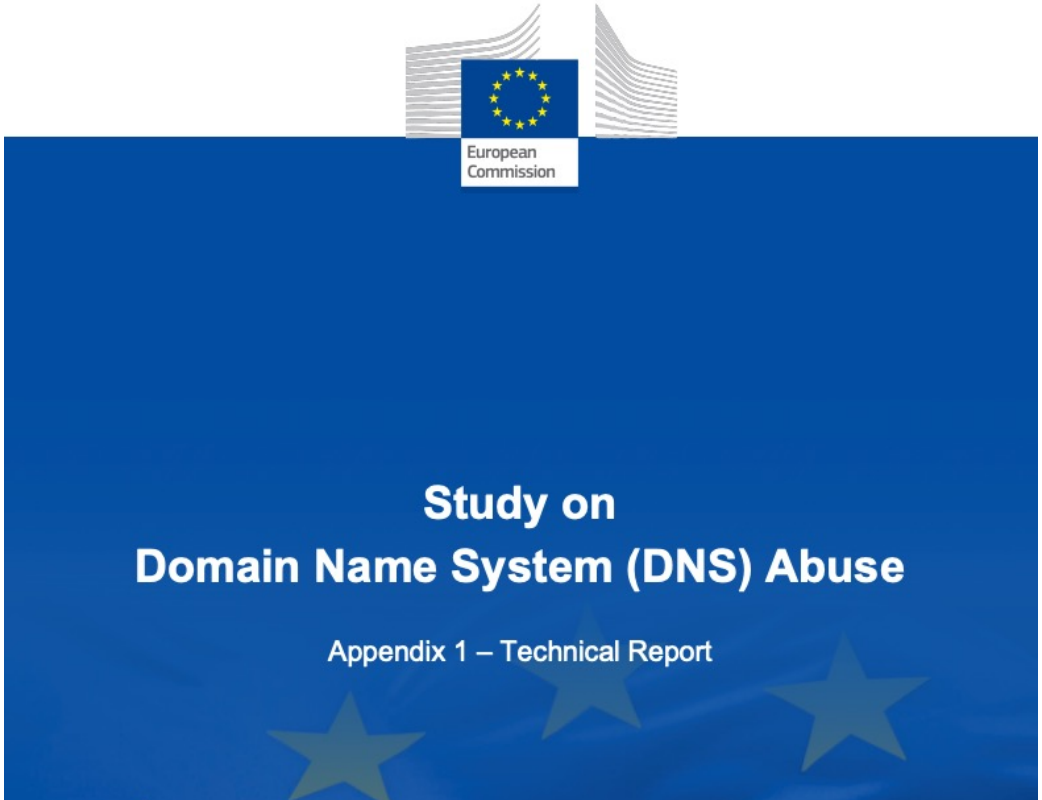
FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

EC Study on Domain Name System (DNS) Abuse

Maciej Korczyński, Jan Bayer, Yevheniya Nosyk, Olivier Hureau, Simon Fernandez, Ivett Paulovics, Andrzej Duda

March 8, 2022



FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

Agenda

1. Objectives
2. Methodology
3. Definition of DNS abuse
4. Role of Intermediaries in Abuse Handling
5. Magnitude of DNS abuse
6. Recommendations for improvements of measures to mitigate DNS abuse

Objectives

- DNS abuse phenomenon (definition, categories, role of actors, magnitude)
- Policies, laws, industry practices
- Recommendations for improvements

Methodology

- **Primary research**: real-time measurements, surveys, in-depth interviews, workshops

    - Real-time measurements and analysis of **2.7 million incidents** and **1.68 million abused domain names** using reputed domain and URL blacklists (APWG, Phishtank, OpenPhish, URLhaus, ThreatFox, SpamHaus, SURBL)

- **Secondary research**: review of third-party reports

Definition of DNS abuse

- Typologies and terminologies used → **a clear distinction *technical* vs *content-related* abuse cannot be made** (e.g., phishing and 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
  1. maliciously registered domain names
  2. compromised domains (mainly websites)

Definition of DNS abuse

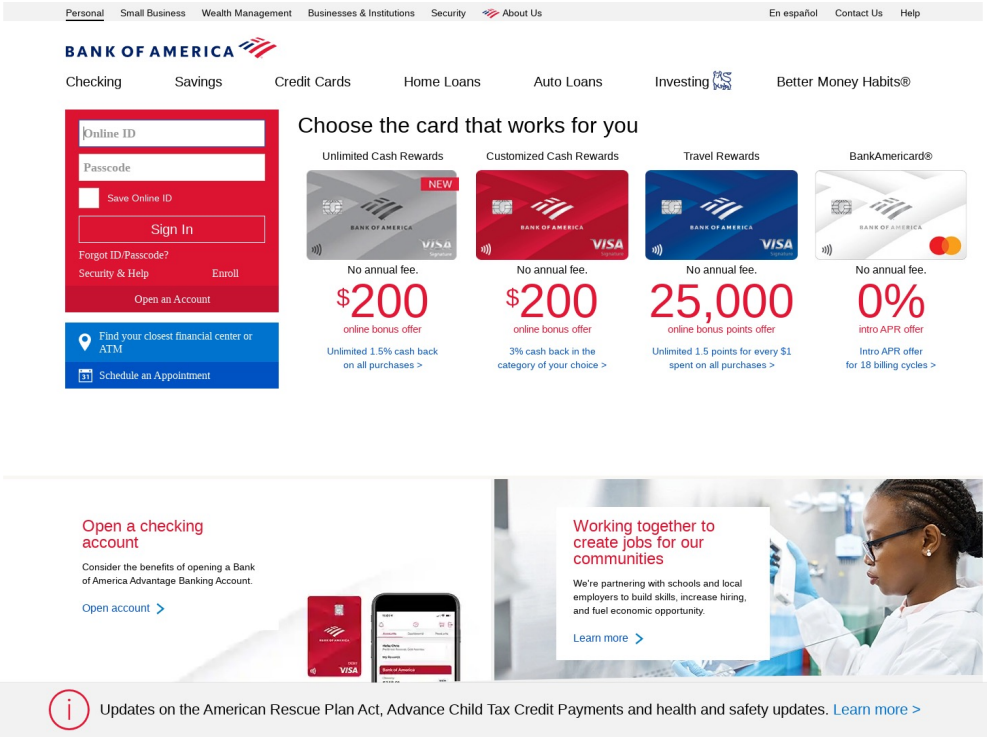
How do we categorize DNS abuse?

- **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** (may take advantage of compromised or maliciously registered domain names!)

Definition of DNS abuse

Examples of common DNS abuse cases

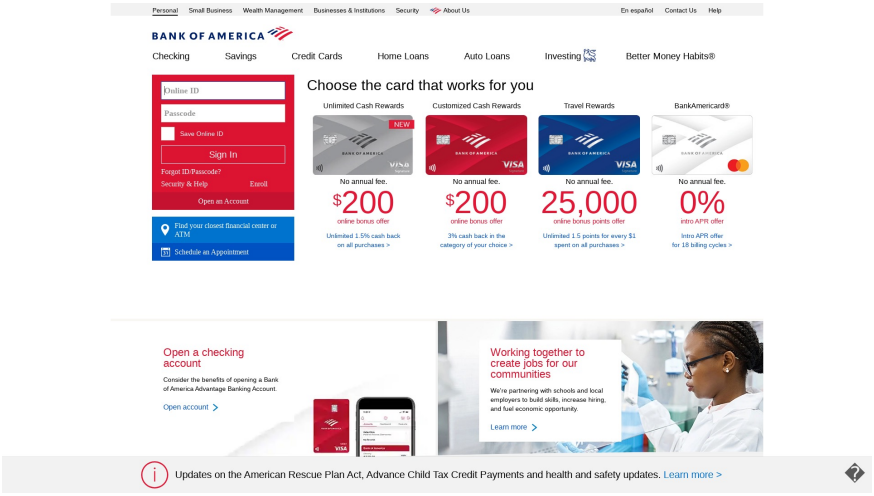
https://boaupdate.bfaoscr.com/www.bankofamerica.com/bofa22_ssl=2.149513588.33295 3745.165491523-611276082.1621298523/



Definition of DNS abuse

Examples of common DNS abuse cases

https://boaupdate.bfaoscr.com/www.bankofamerica.com/bofa22_ssl=2.149513588.332953745.165491523-611276082.1621298523/



bfaoscr.com

No content on the registered domain

```
Blacklisting Date: 2022-01-15 07:00:05

WHOIS:
Updated Date: 2022-01-13T16:46:37Z
Creation Date: 2022-01-13T16:46:37Z
```

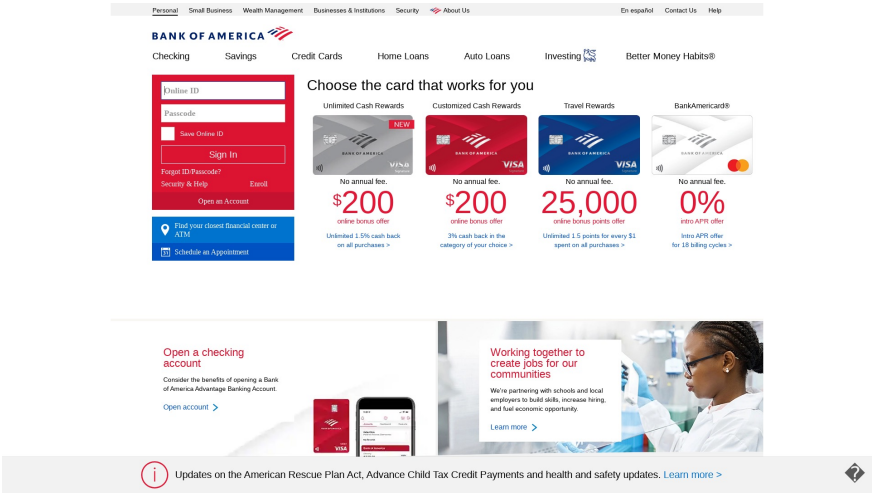
FASANO PAULOVICS
SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

Definition of DNS abuse

Examples of common DNS abuse cases

https://boaupdate.bfaoscr.com/www.bankofamerica.com/bofa22_ssl=2.149513588.332953745.165491523-611276082.1621298523/



bfaoscr.com

No content on the registered domain

```
Blacklisting Date: 2022-01-15 07:00:05

WHOIS:
Updated Date: 2022-01-13T16:46:37Z
Creation Date: 2022-01-13T16:46:37Z
```

Type 1 (maliciously registered domain name) but it's also **Type 3** (used to distribute illegal/abusive content): phishing of credentials, trademark and copyright infringement

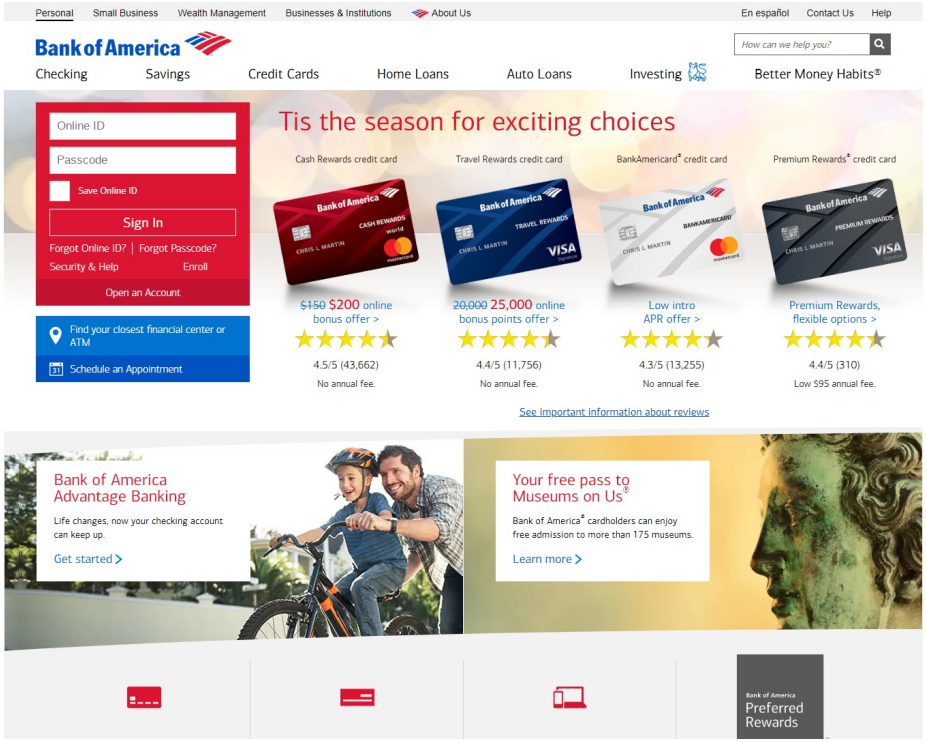
What intermediary should mitigate?

DNS service operator (registrar, registry)… and hosting provider!

Definition of DNS abuse

Examples of common DNS abuse cases

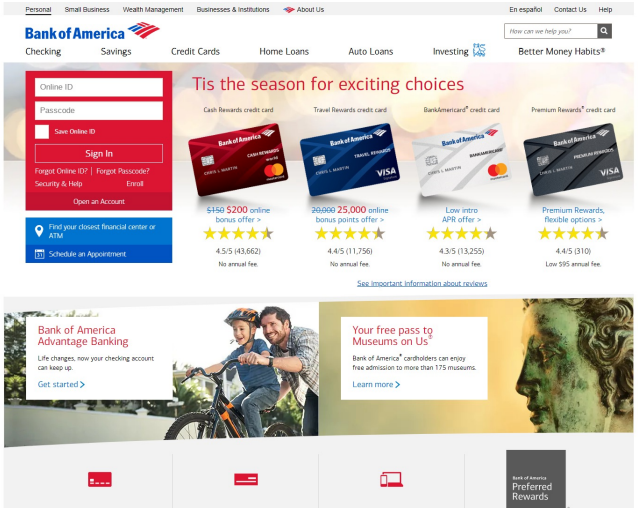
https://huletradgard.se/wp-includes/js/jcrop/cgi/BOfA/80c8cca2841aef7411dcf78a72791526/login.php?cmd=login_submit&id=c89c08bfeeea2f958007edefb48134f8c89c08bfeeea2f958007edefb48134f8&session=c8...



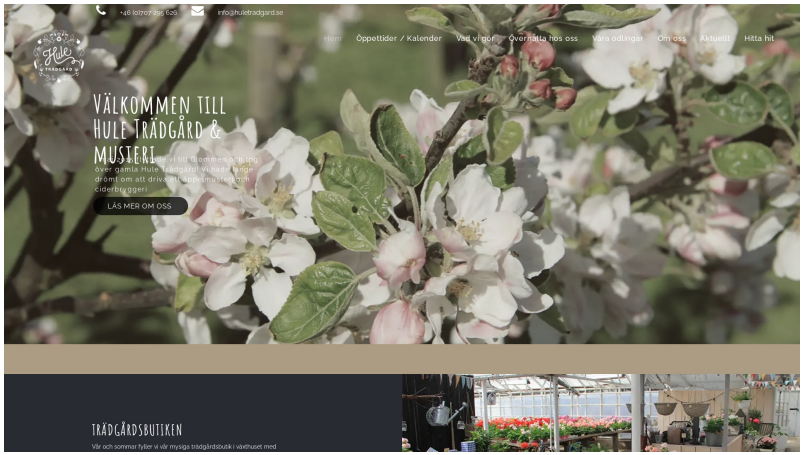
Definition of DNS abuse

Examples of common DNS abuse cases

https://huletradgard.se/wp-includes/js/jcrop/cgi/BOfA/80c8cca2841aef7411dcf78a72791526/login.php?cmd=login_submit&id=c89c08bfeeea...



https://huletradgard.se

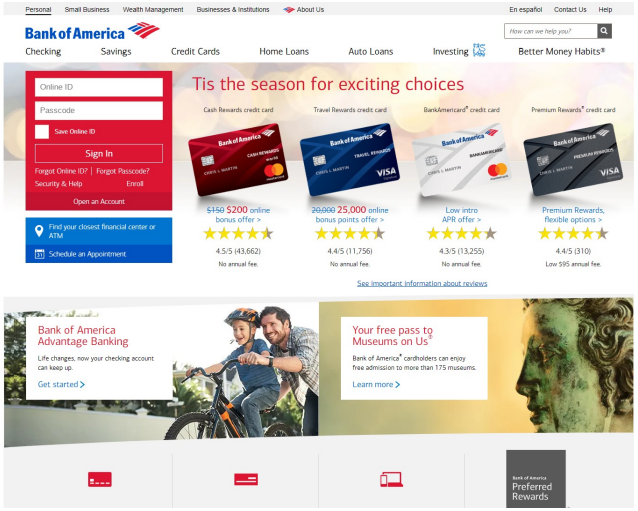



```
Blacklisting date: 2021-10-30 05:00:08
WHOIS
created: 2015-05-06
expires: 2022-05-06
```

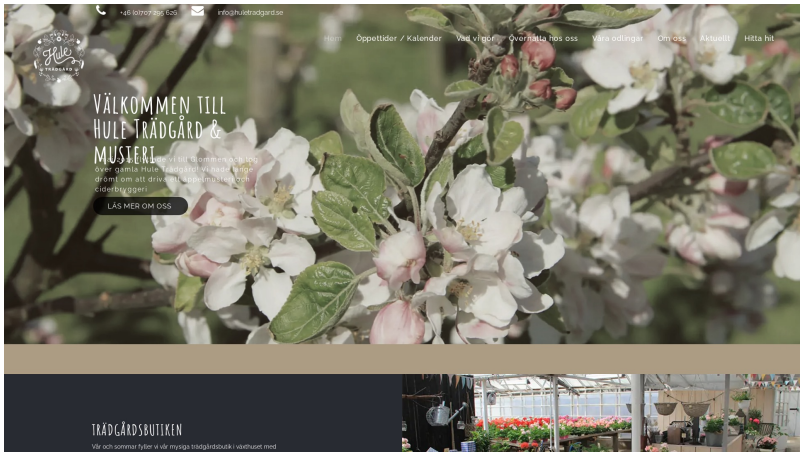
Definition of DNS abuse

Examples of common DNS abuse cases

https://huletradgard.se/wp-includes/js/jcrop/cgi/BOfA/80c8cca2841aef7411dcf78a72791526/login.php?cmd=login_submit&id=c89c08bfeeea...



https://huletradgard.se




```
Blacklisting date: 2021-10-30 05:00:08
WHOIS
created: 2015-05-06
expires: 2022-05-06
```

~~**Type 1** (maliciously registered domain name) but it's also~~ **Type 3** (abused to distribute illegal/abusive content): phishing of credentials, trademark and copyright infringement

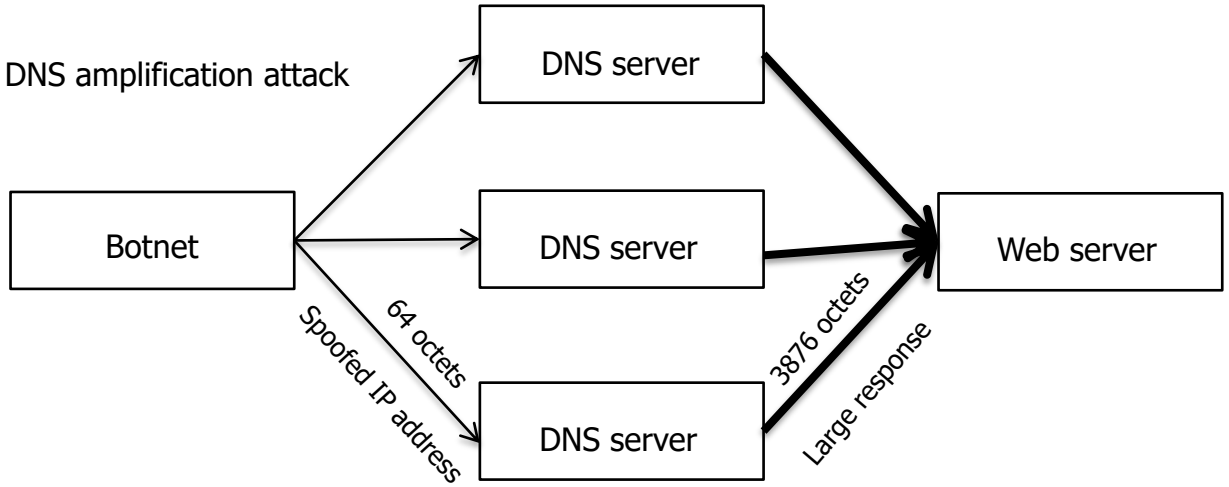
What intermediary should mitigate?

~~DNS service operator (registrar, registry)…~~ hosting provider and the owner/administrator

Definition of DNS abuse

Examples of common DNS abuse cases

Problem: Modern DDoS attacks abuse UDP-based network protocols to launch distributed reflection and amplication DoS attacks (DRDoS) that exceed hundreds of Gbps in traffic volume.



Type 2 (abuse related to the operation of the DNS and other infrastructures**)**

What intermediary should prevent?

Operators of misconfigured open DNS resolvers

Role of Intermediaries in Abuse Handling

Who should take action to mitigate DNS abuse?

1. Abuse related maliciously registered domain names (**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 (**Type 1 & 3**)

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

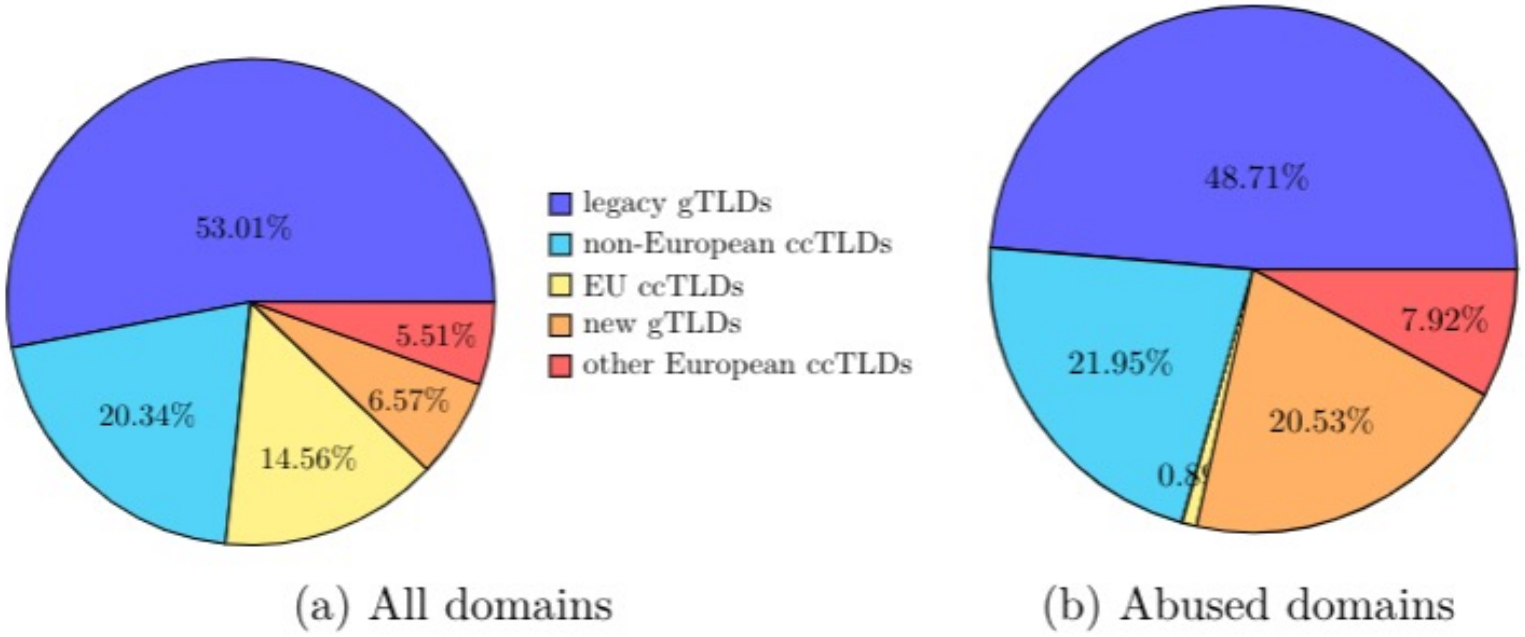
    2.2 Malicious content distributed using compromised websites (**Type 3**)

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

3. Abuse related to DNS operations (**Type 2**) to be addressed **at DNS level**.

Magnitude of DNS abuse

Overall health of TLDs:



- In relative terms, new generic Top-Level Domains (new gTLDs), with an estimated market share of 6.6%, are the most abused group of TLDs
- Not all new gTLDs suffer from DNS abuse to the same extent. The two most abused new gTLDs combined account for 41% of all abused new gTLD names
- European Union country code TLDs (EU ccTLDs) are by far the least abused in absolute terms and relative to their overall market share

Magnitude of DNS abuse

Compromised (websites) vs. maliciously registered domain names

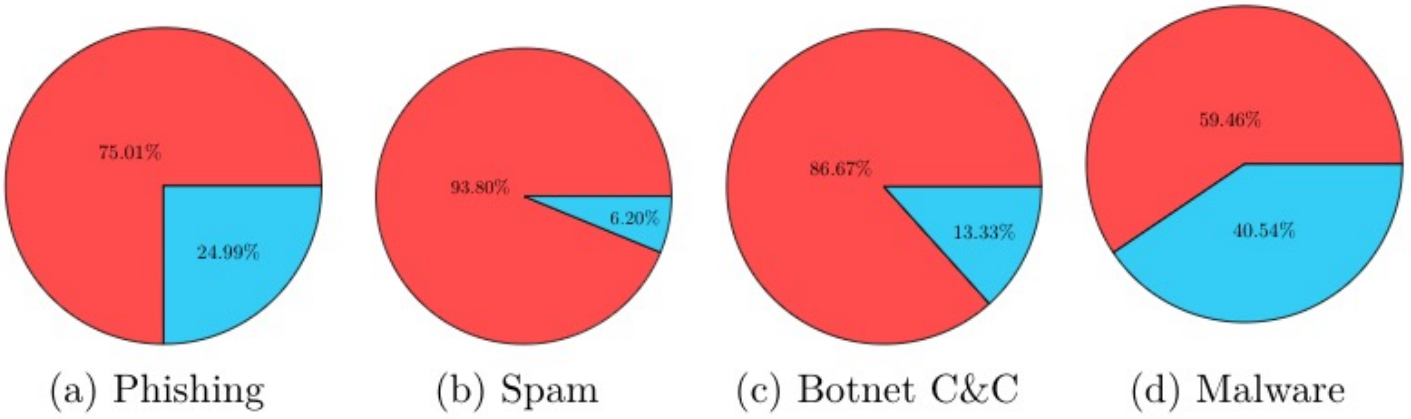


Figure 6: Distribution of compromised (blue) and maliciously registered (red) domain names per abuse type.

- The vast majority of spam and botnet command-and-control domain names are maliciously registered.
- 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.

Magnitude of DNS abuse

Compromised (websites) vs. maliciously registered domain names

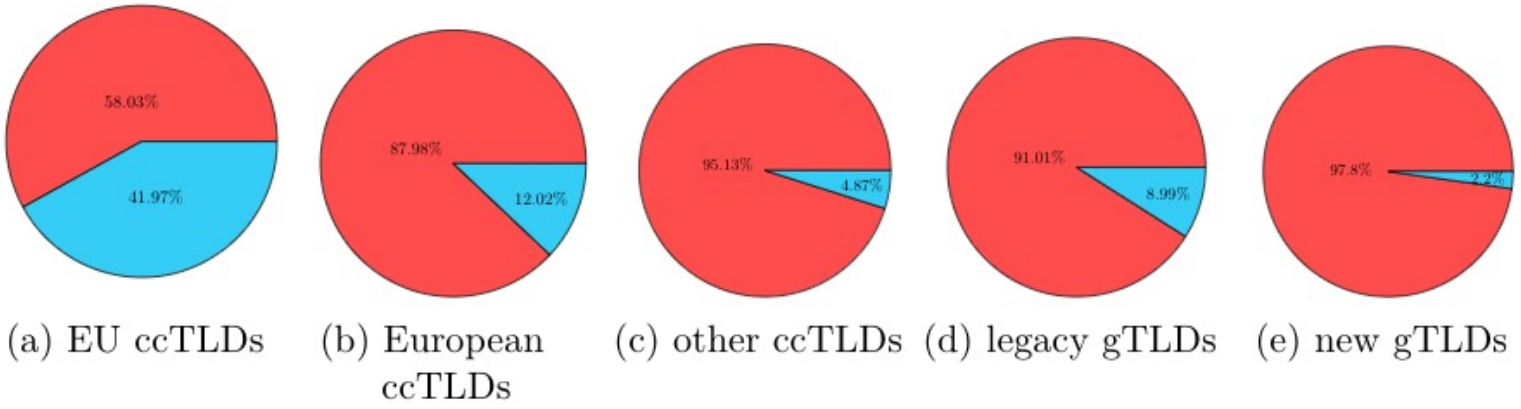


Figure 7: Distribution of compromised (blue) and maliciously registered (red) domain names per TLD type.

Magnitude of DNS abuse

Estimated market share of registrars

Name	Size	Market share (%)
GoDaddy.com, LLC	63,522,904	30.84
NameCheap, Inc.	10,901,924	5.29
Tucows Domains Inc.	9,492,927	4.61
Network Solutions, LLC	6,393,947	3.10
Alibaba Cloud Computing (Beijing) Co., Ltd.	5,668,641	2.75
Google LLC	5,342,956	2.59
1&1 IONOS SE	4,861,279	2.36
eNom, LLC	4,650,888	2.26
PDR Ltd. d/b/a PublicDomainRegistry.com	4,564,240	2.22
TurnCommerce, Inc. DBA NameBright.com	3,583,210	1.74
GMO Internet, Inc. d/b/a Onamae.com	3,403,676	1.65
OVH sas	3,208,371	1.56
NameSilo, LLC	3,166,460	1.54
Wild West Domains, LLC	2,842,400	1.38
FastDomain Inc.	2,272,984	1.10

Table 9: Top 15 registrars based on the overall domain market share.

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

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

Magnitude of DNS abuse

Registrar reputation (uptimes)

Registrar	count	mean	median
NameCheap, Inc.	5,774	1 days 06:50:06	0 days 06:00:00
NameSilo, LLC	1,928	1 days 12:41:29	0 days 12:00:00
Registrar of Domain Names REG.RU LLC	1,025	2 days 07:57:14	0 days 01:00:00
GoDaddy.com, LLC	705	3 days 16:22:11	1 days 00:00:00
PDR Ltd. d/b/a PublicDomainRegistry.com	587	1 days 08:29:26	0 days 12:00:00
GMO Internet, Inc. d/b/a Onamae.com	475	2 days 00:55:39	1 days 00:00:00
Tucows Domains Inc.	409	1 days 07:43:38	0 days 12:00:00
Wild West Domains, LLC	392	1 days 22:08:03	1 days 00:00:00
REGRU-RU	186	1 days 07:44:13	0 days 12:00:00
Alibaba Cloud Computing (Beijing) Co., Ltd.	169	4 days 16:44:01	2 days 00:00:00
Hostinger, UAB	162	0 days 06:43:49	0 days 01:00:00
Squarespace Domains LLC	151	0 days 15:58:04	0 days 12:00:00
Name.com, Inc.	146	1 days 05:15:45	1 days 00:00:00
Google LLC	129	2 days 14:35:48	2 days 00:00:00
Web Commerce Communications Limited dba WebNic.cc	122	1 days 00:03:31	0 days 06:00:00
Alibaba Cloud Computing Ltd. d/b/a HiChina (www...	110	7 days 03:42:40	2 days 00:00:00
Key-Systems, LLC	109	6 days 20:44:35	2 days 00:00:00
Hosting Concepts B.V. d/b/a Registrar.eu	101	0 days 21:17:55	0 days 06:00:00
West263 International Limited	95	10 days 19:38:31	14 days 00:00:00
Porkbun LLC	93	2 days 13:49:01	0 days 12:00:00

Table 12: Uptimes of maliciously registered domain names used in phishing for the top 20 most abused registrars (in terms of abuse counts).

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

Magnitude of DNS abuse

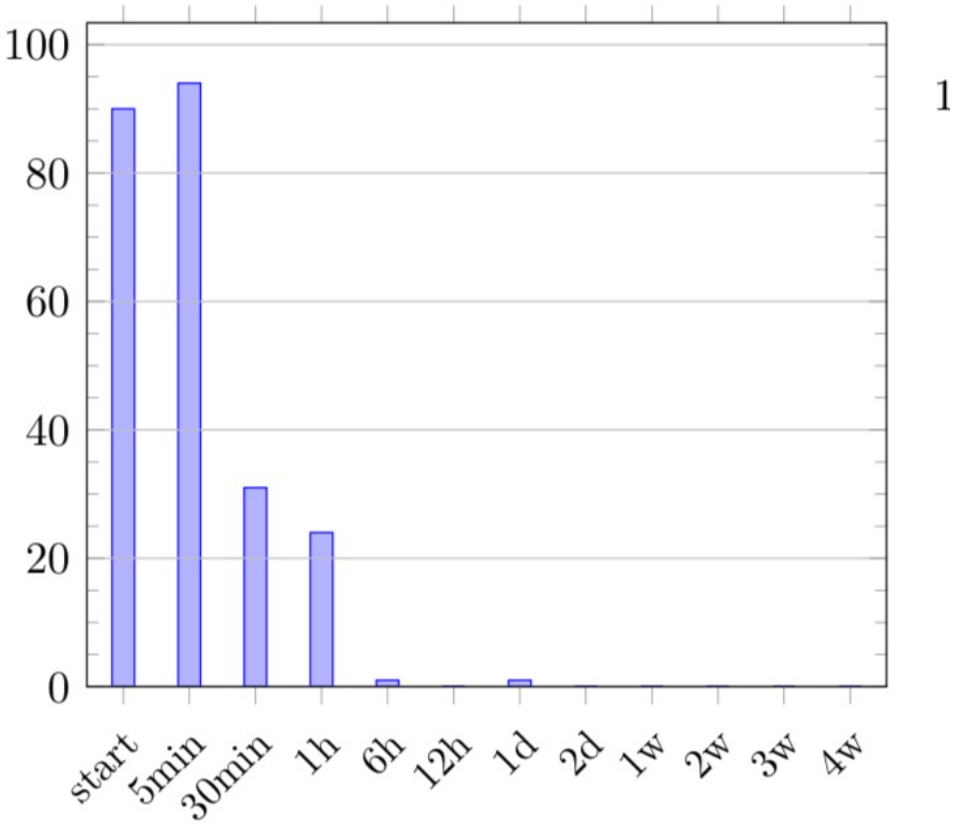
Free services (e.g., free hosting and subdomain provider)

Botnet C&C		Malware		Phishing		Spam	
Provider	# Domains	Provider	# Domains	Provider	# Domains	Provider	# Domains
Duck DNS	9	dns.army	208	ngrok	23,531	Google Cloud	118
ChangeiP	3	NoIP	92	000webhost	16,867	Google Firebase	30
000webhost	2	000webhost	41	Google Firebase	13,371	NoIP	14
		Duck DNS	32	Duck DNS	7,252	amazonaws.com	12
		amazonaws.com	23	Google Cloud	5,440	wixsite.com	11
		soundcast.me	14	NoIP	4,004	blogspot.com	6
		DynuDNS	10	weebly.com	3,853	IBM cloud	6
		tmweb.ru	4	ChangeiP	3,340	glitch.me	5
		weebly.com	3	tmweb.ru	3,125	Duck DNS	4
		blogspot.com	2	yolasite.com	1,952	netlify.app	4

Table 15: Top 10 special service providers with the highest occurrence of blacklisted FQDNs per abuse type.

Magnitude of DNS abuse

Free services (uptime), example:



(a) ngrok.io

Adoption of DNS security extensions

Adoption of DNS security extensions and email protection protocols:

- The overall level of DNS security extensions (DNSSEC), DMARC, SPF adoption remains low
- Analysis of RFC-compliant Email Aliases (abuse@example.com, webmaster@example.com)
- There are 2.5 million open DNS resolvers worldwide that can be effectively used as amplifiers in distributed denial-of-service attacks
- Deployment of Inbound Source Address Validation remains low, exposing DNS infrastructure to external attacks

Recommendations for improvements of measures to mitigate DNS abuse

Set of 27 recommendations in 6 areas

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

Acknowledgements

This study was commissioned by the European Commission (EC reference VIGIE 2020/0653). We would like to thank EU and international institutions and agencies, law enforcement authorities, brand owners, trade and industry associations, TLD registries, registrars, hosting providers, other intermediaries, and security experts for their constructive and valuable comments. We would like to thank Spamhaus, SURBL, Anti-Phishing Working Group, Abuse.ch, Phishtank, and OpenPhish for providing access to their blacklist feeds. The authors also thank Roman Huessy for providing the uptime data for the URLhaus feed, the CENTR community for sharing the sizes of ccTLDs, and Sourena Maroofi for providing valuable comments and discussions on the paper.

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 Korczyński

maciej.korczynski@univ-grenoble-alpes.fr

FASANO PAULOVICS

SOCIETÀ TRA AVVOCATI

GRENOBLE INP UGA

Recommendations for improvements of measures to mitigate DNS abuse

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

ccTLD registries should consider:

- **providing a scalable and unified way of accessing complete registration information using Registration Data Access Protocol (RDAP)**
- **publishing DNS zone file data through DNS zone transfer or a system similar to Centralized Zone Data Service (CZDS)**

Recommendations for improvements of measures to mitigate DNS abuse

B. Contact information and abuse reporting

- Domain name administrators should maintain email aliases for domain name (e.g., abuse / hostmaster / webmaster) to notify security vulnerabilities and domain name abuse
- gTLDs and ccTLDs registries and registrars should consider displaying email addresses of registrants and domain name administrators as anonymized email addresses to notify security vulnerabilities and domain name abuse
- **All DNS operators and intermediaries should set up standardized (centralized) systems for access to registration data and to abuse reporting**
- CERTs and security organizations should exchange information on threats using collaborative platforms

Recommendations for improvements of measures to mitigate DNS abuse

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

gTLD and ccTLD registries, registrars and resellers:

- verify the accuracy of the domain registrant data through KYBC procedures and cross-checks
- develop similarity search tools and surveillance services
- offer preventive blocking services
- use predictive algorithms to prevent abuse registrations
- **have abuse rates being monitored → sanctions, incentives**

Recommendations for improvements of measures to mitigate DNS abuse

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

Hosting providers should:

- **have abuse rates being monitored**
- develop and use technical solutions that effectively curb hosting and content abuse
- employ advanced prevention and remediation solutions to quickly curb abuses of hosting infrastructure and subdomain names

Recommendations for improvements of measures to mitigate DNS abuse

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

- TLD registries and registrars should sign TLD zone files (registries) and domain names (registrars) with DNS security extensions (DNSSEC), facilitate its deployment according to good practices, and be offered discounts for DNSSEC-signed domain names
- Internet Service Providers (ISP) operating DNS resolvers should configure DNSSEC validation
- National governments and CERT teams should intensify notification efforts to reduce the number of open DNS resolvers (and other open services) to prevent distributed reflective denial-of-service (DRDoS) attacks
- The security community should intensify efforts to measure the adoption of email security standards preventing domain spoofing
- Network operators should deploy IP source address validation protecting the Internet against IP spoofing, distributed reflective denial-of-service (DRDoS) and DNS infrastructure attacks

Recommendations for improvements of measures to mitigate DNS abuse

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

- Harmonise ccTLD operation by adoption of good practices
- Require DNS service providers to collaborate with EU and Member States' institutions, law enforcement authorities (LEA), and trusted notifiers
- Encourage awareness-raising and knowledge-building activities to make affected parties aware of existing measures tackling DNS abuse
- Encourage knowledge-sharing and capacity-building activities between intermediaries and stakeholders involved in the fight against DNS abuse