



ccNSO DNS Abuse Session

October 27, 2021



A DNS Abuse Perspective

Dr. James Galvin

Start Where We Agree

- Abuse on, with, via, over, and through the Internet is at an all time high, increasing at an astonishing rate
- It is a global problem affecting:
 - Everyone
 - Countries
 - Physical Infrastructure
 - Service providers
 - Organizations, today specifically ICANN
 - Organizational parts, today specifically gTLDs, ccTLDs, registrars, and others
- We all have a role to play in mitigation, but what is that role?
- We are here today to consider the potential role of the ccNSO

A Contracted Party Perspective

- Contracted parties share a common definition of DNS Abuse
 - It is a technical definition
 - [RrSG](#) website and the [RySG](#) website
- Many contracted parties share a common [Framework of DNS Abuse](#)
 - Baseline is the shared technical definition of DNS Abuse
 - A number of other common opportunities are described
 - Options for individual registries and registrars to add local policies
- Contracted parties share a commitment to advance the remediation and mitigation of DNS Abuse
 - Joint and separate working groups producing guidance
 - Working in collaboration with other parts of the community
- Resources
 - [RySG DNS Abuse Resources](#)
 - [RrSG DNS Abuse Resources](#)

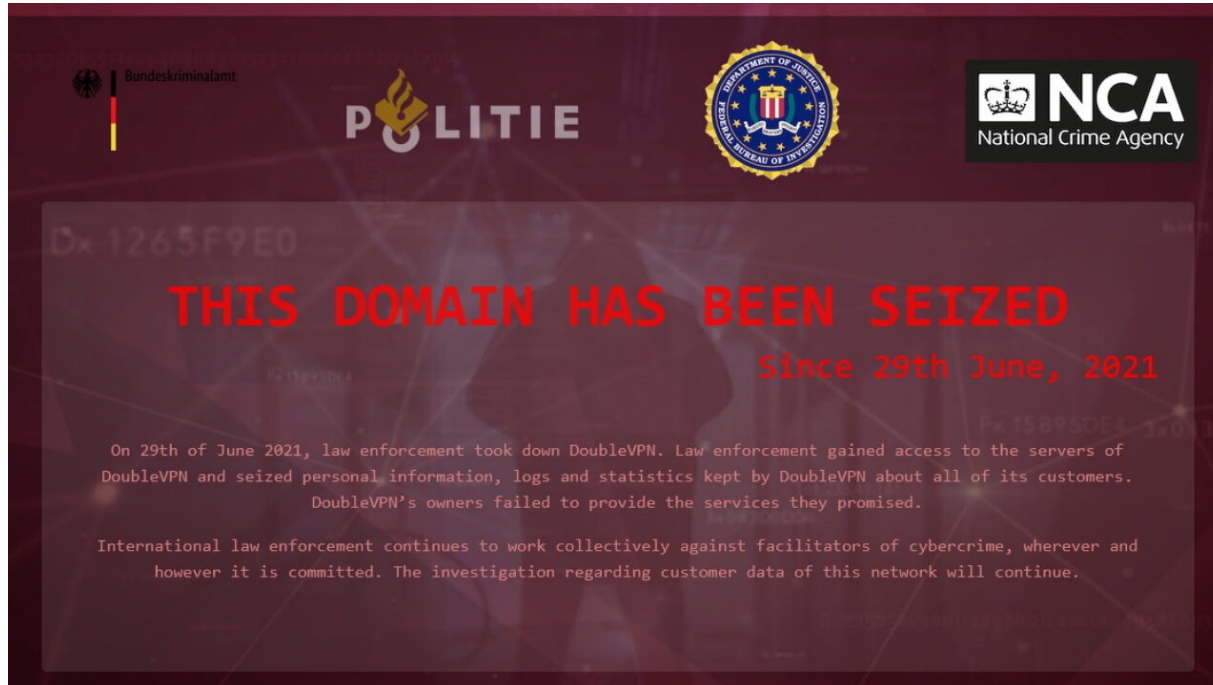
To Do or Not to Do, This Is Our Question

- Do not create another definition of DNS Abuse
 - Find alignment with an existing definition
 - Collaborate with the ICANN community as it considers the problem space within its remit
- Do create a Framework within which each ccTLD can do what is best for it
 - Stick to technical definitions of abuse and actions
 - Local policy should define jurisdiction
 - Local policy should define roles of parties
 - Registry versus registrar action
 - Responsibility of other parties in the ecosystem, e.g., website content service providers
- Do work with the ICANN community to consider evolving issues and seek to improve, on an ongoing basis, whatever you decide to do

10m @ ccNSO

Gabriel @ PSWG

Cop != Sysadmin



The banner features logos for the Bundeskriminalamt (German Federal Criminal Police Office), the Dutch Politie (Police), the FBI Bureau of Investigation, and the National Crime Agency (NCA). The central text, in red, reads "THIS DOMAIN HAS BEEN SEIZED" and "Since 29th June, 2021". Below this, white text explains that law enforcement took down DoubleVPN on June 29, 2021, and seized customer data. It concludes by stating that international law enforcement continues to work against cybercrime facilitators.

Bundeskriminalamt

POLITIE

FEDERAL BUREAU OF INVESTIGATION

NCA
National Crime Agency

THIS DOMAIN HAS BEEN SEIZED
Since 29th June, 2021

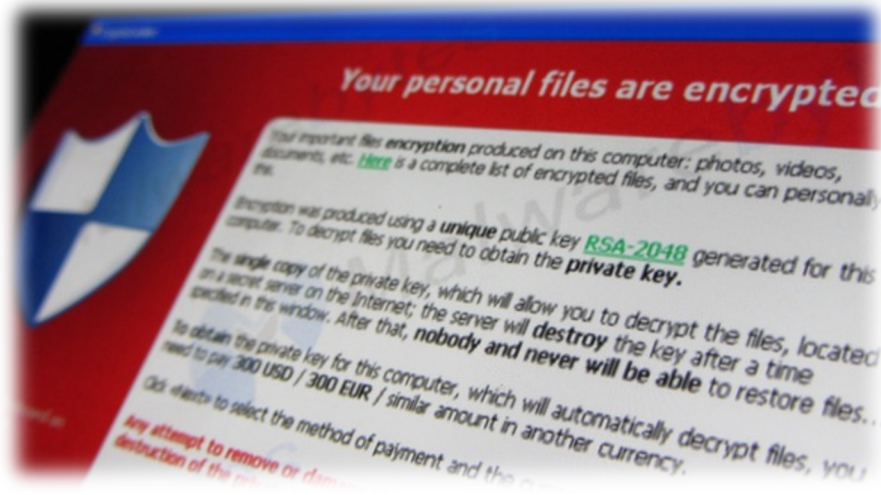
On 29th of June 2021, law enforcement took down DoubleVPN. Law enforcement gained access to the servers of DoubleVPN and seized personal information, logs and statistics kept by DoubleVPN about all of its customers. DoubleVPN's owners failed to provide the services they promised.

International law enforcement continues to work collectively against facilitators of cybercrime, wherever and however it is committed. The investigation regarding customer data of this network will continue.

Two Big Trends

(plus a less common but important one)

Ransomware



BEC



2020 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,866,642,107	Overpayment	\$51,039,922
Confidence Fraud/Romance	\$600,249,821	Ransomware	**\$29,157,405
Investment	\$336,469,000	Health Care Related	\$29,042,515
Non-Payment/Non-Delivery	\$265,011,249	Civil Matter	\$24,915,958
Identity Theft	\$219,484,699	Misrepresentation	\$19,707,242
Spoofing	\$216,513,728	Malware/Scareware/Virus	\$6,904,054
Real Estate/Rental	\$213,196,082	Harassment/Threats Violence	\$6,547,449
Personal Data Breach	\$194,473,055	IPR/Copyright/Counterfeit	\$5,910,617
Tech Support	\$146,477,709	Charity	\$4,428,766
Credit Card Fraud	\$129,820,792	Gambling	\$3,961,508
Corporate Data Breach	\$128,916,648	Re-shipping	\$3,095,265
Government Impersonation	\$109,938,030	Crimes Against Children	\$660,044
Other	\$101,523,082	Denial of Service/TDos	\$512,127
Advanced Fee	\$83,215,405	Hacktivist	\$50
Extortion	\$70,935,939	Terrorism	\$0
Employment	\$62,314,015		
Lottery/Sweepstakes/Inheritance	\$61,111,319		
Phishing/Vishing/Smishing/Pharming	\$54,241,075		

Descriptors*

Social Media	\$155,323,073	*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
Virtual Currency	\$246,212,432	

**** Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.**

Reported Cybercrime Losses in 2020, U.S.



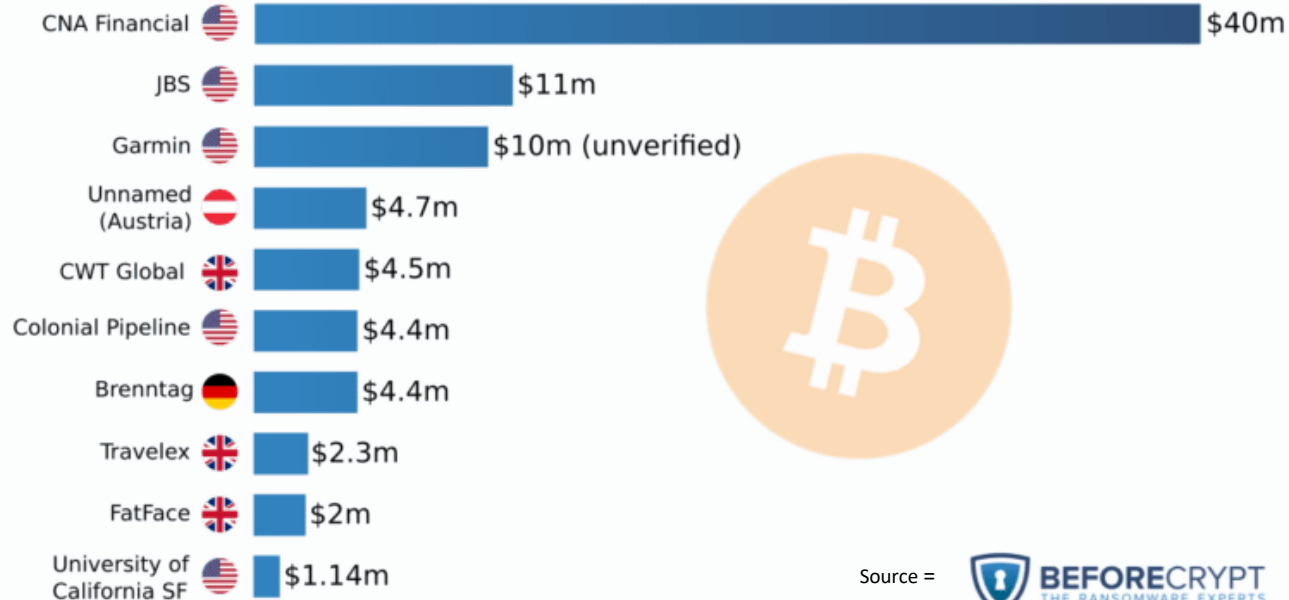
DATA: INTERNET CRIME COMPLAINT CENTER

(www.ic3.gov)

Ransomware

Top 10 Biggest Ransoms Ever Paid

The largest known ransomware ransoms ever paid, in millions of United States Dollars.



Ransomware

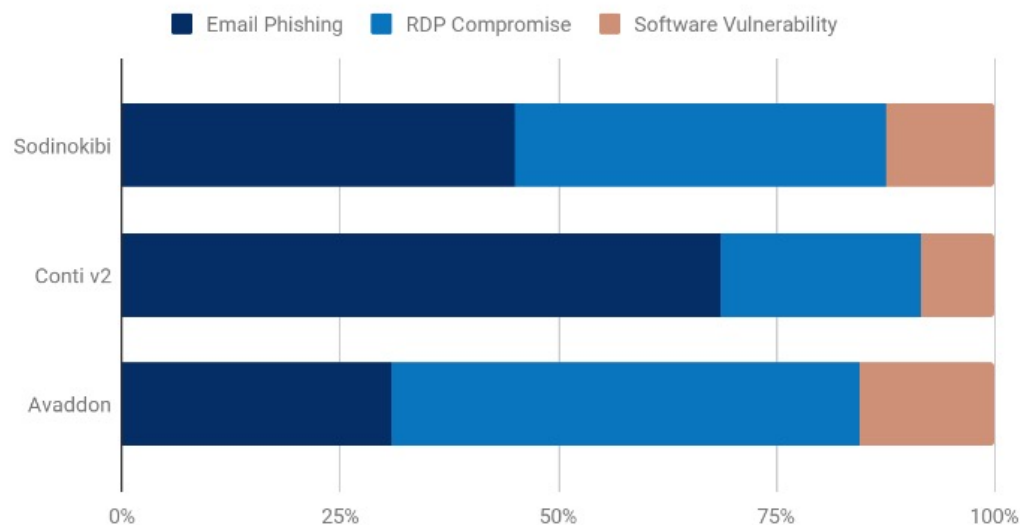
- “Coveware estimates that REvil alone may have collected close to
\$100 million in ransom payments
in just the first 6 months of 2021.

And that is one group.”

- <https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority>

Ransomware

Attack Vectors - Top 3 Ransomware Types



In hour-long call, Biden discusses ransomware with Putin after another massive attack

The president said afterward he's "optimistic," but it's unclear why.

By [Conor Finnegan](#) and [Molly Nagle](#)

July 9, 2021, 3:02 PM • 5 min read



Biden holds call with Putin

After the call, President Joe Biden said that whether or not the Kremlin sponsored the cy... [Read More](#)
Mikhail Metzel/POOL/AFP via Getty Images, FILE

In a nearly one-hour call, President [Joe Biden](#) discussed ransomware attacks with Russian leader Vladimir Putin, saying afterward he was

Colonial Restarts Operations After Cyberattack As Panic-Buying Mounts In Southeast

Updated May 12, 2021 - 6:01 PM ET

Heard on Morning Edition



CAMILA DOMONOSKE



4-Minute Listen

+ PLAYLIST



Cars line up Tuesday at a QuikTrip in Atlanta. Continued panic-buying is leading to shortages at gas stations across the Southeast after a hack attack shut down a critical pipeline.

Megan Varner/Getty Images

What can be done at the DNS level?

Public Safety officials benefit from swift access to accurate domain registrant information.



Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets

It's hard to fight botnets.

RySG and PSWG collaborated on a voluntary framework to make it easier. We hope you'll use it.

<https://www.rysg.info/wp-content/uploads/assets/Framework-on-Domain-Generating-Algorithms-DGAs-Associated-with-Malware-and-Botnets.pdf>

“Do”s

- Share what works (help best practices become common).
 - E.g. .dk’s excellent example on risk-based categorization of registrants presented @ICANN64 [link](#)
- Help the ICANN community to measure what’s happening (contribute to DAAR)
- Support community developed voluntary frameworks where able.
 - E.g. the Framework on Domain Generating Algorithms (DGAs) Associated with Malware and Botnets [link](#)



ccNSO DNS ABUSE SESSION

ICANN 72 – virtual meeting

Kristof Tuyteleers





0. SETTING THE SCENE

“Data collected from DAAR and through the course of the registry audit confirms that the vast majority of registry operators are **committed** to addressing DNS security threats.”

“The prevalence of DNS security threats is **concentrated** in a relatively small number of registry operators.”

Source: <https://www.icann.org/en/system/files/files/contractual-compliance-registry-operator-audit-report-17sep19-en.pdf>

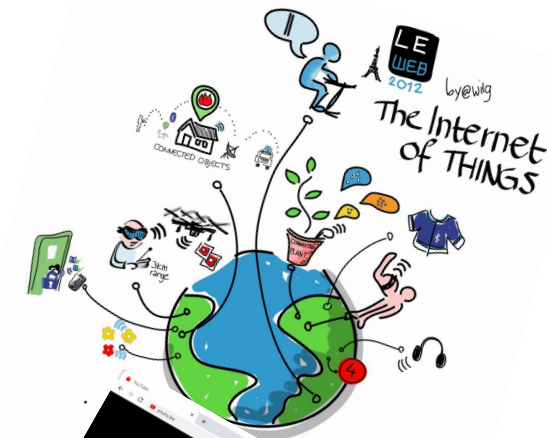
1. PERSPECTIVE



Which angle do you choose?

<https://creativecommons.org/licenses/by-sa/2.0/>

1. PERSPECTIVE



Chrome and Firefox Changes Spark the End of EV Certificates

By Lawrence Abrams

August 14, 2015 06:00 PM 1



Source: <https://www.bleepingcomputer.com>



2. MAJOR ISSUES

We are all part of
the blue team

**Collaboration is not:
give us your data
and we will tell you
whether you are doing
your job well (enough)**





3. DOES

Awareness building

- Increase overall industry maturity level
- Within ccNSO
- For broader internet community

&

Knowledge sharing

- Trust is needed
- “Safe” environment
- Strengthen each other

Expectation management

- Abuse is here to stay
- No silver bullet
- Honest message

3. DONTs

One size fits all

- Local level
- National level
- International level

example



Content police

- Legitimacy
- Accountability
- No full harmonisation

Promote the "wrong" initiatives

- Lack of transparency
- Questions about reliability
- Monetising protection



DNS Abuse

(.in ccTLD)



BY: ANIL KUMAR JAIN

27TH OCTOBER 2021

Definition and Scope:

- ▶ *Hard to define, and broad scope*
- ▶ *Industry players have come together with a working definition – it is a good starting point but what next?*
- ▶ *Reliable and consistent metrics are absent*
- ▶ *Currently metrics are based on incident-based measurements*



DNS Abuse of ccTLD : as per Government

- ▶ Establishing distributed C&C (Command-and-control)
- ▶ Spam and Phishing activities
- ▶ Malware attack on country's critical Information Infrastructure
- ▶ Espionage
- ▶ DDOS Attack
- ▶ Spreading Fake News etc.

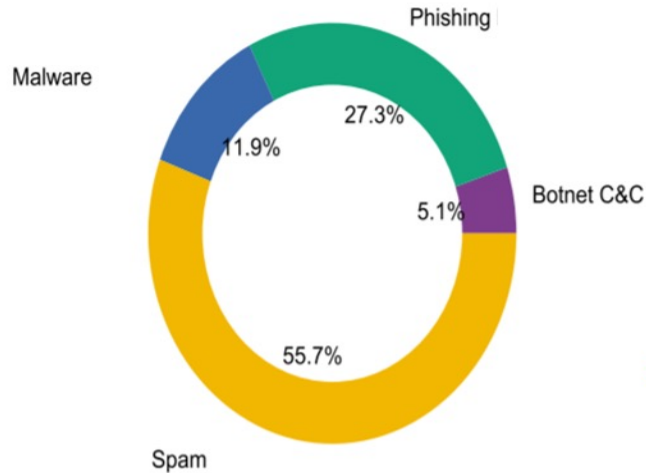


DNS Abuse is There.....

- ▶ *Relatively well studied phenomenon*
- ▶ *Combating it is in the public interest*
- ▶ *Endless discussions at different fora*
- ▶ *Focus on awareness raising seems to yields benefits*
- ▶ *Greater push for coordinated efforts*
- ▶ *ccTLDs at the forefront of the dialogue*



Security Threats for .IN ccTLD

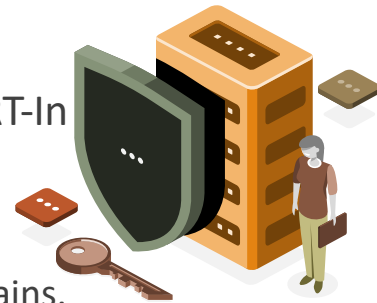


[August, 2021](#) Source :DAAR

Breakdown of domains identified as security threats across all DAAR threat types for .IN ccTLD

Response Strategy (Adopted)

- ▶ Algorithm for blocking key word e.g. ending with gov, mil.
- ▶ Separate Domain for Government and Academia
- ▶ Registry participates in global coordinated bot/spam take down requests along with CERT-In
- ▶ e-KYC verification
- ▶ Permanent blocking of reported Abused domains.



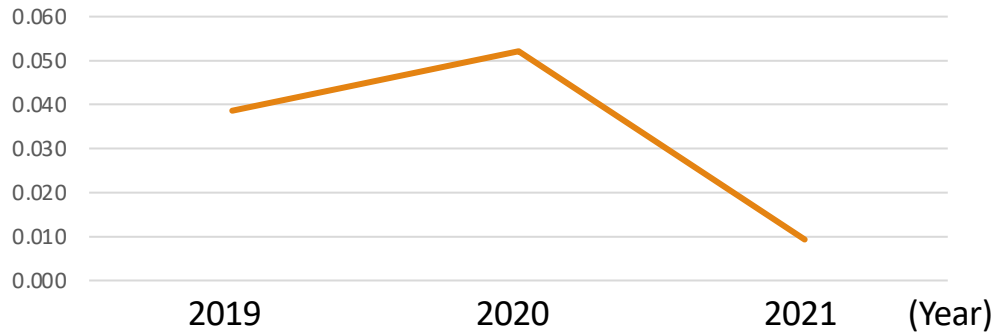
Data Analysis Calendar Year 2019 to 2021

S.NO.	PARTICULARS	2019	2020	2021*
1	Phishing Domains	767	1090	271
2	Pharming Domains	62	107	26
3	MALWARE	2	1	1
4	PORNOGRAPHY	7	5	3
5	SCAM	33	56	3
	Total	871	1259	304

**Status as on 30th Sep 2021*

Phishing Domain Analysis

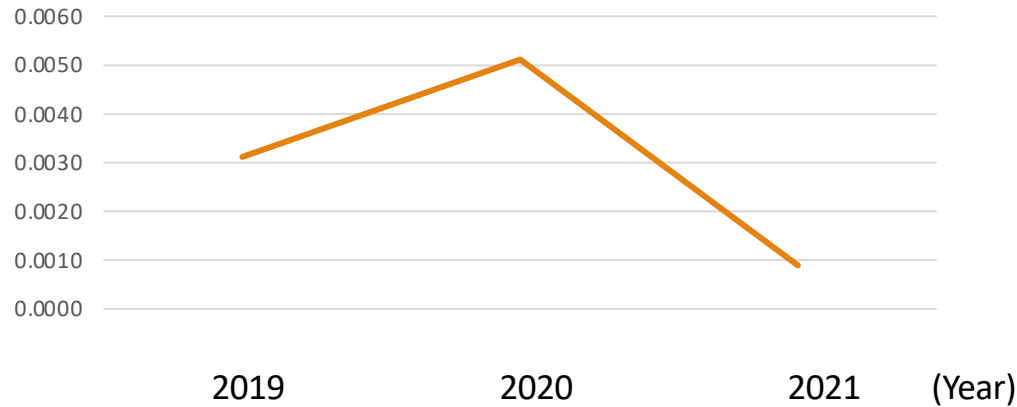
Percentage



Year	2019	2020	2021*
Phishing Domains	767	1090	271
Total Domains Under .In	19,89,482	20,91,172	29,09,452
Percentage	0.039	0.052	0.009

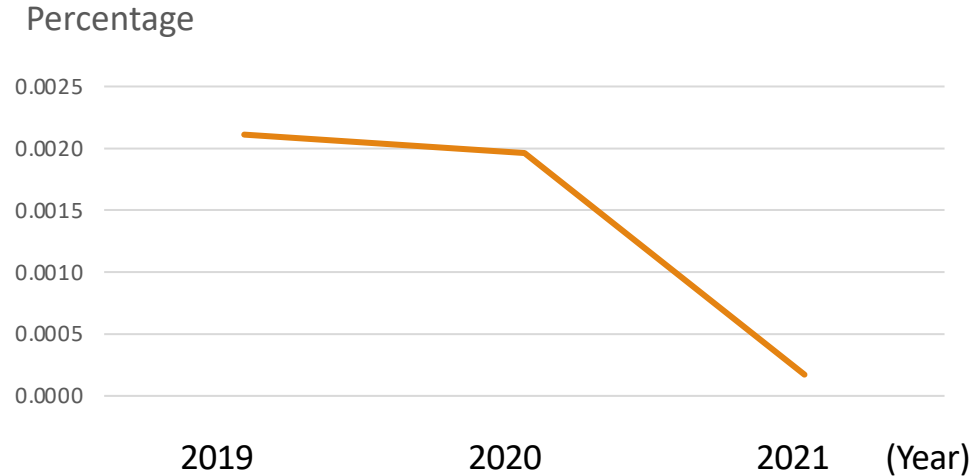
Pharming Domain Analysis

Percentage



Year	2019	2020	2021*
Pharming Domains	62	107	26
Total Domains Under .In	19,89,482	2091172	2909452
Percentage	0.0031	0.0051	0.0009

Other Domain Abuse Analysis



Year	2019	2020	2021*
Other DNS Abuse	42	41	5
TOTAL DOMAINS UNDER .IN	19,89,482	20,91,172	29,09,452
Percentage	0.0021	0.0020	0.0002

Way forward

- ▶ Building analysis in DAAR (Domain Abuse Activity Report) Project of ICANN
- ▶ Creation of global database of Abusive domains.
- ▶ Model terms & conditions for ccTLD Registrars
- ▶ Explore the role of technical solutions in mitigation of DNS abuse



DOs

- ▶ DAAR
 - ▶ Add analysis to DAAR Programme
 - ▶ Encourage all to join
- ▶ Create Global Data base of abused domains & share with all ccTLDs
- ▶ Create Co-operations and associations for regular and sustainable audit mechanism



**“And let us not grow weary of doing good, for in due season we will
reap, if we do not give up” (Galatians 6:9)**

*Thank
you*



Do's

- 1. Get an understanding of the extent of DNS abuse in your registry**
 - DAAR is a good first start and there are other third party services out there**
- 2. Continue to use Tech Day and member meetings to share best practices on DNS Abuse Mitigation**
 - Consider Creating a DNS Abuse group modelled on TLD Ops**

Don'ts

1. Forget that ccTLDs are different than gTLDs

- Capacity varies - some are very small; others larger than many gTLDs
- Most don't have contracts with ICANN

2. Ignore the relationship between ccTLDs and national govt's

- Many are part of, or close to, national governments
- ccTLDs should be building relationships with their national CERTS

Things to Think About

1. Joining DAAR

- There is no cost to joining
- A registry would have monthly reports about where it stands relative to its peers

2. Establishing a DNS Abuse group

- Need not to be a committee or working group in the normal sense
- Modelled on TLD Ops, it could be as simple as a contact list of the 'right people' in a registry to talk to about DNS abuse
- Would allow for dissemination of information e.g. on DGA's
- Members could reach out individually for help

3. Voluntary Code of Conduct

- Basically, a list of common 'best practices' e.g. join DAAR
- Emphasis would be on voluntary

Break time!
We will resume in 30
minutes (at 23:30 UTC)

DNS Abuse: What are the does and don'ts for the ccNSO?

What should the ccNSO do? What should the ccNSO not do?

Does for the ccNSO

The ccNSO should:

1

Share information with the ccTLD community

2

Share information with other parts of ICANN

3

Share best practices

4

Encourage ccTLDs to join DAAR

5

Create a DNS Abuse Mitigation Working Group

Don'ts for the ccNSO

The ccNSO should NOT:

1

Create unrealistic expectations regarding what ccTLDs and their registrars can do

2

Ignore the relation between ccTLDs and their local authorities

3

Promote commercial initiatives, studies, etc.



ccNSO

Thank you!