



“DNS Abuse” an introduction

John Crain | ICANN 57 | March 2017

This is an introductory level talk

Hopefully it will peak your interest and you will be able to go learn more

Agenda 1 Slide

1

What is DNS Abuse?

2

Abuse in an ICANN
context

3

Examples of abuse

4

Learn more about
abuse

What is DNS Abuse?

Agenda Item #1

What is DNS Abuse

“**DNS abuse**” covers a wide range of activities.

No globally accepted definition exists, but definitional variants include

- Cyber crime
- Hacking
- And, as ICANN has used in the past, “**malicious conduct**”. Researchers from the University of Rome and the Global Cyber Security Center classify such threats to the DNS as falling under three categories: *data corruption*, *denial of service*, and *privacy*.

“DNS abuse” 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.

<https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf>

What is DNS Abuse

In simpler terms “DNS abuse” refers to anything that either directly abuses the DNS infrastructure,

or

misuses the DNS protocol and the registration domain processes for malicious purposes.

Abuses of Other People's Domains & DNS

Attackers
compromise
legitimate domain
registrations.

- ⊙ Host criminal DNS infrastructure
- ⊙ Domain, NS, or MX Hijacking
- ⊙ Hacktivism (e.g., defacement)
- ⊙ Tunneling (covert communications)
- ⊙ Attack obfuscation
- ⊙ Host file modification (infected devices)
- ⊙ Changing default resolvers (DNSChanger)
- ⊙ Poisoning (resolver/ISP)
- ⊙ Man in Middle attacks (insertion, capture)

How Can Bad Actors Attack the DNS?

Attack	Description
Cache Poisoning	Dupe a resolver into adding false DNS records to its cache (example: basic cache poisoning)
Indirection attack	Use malware to poison a client computer's /etc/hosts file (example: DNSChanger)
Distributed Denial of service (DDoS) attack	A resource depletion attack where 1000s of bots send DNS queries to a target NS
DDoS amplification (reflection) attack	1000s of bots issue queries that evoke a very large response message, they all "spoof" the address of a targeted name server, and the targeted NS is flooded with very large DNS response messages requested by the compromised computers
Exploitation attacks	Exploit a software flaw that causes DNS server software to fail or behave in an unintended way

Abuse in an ICANN context

The ICANN policy world

ICANN discussions often touch on issues relating to “abuse”

Whois accuracy discussions have been ongoing for years...

Issues of public safety are always a concern for governments, users, industry, everyone.

Governments

Beijing GAC communique, April 2013

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.**

Most recent GAC communiqués have some “abuse” elements raised.

<https://www.icann.org/en/system/files/correspondence/gac-to-board-18apr13-en.pdf>

Public Safety Working Group (GAC)

ICANN's Governmental Advisory Committee formed a working group to specifically discuss issues related to public safety:

Public Safety Working Group (PSWG)

Contractual elements

Registry base agreement contains some abuse-specific provisions:

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>

Contractual elements

Registrar Accreditation Agreement (RAA) contains some abuse-specific provisions:

Section 3.18:

- Abuse Point of Contact
- Duty to investigate reports of abuse: “shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse”

This week's sessions

Monday, March 13 • 1:45pm - 3:00pm

[Cross-Community Session: Towards Effective DNS Abuse Mitigation: Prevention, Mitigation & Response](#)

<http://sched.co/9now>

Tuesday, March 14 • 11:00am - 12:15pm

[ICANN GDD: Statistical Analysis of DNS Abuse in gTLDs Study Results Preview](#)

<http://sched.co/9nmp>

Tuesday, March 14 • 1:45pm - 2:30pm

[GAC PSWG presentation to GAC Plenary](#)

<http://sched.co/9np5>



Some examples of abuse

Agenda Item #3

Malware

When perpetrating nefarious behavior, on line criminals use exactly the same types of resources that everyone else uses. They may have web servers, email systems, social media profiles and of course the underlying identifiers such as names and IP addresses. Although sometimes criminals may purchase resources just like you and I, often they will build infrastructure by using compromised machines belonging to other people (usually without that person knowing). The software used to compromise those machines is generically called malware.

Malware comes from the term "MALicious softWARE"

<https://newgtlds.icann.org/en/reviews/dns-abuse/safeguards-against-dns-abuse-18jul16-en.pdf>

BotNet Command and Control

When a group of compromised machines are combined to form infrastructure then that often gets referred to as a “botnet”. Botnets can be defined as an interconnected network or computers infected with malware without the users knowledge and controlled by a third party. (Usually criminal)

Botnet comes from the term "roBOT NETwork"

The way in which these botnets are often controlled, like most things on the Internet, involves using DNS names.

Why are BotNets interesting?

Command & Control mechanisms use names in a unique manner:

Instead of just using a single name they generate random seeming names for use on a specific date.

The mechanism for generating these names is called Domain Generation Algorithms or DGA

2013-01-01 a oelzprhkm.info

2013-01-01 a sijrnpxm.biz

2013-01-01 a klzmlun.info

2013-01-01 a yosgphkcvzu.net

Conficker A names

Why are BotNets interesting?

To prevent the “bad guys” from using the botnet requires preventing them from registering and using all of the algorithmically generated names.

+/- 50,000 per day in conficker

For the “bad guys’ to maintain control they need one successful registration per day.

This type of action continues today. Avalanche blocked 800,000 names

<https://www.europol.europa.eu/newsroom/news/‘avalanche’-network-dismantled-in-international-cyber-operation>

..on to DDoS

A Distributed Denial of Service (DDoS) uses multiple, often thousands, of compromised machines (a BotNet) to attack an explicit target.

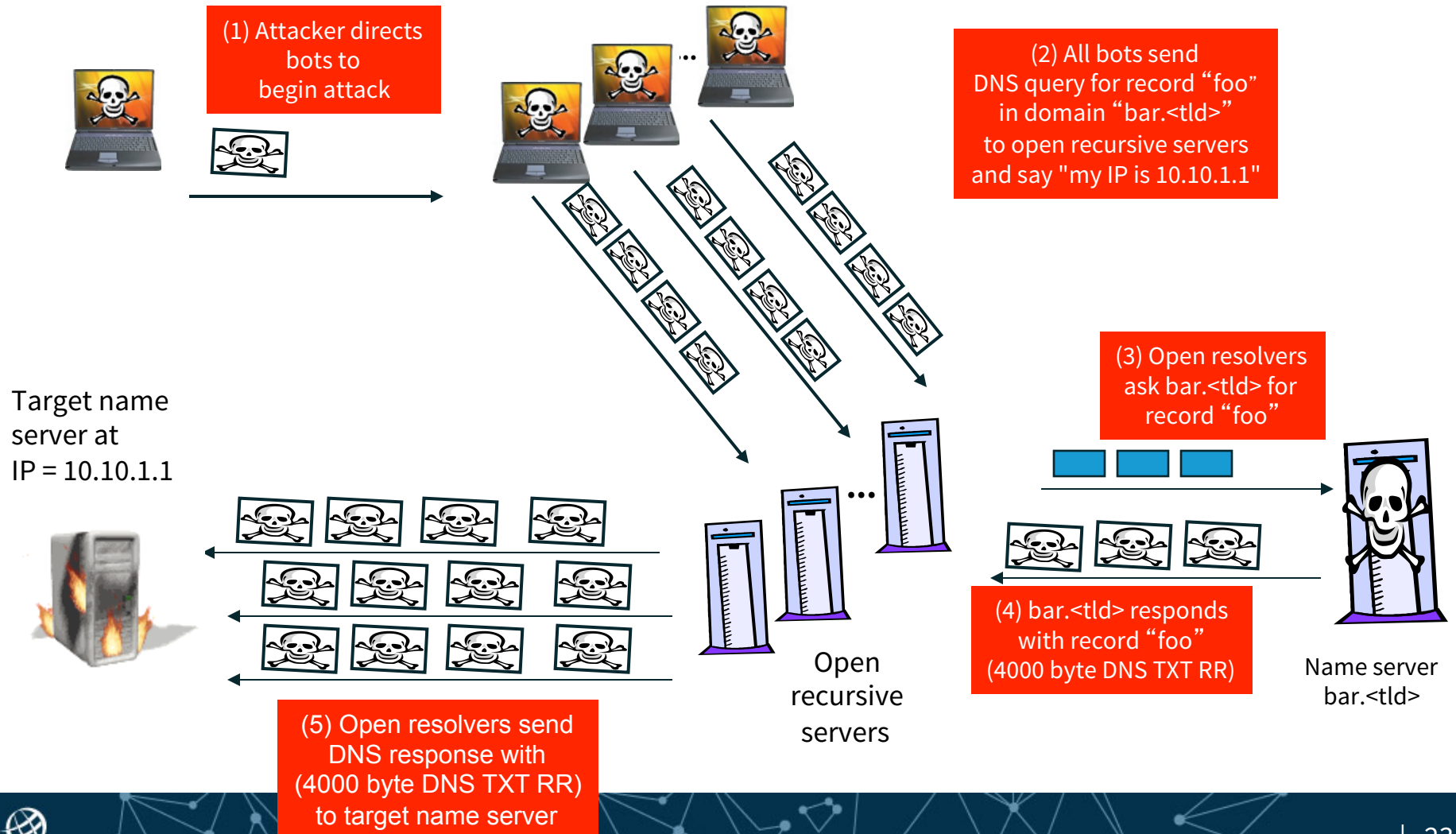
Because of the characteristics of how the DNS works it is a common medium for attacks.

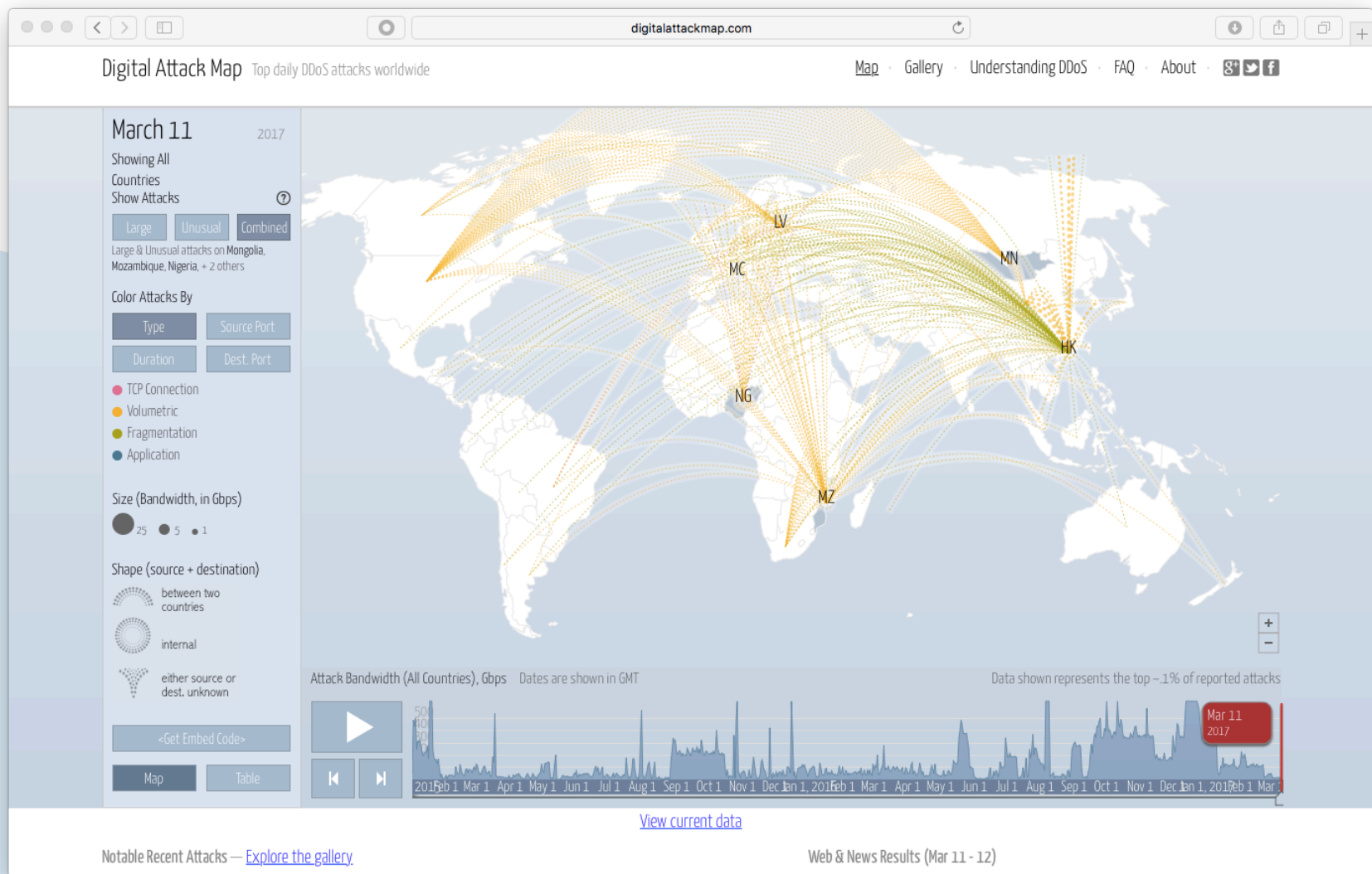
User Datagram Protocol (UDP) and the ability to use small queries to produce large responses makes it very attractive

DDoS Amplification Attack

Attacker

Zombies





Source: digitalattackmap.com

Phishing

Phishing:

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.



Spear-Phishing:

Targeted phish.

Phishers will use confusing domains to launch attacks,
compliance@ica-nn.com

Phishing

Original Message:

To: xxxxxx@berkeley.edu 
From: ADP PORTAL <director.stics@boyaca.gov.co> 
Date: Tue, 24 Jan 2017 13:31:49
Subject: Update Portal

The Human Resources/Payroll Department has completed the final paystub changes for 2017 tax year.

To view the changes to your paystub information and view/download your W-2 forms (2014 - 2016 tax years), go to: [Adp Portal](#)

We hope you find the changes to your paystub information useful and welcome any comments you may have.

Yours Sincerely,
Danielle Carrel.

Source: security.berkeley.edu

Learning more about abuse

Agenda Item #4

Malware

Nice simple explanation:

<https://ist.mit.edu/security/malware>

Malware Domains:

<https://www.malwaredomains.com>

Blocklist of Ransomware Domains

https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt

SANS Internet Storm Center (includes the above)

https://isc.sans.edu/suspicious_domains.html

BotNets and Command & Control

Enisa paper on botnets:

<https://www.enisa.europa.eu/publications/botnets-measurement...and.../fullReport>

Detecting and Tracking the Rise of DGA-Based Malware

https://www.usenix.org/system/files/login/articles/login1212_antonakakis.pdf

DDoS

Daily DDoS stats

<https://www.digitalattackmap.com>

Verisign DDoS trends report

<https://www.verisign.com/assets/infographic-ddos-trends-Q42016.pdf>

Phishing

Anti-Phishing Working Group reports

https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Phishtank

Lists recently reported Phishing domains.

<https://www.phishtank.com>

Engage with ICANN



Thank You and Questions

Reach us at:

Email: engagement@icann.org

Website: icann.org



twitter.com/icann



facebook.com/icannorg



youtube.com/user/icannnews



linkedin.com/company/icann



soundcloud.com/icann



weibo.com/ICANNorg



flickr.com/photos/icann



SlideShare

slideshare.net/icannpresentations