How It Works: DNS Abuse: An Introduction

Carlos Alvarez | March 2018

Agenda

- What is DNS Abuse? DNS Misuse?

- Examples of DNS Abuse or Misuse

- Evolving DNS Threat Landscape

- Abuse in an ICANN Context

What is DNS Abuse?

- No globally accepted definition exists, but definitional variants include
  - Cyber crime
  - Hacking
  - **Malicious conduct**

- Threats to the DNS fall under three categories:
  - *data corruption*, *denial of service*, and *privacy*.

- DNS misuse is distinguished from DNS Abuse
  - Misuse refers to intentionally deceptive, conniving, or unsolicited activities that actively make use of the the DNS and/or the procedures used to register or resolve domain names.

GAC on DNS Abuse

GAC Communiqué, Beijing, April 2013

- **Safeguards Applicable to all New gTLDS**

  - **Mitigating abusive activity**—Registry operators will ensure that terms of use for registrants include prohibitions against the **distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law**.
    - https://www.icann.org/en/system/files/correspondence/gac-to-board-18apr13-en.pdf

GAC on DNS Abuse

GAC Communiqué, Hyderabad, November 2016

◉ The GAC would like to remind ICANN that the list of Security Threats in the New gTLD Safeguards is not meant to be exhaustive. In fact, the Security checks Safeguard applicable to all New gTLDs refers to "security threats such as phishing, pharming, malware, and botnets" (emphasis added), which does not exclude other relevant threats. Please describe what analysis and reporting is conducted regarding other relevant threats not listed above, including **spam**?

   ○ https://www.icann.org/en/system/files/correspondence/gac-to-icann-08nov16-en.pdf

Keep It Simple

In simpler terms "DNS abuse" refers to anything that attacks or abuses the DNS infrastructure,

or

DNS misuse refers to exploiting the DNS protocol or the domain name registration processes for malicious purposes.

Why Is the DNS a Target for Attacks

- Everyone uses the DNS to resolve user friendly names to Internet Protocol addresses

- Disrupt the DNS and you disrupt e-merchant transactions, government services, e-learning, or social engagement

- Exploit the DNS and you can trick, defraud or deceive users

- Vectors for exploitation
    - Maliciously register domain names
    - Hijack name resolution or name registration services
    - Corrupt DNS data

Operational elements of the DNS: Targets for attacks

CLIENTS ASK QUESTIONS	⟷	RESOLVERS ANSWER QUESTIONS	⟷	AUTHORITIES PUBLISH ANSWERS
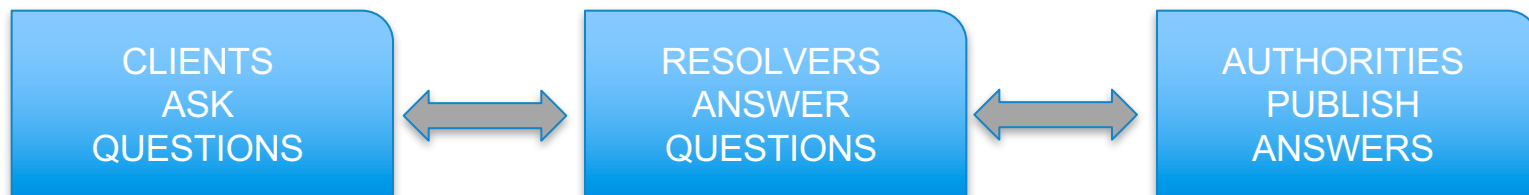
- **Authoritative** Name Servers host zone data
  - The set of "DNS data" that the registrant publishes
- **Recursive** Name Resolvers ("resolvers")
  - Systems that find answers to queries for DNS data
  - **Caching** resolvers find and store answers locally for "TTL" period of time
- **Client** or "**stub**" resolvers
  - Software in applications, mobile apps or operating systems that query the DNS and process responses

Agenda

- What is DNS Abuse? DNS Misuse?

- Examples of DNS Abuse or Misuse

- Evolving DNS Threat Landscape

- Abuse in an ICANN Context

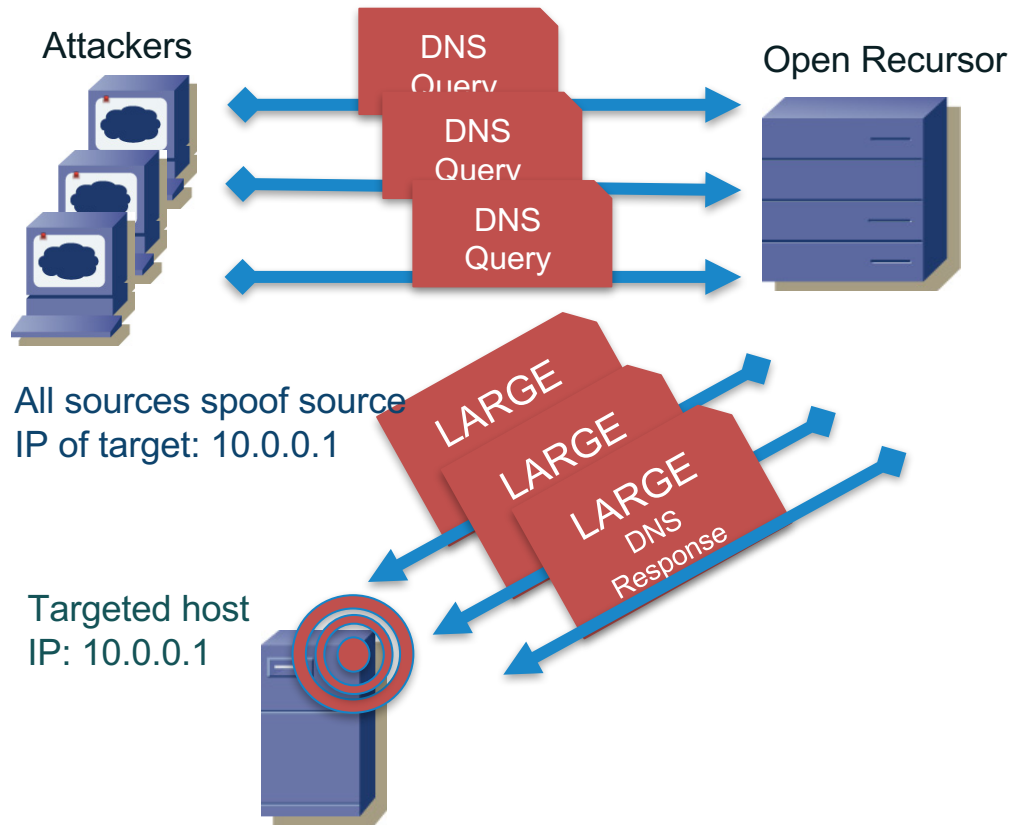# Attacks Against Name Servers or Recursors

- "Exploit to own" DOS attack

- Reflection attack (spoofing)

- Amplification attack (*ANY)

- Distributed Reflection and Amplification

- (Host) Resource Depletion Attack

- Cache Poisoning or Exhaustion attacks

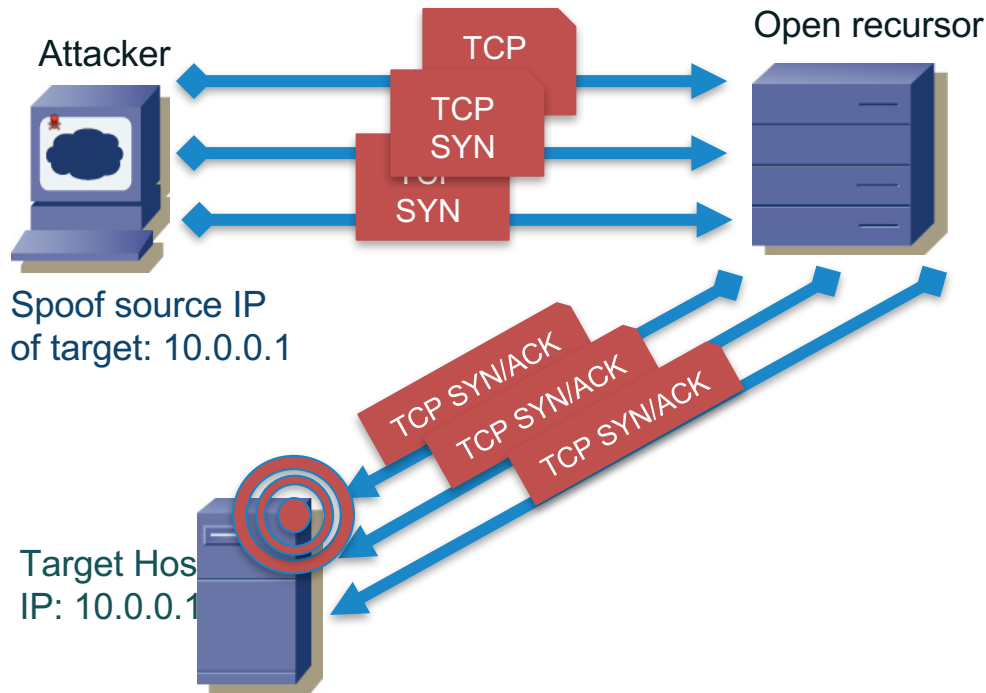- DNS Man-in-the-Middle attack

Enablers for…

DDoS attacks

Let's look at some examples

Distributed reflection and amplification attack (DDoS)

Attackers

DNS Query

DNS Query

DNS Query

Open Recursor

All sources spoof source
IP of target: 10.0.0.1

LARGE

LARGE

LARGE
DNS
Response

Targeted host
IP: 10.0.0.1

- Launch reflection and amplification attack from 1000s of origins
- Reflect through open recursor
- Deliver 1000s of large responses to target

(Host) Resource Depletion DOS attack

Attacker

Spoof source IP
of target: 10.0.0.1

TCP

TCP
SYN

TCP
SYN

Open recursor

TCP SYN/ACK

TCP SYN/ACK

TCP SYN/ACK

Target Host
IP: 10.0.0.1

- ◉ Attacker sends flood of DNS messages over TCP from spoofed IP address of target

- ◉ Name server allocates resources for TCP connections until resources are exhausted

- ◉ Name resolution is degraded or interrupted

Poisoning a Cache

- Attacker launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com **with malicious data about ebay.com**
- Vulnerable resolvers ad malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry

My Mac

What is the IPv4 address for loseweightfastnow.com

I'll cache this response… and update www.ebay.com

My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1 **ALSO *www.ebay.com is at 192.168.1.2***
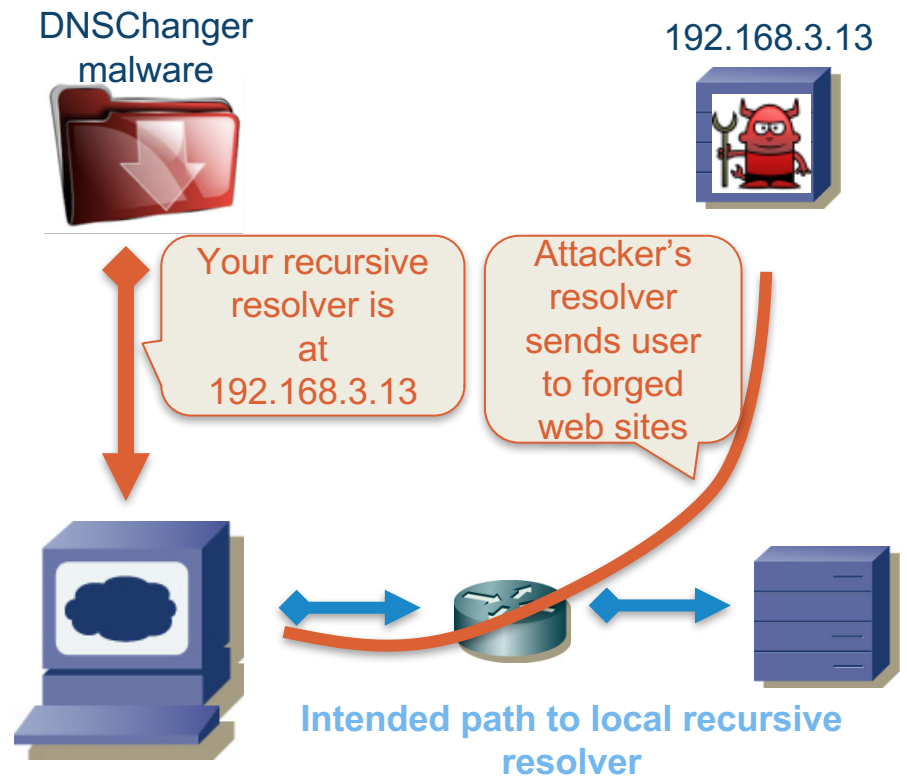
ecrime name server

Poisoning a host (DNSChanger)

Attacker distributes DNS configuration altering malware via

- Spam, drive-by download…

DNSChanger malware

- Alters DNS configuration of infected PC

- Causes all requests to go to a malicious name server run by attackers

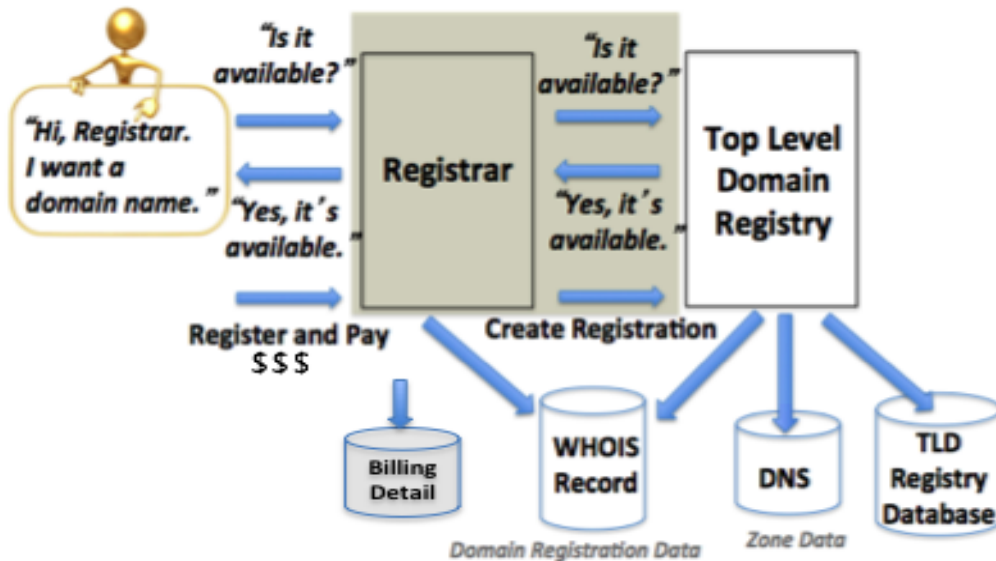- Attacker updates malware to redirect web traffic to a destination of his choosing

DNSChanger malware

192.168.3.13

Your recursive resolver is at 192.168.3.13

Attacker's resolver sends user to forged web sites

Intended path to local recursive resolver

DNS protocol and registration system misuse

- Domain name registration hijacking, DNS hijacking

- DNS protocol as a Covert Exfiltration Channel

- DNS protocol as a Covert Malware Channel

- Fast Flux

Let's look at some examples

Domain name registrations are sweet targets for attacks

"Is it available?"

"Hi, Registrar. I want a domain name."

"Yes, it's available."

Registrar

"Is it available?"

"Yes, it's available."

Top Level Domain Registry

Register and Pay $$$

Create Registration

Billing Detail

WHOIS Record

DNS

TLD Registry Database

Domain Registration Data

Zone Data

How to register a gTLD domain:

1. Choose a string e.g., `example`
2. Visit a registrar to check string availability
3. Pay a fee to register the name
4. Submit registration information

Registrar and registries manage:
- "string" + TLD (managed in registry DB)
- Contacts, DNS (managed in Whois)
- DNS, status (managed in Whois DBs)
- Payment information

> **Process is automated, rapidly provisioned.**
> **Correspondence is largely email**
> **Inexpensive registrations are plentiful…**
> **Good for consumers, good for attackers, too**

Why do attackers and criminals register domain names?

Register names, sometimes in volume to host

- Phishing (fraud) pages
- Ransomware payment web pages
- Malware distribution sites
- Scam sites (advance fee fraud, reshipping etc.)
- Counterfeit goods sites
- Illegal pharmaceutical or piracy sites

Domain names also play roles in criminal DNS Infrastructures

- Name server names for ecrime name resolution
- Names for command-control administration for botnet

Hijacking (theft) to acquire domain names

Why pay if you can crack?

- Attacker gains control of a domain registrar or registry customer account
  - Social engineering
  - Phishing attack
  - Data breach

- Attacker modifies/adds name server record for domain
  - NS record that is published in TLD zone associates domain's name server with IP address of attacker's host

- Attacker publishes "attack" zone data
  - Resource records in zone data support phishing, fraud, or defacement sites, spam mail exchanges, VoIP servers…

Exploiting registrar email correspondence (Phishing)

How many domain registrants are victims of compromised email accounts?

How many use compromised account credentials from Yahoo! or Equifax breaches?

DNS Abuse: Evade, obfuscate

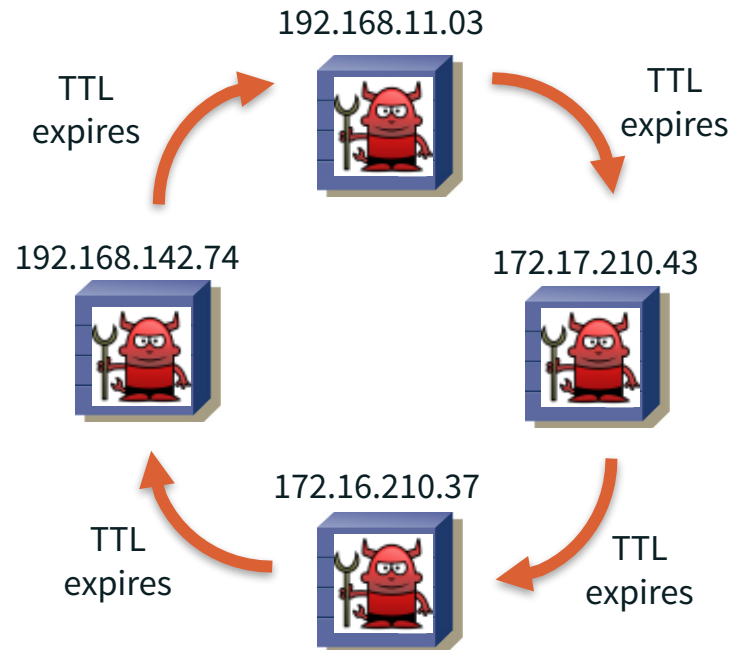## Fast flux

◉ **Attacker** associates IP address with a web proxy or name server for short time to live (TTL)

◉ Attacker changes IP of host or name server at low TTL frequency to thwart investigators

Double (fast) flux

◉ Apply fast flux technique to both web proxy and name server

192.168.11.03

TTL expires

TTL expires

192.168.142.74

172.17.210.43

172.16.210.37

TTL expires

TTL expires

DNS as a Covert Exfiltration Channel

Infected PC sends sensitive data to C&C over port 53/DNS

Infected PC 'bot'

botnet C&C

Firewall allows outbound Port 53/DNS
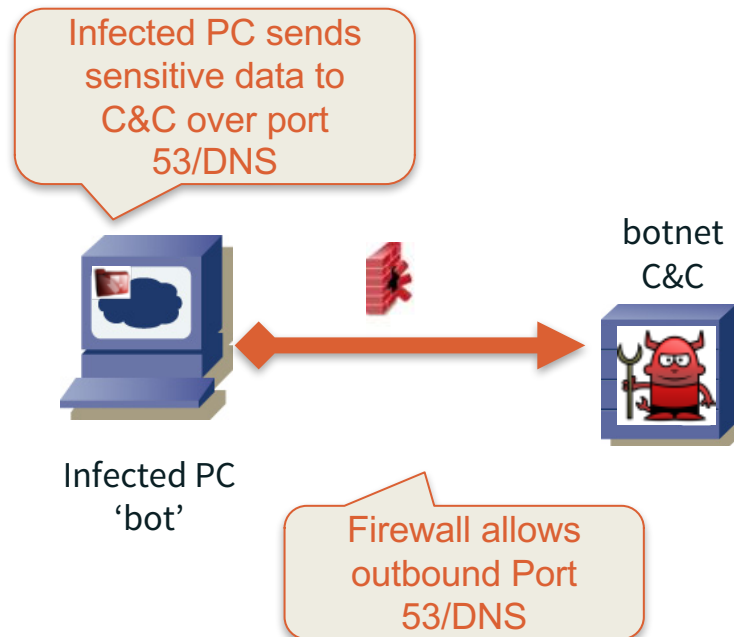
- DNS messages manipulated to forward sensitive data from infected PC *through firewall* to botnet command and control (C&C)

- Proof of concept: exfiltrate results of SQL injection attacks

DNS as a Covert Malware Channel

botnet C&C
encodes
instructions in DNS
TXT responses

Infected PC
'bot'

botnet
C&C

Firewall allows
inbound responses
via port 53/DNS
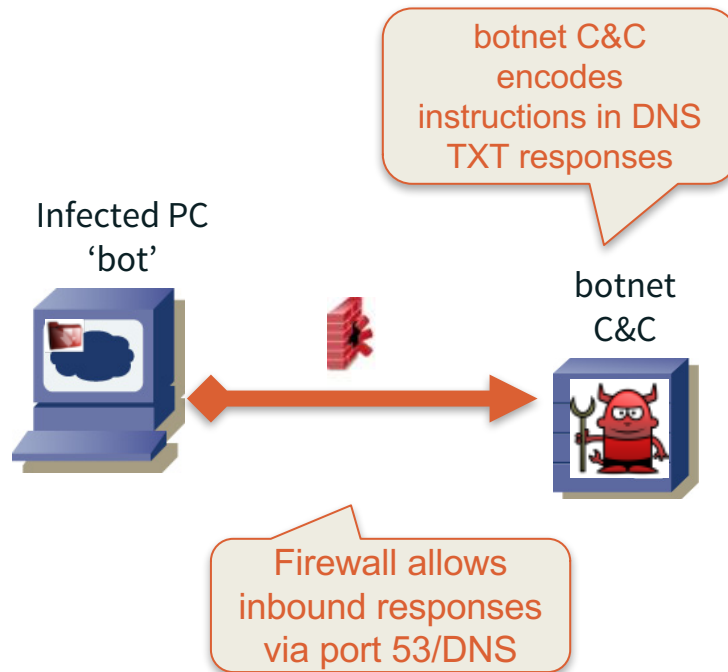
- ⦿ Malware on infected PC performs TXT lookups to botnet C&C

- ⦿ TXT responses contain instructions for bot

- ⦿ Examples in wild:
  - ○ Feederbot
  - ○ Morto

Agenda

- What is DNS Abuse? DNS Misuse?

- Examples of DNS Abuse or Misuse

- Evolving DNS Threat Landscape

- Abuse in an ICANN Context

The outlook gets grimmer and grimmer, every day…

- More and better botnets
  - DDoS as a Service?
  - Fast-flux, double-flux redux!
  - Spam as a cloud service
  - Example: Avalanche malware and DNS hosting infrastructure

- Internet of Vulnerable Things
  - Botnet recruitment to next level
  - Example: Mirai malware capable of IP, TCP, UDP, DNS volumetric attacks

- DNS: "Ignition key" or "kill switch" for emerging class of attacks?
  - Example: Wannacry, Wannacrypt

https://www.flickr.com/photos/roach/

Avalanche use of domain names

Avalanche service supported DGAs, e.g., TINYBANKER malware DGA domains of form:

qvehqbeemgfp.com

qwdssurudtpf.biz

qwdssurudtpf.pw

qwdssurudtpf.space

qwdssurudtpf.us

Top-level Domains Used			
com	xyz	top	ua
net	us	kz	at
in	uk	mobi	au
biz	space	tk	website
cn	pk	cx	am
cc	bid	aaa	br
ru	club	pl	desi
pw	eu	asia	host
me	it	bike	ml
su	ca	nl	press
tw	co	online	py
sg	tech	site	win
ws	click	info	org
	rent		

Avalanche Outcome

5 arrests in 4 countries

37 searches in 7 countries

39 servers seized in 13 countries 221 servers taken offline

64 TLDs 830,000 domains in 26 countries

Victim remediation

Awareness raising and prevention
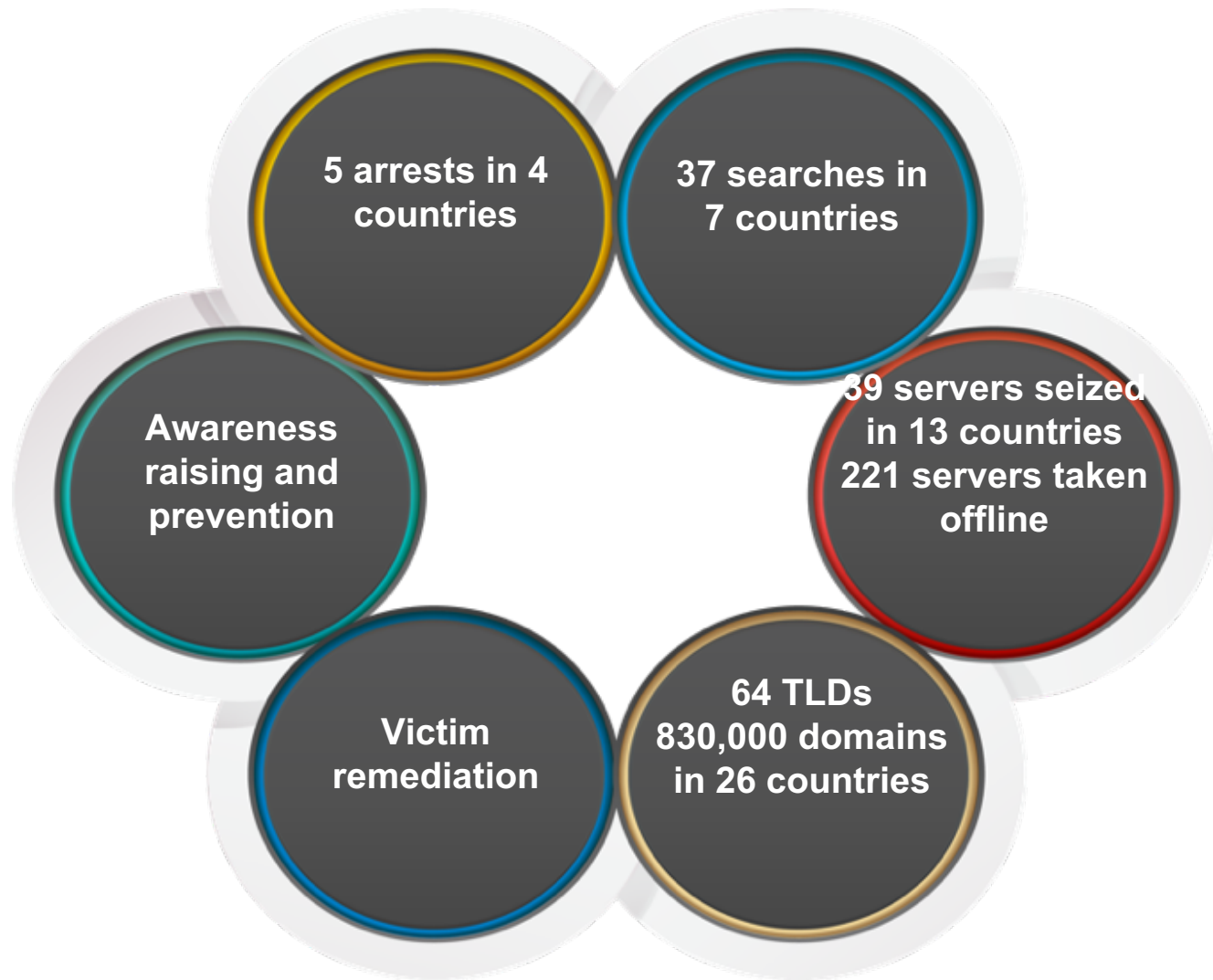
Wannacry – Kill Switch?

- Malware author may have outwitted himself while attempting to protect code against analysis
  - Intention was to have malware detect sandbox (analysis)
  - Instead, malware on infected computers attempted to connect to Command-Control server

- By registering the domains for sinkholing purposes, the researcher "unknowingly killed the malware"
  - https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

IF my ransomware fails to connect to the C2 then it's safe to *encrypt* the victim system
ELSE IF
my ransomware does connect to the C2 then exit process to avoid analysis

That's right… I think… yeah... Ok… coffee

https://www.flickr.com/photos/striatic/

Agenda

- What is DNS Abuse? DNS Misuse?

- Examples of DNS Abuse or Misuse

- Evolving DNS Threat Landscape

- Abuse in an ICANN Context

DNS Abuse in the ICANN policy world

https://www.flickr.com/photos/mypublicjournal/

- ◉ ICANN discussions often *touch* on issues relating to "abuse"
  - ○ Deliberations are often heated or controversial

- ◉ Topics with highest heat map at ICANN 61
  - ○ Whois accuracy
  - ○ GDPR
  - ○ Public safety
  - ○ Reporting abuse

Public Safety Working Group

⦿ Working group reports to and advises GAC on matters of abuse, public safety or public interest policy

⦿ Law enforcement and invited cybersecurity SMEs

⦿ Issues that the PSWG considers
  - DNS Abuse
  - GDPR
  - Whois accuracy
  - Carrier Grade Network Address Translation (CGN)
  - Fast Flux

Consideration of DNS abuse in contractual agreements

Registry base agreement

Specification 6 (4):
- Abuse PoC, malicious use of orphan glue records

Specification 11 (3):
- Registry Operator agrees to perform the following specific public interest commitments…

https://www.icann.org/resources/pages/registries/registries-agreements-en

Registrar Accreditation Agreement (RAA13)

Section 3.18:
- Abuse Point of Contact,
- Duty to investigate reports of abuse: "reasonable and prompt steps to investigate and respond appropriately to any reports of abuse"
- Publish procedures for receipt, handling, and tracking of abuse reports

Section 2.2:
- Abuse/Infringement Point of Contact for Privacy/Proxy Provider
- Publish process or facilities to report abuse of a domain name registration managed by the P/P Provider

- https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

DNS Abuse at ICANN 61

Sunday, March 11 • 11:30am
GAC PSWG Update
https://61.schedule.icann.org/meetings/647648

Tuesday, March 13 • 08:30am
GAC PSWG Meeting
https://61.schedule.icann.org/meetings/647662
GAC & PSWG: GDPR & Whois 9:30
https://61.schedule.icann.org/meetings/647663

Wednesday, March 14 • 08:30am
DNA Healthy Domains Initiative
https://61.schedule.icann.org/meetings/6447750

Thursday, March 15 • 11:30
Domain Abuse Activity Reporting (DAAR)
https://61.schedule.icann.org/meetings/647592

Engage with ICANN

Thank You and Questions

Visit **icann.org**
Email: carlos.alvarez@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann