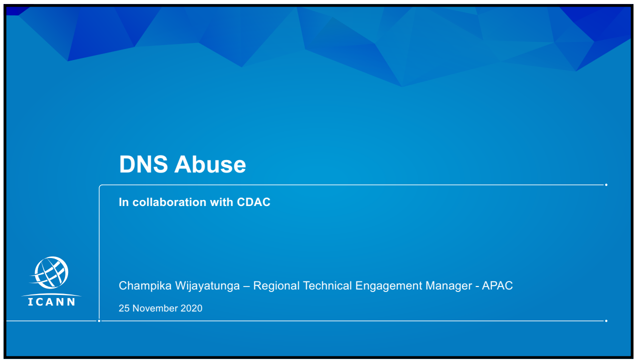
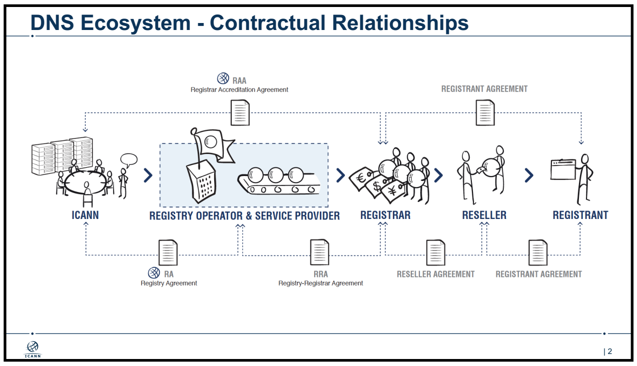


DNS Abuse

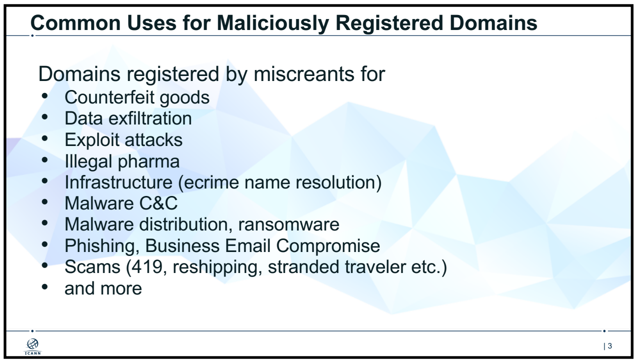
In collaboration with CDAC

Champika Wijayatunga – Regional Technical Engagement Manager - APAC

25 November 2020



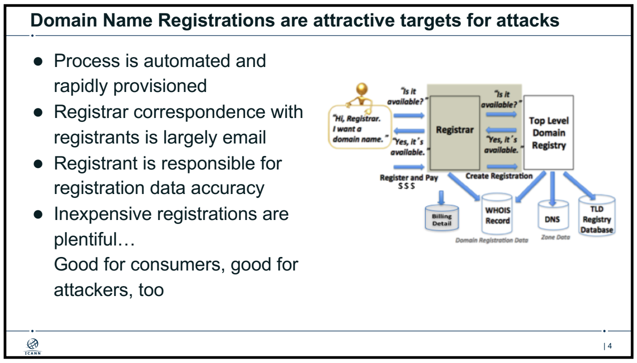
DNS Ecosystem - Contractual Relationships



Common Uses for Maliciously Registered Domains

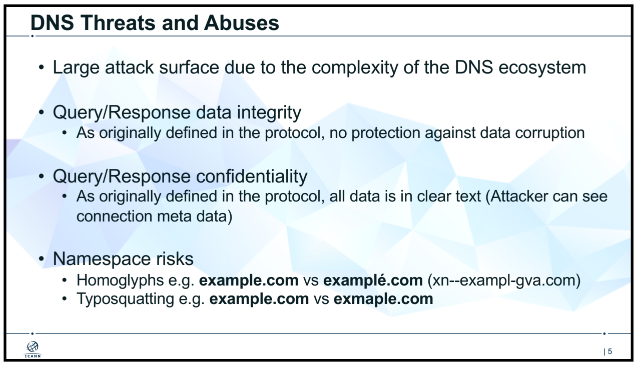
Domains registered by miscreants for

- Counterfeit goods
- Data exfiltration
- Exploit attacks
- Illegal pharma
- Infrastructure (ecrime name resolution)
- Malware C&C
- Malware distribution, ransomware
- Phishing, Business Email Compromise
- Scams (419, reshipping, stranded traveler etc.)
- and more



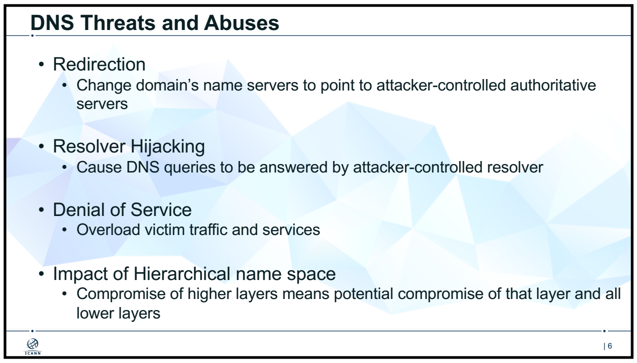
Domain Name Registrations are attractive targets for attacks

- Process is automated and rapidly provisioned
- Registrar correspondence with registrants is largely email
- Registrant is responsible for registration data accuracy
- Inexpensive registrations are plentiful…
  Good for consumers, good for attackers, too



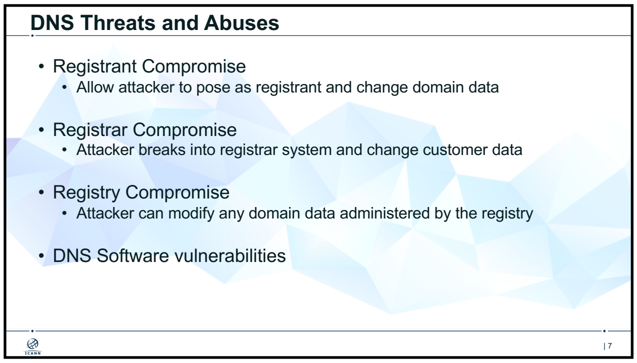
DNS Threats and Abuses

- Large attack surface due to the complexity of the DNS ecosystem
- Query/Response data integrity
  - As originally defined in the protocol, no protection against data corruption
- Query/Response confidentiality
  - As originally defined in the protocol, all data is in clear text (Attacker can see connection meta data)
- Namespace risks
  - Homoglyphs e.g. **example.com** vs **examplé.com** (xn--exampl-gva.com)
  - Typosquatting e.g. **example.com** vs **exmaple.com**



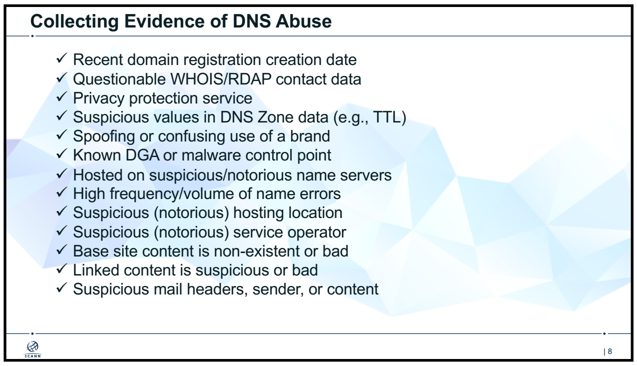
DNS Threats and Abuses

- Redirection
  - Change domain's name servers to point to attacker-controlled authoritative servers
- Resolver Hijacking
  - Cause DNS queries to be answered by attacker-controlled resolver
- Denial of Service
  - Overload victim traffic and services
- Impact of Hierarchical name space
  - Compromise of higher layers means potential compromise of that layer and all lower layers



DNS Threats and Abuses

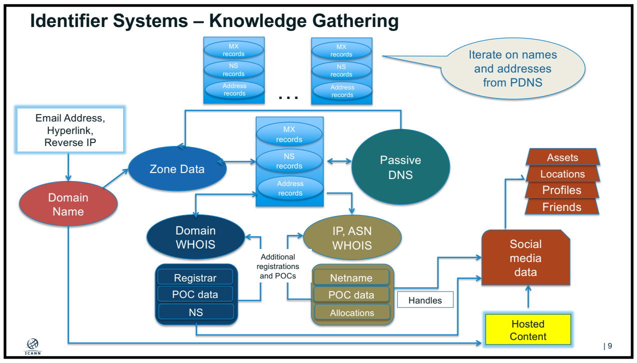
- Registrant Compromise
  - Allow attacker to pose as registrant and change domain data
- Registrar Compromise
  - Attacker breaks into registrar system and change customer data
- Registry Compromise
  - Attacker can modify any domain data administered by the registry
- DNS Software vulnerabilities



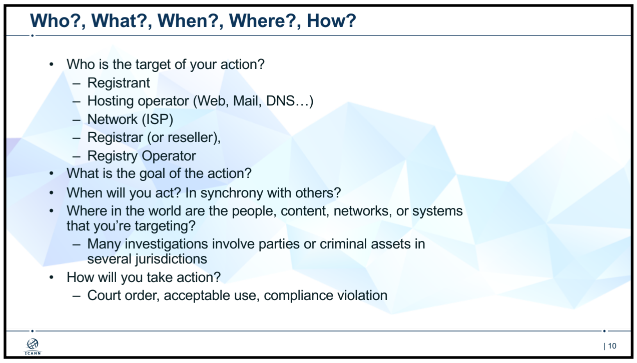
Collecting Evidence of DNS Abuse

- ✓ Recent domain registration creation date
- ✓ Questionable WHOIS/RDAP contact data
- ✓ Privacy protection service
- ✓ Suspicious values in DNS Zone data (e.g., TTL)
- ✓ Spoofing or confusing use of a brand
- ✓ Known DGA or malware control point
- ✓ Hosted on suspicious/notorious name servers
- ✓ High frequency/volume of name errors
- ✓ Suspicious (notorious) hosting location
- ✓ Suspicious (notorious) service operator
- ✓ Base site content is non-existent or bad
- ✓ Linked content is suspicious or bad
- ✓ Suspicious mail headers, sender, or content

Identifier Systems – Knowledge Gathering



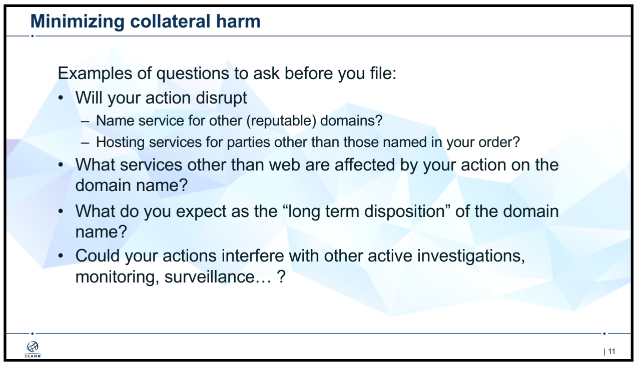
MX records
NS records
Address records
. . .
MX records
NS records
Address records
Iterate on names and addresses from PDNS
Email Address, Hyperlink, Reverse IP
Zone Data
MX records
NS records
Address records
Passive DNS
Domain Name
Assets
Locations
Profiles
Friends
Domain WHOIS
IP, ASN WHOIS
Additional registrations and POCs
Social media data
Registrar
POC data
NS
Netname
POC data
Allocations
Handles
Hosted Content



Who?, What?, When?, Where?, How?

- Who is the target of your action?
  - Registrant
  - Hosting operator (Web, Mail, DNS…)
  - Network (ISP)
  - Registrar (or reseller),
  - Registry Operator
- What is the goal of the action?
- When will you act? In synchrony with others?
- Where in the world are the people, content, networks, or systems that you're targeting?
  - Many investigations involve parties or criminal assets in several jurisdictions
- How will you take action?
  - Court order, acceptable use, compliance violation

| 10



Minimizing collateral harm

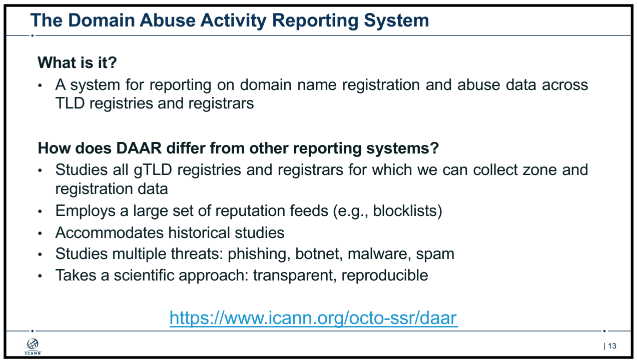
Examples of questions to ask before you file:

- Will your action disrupt
  - Name service for other (reputable) domains?
  - Hosting services for parties other than those named in your order?
- What services other than web are affected by your action on the domain name?
- What do you expect as the "long term disposition" of the domain name?
- Could your actions interfere with other active investigations, monitoring, surveillance… ?

| 11

ICANN DNS Abuse Initiatives

| 12



The Domain Abuse Activity Reporting System

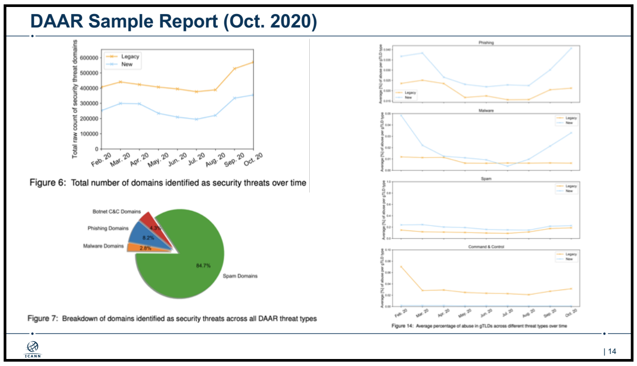
What is it?

- A system for reporting on domain name registration and abuse data across TLD registries and registrars

How does DAAR differ from other reporting systems?

- Studies all gTLD registries and registrars for which we can collect zone and registration data
- Employs a large set of reputation feeds (e.g., blocklists)
- Accommodates historical studies
- Studies multiple threats: phishing, botnet, malware, spam
- Takes a scientific approach: transparent, reproducible

https://www.icann.org/octo-ssr/daar

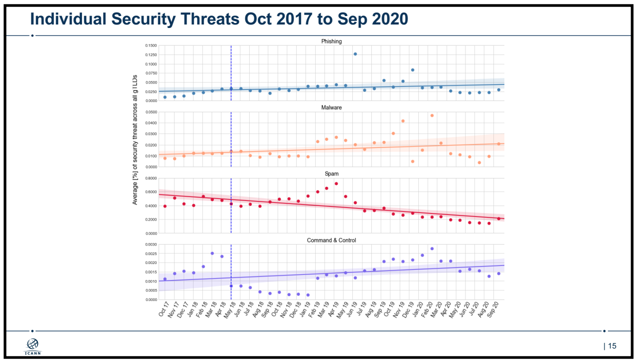


DAAR Sample Report (Oct. 2020)

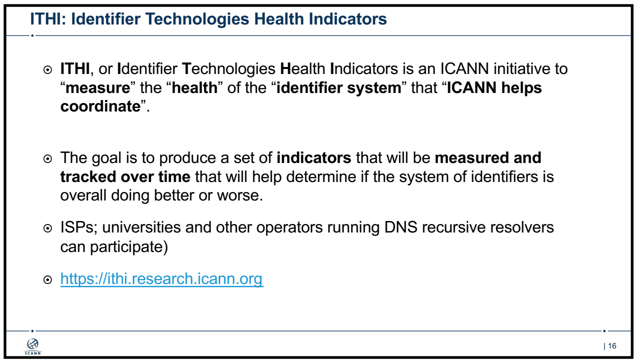
Figure 6: Total number of domains identified as security threats over time

Figure 7: Breakdown of domains identified as security threats across all DAAR threat types

Figure 14: Average percentage of abuse in gTLDs across different threat types over time

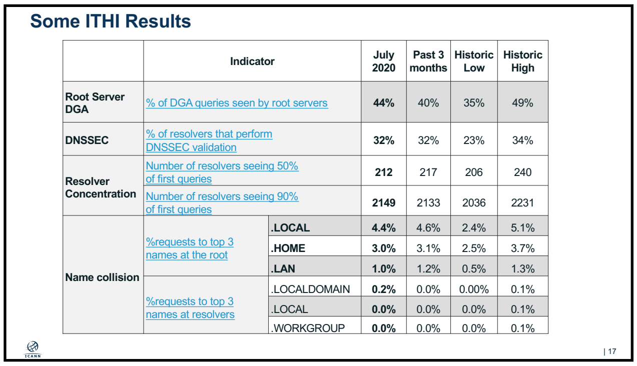


Individual Security Threats Oct 2017 to Sep 2020



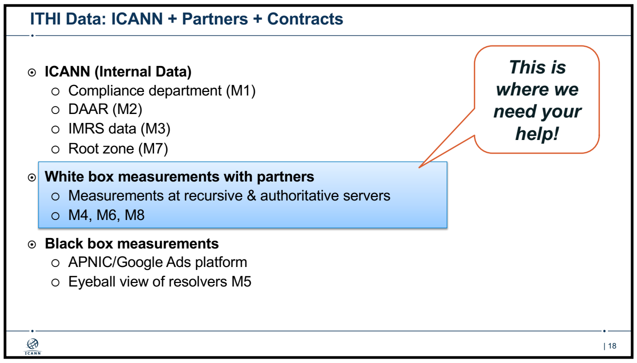
ITHI: Identifier Technologies Health Indicators

- **ITHI**, or **I**dentifier **T**echnologies **H**ealth **I**ndicators is an ICANN initiative to "**measure**" the "**health**" of the "**identifier system**" that "**ICANN helps coordinate**".
- The goal is to produce a set of **indicators** that will be **measured and tracked over time** that will help determine if the system of identifiers is overall doing better or worse.
- ISPs; universities and other operators running DNS recursive resolvers can participate)
- https://ithi.research.icann.org



Some ITHI Results

	Indicator		July 2020	Past 3 months	Historic Low	Historic High
Root Server DGA	% of DGA queries seen by root servers		**44%**	40%	35%	49%
DNSSEC	% of resolvers that perform DNSSEC validation		**32%**	32%	23%	34%
Resolver Concentration	Number of resolvers seeing 50% of first queries		**212**	217	206	240
	Number of resolvers seeing 90% of first queries		**2149**	2133	2036	2231
Name collision	%requests to top 3 names at the root	**.LOCAL**	**4.4%**	4.6%	2.4%	5.1%
		.HOME	**3.0%**	3.1%	2.5%	3.7%
		.LAN	**1.0%**	1.2%	0.5%	1.3%
	%requests to top 3 names at resolvers	.LOCALDOMAIN	**0.2%**	0.0%	0.00%	0.1%
		.LOCAL	**0.0%**	0.0%	0.0%	0.1%
		.WORKGROUP	**0.0%**	0.0%	0.0%	0.1%



ITHI Data: ICANN + Partners + Contracts

- **ICANN (Internal Data)**
  - Compliance department (M1)
  - DAAR (M2)
  - IMRS data (M3)
  - Root zone (M7)
- **White box measurements with partners**
  - Measurements at recursive & authoritative servers
  - M4, M6, M8
- **Black box measurements**
  - APNIC/Google Ads platform
  - Eyeball view of resolvers M5

This is where we need your help!

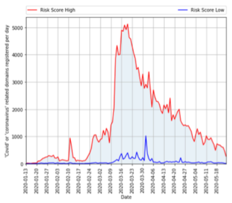
ICANN Community Work

- Domain Name Security Facilitation Initiative (DSFI) technical study group
- Outside ICANN the contracted parties (Registries & Registrars) have their project on the DNS Abuse Framework:
  - http://dnsabuseframework.org/

DNS Abuse During Covid-19

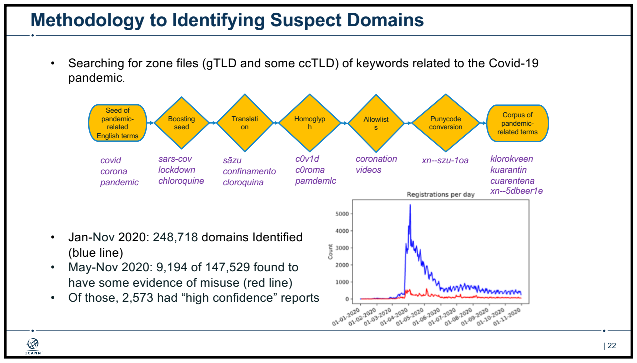
Covid-19: Some Observations

Domain trends update



(Source: John Conwell, DomainTools)

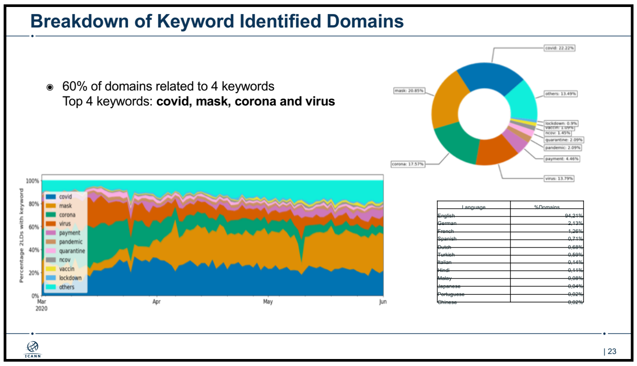
- Important events in the world leads to increase in domain name registrations conversely "DNS abuses" as well.
- Covid-19: same, especially with confinement and work from home (WFH).



Methodology to Identifying Suspect Domains

- Searching for zone files (gTLD and some ccTLD) of keywords related to the Covid-19 pandemic.

- Jan-Nov 2020: 248,718 domains Identified (blue line)
- May-Nov 2020: 9,194 of 147,529 found to have some evidence of misuse (red line)
- Of those, 2,573 had “high confidence” reports



Breakdown of Keyword Identified Domains

- 60% of domains related to 4 keywords
  Top 4 keywords: **covid, mask, corona and virus**

Language	%Domains
English	94,21%
German	2,13%
French	1,26%
Spanish	0,71%
Dutch	0,68%
Turkish	0,59%
Italian	0,14%
Hindi	0,11%
Malay	0,08%
Japanese	0,04%
Portuguese	0,02%
Chinese	0,02%

Engage with ICANN – Thank You and Questions

ICANN One World, One Internet

Visit us at **icann.org** Email: champika.wijayatunga@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann