



MASTERING DNS SECURITY IN JUST 30 MINUTES

@ BE-CYBER

Kristof Tuyteleers – 08.10.2024

dnsbelgium

.be

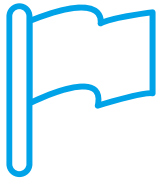
.vlaanderen

.brussels



INTRODUCING DNS BELGIUM

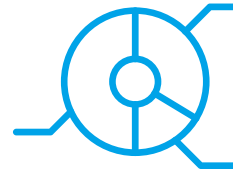
WHO WE ARE



Not-for profit
organisation

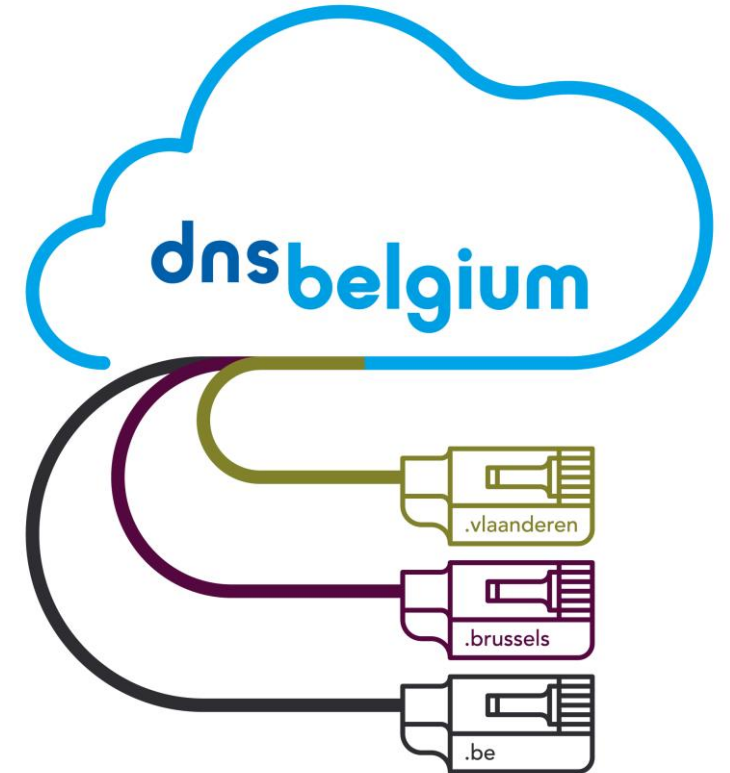


Top Level Domain
registry



Our core
tasks are to:

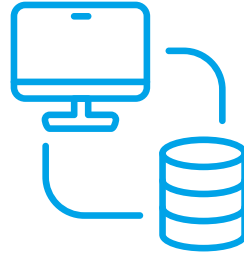
- register domain names,
- make the internet more accessible,
- encourage its usage.



KEY FIGURES



40
Employees



Domain names

1,73m .be
8,500 .brussels
6,000 .vlaanderen



356
Registrars



20,000
New registrations
per month



€+7,6m
Income

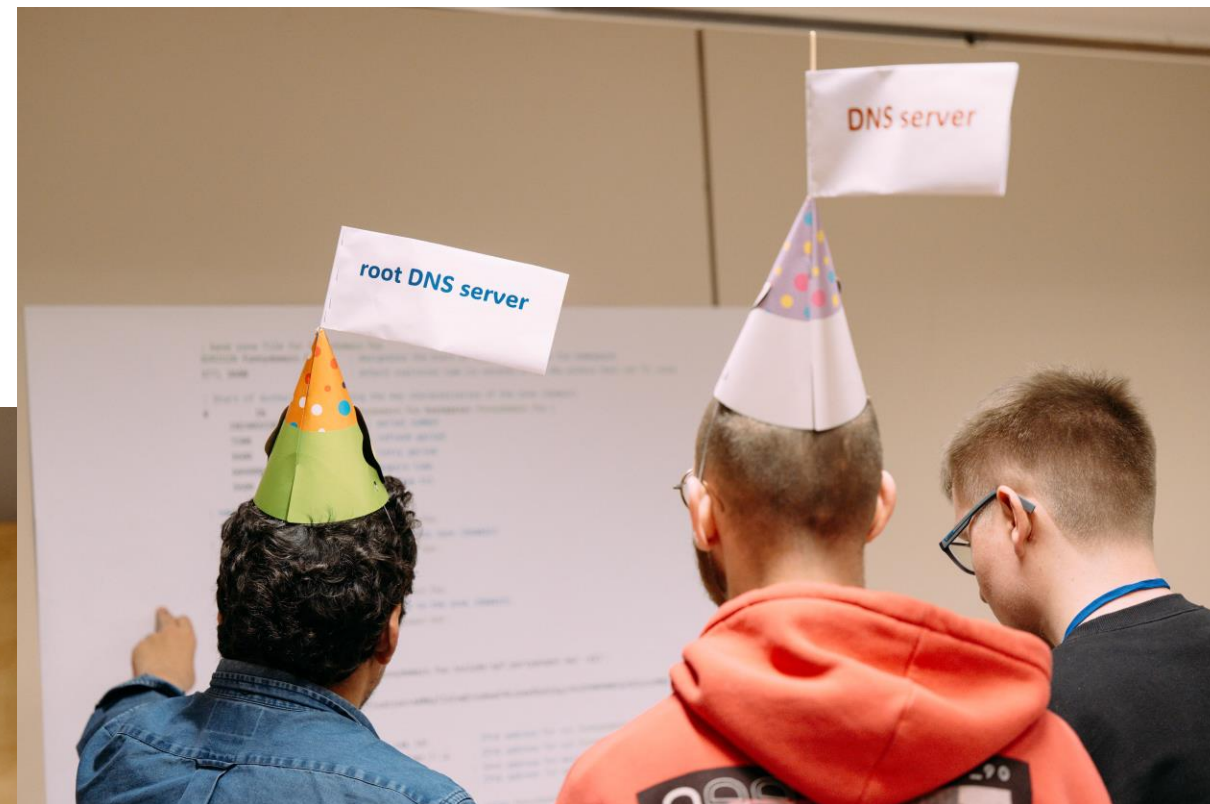
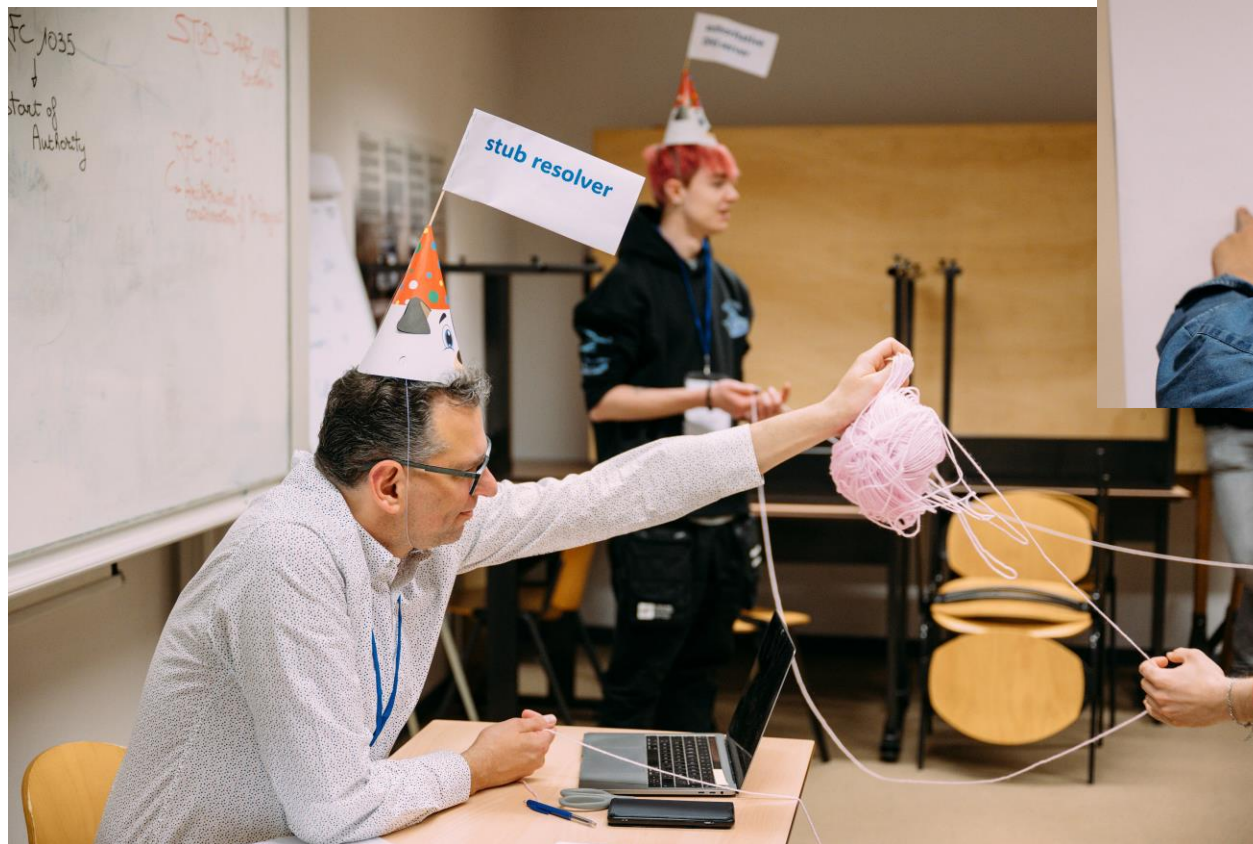


ISSUE #1

DNS IS NOT SEXY

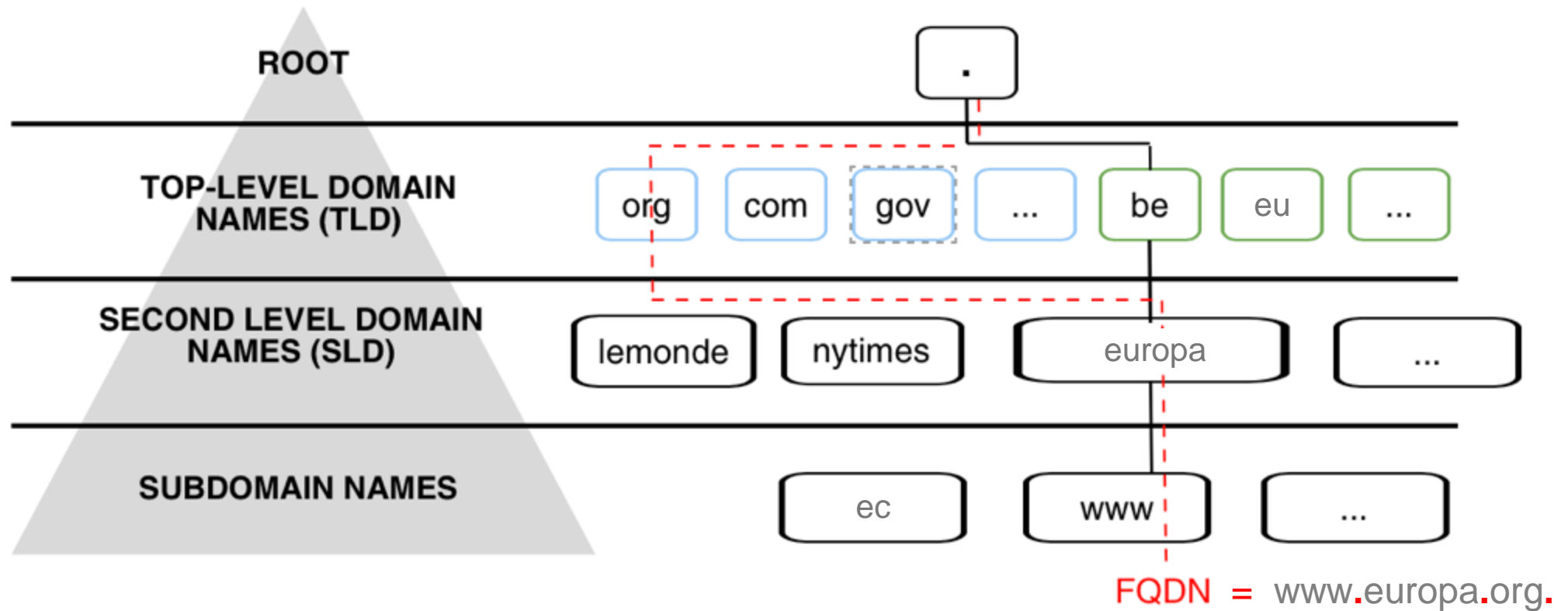
EDUCATION

- Fill the gap

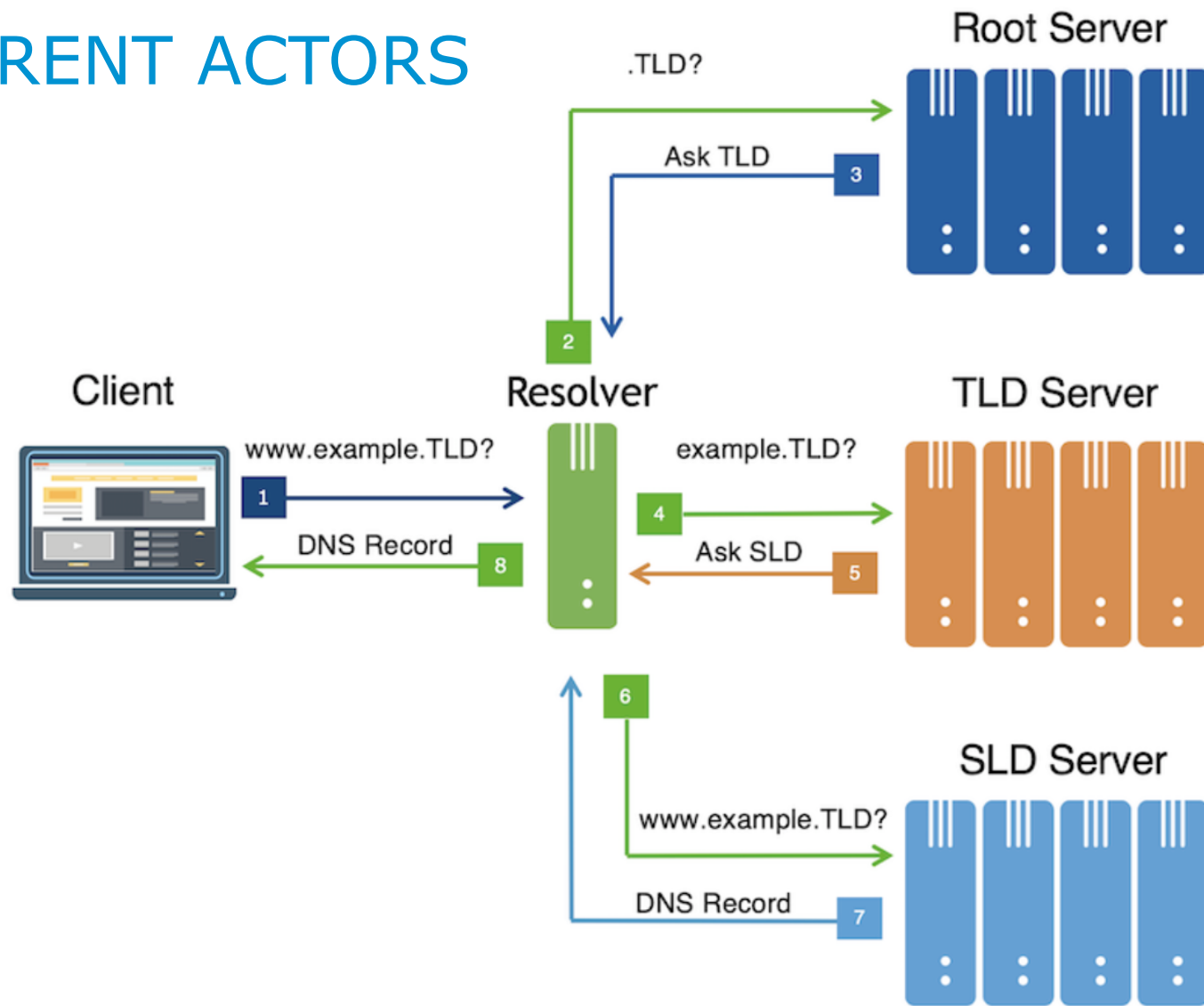


HIERARCHY

- DNS is a tree-structured namespace



THE DIFFERENT ACTORS



Source: <https://blog.verisign.com>



NAME SERVERS IN DIFFERENT FLAVOURS

- Root name server
- TLD name server
- Authoritative name server
- Recursive resolver
- Client / Stub resolver

AWARENESS RAISING



DE
SCHAAL
VAN



Campagne de cybersécurité pour les seniors | DNS Belgium

Wordt jouw klas de meest
mediawijze klas van
Vlaanderen?





ISSUE #2

GOLDDIGGERS



TOP LEVEL DOMAINS

- (legacy) gTLDs
- new gTLDs
 - Generic TLD - examples: .car, .pictures
 - Community TLD - examples: .catholic, .thai, .gay
 - Geographical TLD - examples: .brussels, .vlaanderen
 - Brand TLD - examples: .unicef, .politie
- ccTLDs

CONFUS. ING



Google Registry

Home

For partners

Register a domain

Announcements

FAQs

More domains ▼

Introduc....ing the .ing top-level domain

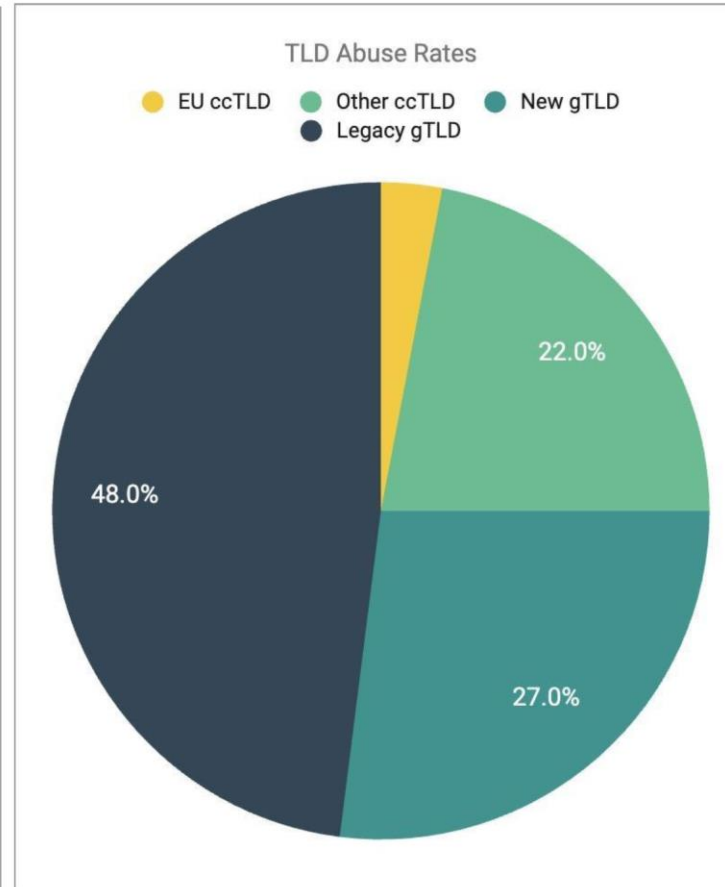
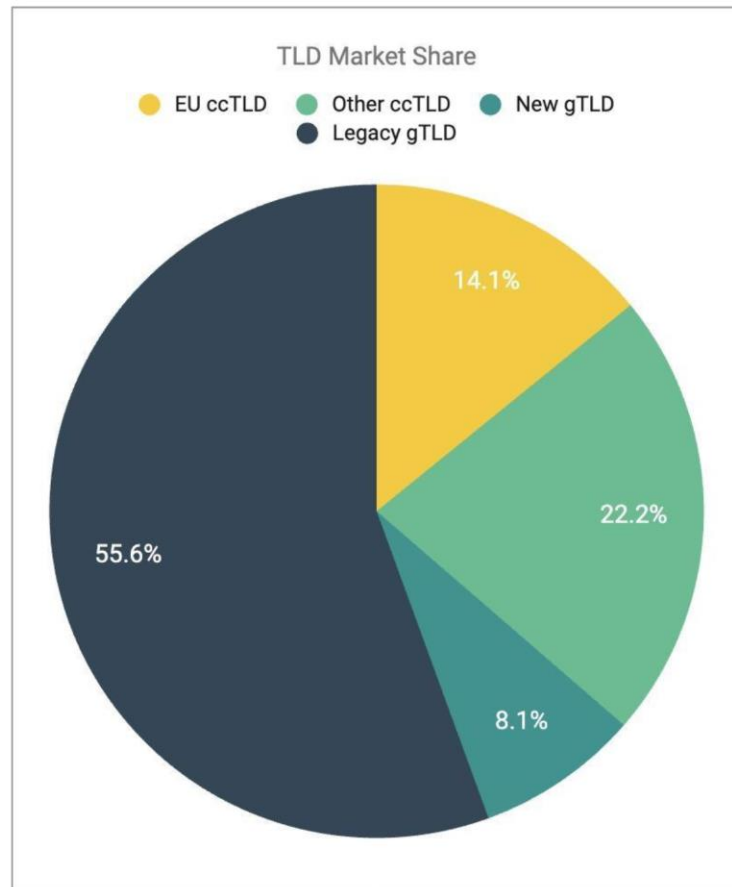
31st October 2023

Launch.ing today is a new top-level domain that allows you to build a website in a single word: .ing. [Design.ing](#), [edit.ing](#), [mak.ing](#) — the possibilities are endless. With .ing, people, businesses, and brands can express themselves in a whole new way and find a short memorable domain — all while getting built-in security.

To learn more about .ing, please check out our [latest blog post](#) and visit [get.ing](#) to find out where you can register your own .ing domain.

We're look.ing forward to find.ing out what makes people s.ing, see.ing who will be k.ing on the internet, and learn.ing what this new launch will br.ing.

2012 -> NOW: EFFECTS OF THE NEWGTLD ROUND



- EU ccTLDs have an exceptionally low abuse level
- Where the global median abuse level is at 0.22%, EU ccTLDs have a 0.05% abuse rate

Source: DNS Research Federation;
Habits of excellence: why are European
ccTLD abuse rates so low?; 11/2023



ISSUE #3

EVERYONE WANTS 15 MINUTES OF FAME

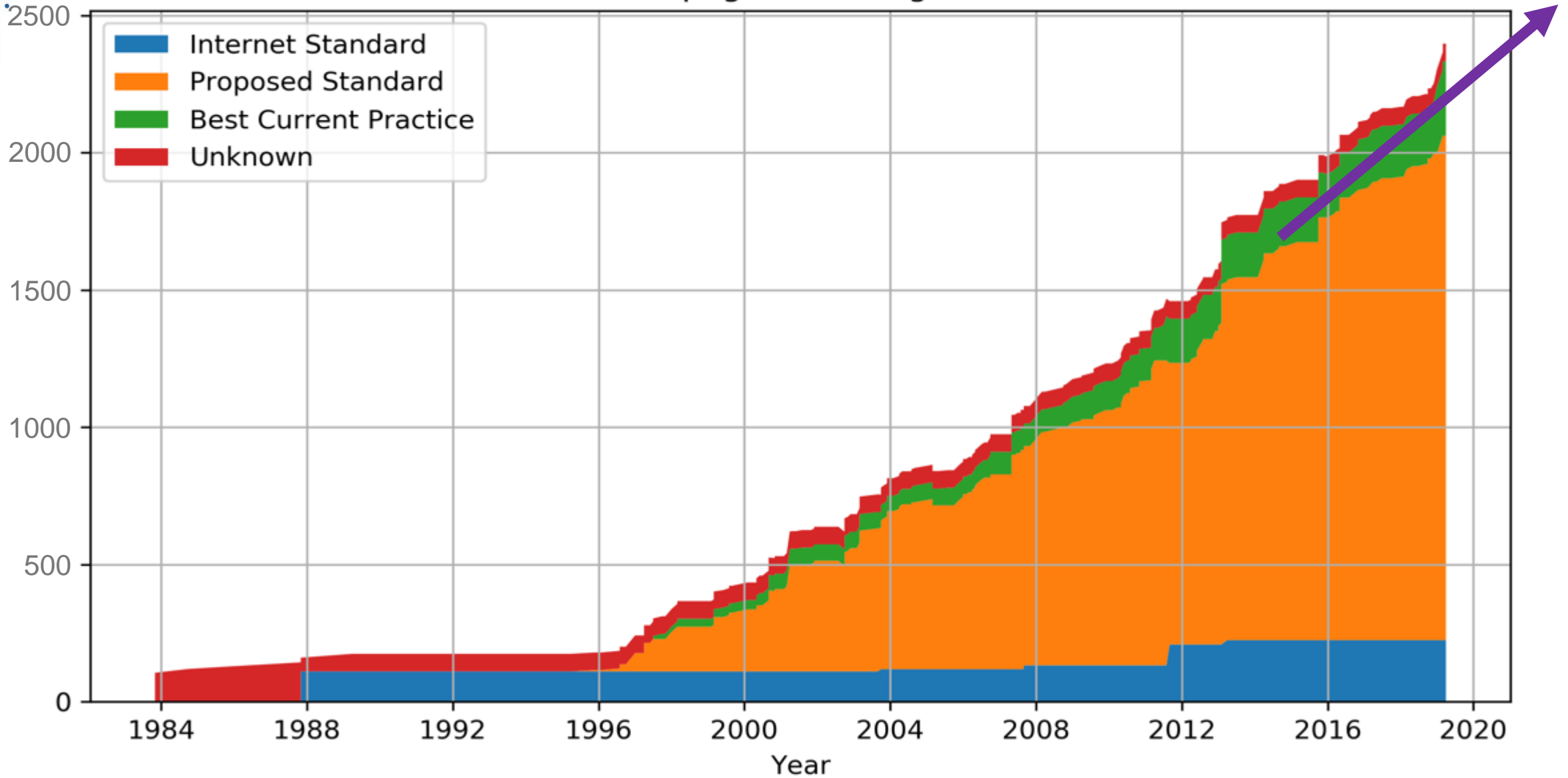


WHAT MAKES THE INTERNET WORK

- The various standards and protocols involved

= documented, collective agreement on how the Internet and its protocols should function, and the provider companies who pledge to make them work the way they should
- RFCs
(<https://tools.ietf.org/rfc/index>)

Number of RFC pages covering DNS over time





ISSUE #4

NOBODY READS THE MANUAL(?)

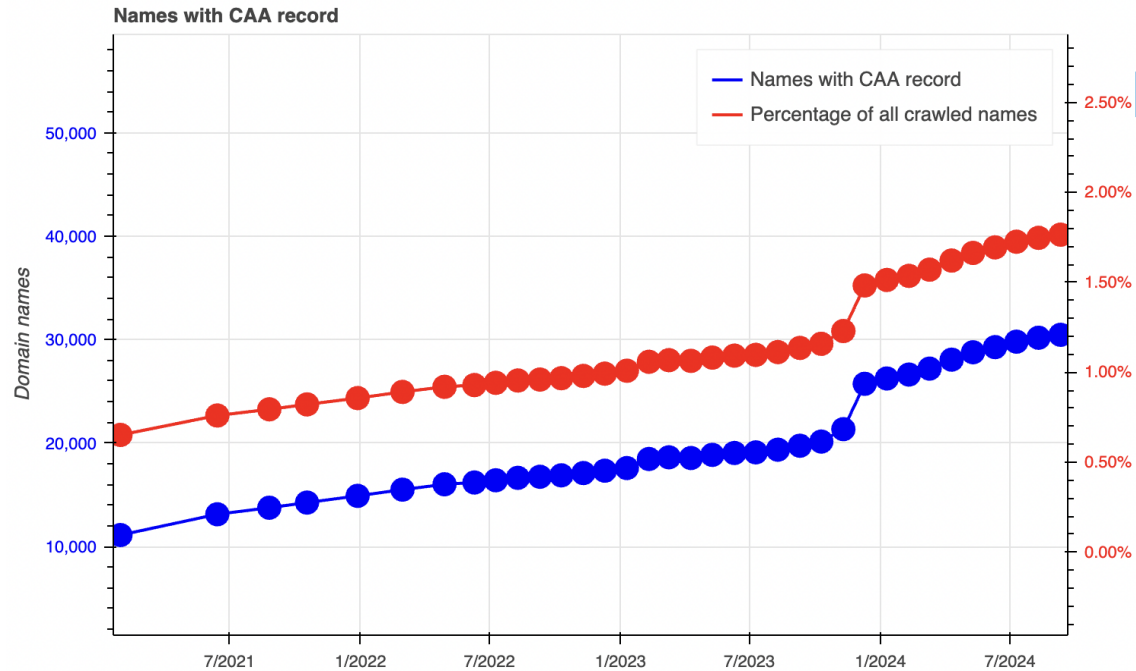


RECORD TYPES

- Several types of records used

RECORD TYPE	DETAILS
SOA record	A mandatory record used in all zone files. SOA specifies authoritative information about a DNS zone, including primary name server
A record	IPv4 Host Record, used for mapping a Domain Name to an IPv4 address
AAAA record	IPv6 Host Record, used for mapping a Domain Name to an IPv6 address
MX record	Mail Exchanger, used for mapping a DNS domain name to the mail server
PTR record	Pointer, used for reverse lookup (IP Address to Domain Name resolution)
CNAME	Alias Record, used for mapping an alias of a DNS domain name CNAME Records allow using different names for same host

THE CAA RECORD



```
$ dig CAA dnsbelgium.be.
```

```
;; QUESTION SECTION:
```

```
;dnsbelgium.be. IN CAA
```

```
;; ANSWER SECTION:
```

```
dnsbelgium.be. 3600 IN CAA 0 issue "globalsign.com"
```

```
dnsbelgium.be. 3600 IN CAA 0 issue "amazon.com"
```

```
dnsbelgium.be. 3600 IN CAA 0 issue "letsencrypt.org"
```

```
dnsbelgium.be. 3600 IN CAA 0 iodef "mailto:cert-abuse  
@dnsbelgium.be"
```

TXT RECORDS CAN BE HANDY

- `$ dig TXT fetch.vxpapub.ourmazdcompany.net.`

`:: ANSWER SECTION:`

```
fetch.vxpapub.ourmazdcompany.net. 120 IN TXT
"window.location.replace(\"http://www.95249bfg36abp.solditin30days.com/73856.html\");"
```

`:: AUTHORITY SECTION:`

```
ourmazdcompany.net. 172582 IN NS ns2.firstdnshoster.com.
```

```
ourmazdcompany.net. 172582 IN NS ns1.firstdnshoster.com.
```



DuuuuH DoH

- DNS over HTTPS, defined in IETF RFC 8484
- Uses HTTPS and HTTP/2 to make the connection
Uses port 443
- ⇒ Encrypted
- ⇒ DNS camouflaged within other HTTPS traffic
- To secure connections between client and recursive resolver



PsiXBot Now Using Google DNS over HTTPS and Possible New Sexploitation Module

SEPTEMBER 06, 2019 | THE PROOFPOINT THREAT INSIGHT TEAM



OVERVIEW

Since posting [our last PsiXBot update](#), the group or actor behind this malware has continued to make changes. Most notably, we have observed

- The introduction of DNS over HTTPS
- A new version number (1.0.3)
- New Fast Flux infrastructure
- A newly observed "PornModule"
- Distribution via Spelevo EK



ISSUE #5

IT'S OLD (SCHOOL)



DNS PROTOCOL IN THE EIGHTIES

- Clear-text protocol
- Trust
- Open
- Small namespace with very limited number of TLDs
(.be operational since 1989)

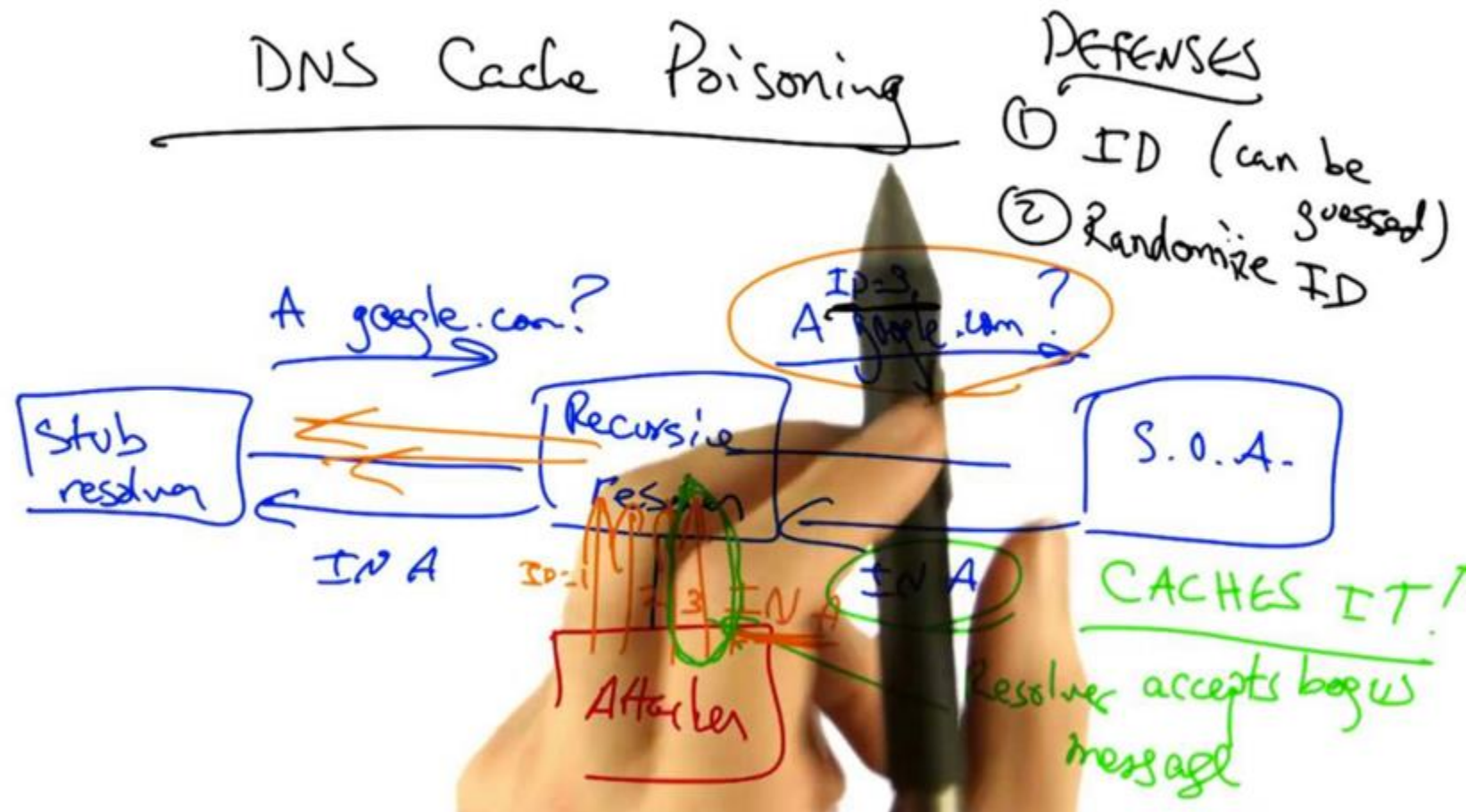
BECAUSE BACK THEN ...

- The world was a safe space ...



THE START OF MODERN TIMES

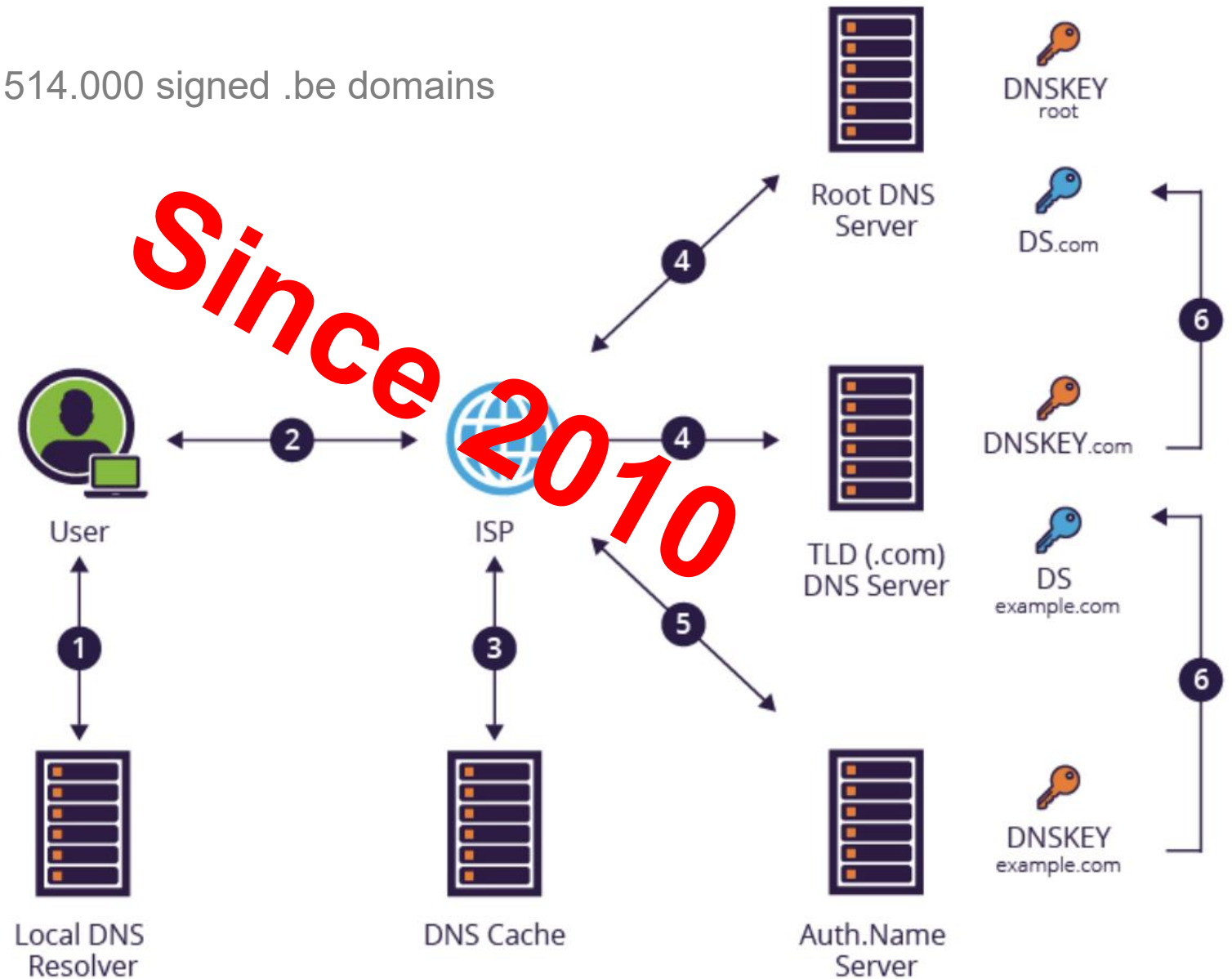
- Kaminsky attack (2008): DNS cache poisoning



Grade	Hours per Week
1	10
2	12
3	14
4	16
5	18
6	20

⇒ Currently ≈ 514.000 signed .be domains

- Registrants/registrars:
sign DNS zones
associated
with domains
- Caching recursive
name servers:
enable **validation**



Source: imperiva.com



ISSUE #6

THE INTERNET IS BROKEN

RESTRICTING THE INTERNET

Russia to disconnect from the internet as part of a planned test

11-Feb-2019 tjack



Russia's internet contingency plan gets closer to reality.

By Catalin Cimpanu for Zero Day | February 11, 2019



DOMAIN INCITE

DI PRO TLD HEALTH CHECK ABOUT ADVERTISE

Turkish government takes over ccTLD

Kevin Murphy, May 7, 2019, 15:06:05 (UTC), Domain Registries

Turkey's ccTLD has been transferred into government hands.

ICANN's board of directors at the weekend formally approved a redelegation request from the country to its IANA division.

The new official ccTLD manager is Bilgi Teknolojileri ve İletişim Kurumu (BTK), which translates as Information and Communication Technologies Authority.

That's Turkey's telecommunications regulator, part of the government.

DNS, INTERNET FRAGMENTATION & BIG TECH

- Increasing pressure for national and European **regulation** of the Internet
 - Enforcing local regulations on global network requires establishing points of control ... (unfortunately) DNS resolution offers such **control point**
 - => Push for DNS resolution to happen in the same jurisdiction of the end user
 - **Encrypted DNS** transport = explicitly designed to prevent the use of the DNS as a monitoring/content control tool
 - ↳ *Side effect:* tends to increase the **centralisation** of DNS queries into the hands of Big Tech (↔ Internet & DNS were designed to be decentralised)
 - Increasing market concentration (too big to fail/regulate?)
 - Encrypted DNS transport can be used to reduce competition in the **data market**
- => End users get **unpredictable experiences** depending on OS, browser, resolver, ...



ISSUE #7

TOO INEXPENSIVE

IT'S ALL ABOUT ASSET MANAGEMENT

Inti De Ceukelaire

When privacy expires: how I got access to tons of sensitive citizen data after buying cheap domains

As part of a large-scale privacy investigation, I have bought more than 100 domain names previously belonging to social welfare and justice institutions in Belgium. What I observed was unsettling.



INTI DE CEUKELAIRE

MAY 21, 2024

INFORMATION LEAKAGE AND IDENTITY THEFT

How Abandoned Domain Names Pose a Major Cyber Risk to Your Business

Iron Bastion's cybersecurity expert Gabo Athmari, recently published novel research on abandoned internet domains, and how they are a significant cyber risk which threatens businesses and in particular the Australian legal profession.



NICHOLAS KAVADIAS, EMILY WILSON
18 SEP 2018 • 4 MIN READ

GDPR?





ISSUE #8

IT ALWAYS WORKS
("AS EXPECTED")

SMALL TYPO, BIG CONSEQUENCES

Menselijke fout stuurt bezoekers Scarlet.be naar malwaresite



Pieterjan Van Leemputten
is redacteur bij Data News

07/09/18 om 12:18
Bijgewerkt om 12:17
Bron : DataNews

Door een menselijke fout stuurt Scarlet bezoekers van haar website per ongeluk naar een onveilige Chinese site met malware. De fout is rechtgezet maar kan hier en daar nog merkbaar zijn.

Basingstoke, United Kingdom Global Crossing	ns1.scartech.be ns2.scartech.be ns3.scartech.be	✓
Paris, France France Telecom	ns1.scartech.be ns2.scartech.be ns3.scartech.be	✓
Dortmund, Germany Verizon	ns1.scartech.be ns2.scartech.be ns3.scartech.be	✓
Lecco, Italy Easynet	ns1.scartech.be ns2.scartech.be ns3.scartech.be	✓
Yeditepe, Turkey Yeditepe University	ns1.scartech.be ns2.scartech.be ns3.scartech.be	✓
Kaliningrad, Russia VimpelCom	ns1.scartech.be ns2.scartech.be ns3.scartech.be	✓
Karachi, Pakistan Supernet	ns1.scartech.be ns2.scartech.be ns3.scartech.be	✓

NEW TECHNOLOGIES, NEW CHALLENGES

Black Hat 2021: DNS loophole makes nation-state level spying as easy as registering a domain

Wiz CTO Ami Luttwak discusses a new class of vulnerabilities discovered by Wiz Research, which exposed valuable dynamic DNS data from millions of endpoints worldwide.



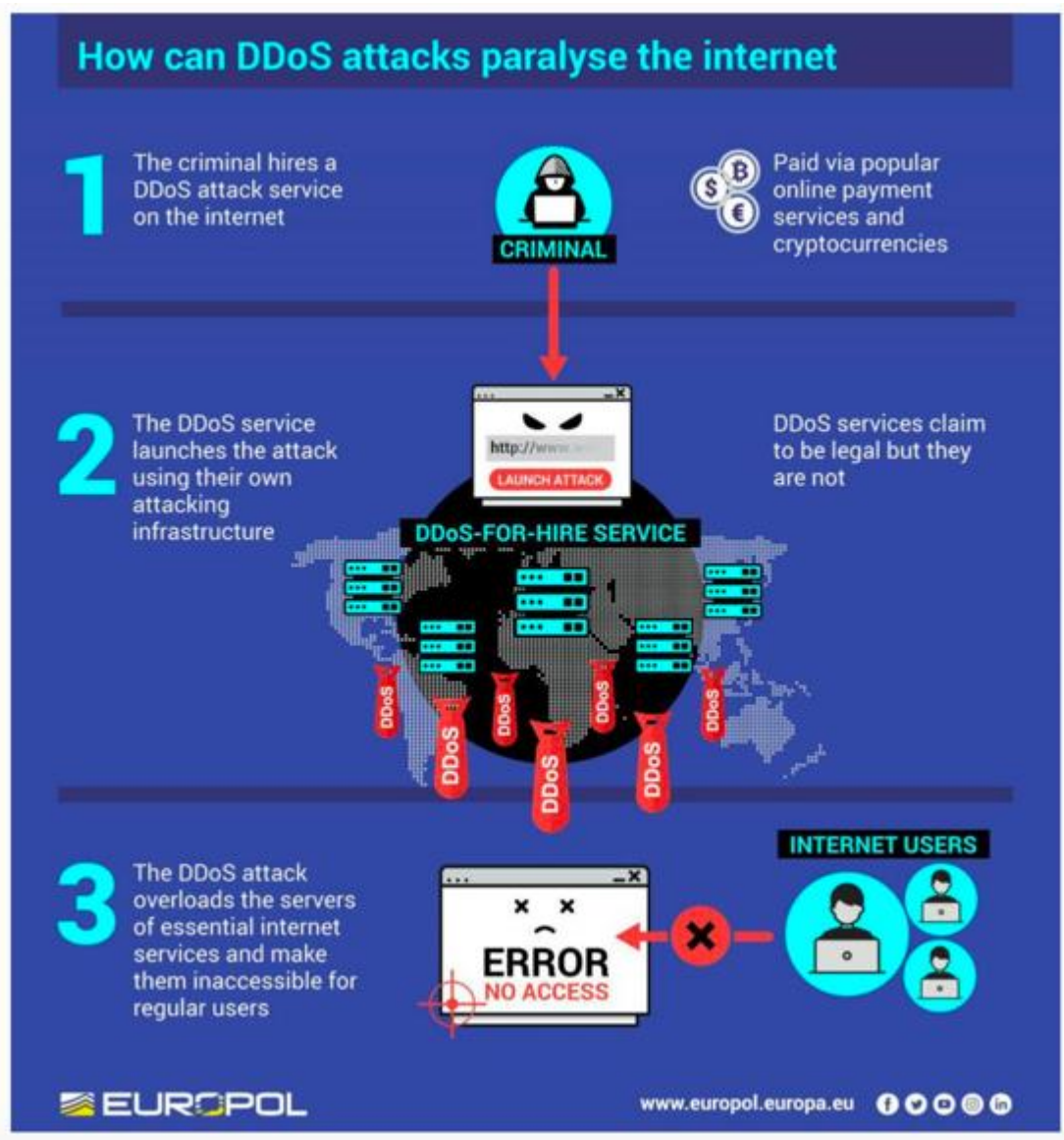
Shir Tamari
August 4, 2021

6 min read



A new class of vulnerabilities discovered by Wiz Research which exposed valuable **dynamic** DNS data from millions of endpoints worldwide

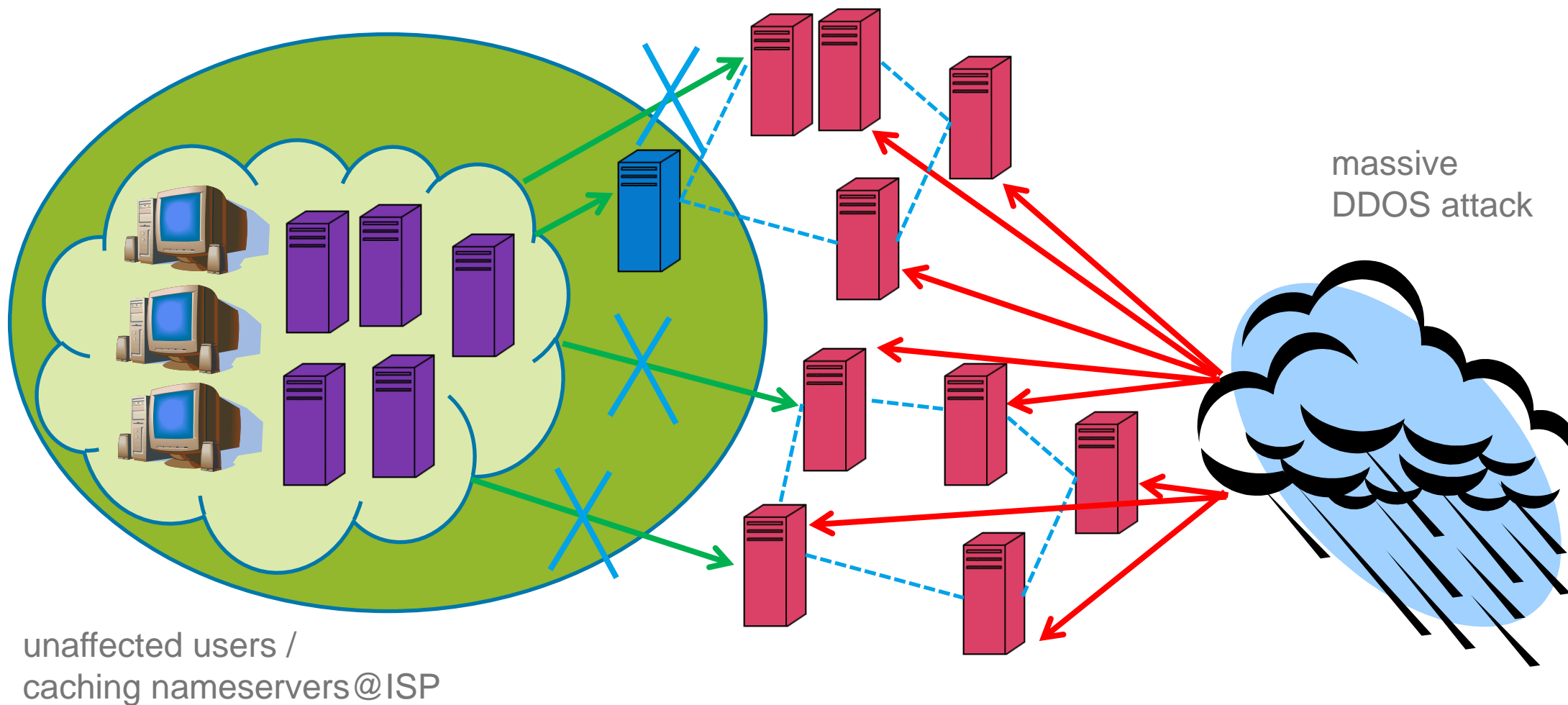
THE MARKET FOR DDOS STRESSERS



Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
Order Now	Order Now	Order Now	Order Now	Order Now

DDOS PROTECTION: ANYCAST@ISP



DNS HIJACKING – FACEBOOK vs NY TIMES

Domain Name: facebook.com
Registry Domain ID:
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: <http://www.markmonitor.com>
Updated Date: 2013-06-06T04:00:37-0700
Creation Date: 2010-04-01T11:56:37-0700
Registrar Registration Expiration Date: 2020-03-29T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: compliance@markmonitor.com
Registrar Abuse Contact Phone: +1.2083857740
Domain Status: clientUpdateProhibited
Domain Status: clientTransferProhibited
Domain Status: clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Facebook, Inc.
Registrant Street: Syria,
Registrant City: Damascus
Registrant State/Province: SY
Registrant Postal Code: 94025
Registrant Country: SY
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
Registrant Fax Ext:
Registrant Email: syrian.es.sy@gmail.com

Overview for nytimes.com

Registrar Info

Name	MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE
Whois Server	whois.melbourneit.com
Referral URL	http://www.melbourneit.com
Status	clientTransferProhibited

Important Dates

Expires On	January 19, 2014
Registered On	January 18, 1994
Updated On	August 27, 2013

Name Servers

m.sea.sy	141.105.64.37
mob.sea.sy	



WHY IS DNS HIJACKING HOT?

- No need to send phishing e-mails
- No need to use lookalike domains
- Can be used for very targeted (below the radar) attacks
- Bypass two-factor authentication
- Control over DNS = able to request genuine certificates
- Can be used for all types of abuse
(advertisement fraud, malware distribution, espionage, ...)

DNS HIJACKING AND CERTIFICATES



April 5, 2017

Author



Vincent Lynch

The SSL Store's encryption expert makes even the most complex topics approachable and relatable.

f t in



Banrisul: SSL Certificates Used In Major Bank Hack

Banrisul Website Taken Over By Hackers, SSL Helped Mask The Attack.



HOW TO PREVENT THIS

- Two-factor authentication at registrar
- Registry lock
- Monitoring of DNS records / changes + **CT** logs
- DNSSEC (+ DKIM/DANE/...)
- Certificate Authority Authorisation (CAA)

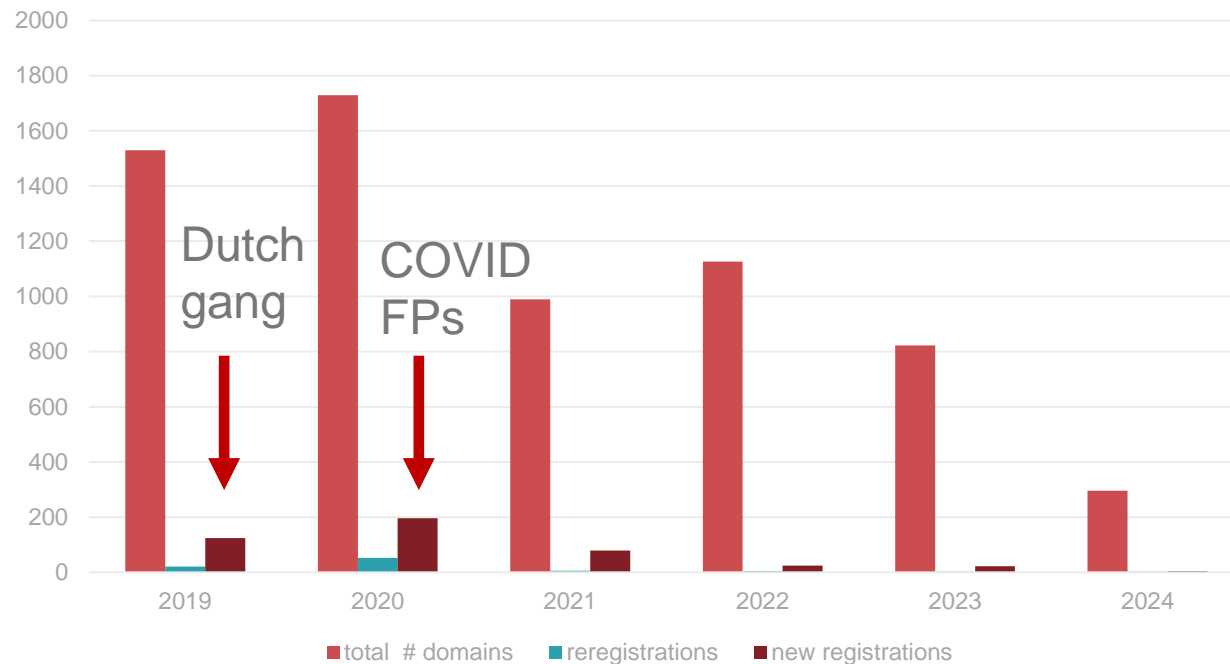


ISSUE #9

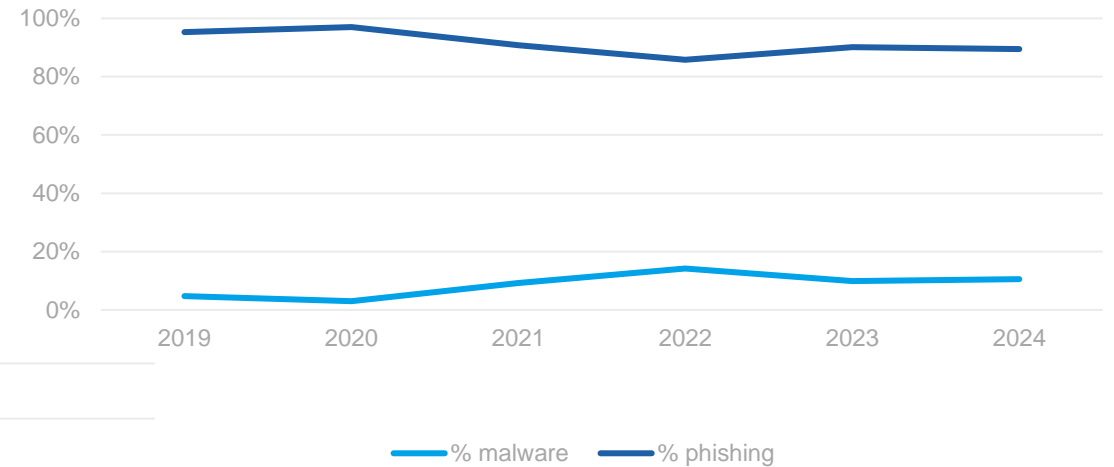
INFRASTRUCTURE MEETS CONTENT

ABUSE TRENDS IN .BE

Domain name freshness



Phishing versus Malware



AUTOMATED REGISTRANT VERIFICATION



- 206.799 new .be domains (2023)



- 48.987 domains 'delayed'
- 43.288 selected contacts (risk-based)



- 31.371 domains 'delayed' delegated
- 28.151 contacts verified
- 84,5% fully automatic

ABUSETOOL & SAFEBROWSING.BE

dnsbelgium

nl en fr

Safebrowsing

This website is a free service provided by DNS Belgium to holders of a .be, .brussels or .vlaanderen domain name. You received a message from us that your website is being used for fraudulent practices (e.g. phishing, malware, etc.) or has been hacked. You can verify below which domain name is at issue. You are urgently requested to remove the fraudulent pages from your website as promptly as possible and to take such measures as necessary to prevent inappropriate use in future. The administrator of your website can help.

For more information on this message and the steps you can take, go to <https://www.dnsbelgium.be/en/knowledgebase-security/safebrowsingbe>. You can address further questions to support@dnsbelgium.be.

Infected URL	Detection Date	Infection Type	Report
https://www.██████████.be/logs/ccbfe9fc2421a68/index.php?ID=login&Key=f89cde3e512cec150eb63edb29d6d631&login&path=/signin/?referrer	June 13, 2019 22:06:54 CEST	PHISHING	Go to report

Disclaimer: DNS Belgium is not responsible for possible damage caused by using the mentioned URL.

NOTICE & ACTION PROTOCOL



DNS Belgium is waging the fight against fraudulent websites in unison with the FPS Economy. This cooperation is constantly increasing the possibilities of suspending such sites within one day. By acting boldly, DNS Belgium and the FPS Economy ensure that consumers can trust .be websites.

The new protocol authorises DNS Belgium to delete .be domain names because of their fraudulent nature, at the request of the FPS Economy. The protocol will be used as of 1st December 2018 to block in particular .be domain names which:

- are used for fraudulent webshops
- host phishing websites (i.e. websites which imitate other websites in order to obtain credit card details, for instance).

The new procedure will be applied only in the event of serious crimes. The registrant has two weeks to react. After six months, the blocked domain name expires.



ISSUE #10

BLAME THE DPO

INFORMATION SHARING AND ANALYSIS CENTRE



EUROPEAN TLD ISAC

TLD ISAC members



The members of the European TLD ISAC are:

- > Afnic, the ccTLD registry for .fr
- > CARNET, the ccTLD registry for .hr
- > CENTR, the Council of European top-level domain registries
- > Denic, the ccTLD registry for .de
- > DNS Belgium, the ccTLD registry for .be
- > EURid, the ccTLD registry for .eu
- > Internetstiftelsen, the ccTLD registry for .se
- > Nic.at, the ccTLD registry for .at
- > Nominet, the ccTLD registry for .uk
- > .PT, the ccTLD registry for .pt
- > Punktum dk, the ccTLD registry for .dk
- > Red.es, the ccTLD registry for .es
- > Register.si, the ccTLD registry for .si
- > SIDN, the ccTLD registry for .nl
- > SK-NIC, the ccTLD registry for .sk
- > Switch, the ccTLD registry for .ch



#Conclusion

INFORMATION TO REMEMBER



SO, WHAT CAN YOU DO?

- Awareness
- Security hygiene
- Monitoring
- Technical improvements
- Share knowledge & experiences

dnsbelgium