
- The vast majority of spam and botnet command-and-control domain names are maliciously registered.

5. Magnitude of DNS abuse

Malicious vs. compromised domain names: where does the abuse occur?

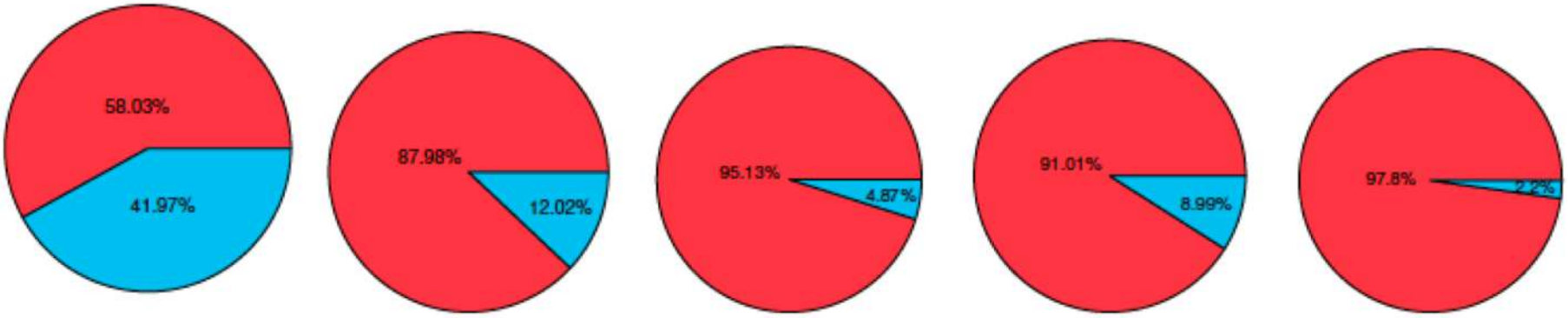

Figure 7: Distribution of compromised (blue) and maliciously registered (red) domain names per TLD type.

5. Magnitude of DNS abuse

Registrar reputation:

- the top five most abused registrars account for 48% of all maliciously registered domain names

Hosting provider reputation:

- hosting providers with disproportionate concentrations of spam domains reach 3,000 abused domains per 10,000 registered domain names

Adoption of DNS security extensions and email protection protocols:

- the overall level of DNSSEC, DMARC and SPF adoption remains low

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

6. Good practices

Type	Good practices	Example
Preventive	Anti-abuse / acceptable use policy	PIR, Donuts, .eu, .hu
	KYBC procedure	.eu, .dk
	Employment of machine learning predictive technology to identify abusive registrations	.eu, .nl
	Delayed delegation	.eu, .dk, .hu
	Cross-checks in public databases	.eu, .dk, .no
	Incentive programs (discount) to promote healthy registrations	PIR, .eu
	DNSSEC deployment and other security solutions	PIR, .eu, .dk, .nl, .se, .cz, .no, .sk
	Preventive blocking services	Donuts, UNR
Reactive	Regular WHOIS accuracy verification	.eu, .dk, .be, .no, .hu
	Manual content check	.eu
	Surveillance / search service	.be, .nl
	Collaborations with LEA and trusted notifiers	PIR, Donuts, .eu, .dk, .be
	Notice & take down procedures	.be, .nl
	Appeal mechanism against suspension before third neutral party	PIR
Transparency and information	**Publication of abuse metrics and statistics**	PIR
	Foreseeable response time to abuse reports	Donuts
	Easy to access information on how to report abuse / abuse point of contact	Donuts, .eu, .be, .fr, .at, .uk, .no
	Adherence to voluntary / self-regulatory initiatives promoting collaborations among DNS service providers	PIR, Donuts

7. Recommendations

Set of 27 recommendations in 6 areas for improvements of measures to mitigate DNS abuse

A. Better DNS metadata for identifying resources and their attribution to intermediaries

B. Contact information and abuse reporting

C. Improved prevention, detection, and mitigation of DNS abuse related to maliciously registered domain name (Type 1)

D. Improved detection and mitigation of DNS abuse related to malicious content (Type 3)

E. Better protection of the DNS operations and other infrastructures and preventing DNS abuse (Type 2)

F. DNS abuse awareness, knowledge building, and mitigation collaboration at EU level

Download the study here:

Main Report: https://op.europa.eu/s/vLE5

Technical Report: https://op.europa.eu/s/vLE6

Ivett Paulovics

paulovics@fasano.pro

Maciej Korczynski

maciej.korczynski@univ-grenoble-alpes.fr

FASANO PAULOVICS

SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA