DNS Abuse

Anoop Kumar Pandey
Principal Technical Officer
Centre for Development of Advanced Computing (C-DAC)
Electronics City, Bangalore 560 100

Centre of Excellence in DNS Security
01st November 2021

/iiref coednssecurity.in @IIRnEF

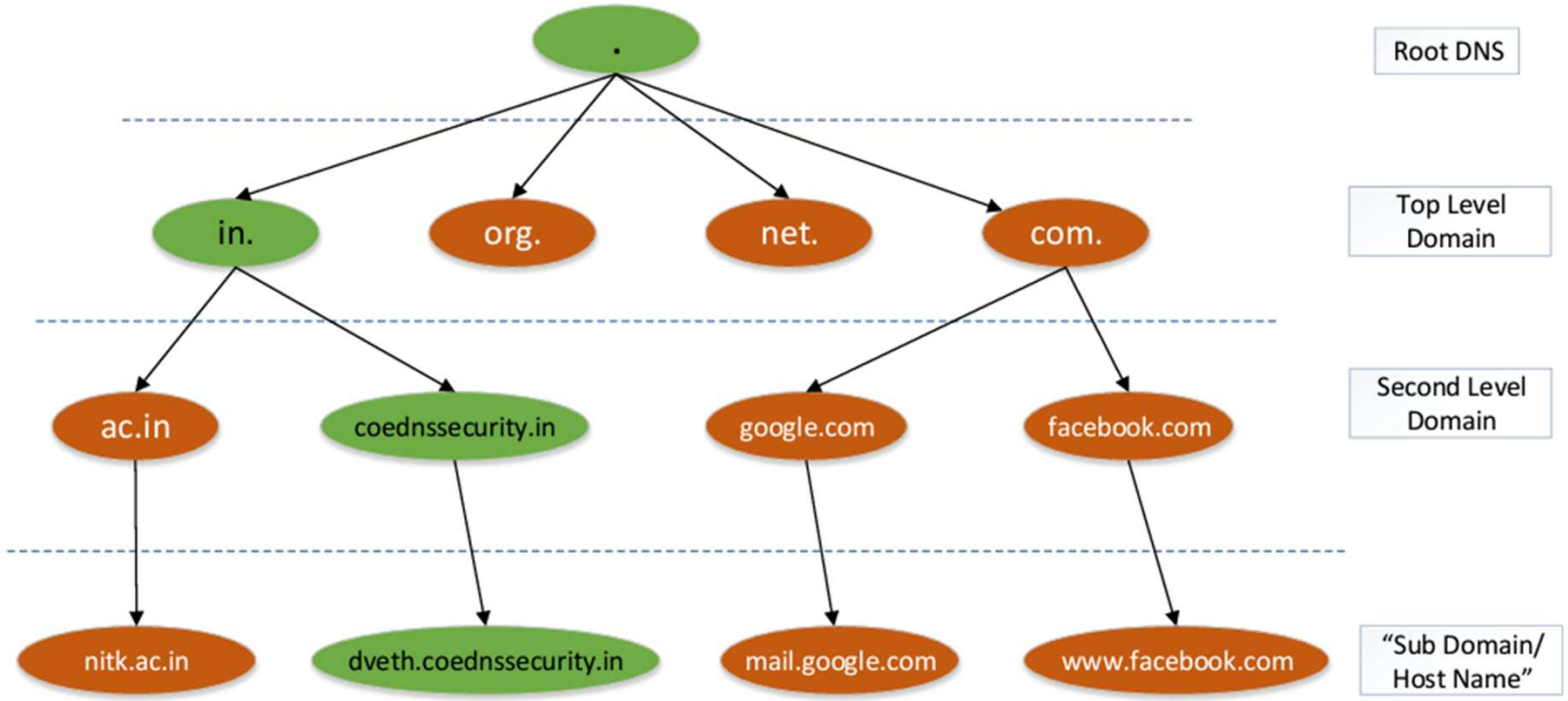
Agenda

- DNS – What, Why & How
- DNS Abuse
  - Introduction
  - Motivation & usage
  - Types & Methodologies
  - Famous attacks
  - DNS Abuse during Covid Era
  - Tools to identify abuse
  - Do's & Don'ts

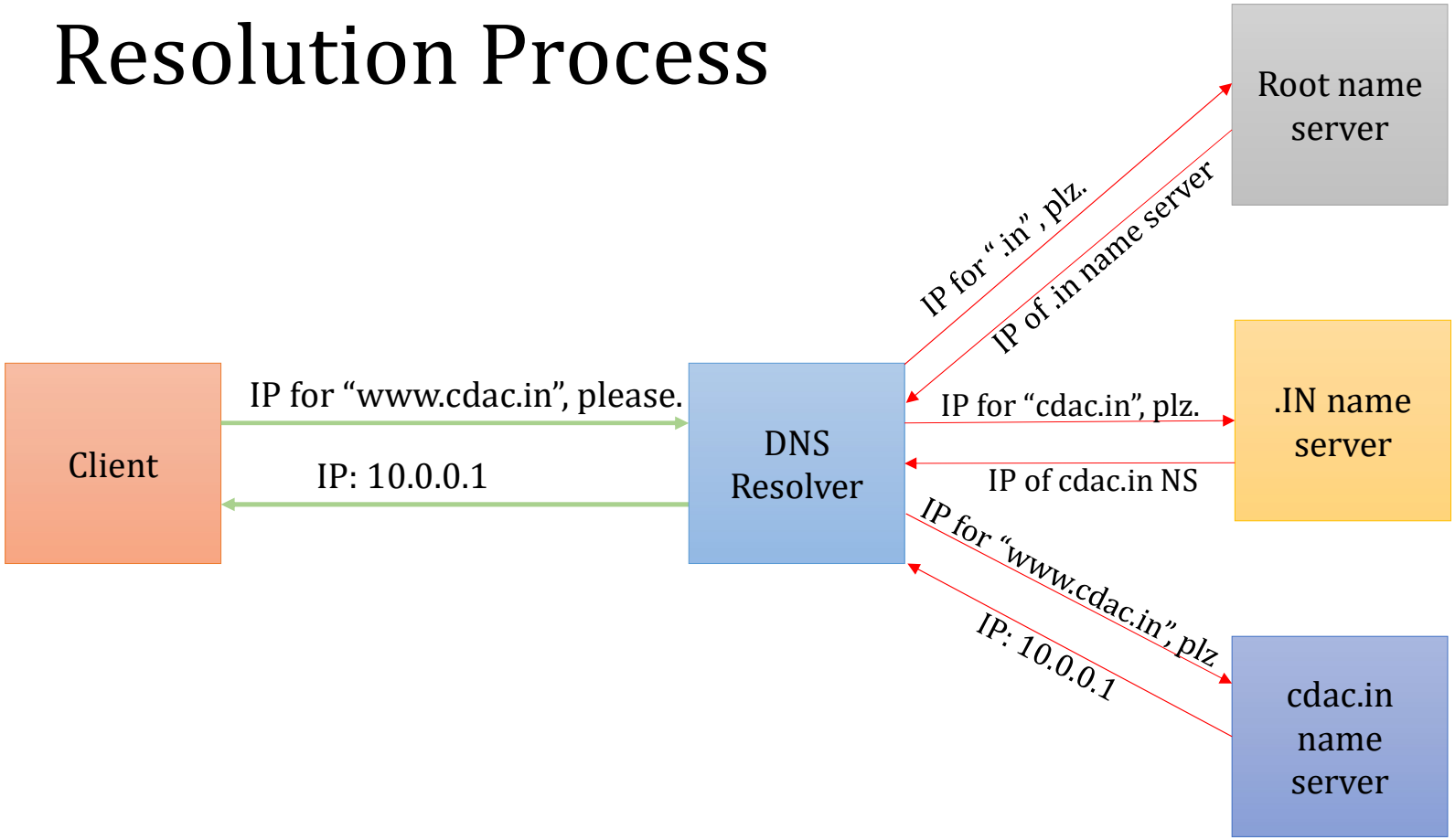
DNS

- A map from Domain name to IP Address & Back
  - www.cdac.in. → 196.1.113.45
  - www.cdac.in. → 2405:8a00:6029::45
- Technically
  - Application Layer Protocol
  - Uses UDP 53
  - TCP for Zone Transfer
  - Decentralized structure
  - Hierarchical Namespace

Structure of DNS



Resolution Process



DNS Abuse

- Abuse of the DNS
  - Disrupt the DNS infrastructure
  - E.g.: Denial of service, Data modification
- Abuse using the DNS (Misuse)
  - Perpetrate using DNS infrastructure
  - E.g. Reflection, Amplification, Tunnelling

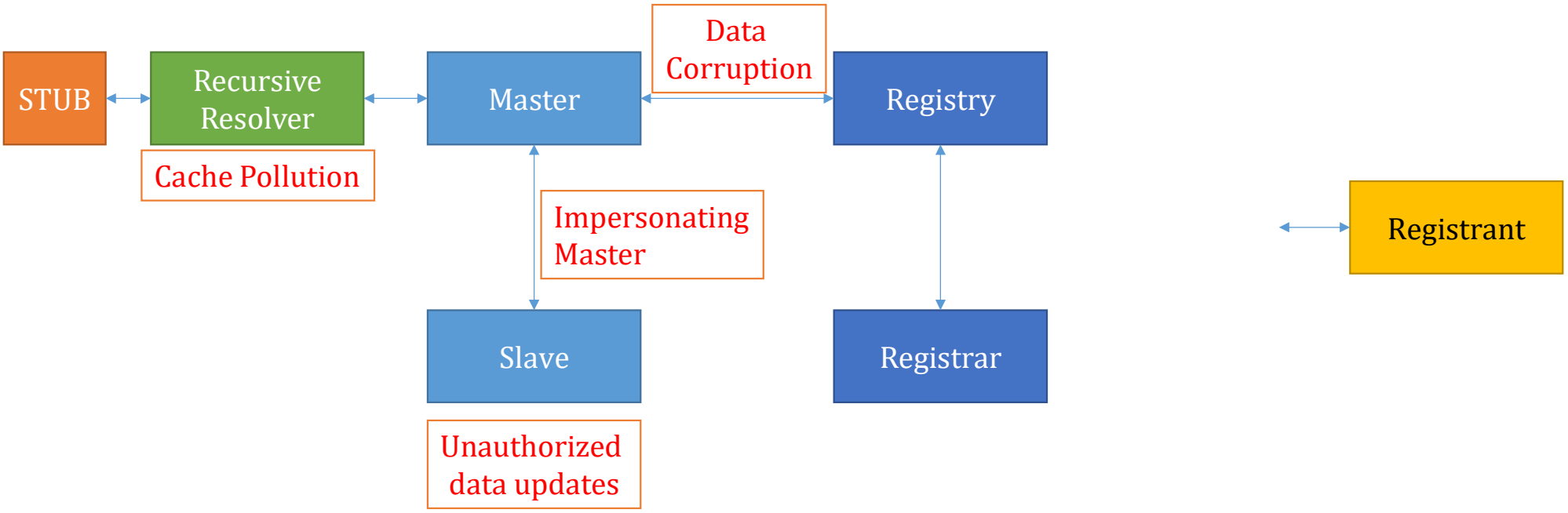
Purpose/usage

- Domains for malicious purposes
  - Website Content Abuse
    - CSAM
    - Human Trafficking
    - Material inciting violence
    - Selling Illegal/Counterfeit Products/Medicines
  - Data Exfiltration (Malware)
  - Phishing (Bait & Switch, imitator, traffic monetization, surveys….)
  - Scam (Stranded Traveller, Advance-fee scam, Lottery, Shipping, Romance…)
  - Malware distribution/C&C
  - Cybersquatting (Domain Parking)

Purpose/usage

- DNS Infrastructure or other's domain
  - Cache Poisoning
  - Attack obfuscation
  - Host Bots
  - DNS Hijacking
  - DNS data modification
  - Denial of service (NX/All Query)
  - Man in the Middle attacks
  - Tunnelling (Bypassing peripheral enterprise security)

DNS Infrastructure Attack Landscape



*MiTM between each entity

*DNS Software Vulnerability wherever applicable

Few Culprits

- Hackers
- Scammers
- Hacktivists
- Human Hacking (Social engineering)
- DNS software vulnerability
- Lack of DNSSEC, Key Rollover
- Open Resolver misconfigurations
- Lack of skilled manpower

Why DNS is targeted?

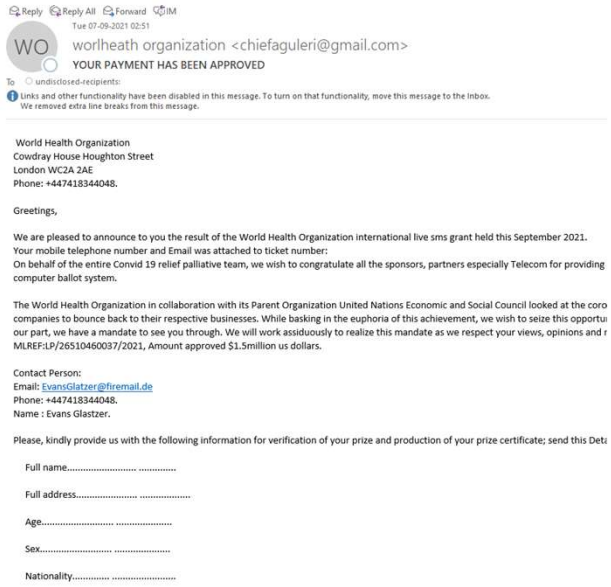
- Disrupt DNS = Disrupt Internet = Disrupt Service
  - Disruption of e-commerce activities, government services, social media engagement, learning, entertainment
- Exploit Vector
  - Malicious domain registration (Anyone can register even free of cost)
  - DNS data corruption (No integrity check)
  - DNS cache poisoning (No query response authentication)
  - Hijack name resolution/registration service
  - Large namespace
    - Homoglyphs: covid.info, c0v1d.info, covid.iṅfo
    - Typosquatting: onlinesbi.com, onlinsbi.com
    - Punycode: covid.iṅfo -> covid.xn--info-wwc

Categories of DNS Abuse

- Malware
  - Domains that facilitate hosting or distribution of malware
  - Malicious software (virus, spyware, adware, ransomware etc.) disrupting/exploiting/taking control of user's system and/or divulge information to remote system.
- Phishing
  - Domains that masquerade as trusted websites
  - Tricking/Luring users to copycat website to divulge sensitive information
- Botnet
  - Domains that are used for hosts controlling botnets and their C&C
  - Malware infected systems under command of remote admin. Used in DNS reflection/amplification attack.
- Pharming
  - Domains that host fraudulent sites
  - Redirection to fraudulent sites or services usually through DNS hijacking/poisoning.
- SPAM:
  - Domains that are included in spams and those who host spam mail exchange
  - Unsolicited bulk email. (Serves as Delivery mechanism for above ones)

Source: dnsabuseframework.org/

Examples



Reply Reply All Forward IM

Tue 07-09-2021 02:51

WO worlheath organization <chiefaguleri@gmail.com>

YOUR PAYMENT HAS BEEN APPROVED

To undisclosed-recipients:

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
We removed extra line breaks from this message.

World Health Organization
Cowdray House Houghton Street
London WC2A 2AE
Phone: +447418344048.

Greetings,

We are pleased to announce to you the result of the World Health Organization international live sms grant held this September 2021.
Your mobile telephone number and Email was attached to ticket number:
On behalf of the entire Convid 19 relief palliative team, we wish to congratulate all the sponsors, partners especially Telecom for providing computer ballot system.

The World Health Organization in collaboration with its Parent Organization United Nations Economic and Social Council looked at the coro companies to bounce back to their respective businesses. While basking in the euphoria of this achievement, we wish to seize this opportu our part, we have a mandate to see you through. We will work assiduously to realize this mandate as we respect your views, opinions and r MLREF:LP/26510460037/2021, Amount approved $1.5million us dollars.

Contact Person:
Email: EvansGlatzer@firemail.de
Phone: +447418344048.
Name : Evans Glastzer.

Please, kindly provide us with the following information for verification of your prize and production of your prize certificate; send this Det

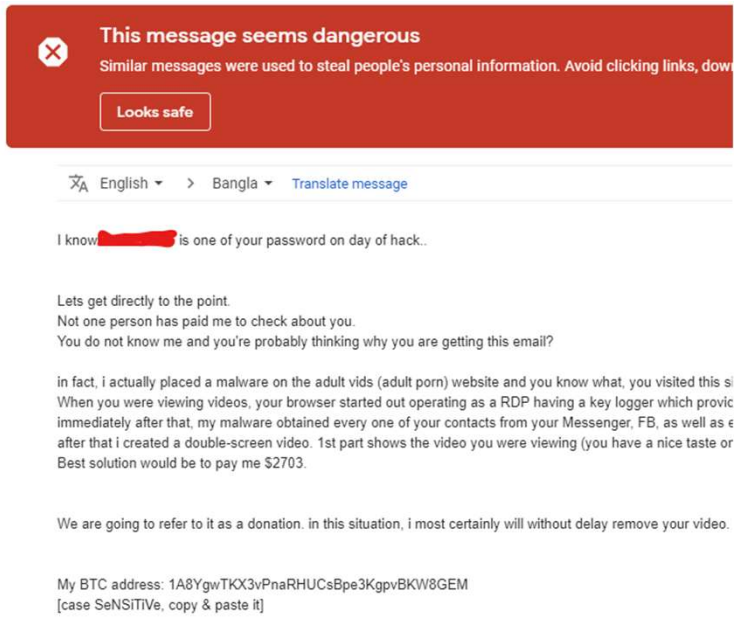
Full name..... .....

Full address..... .....

Age..... .....

Sex..... .....

Nationality..... .....



This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, dow

Looks safe

English > Bangla Translate message

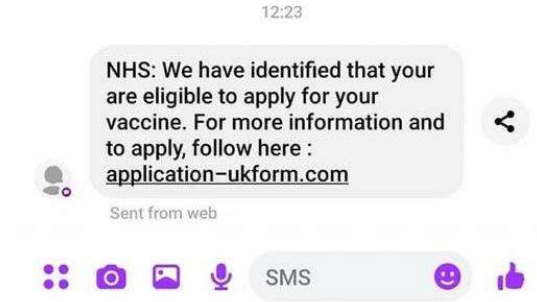
I know [redacted] is one of your password on day of hack..

Lets get directly to the point.
Not one person has paid me to check about you.
You do not know me and you're probably thinking why you are getting this email?

in fact, i actually placed a malware on the adult vids (adult porn) website and you know what, you visited this s
When you were viewing videos, your browser started out operating as a RDP having a key logger which provic
immediately after that, my malware obtained every one of your contacts from your Messenger, FB, as well as e
after that i created a double-screen video. 1st part shows the video you were viewing (you have a nice taste or
Best solution would be to pay me $2703.

We are going to refer to it as a donation. in this situation, i most certainly will without delay remove your video.

My BTC address: 1A8YgwTKX3vPnaRHUCsBpe3KgpvBKW8GEM
[case SeNSiTiVe, copy & paste it]



12:23

NHS: We have identified that your are eligible to apply for your vaccine. For more information and to apply, follow here : application–ukform.com

Sent from web

SMS

Monday, 16 March 2020

You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

1:25 pm

/iiref coednssecurity.in @IIRnEF

Difficulty in Tracking/Tracing

- Privacy Protected or Bogus Whois data
- Fast Flux, Double Flux Hosting
- Obfuscation (URL shortening, One-time use URL)
- Attackers are sophisticated, motivated, creative
- IoT Scale and vulnerability (Default Password, Misconfiguration,
- Slow Attack
- Easy to obtain TLS certificates

Source: dnsabuseframework.org/

Famous Attacks

The 2013 Spamhaus attack

- Attack traffic rate upto 300 Gbps
- A teenage hacker-for-hire in Britain
- Resource
  - 31,000 misconfigured open DNS resolvers, each at 10 Mbps
  - Source: 3 networks that allowed IP spoofing
- Attack on IX
- Lasted for 4 days (intermittently)
- Cloudflare helped mitigate

Source: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

DDoS attack on Dyn (2016)

- Claimed magnitude of 1.2 Tbps
- Access to major sites like Twitter, Netflix, Paypal disrupted
- Resource
  - Mirai Malware
  - 1 Lakh+ malicious endpoints (IoT)
  - Numerous DNS lookup requests.

Source: https://www.wsj.com/articles/denial-of-service-web-attack-affects-amazon-twitter-others-1477056080

DNSpionage (2018) & Sea Turtle (2019)

- Attack campaign using HTTP and DNS communication with C&C
- Method
  - Used Spear-phishing emails
  - Change NS record
  - Slow attack
  - Data & Intelligence gathering (Email Transcripts)
  - Target TLD: .se & .ch
- Target:
  - public and private entities (ISP, Telecom), including national security, law enforcement organization
  - primarily in the Middle East and North Africa.
  - ~40 organizations in 13 countries

Source: https://blog.talosintelligence.com/2019/04/seaturtle.html
https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html

Sea Turtle (2019)

Source: https://blog.talosintelligence.com/2019/04/seaturtle.html

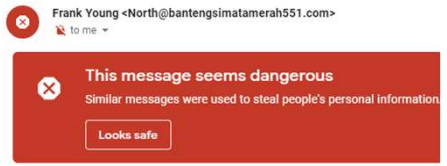
DNS Abuse (Covid Times)

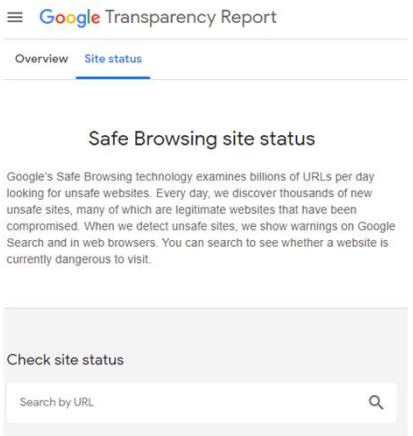
- Domains Registered
  - Jan - Nov 2020: 2.5 Lakh (approx.)
  - May – Nov 2020: 9K out of 1.47 Lakh found to have some misuse out of which 2.5K with high confidence
- Pattern of Registration
  - Keywords: covid, corona, pandemic, sars-cov, lockdown, chloroquine
  - Translated: confinmento, cloroquina
  - Homoglyphs: c0v1d, c0rona, pamdemic
  - Punycode: xn--corona-0yd
  - 60% of domains contained keywords corona, mask, covid and virus
  - 94% domains in english

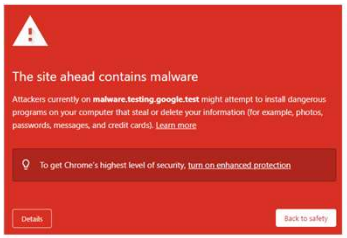
Source: data from ICANN

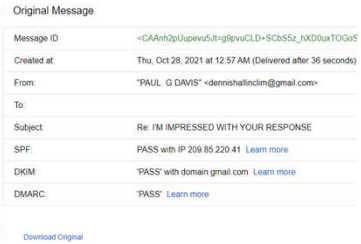
DNS Abuse (Some Checks)

- Whois data
  - Recent domain registration creation date
  - Questionable Whois contact data
  - Privacy protection service
- Email
  - Show Original
  - Name & Email
- URL check
  - Brand misuse
  - Long URL, base site absent
- TLS Certificate check
- Suspicious host, operator, NS
- Safe Browsing Check
- URL Filter
- Tools like nslookup, dig









Source: data from ICANN

/iiref coednssecurity.in @IIRnEF

Some Remedies

- DNSSEC
- Mail Exchanger Security: SPF, DKIM
- Awareness: DNS Tools, Modus Operandi
- Open DNS Resolver
  - Configure well!
- Scam: Don’t believe too much on your luck
- End Point Protection
- Report

Thank You

/iiref coednssecurity.in @IIRnEF