FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

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

Ivett Paulovics

8 March 2022 – IPC Membership Meeting

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

Agenda

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

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

1. Objectives

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

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

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!)

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

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**.

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

5. Magnitude of DNS abuse

Overall health of TLDs:

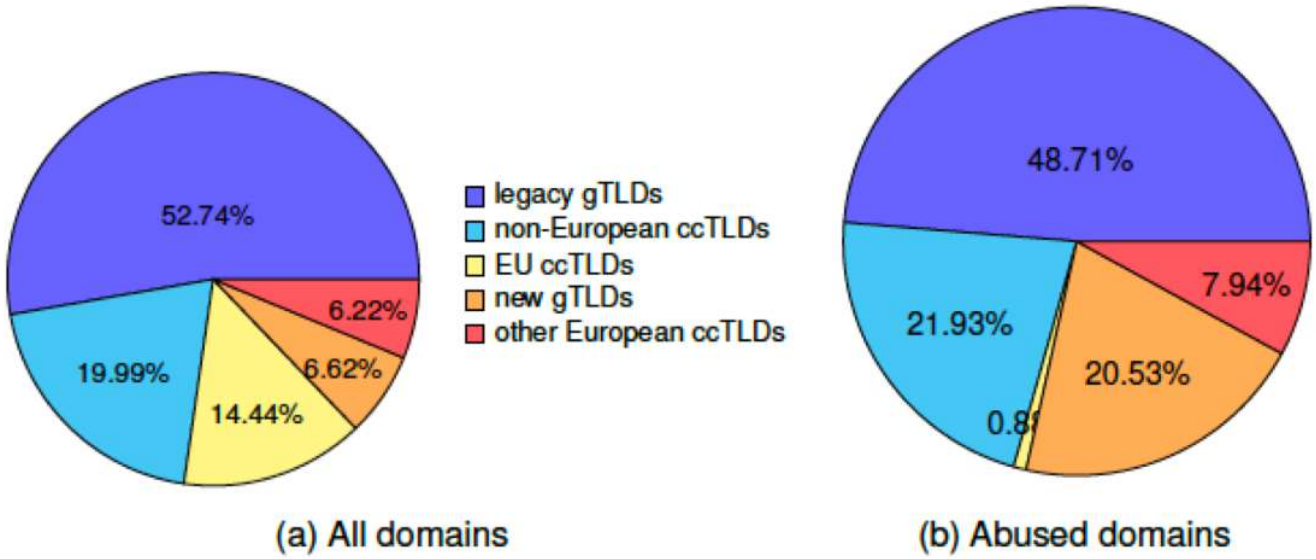

Figure 1: Divison of the domain namespace per TLD type

- EU ccTLDs are by far the least abused in absolute terms (0.8%) and relative to their market share (14.4%)
- In relative terms, new gTLDs, with an estimated market share of 6.6%, are the most abused the most abuse group of TLDs (20.5%)
- The two most abused new gTLDs combined account for 41% of all abused new gTLDs

5. Magnitude of DNS abuse

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

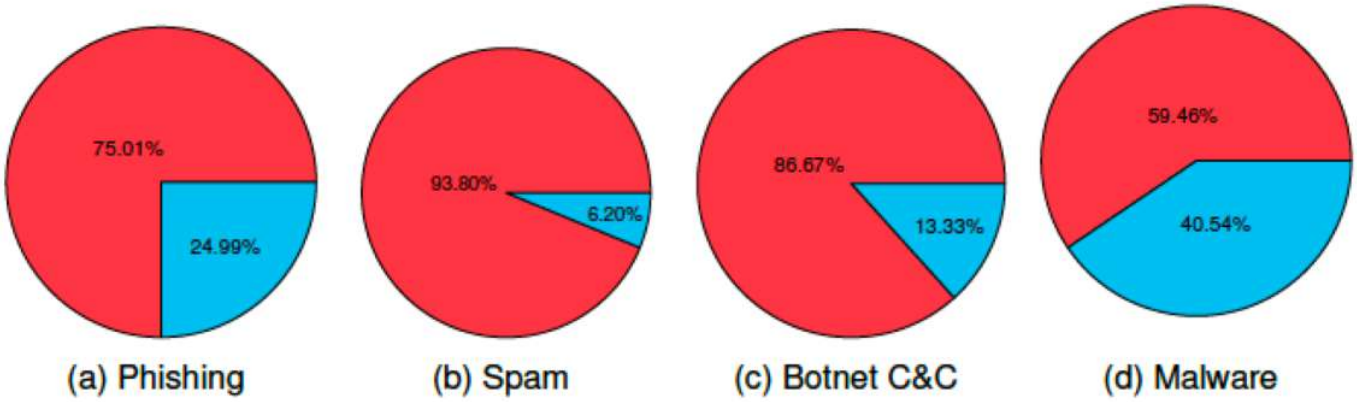

Figure 6: Distribution of compromised (blue) and maliciously registered (red) domain names per abuse type.

- About 25% of phishing 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?

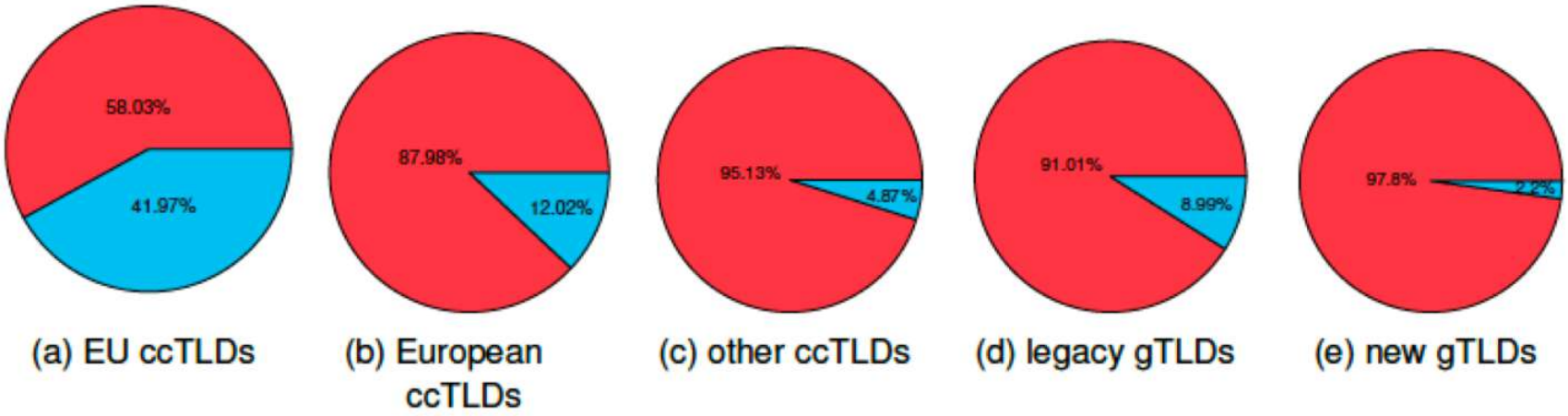

Figure 7: Distribution of compromised (blue) and maliciously registered (red) domain names per TLD type.

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

Magnitude of DNS abuse

Registrar reputation (maliciously registered domains):

Name	IANA ID	# of domains	Rate
NameCheap, Inc.	1068	131,925	121
GMO Internet, Inc. d/b/a Onamae.com	49	93,905	276
GoDaddy.com, LLC	146	53,185	8
NameSilo, LLC	1479	52,188	165
PDR Ltd. d/b/a PublicDomainRegistry.com	303	38,804	85
Alibaba Cloud Computing (Beijing) Co., Ltd.	420	35,242	62
PSI-USA, Inc. dba Domain Robot	151	23,485	181
ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	3775	22,139	321
Xin Net Technology Corporation	120	18,497	110
Hongkong Domain Name Information Management Co....	2251	16,000	800
Key-Systems GmbH	269	15,056	87
Dynadot, LLC	472	14,835	69
Web Commerce Communications Limited dba WebNic.cc	460	11,700	324
Launchpad.com Inc.	955	11,251	154
Eranet International Limited	1868	10,097	623

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

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

Magnitude of DNS abuse

Registrar reputation (maliciously registered domains):

Name	IANA ID	# of domains	Rate
Xi'an Qianxi Network Technology Co. Ltd.	3825	454	6,921
EIMS (Shenzhen) Culture & Technology Co., Ltd	2485	2,337	2,366
Tencent Cloud Computing (Beijing) Limited Liabi...	3755	2,315	2,351
Global Domain Name Trading Center Ltd	3792	892	1,231
FLAPPY DOMAIN, INC.	1872	1,538	1,097
DotMedia Limited	1863	925	1,037
DOMAINNAME BLVD, INC.	1870	903	1,001
DOMAIN ORIENTAL LIMITED	3252	428	972
DOMAINNAME FWY, INC.	1871	715	907
MainReg Inc.	1917	182	836
Hefei Juming Network Technology Co., Ltd	3758	3,180	798
Hongkong Domain Name Information Management Co....	2251	16,000	800
NICENIC INTERNATIONAL GROUP CO., LIMITED	3765	987	726
Hong Kong Juming Network Technology Co., Ltd	3855	8,478	721
Shinjiru Technology Sdn Bhd	1741	908	601

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

5. Magnitude of DNS abuse

Hosting provider reputation:

Spam		
AS	# Domains	Rate
GROUP-IID-01	12,282	3,430
Equinix Japan Enterprise K.K.	8,205	3,305
FEDERAL-ONLINE-GROUP-LLC	7,139	3,292
EONIX-COMMUNICATIONS-ASBLOCK-62904	9,165	3,009
Network-Transit	5,592	1979
SANREN DATA LIMITED	8,065	1,605
DataWeb Global Group B.V.	2,740	1,488
TIER-NET	2,577	1,331
SERVER-MANIA	2,133	1,312
H4Y-TECHNOLOGIES	1,332	1,275

Table 13: Top 10 AS with the highest absolute (# Domains) relative concentrations (Rate) of blacklisted domains grouped by their corresponding AS size (10k, 100k) and abuse type

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

5. Magnitude of DNS abuse

Targeted brands and names:

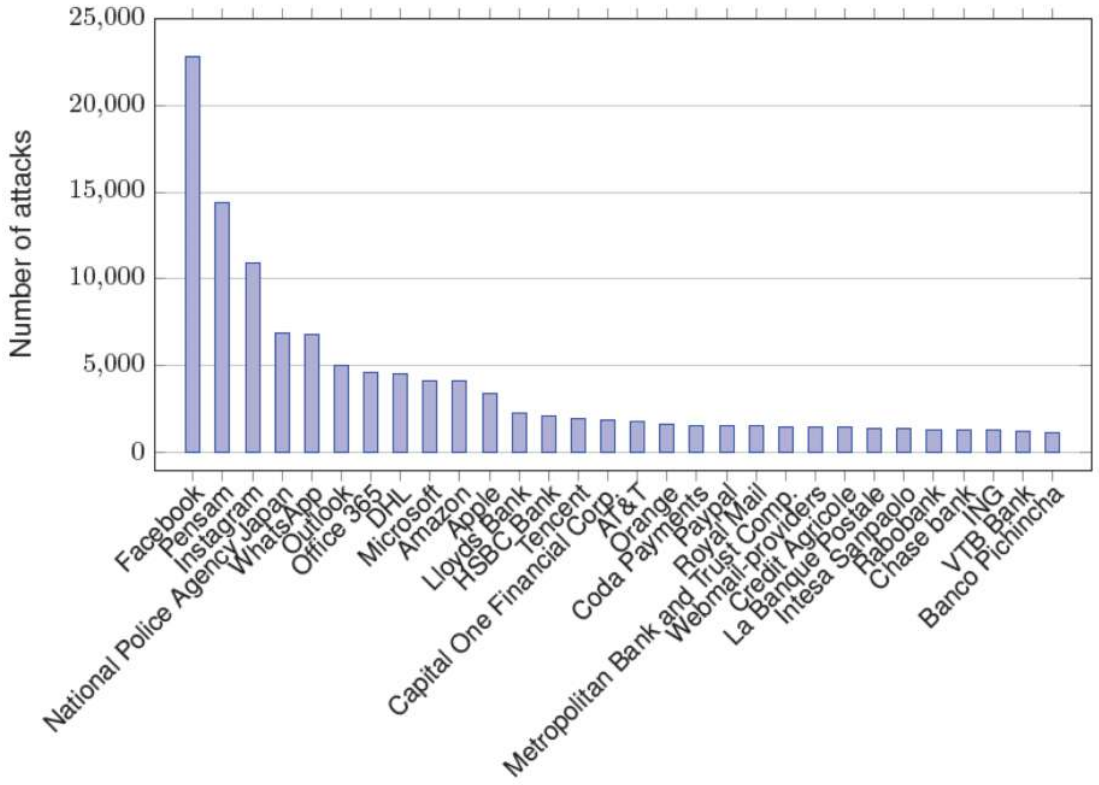

Figure 17: Top 30 most targeted brands.

- 30 most frequent brands in 405,431 URLs that were identified by APWG, PhishTank, and OpenPhish blacklists as phishing

5. Magnitude of DNS abuse

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

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

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

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

7. Recommendations

Registries – registrars – resellers:

- build standard (centralized) systems for abuse reporting
- verify accuracy of domain registration data (KYBC)
- use of predictive algorithms (or the like) to prevent abusive registrations
- identify registries/registrars/resellers with respect to concentration and rates of abuse in their ecosystems
- monitor abuse rates by independent researchers
- sanctions: revoke accreditation if abuse rates exceed predetermined thresholds
- incentives: financial rewards for lower abuse rates

FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

7. Recommendations

Hosting providers:

- identify hosting providers with respect to concentration and rates of abuse and hosting infrastructure abuse in their ecosystems
- monitor of abuse rates by independent researchers
- abuse rates not to exceed predetermined thresholds
- encourage development financial or technical solutions to effectively curb hosting and content abuse
- employ advanced prevention/remediation techniques to quickly curb abuses of hosting infrastructure and subdomain names

Collaboration, awareness and knowledge building at EU level:

- harmonize ccTLD operation by adoption of good practices
- require cooperation with gov't institutions, LEAs and trusted notifiers
- encourage awareness raising, knowledge building to make affected parties aware of existing measures tackling DNS Abuse

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

FASANO PAULOVICS

SOCIETÀ TRA AVVOCATI