DNS: usage, (mis)usage, ... and abuses.

(A NOT-SO-SHORT TALK)

⇒ Santandev 2023 ⇐

About me

Pablo Carboni (46), Buenos Aires, Argentina.

- Present: SRE
- Past times: Admin *Nix, DNS, Net, etc

Twitter: @pcarboni


Mastodon: @pcarboni@bsd.network

Some motivations for this talk.

- **"It was the DNS":** Every time, everywhere, there is (bad) news about this topic, in particular due to the misusage for commercial reasons, financial, governmental, etc.
- **Advise** and raise awareness about the dimension of this problem.
- **Mainly**, we will be talking about a publication from First DNS Abuse SIG (*), published a few months ago, that lists **DNS Abuse Techniques.**

(*) Link: ⟹

Prologue.

“This presentation describes different uses of the DNS protocol, keeping in mind how it’s used everyday...

... But, when it’s not used properly, this impacts negatively in human being life."

Usage (protocol):

What's the DNS usage for (us)?

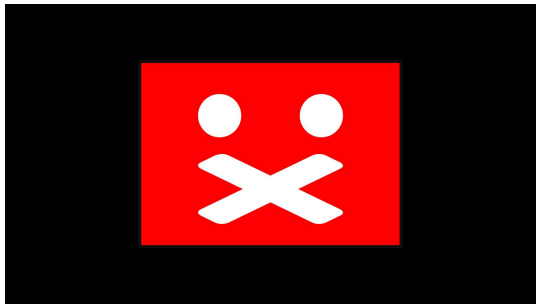
- ***ESSENTIAL:*** it's a fundamental pillar for the internet to work. Distributed, and one of the oldest protocols.
- ***Basic usage:*** links names to IP addresses, helps to send emails, etc.
- ***Daily life services*****:** part of the internet, telephony, streaming, games, all kind of transactions (commercial, etc), IoT, cloud, geolocalization, etc.

Google Maps

“Usage”? (protocol):

What’s “the DNS” usage for (us)?

- ➔ ***Other uses:*** The DNS leaves fingerprints usage like service logs.
  - ➔ *In addition, for different reasons, there is censorship and blocking of services, even persecutions…*
  - ➔ *How?! … Through the DNS!* 😞



Misusage (protocol):

- ➔ **Unwanted traffic capture:** A malicious DNS resolver, is able to store the query to be used for other (commercial) purposes.
- ➔ **Site redirection with harmful intent:** it's able to redirect queries - silently - to web sites with unsolicited software (virus, malware, etc)
    - In this case, DNSSEC, RPKI, and SSL certs (green lock) cam help to mitigate this situation...

Misusage (protocol):

Special addendum:

- **Censorship or blocking specific sites:** by governments, by court order (sometimes controversial), or by the service provider itself, etc.

- **Blocking of access to information:** same reasons as above, but this time, applied to social networks, newspapers, news, etc.

Some protocol abuses (the indirect way):

- **By modifying routes, BGP in particular:**

  By using malicious advertised routes, it is possible to redirect traffic from DNS authoritative and web servers specially crafted to impersonate legit servers.

  - **A way of mitigate this, is using RPKI (route validation)+DNSSEC.**

Note: This happened with **MyEtherWallet**, in **2018** (It's a crypto wallet), causing ***significant losses with Ethereum.***

Some protocol abuses (explicit):

- **By wildcard redirection.** If the query doesn't match with a valid query, then it answers a default record value.

⇒ In 2003, **Verisign**, as an entity authorized to provide registry services to the .com / .net TLD, adopted this form of redirection, by capturing traffic, but also causing problems in different services such as email.

(Source: ICANN)

More abuse and collateral damage. (the indirect way):

- **Sending SPAM:** The abuse of SMTP services to send spam (or other threats such as viruses, etc.), also involves the DNS, potentially slowing down the service.

- **Collateral damage:** In 2016, an attack to the former provider Dyn DNS with Mirai botnet (IoT), caused the heating system for two blocks in **Lappeenranta, Finland**, to fail ... restarted by itself due to security measures.

A recent abuse: Water Torture Attack

This is an attack type of "random hostname queries", with valid domains.

- Based on algorithms, *non-existent random FQDN valid* queries are sent, in **large** volumes, to the **authoritative DNS**, for example, via **botnets**. (Cloudflare, Feb '2023)

```
DNS Query Flood (Mirai DNS Water Torture Attack)
08:10:13.574610 IP x.x.x.x.47565 > x.x.x.x.53: 10077 [1au] A? e4hob2e7w1t7.<redacted>. (xx)
08:10:13.591581 IP x.x.x.x.52465 > x.x.x.x.53: 15764 [1au] A? sjjbm0s2ov00.<redacted>. (xx)

06:50:44.189382 IP x.x.x.x.49326 > x.x.x.x.53: 63481% [1au] A? io1f786uo3bd.<redacted>. (xx)
06:50:44.189429 IP x.x.x.x.40566 > x.x.x.x.53: 12345% [1au] A? 0hagnikgj2vq.<redacted>. (xx)

11:14:10.707489 IP x.x.x.x.37569 > x.x.x.x.53: 25550% [1au] A? 1hartrmnaiew.<redacted>. (xx)
11:14:10.709341 IP x.x.x.x.22945 > x.x.x.x.53: 31835% [1au] A? c7wnmqek2eww.<redacted>. (xx)

04:56:19.326305 IP x.x.x.x.4210 >  x.x.x.x.53: 47369% [1au] A? lmjtjgfh7b6j.<redacted>. (xx)
04:56:19.326315 IP x.x.x.x.36408 > x.x.x.x.53: 36684% [1au] A? 2vfedrv6aha5.<redacted>. (xx)

11:48:43.171738 IP x.x.x.x.47645 > x.x.x.x.53: 59218 [1au] A? 02uqhuovfilf.<redacted>. (xx)
11:48:43.171749 IP x.x.x.x.47371 > x.x.x.x.53: 62949 [1au] A? qo5etoh5foab.<redacted>. (xx)
```

First DNS Abuse SIG (Special Interest Group)

- In response to computer attacks, FIRST **(Forum of Incident Response and Security Teams)** was created in 1990. More info at: https://www.first.org/about/history

- Much later, DNS Abuse SIG was founded: https://www.first.org/global/sigs/dns/, whose objectives among others: * Define a common language * Best practices * Classify attacks * Organize meetings - conferences, etc.

- As a **result**, they published their first significant document, with a list available in the next slides, involving abuse techniques, mitigation, and interested groups (stakeholders):

“DNS Abuse Techniques and Stakeholders v1.1”

List of published abuses (1/6):

- **DGA or Domain Generation Algorithms.**
  - E.g., istgmxdejdnxuyla.ru.
- **Domain name compromise.** ***(Illegal takeover of a domain with a legitimate owner)***
  - Used for malicious activity such as sending SPAM, phishing, distributing malware, or using botnets.
- **Lame delegations.**
  - It happens with expired nameserver domains, re-registering and re-pointing them.

List of published abuses (2/6):

- **DNS cache poisoning – (also known as DNS spoofing).**
  - When the DNS resolver cache gets corrupted.
- **DNS rebinding.**
  - Redirection to a local network address, for later control of the attacker.
- **DNS server compromise.**
  - Gain administrative privileges on the DNS server.

List of published abuses (3/6):

- **Stub resolver hijacking.**
  - Intercept DNS queries and return false responses in the local resolver.
- **Local recursive resolver hijacking (CPE, etc)**
  - E.g., a (C)ustomer (P)remise (E)quipment (WiFi Router, CableModem with WiFi, ONT, etc), which gets modified externally, and a specially crafted DNS provides modified responses to the residential customer.

List of published abuses (4/6):

- **On-path DNS attack (MITM attack).**
  - When the communication between the user and the DNS service is intercepted, modifying the response.
- **DoS against the DNS.**
  - Multiple systems send malicious traffic to the destination.
- **DNS as a vector for DoS.**
  - Reflection and amplification with IP spoofing, rendering the service useless.

List of published abuses (5/6):

- **Dynamic DNS resolution** (To avoid detections)
- **Dynamic DNS resolution: Fast Flux** (To mask multiple destination hosts, with very low TTLs and multiple IPs).
- **Infiltration and exfiltration (via DNS) –** requires a delegated domain, or internally the operation of a preconfigured resolver with the zone to receive/respond to queries sent by compromised devices.

List of published abuses (6/6):

- **Malicious registration** of (S)econd (L)evel (D)omains.
- **Creation of malicious subdomains** under dynamic DNS providers.
- **Server compromise (in general)** that use DNS.
- **Spoofing with unregistered domains.**
- **Spoofing with a registered domain** (Email, URL)
- **DNS tunneling** - Tunnel another protocol over DNS. (e.g., data exfiltration)
- **DNS beacons** - C2 communication (C&C or command and control)

List of published abuses (the end):

The QR code below contains the PDF detailing the abuse techniques described before. (Feb 9, 2023, v1.1)

⇒ Credits: The author of the mentioned PDF is DNS Abuse SIG (Special Interest Group).

Special thanks to Peter Lowe for his kind help with English corrections as well. Thanks Peter!!! 😀

Thank you!


thank you
danke
格雷西
ngiyabonga
teşekkür ederim
gracias
дзякуй
hvala
mauruuru
dziękuję
obrigado
sukriya
kop khun krap
go raibh maith agat
mochchakkaram
хвала
dakujem
eskerrik asko
dankawol

Questions?