VORACLE

COMPRESSION ORACLE ATTACK

Yunie Lucatero

@yunniscan

#whoami

- Yunuen Lucatero
- Consultor de seguridad @ Minsait

- Crypto fanatic
- CTF | Challenges (wannabe)
- Blogger ocasional

@yunniscan

https://enigmagirl.com

Contenido

- VORACLE
- Circunstancias del ataque
- Oracle | Oracle Attack
- Compresión de datos
- Compression Oracle Attack
- VOracle Attack
- Recomendaciones

VORACLE

Ataque que permite recuperar tráfico HTTP, que es enviado a través de una VPN (OpenVPN), bajo ciertas circunstancias.

- by Ahamed Nafeez (Black Hat & DefCon)

VORACLE = CRIME para VPNs

Circunstancias del ataque

- Protocolo **OpenVPN**

- **Compresión** habilitada (cliente y servidor)

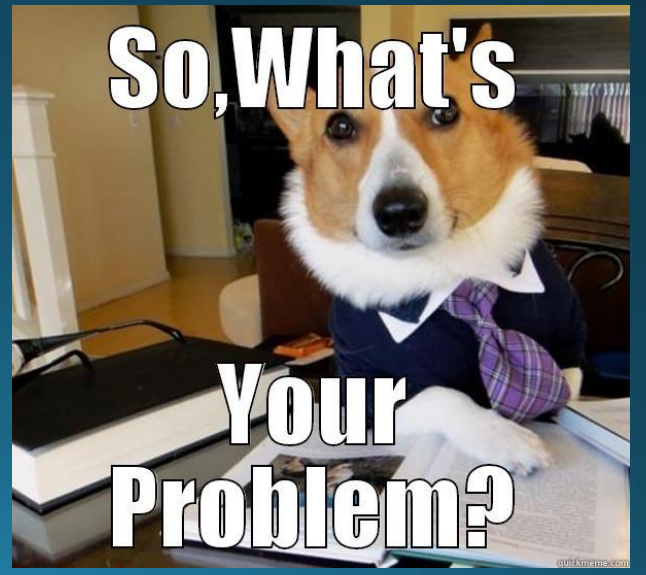
- El atacante puede observar el tráfico **VPN**.

- El usuario visita un sitio HTTP (controlado por el atacante).

¿Problema?

El texto claro (tráfico HTTP) se comprime antes de ser cifrado.

Es una característica por defecto de OpenVPN.



Oracle

"Individuo que sabe el *número personal de un dios*, lo cual le permite obtener información que es usualmente inaccesible para los mortales, como por ejemplo: premoniciones. "

Oracle

En criptografía es lo mismo. Un **oracle** es cualquier información extra que un sistema divulga sobre algo, que de otra forma no estaría disponible.

Oracle attack

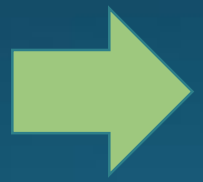
Ataque que explota una vulnerabilidad en un sistema que puede ser usado como un “oracle”, indicándole al atacante si está cerca o no de alcanzar su objetivo.

Compresión de datos

- Familia LZ77 (LZO / LZ4)
- Reemplaza patrones redundantes

102 caracteres

Everything looked dark and bleak, **everything looked** gloomy and **everything** was under a blanket of mist



89 caracteres

Everything looked dark and bleak, (-34,18)gloomy, and (-54,11)was under a blanket of mist

Compresión de datos

Longitud de los datos cifrados

No.	Time	Source	Destination	Protocol	Length	Info
62	6.768544	192.168.1.135	213.199.179.148	UDP	75	25594 → 40043 Len=33
63	6.929744	213.199.179.148	192.168.1.135	UDP	489	40043 → 25594 Len=447
64	6.931125	192.168.1.135	81.167.8.24	UDP	147	25594 → apx500api-2(2265) Len=105
66	7.113726	81.167.8.24	192.168.1.135	UDP	88	apx500api-2(2265) → 25594 Len=46
81	8.975899	192.168.1.135	111.221.74.32	UDP	178	25594 → 40007 Len=136

Longitud = Oracle

Compression Oracle Attack

MITM

secreto=3245777

Compresión
+
Cifrado

Texto cifrado
+
Longitud de datos comprimidos

Compression Oracle Attack

MITM

secreto=3245777;secreto=1

Compresión
+
Cifrado

Longitud (datos cifrados) = 30

Compression Oracle Attack

MITM

secreto=3245777;secreto=2

Compresión
+
Cifrado

Longitud (datos cifrados) = 30

Compression Oracle Attack

MITM

secreto=3245777;secreto=3

Compresión
+
Cifrado

Longitud (datos cifrados) = **29**

Más compresión, menor longitud

VOracle Attack

Aplicación Web
(HTTP)

VPN
(Compresión habilitada)

Usuario VPN

MITM
(pasivo)

El atacante lleva a cabo *Compression Oracle Attacks* sobre las peticiones y respuestas de HTTP

Envía peticiones de Cross-Domain a la aplicación Web

Inyecta Ads, blogs maliciosos, etc.

Navegador

atacante.com

Cross Domain Request
POST + cookie aplicación

Controlado por el atacante

Contiene los "secretos" a obtener (agregado por el navegador)

Recomendaciones

- Utilizar protocolos seguros (HTTPS)

- Deshabilitar compresión
  - --comp-lzo no → Sólo sirve para unas versiones de OpenVPN
  - Editar *server.conf* y *serverudp.conf* y reemplazar:

    compress lz4

    Por:

    compress

- Usar configuraciones seguras en OpenVPN:
  - https://cryptostorm.is/blog/new-features

Referencias

- https://cryptostorm.is/blog/new-features
- https://speakerdeck.com/skepticfx/voracle-compression-oracle-attacks-on-vpn-tunnels?slide=83
- https://www.youtube.com/watch?v=C6yUfzGmNrk