DNS Abuse and Misuse

OF48 Open Forum on DNS abuse and misuse
IGF 2019

Dr. Cristine Hoepers
General Manager, CERT.br/NIC.br
cristine@cert.br

cert.br nic.br cgi.br

DNS Abuse and Misuse

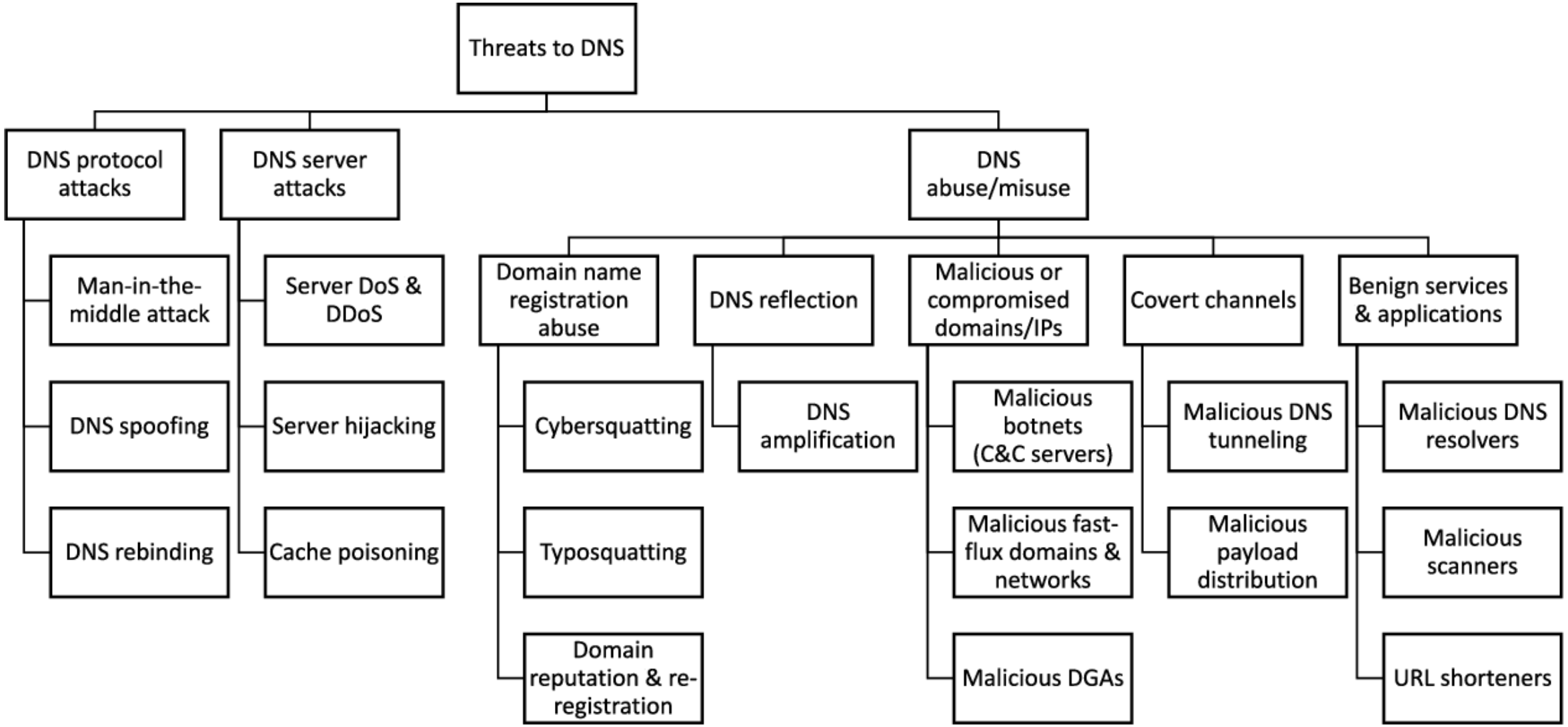
What are we talking about?

- DNS is both
  - a distributed database of domain names
  - a protocol
- attack vs abuse vs misuse

Who can do something about it?

- DNS operators
- CERTs
- Hosting providers
- ISPs
- ???

There are some attempts to map the problem – but is it enough?



Source: Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems; DOI: 10.1109/COMST.2018.2849614

DNS Hijacking is on the Media Lately:
But to describe two very different types of attacks

us-cert.gov

CISA

DNS Infrastructure Hijacking Campaig

Original release date: January 10, 2019 | Last revised: January 11, 2019

Print Tweet Send Share

The National Cybersecurity and Communications Integration Center (NCCIC), part
Cybersecurity and Infrastructure Security Agency (CISA), is aware of a global Domain Name System (DNS) infrastructure hijacking campaign. Using compromised credentials, an attacker can modify the location to which an organization's domain name resources resolve. This enables the attacker to redirect user traffic to attacker-controlled infrastructure and obtain valid encryption certificates for an organization's domain names, enabling man-in-the-middle attacks.

securityweek.com

Ongoing DNS Hijacking Campaign Targets Gmail, PayPal, Netflix Users

By Ionut Arghire on April 05, 2019

Share Tweet Recommend 62 RSS

A DNS hijacking campaign that has been ongoing for the past three months is targeting the users of popular online services, including Gmail, PayPal, and Netflix.

As part of the campaign, the attackers compromised consumer routers to modify their DNS settings and redirect users to rogue websites to steal their login credentials.

Bad Packets security researchers, who have been following the attacks since December, have identified four distinct rogue DNS servers being used to redirect web traffic for malicious purposes.

"All exploit attempts have originated from hosts on the network of Google Cloud Platform (AS15169)," the researchers reveal.

DNS Hijacking 1/2:
Credential Compromise at the Registry/Registrar/Reseller

What is compromised:

– credentials at the registry/registrar level

What is "hijacked":

– The domain itself

Who needs to act:

– The registry/registrar
  – re-instate the domain
– The domain owner
  – detection
  – adoption of best practices

DNS Hijacking 2/2:
Malicious DNS Resolver + Consumer Router Compromise

securityweek.com

Ongoing DNS Hijacking Campaign Targets Gmail, PayPal, Netflix Users

By Ionut Arghire on April 05, 2019

Share Tweet Recommend 62 RSS

A DNS hijacking campaign that has been ongoing for the past three months is targeting the users of popular online services, including Gmail, PayPal, and Netflix.

As part of the campaign, the attackers compromised consumer routers to modify their DNS settings and redirect users to rogue websites to steal their login credentials.

Bad Packets security researchers, who have been following the attacks since December, have identified four distinct rogue DNS servers being used to redirect web traffic for malicious purposes.

"All exploit attempts have originated from hosts on the network of Google Cloud Platform (AS15169)," the researchers reveal.

What is compromised:

– the user home router

What is "hijacked":

– The resolution path

Who needs to act:

– The hosting provider where the Malicious DNS Resolver is hosted

– The ISP

  – to disinfect the home router

Final Thoughts on How to Handle DNS Abuse/Misuse

What are we talking about?

- It is more than domain takedown
- There are multiple ways to [mis]use DNS
  - but not necessarily involving malicious domains
- It is hard for the user to detect if
  - the resolution path is being manipulated
  - the domain is malicious

Who can do something about it?

- DNS operators
  - provide 2FA/MFA
  - encourage adoption of best practices
- CERTs
  - analysis and coordination
- Hosting providers
  - update their policies
- ISPs and everyone else
  - best practices & cyber hygiene

Thank You

Cristine Hoepers
General Manager, CERT.br/NIC.br
cristine@cert.br

November 29, 2019

cert.br nic.br cgi.br