DNS: uso, (mal)uso, … y abusos.

(Una charla no tan breve)

⇒ Santandev 2023 ⇐

Acerca del autor

Pablo Carboni (46), Buenos Aires, Argentina.

- Actualmente SRE
- Epocas pasadas: Admin *Nix, DNS, Net, etc

Twitter: @pcarboni


Mastodon: @pcarboni@bsd.network

Algunas motivaciones de esta charla.

- **"Era el DNS":** Siempre hay (malas) noticias sobre esto, en particular por el mal uso con motivos comerciales, financieros, gubernamental, etc.
- **Informar** y concientizar en cuanto a la dimensión de la problemática.
- **Principalmente**, hablaremos sobre una publicación del First DNS Abuse SIG (*), hecha hace algunos meses, y que enumera **abusos en el DNS.**

(*) Link: ⟼

SCAN ME

Prólogo.

“La presentación describe diferentes usos del protocolo DNS, teniendo en cuenta los cotidianos.

... Pero cuando su uso no es el adecuado, el mismo impacta negativamente en la vida del ser humano."

Uso (del protocolo):

¿ Para qué nos sirve "el DNS" ?

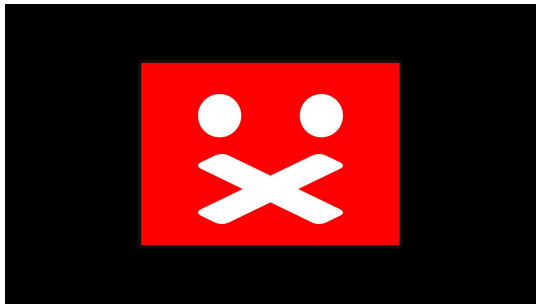
- ***IMPRESCINDIBLE:*** es pilar fundamental para que funcione internet. Es distribuido y de los más antiguos.
- ***Uso básico:*** asocia nombres a direcciones IP, ayuda al envío de e-mail, etc.
- ***Servicios de la vida diaria*****:** parte de internet, telefonía, streaming, juegos, todo tipo de transacciones (comerciales, etc), IoT, cloud, geolocalización, etc.

Google Maps

“Uso”? (del protocolo):

¿ Para qué me sirve "el DNS" ?

- ➔ ***Otros usos:*** El DNS deja huellas de uso como servicio (log).
  - ➔ *Además, por diferentes motivos, hay censura y bloqueo de servicios, incluso persecuciones…*
  - ➔ *¡¿Cómo?! … ¡A través del DNS!* 😞



Mal uso (del protocolo):

- ➔ **Captura no deseada de tráfico:** Un DNS resolver malicioso, es capaz de guardar la consulta y utilizarla con otros fines (comerciales)
- ➔ **Redirección a sitios con contenido malicioso:** es capaz de redirigir consultas - sin que lo notes - a páginas con software no deseado (virus, malware, etc).
    - En este caso, DNSSEC, RPKI, y certificados SSL (candado verde) pueden ayudar a mitigar la situación...

Mal uso (del protocolo):

Apartado especial:

- **Censura o bloqueo a sitios específicas:** Por parte de gobiernos, por orden judicial (a veces controversial), o bien por el mismo proveedor del servicio, etc.

- **Bloqueo de acceso a la información:** mismos motivos que lo anterior, pero esta vez, aplicado a redes sociales, diarios, noticias, etc.

Algunos abusos del protocolo (de forma indirecta):

- **Por modificación de enrutamiento, BGP en particular**

  Anunciando rutas maliciosamente (o por error), es posible redirigir tráfico de DNS autoritativo y webservers hacia servidores modificados para impersonar a los legítimos.

  - **Una forma de mitigar, es usando RPKI (validación de rutas)+DNSSEC.**

N.de.R.: Esto sucedió con **MyEtherWallet** en **2018** (una billetera virtual), ocasionando *pérdidas importantes con Ethereum.*

Algunos abusos del protocolo (explícito):

- **Por redirección de wildcards.** Si la consulta no matchea una consulta válida, entonces devuelve una respuesta por default.

⇒ En 2003, **Verisign** como entidad autorizada para proveer servicios al TLD .com / .net como registry, adoptó esta forma de redirección, capturando trafico, pero también ocasionando inconvenientes en diferentes servicios tales como e-mail.

(Fuente: ICANN)

Más abusos y daños colaterales (de forma indirecta):

- **Envío de SPAM:** El abuso de servicios de SMTP para envío de spam (u otras amenazas como virus, etc), involucra también el DNS, potencialmente haciendo mucho mas lento el servicio.

- **Daño colateral:** En 2016, un ataque a un proveedor de esa época, Dyn DNS, con la botnet Mirai (de IoT), dejó sin servicio de calefacción a dos cuadras en **Lappeenranta, Finlandia.** (este se reiniciaba x seguridad)

Un abuso reciente: Water Torture Attack

Es un ataque del tipo queries de hostnames random con dominios válidos.

- En base a algoritmos, se envían consultas válidas de **FQDN random inexistentes**, en volúmenes importantes al **DNS autoritativo**, por ejemplo, via **botnets**. (Cloudflare en Feb'23)

```
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 Group of Interest)

- En respuesta a ataques informáticos, se creó en 1990, el FIRST **(Forum of Incident Response and Security Teams)**. Mas info en: https://www.first.org/about/history

- Mucho más cercano en el tiempo, se fundó el DNS Abuse SIG: https://www.first.org/global/sigs/dns/, cuyos objetivos entre otros:
  - Definir un lenguaje en común * Mejores prácticas * Clasificar ataques * Organizar reuniones - conferencias, etc.

- Como **resultado**, hay una primera publicación importante, con un listado disponible en los próximos slides, involucrando técnicas de abuso, mitigación, y grupos interesados (stakeholders):

“Matriz de técnicas de abuso y stakeholders v1.1”

Listado de abusos publicados (1/6):

- **DGA o *dominios generados por un algoritmo.***
  - Ej, istgmxdejdnxuyla.ru.
- **Domain name compromise. *(Toma ilícita de un dominio con titular legítimo)***
  - Usado para actividad maliciosa como enviar SPAM, phishing, distribuir malware, o uso de botnets.
- **Lame delegations.**
  - Sucede con dominios de nameservers expirados, re-registrando y re-apuntando los mismos.

Lista de abusos publicados (2/6):

- **DNS cache poisoning – (también DNS spoofing).**
  - Es cuando se corrompe el cache del resolver.
- **DNS rebinding.**
  - Redirección a una dirección IP local, para control posterior del atacante.
- **DNS server compromise. (servidor comprometido)**
  - Ganar privilegios administrativos en el servidor de DNS.

Lista de abusos publicados (3/6):

- **Stub resolver hijacking.**
  - Interceptar consultas de DNS y devolver falsas respuestas en el resolver local.
- **Local recursive resolver hijacking (CPE, etc)**
  - Por ej, el (C)ustomer (P)remise (E)quipment (Router WiFi, CableModem con WiFi, ONT, etc), que sea modificado externamente, y un DNS server especialmente diseñado provea respuestas modificadas al cliente hogareño.

Lista de abusos publicados (4/6):

- **On-path DNS attack (ataque MITM).**
  - Cuando se intercepta la comunicación entre el usuario y el servicio de DNS, modificando la respuesta.
- **DoS against the DNS.**
  - Múltiples sistemas envian trafico malicioso al destino.
- **DNS as a vector for DoS.**
  - Reflexión y amplificación con IP spoofing, dejando inutilizado al servicio.

Lista de abusos publicados (5/6):

- **Dynamic DNS resolution** (Para evadir detecciones)
- **Dynamic DNS resolution: Fast Flux** (Para evadir con TTL muy pequeño, multiples IPs).
- **Infiltration and exfiltration (via el DNS) –** requiere un dominio delegado, o internamente la operación de un resolver preconfigurado con la zona para recibir/responder queries enviados por los dispositivos comprometidos.

Lista de abusos publicados (6/6):

- **Registración maliciosa** de (S)econd (L)evel (D)omains.
- **Creación de subdominios maliciosos** con proveedores de DNS dinámicos.
- **Compromiso de servidores** (en general) pero que usan DNS.
- **Spoofing con dominios sin registrar.**
- **Spoofing de dominio registrado** (Email, URL)
- **DNS tunneling** - Túnel de un protocolo sobre DNS (exfiltración de datos)
- **DNS beacons** - comunicación C2 (C&C o comando y control)

Lista de abusos publicados (fin):

El código QR de abajo contiene el PDF que detalla las técnicas de abuso descriptas anteriormente. (Feb 9, 2023, v1.1)

⇒ Créditos: El autor de dicho PDF es DNS Abuse SIG (Special Interest Group).

Mi agradecimiento a Peter Lowe por su amable ayuda con correcciones de la traducción al inglés.

Gracias Peter!!! 😀

¡Muchas gracias!

¿Preguntas?