TLP:RED

NXDOMAIN, ¡déjenlo hacer su labor!

Ing. Paul Bernal Mg. / Ing. Ernesto Pérez Mg.

lacnic31
06/10 DE MAYO 2019
REPÚBLICA DOMINICANA

Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia
www.cedia.edu.ec

Agenda

- Sobre Nosotros
- NXDOMAIN
- Escenario Inicial
- Análisis
- Diagnóstico
- Problemas Asociados
- Escenario Final (Resolución?)
- Propuesta

CSIRT en CEDIA

- Atendemos a los miembros de la NREN @ EC
- Comenzamos a operar en 2013
- Miembros de diversos foros de apoyo (WARP, TI, FIRST)
- Disminución de eventos de seguridad
- Creación de sistema de monitoreo y estadísticas
- Punto de contacto para incidentes
- Generación de aplicaciones y conocimiento:
  - investigaciones, sistemas
- Continuo intercambio con otros CSIRT:
  - Congresos, listas, foros
- Apoyo ante problemas suscitados.

NXDOMAIN

- DNS traduce nombres a direcciones (& viceversa)
- ¿Qué responder si el nombre no existe o es inválido?
- **NXDOMAIN** representa esta condición
- Elementalmente es un estado de error (404 del DNS)

```
[pbernal@t470s ~]$ host undominioquenoexiste.com
Host undominioquenoexiste.com not found: 3(NXDOMAIN)
```

```
[pbernal@t470s ~]$ host unhost.cedia.org.ec
Host unhost.cedia.org.ec not found: 3(NXDOMAIN)
```

Así sabemos que un dominio no está registrado o
Que el host dentro de esa zona no existe.

TLP:RED

Escenario Inicial

- Ofrecemos DNS Resolvers para nuestras IES
- IES reporta problemas de intermitencia en acceso
- “Pensamos eran sus DNS … pero probamos con otros”:
  - **universidaddeloja.edu.ec** dice estar en venta
  - **universidaddeloja.edu.ec** resuelve a una **IP rara**
- Susto, alarma, verificaciones
- Desconcierto y desorientación!

TLP:RED

Análisis (de la IES)
[por suerte son de los que prueban]

- **Navegador:**
  - **www.cedia.org.ec** abre correctamente
- **NSLookup (@Windows):**
  - **www.cedia.org.ec.edu.ec**[1] resuelve la **IP rara**

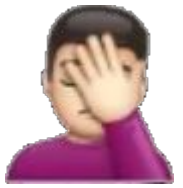
[1] Busca primero agregar el search-domain **unl.edu.ec/edu.ec**

TLP:RED

Análisis (nuestro)

- **Navegador:**
  - **www.cedia.org.ec** abre correctamente
- **NSLookup (@Linux):**
  - **www.cedia.org.ec** resuelve bien
  - **universidaddeloja.edu.ec** resuelve la **IP rara**
  - **unl.edu.ec** resuelve bien
- universidaddeloja.edu.ec **≠** unl.edu.ec
- cualquiercosa**.ec** resuelve la **IP rara**
- ter**n**a.unl.edu.ec **≠** te**m**a.unl.edu.ec

Diagnóstico

- NIC.ec está haciendo:
  - DNS hijacking https://bit.ly/2DU0Gla
  - Corrupting DNS https://bit.ly/2H5Oj7z
  - typo-squatting https://go.icann.org/2V9Sgfw
  - Capturando solicitudes para … ???
- La **IP rara** además es un resolver!
  … que siempre responde con: la **IP rara** 

Problemas asociados (los simples)

- Si no se devuelve NXDOMAIN no se puede adivinar que el dominio/host está mal o no existe.
- Si se hace una pregunta (cualquiercosa.ec) incorrecta, siempre responde la **IP rara**.
- Qué tal si alguien consulta/configura: **dms.unl.edu.ec**
- Al no ser autoritativo, el resolver de la **IP rara** devuelve **REFUSED** a toda pregunta que no es **.ec**.
- Dificultades en el troubleshooting: te**rn**a.unl.edu.ec

Problemas asociados (más graves)

- Rompe qname-minimization:
  - Si **nombre.tld** no existe ⟹ **ftp.nombre.tld** tampoco
  - Si resuelve ***.tld** debe preguntar y guardar cada variante
  - Más propenso a consumo de RAM & recursos

Problemas asociados (más graves)

- Otros ataques de RAM:
  - Malware podría intentar resolver millones de records dentro de un **dominio.tld** hasta agotar la RAM
  - Aplicaría al DNS del registrar o al resolver particular

Problemas asociados (más graves)

- Otros ataques de RAM:
  - Comprometer un sitio web importante.
    Ejm: **sitiopopular.com**
  - (Nada que ver con el **tld** objetivo...)
  - A cada usuario de ese sitio que se conecte se le obliga a resolver **$RANDOM.dominio.tld**
  - O a resolver **$RANDOM.$RAND.tld**
  - Sería un ataque de miles de usuarios repentinamente

Problemas asociados (más graves)

- Los correos no rebotarían adecuadamente, o a tiempo:
  - Correo a **mail.umiversidad.edu.tld** posiblemente dé timeout (no tiene SMTP abierto en esa IP [quizá])... pero:
  - Me daré cuenta dentro de varios días.
  - O quizá rebote el mensaje con un delivery failure
  - O peor aún, pudiera tragarse el mensaje y almacenarlo sin nuestro consentimiento

Problemas asociados (más graves)

- Algunos servidores de correo, si no encuentran un **MX** buscan el **A**
  - Entonces **umivesidad.edu.tld** podría resolver el A y sucederá lo descrito en el slide anterior.

Problemas asociados (más graves)

- Podría dificultar el proceso de encontrar los **NRD**:
  - Los spammers se orientarían rápidamente a los **tld** que permitan * para poder ocultar la primera vez que se vió un dominio
  - Pueden provocar que un dominio “se vea” al realizar consultas que sabe que serán respondidas

TLP:RED

Escenario Final (resolución?)

- NIC.ec jugó un rato al escalamiento del caso
- Gran Jefe Pluma Blanca confesó la práctica aplicada
- Respondió pronto / favorablemente y
- Detuvo la práctica aplicada… pero… **No son los únicos!**

Propuesta de Verificación Continua

- Descargamos lista de sufijos:
  - https://publicsuffix.org/list/public_suffix_list.dat
- Filtramos sólo los ICANN domains
- Filtramos el sufijo museum (generan ruido por ahora)
- Generamos una consulta A a $RAND.sufijo
- Registramos si la respuesta no contiene:
  - NXDOMAIN
  - SERVFAIL
  - 127.0
  - your-dns-needs-immediate-attention

Propuesta de Verificación Continua

- Resultado de 7339 dominios y sufijos tenemos:
  - 41 responders de records A $\Longrightarrow$ 0.56%
  - 12 responders de records MX $\Longrightarrow$ 0.16%

Propuesta de Contribución (ToDo)

- Un sitio web con
  - Publicación de resultados (def frecuencia revisión)
  - Consultas en línea con:
    - Filtrado
    - Listar/descargar todos los evaluados
    - Marcado visual de los incorrectos
    - Históricos
    - Stats
    - Captura de pantalla (de página incorrecta)
  - Consultas vía API?

TLP:RED

Para Terminar …

★ NO hemos considerado aún aspectos, responsabilidades, obligaciones legales:

- ¿Porqué **estenombre.unl.edu.ec** está a la venta?
- ¿Qué hacer si NIC.ec no respondía como lo hizo?
- ¿Qué datos se guardaban de las solicitudes?
- ¿Quién(es) debe(n) controlar / regular esto?
- …

Gracias !

Paul Bernal / CSIRT-CEDIA
paul.bernal@cedia.org.ec