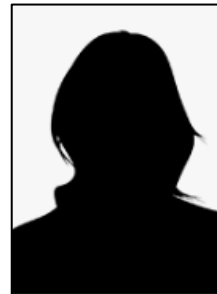
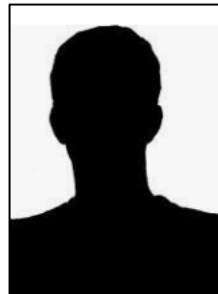
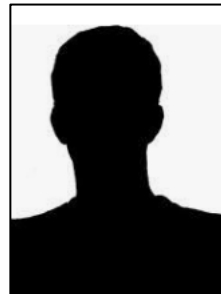
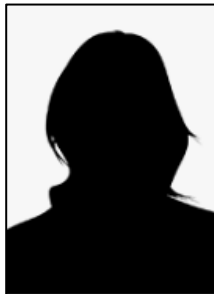


XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva



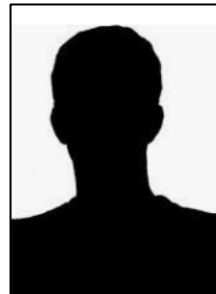
Red Team como herramienta
de protección frente a *APTs*



CaixaBank

Jordi Aguilà

jaguila@caixabank.com



LAYAKK

José Picó

David Pérez

info@layakk.com



Índice

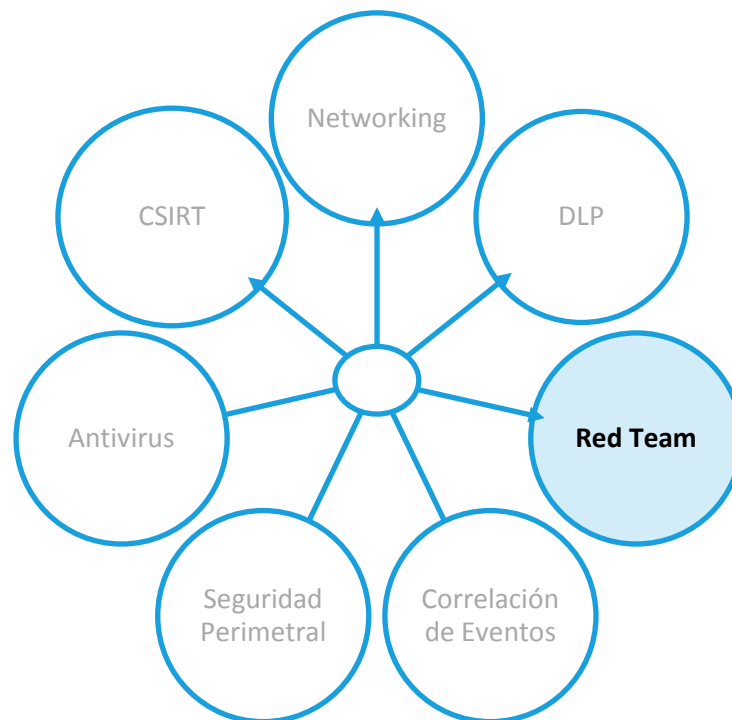
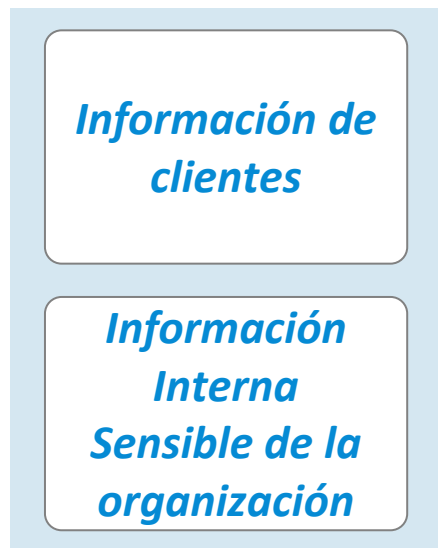
1. *Red Team*: ¿Qué es, qué implica y cómo se gestiona?
2. *Red Team*: Historias de guerra



Red Team: ¿Qué es, qué implica y cómo se gestiona?

Objetivo del Red Team: Proteger Información Sensible

Todas las compañías operan con dos tipos de información sensible que necesitan proteger:





Red Team: Background

El término “*red team*” proviene de una práctica durante la Guerra Fría donde los militares estadounidenses adoptaban una perspectiva soviética, es decir, una perspectiva “roja”.

Los militares estadounidenses tenían que pensar en “rojo” para intentar atentar y derrotar sus propios planes y sistemas como si fueran soviéticos.

Moscú hizo lo mismo llamándose “*blue team*”.

Por ejemplo, la Marina de los EEUU usó al *red team* para intentar derrotar su propia fuerza submarina usando conceptos y tecnología soviética.

Fuente: Financial Times



Red Team: Definición

Un grupo independiente de ciber-atacantes que quieren retar a la organización para mejorar su efectividad y están dedicados a comprometer la organización de la misma forma que si fuera un enemigo real.

Este grupo utiliza habilidades reales de los enemigos sin ninguna guía interna o soporte. El objetivo es encontrar la vulnerabilidad para entrar a la organización.

Este hecho permite que la organización descubra sus debilidades y luche en contra de éstas.

(DJJ & FIRST)



Red Team: Actividad Principal

Red Teaming es la simulación y emulación de tus adversarios en sus tácticas, manera de pensar, forma de operar y **exfiltración de activos e información**.

Red Team es “pensar como el enemigo”



Red Team: ¿Qué hace?

- Ser secreto
- Recoger fuentes abiertas
- Investigación web sobre el objetivo
- Realización de reconocimiento y preparación de operaciones en ambos ámbitos, tanto físico como digital
- Seguir y trazar un perfil de las personas, su comportamiento y su presencia online
- El objetivo pueden ser personas VIPs también
- Analizar la compañía objetivo: sistema, redes, productos y servicios
- Desarrollar diversos vectores de ataque
- Desarrollo de exploits para obtener la entrada
- Escalado de privilegios hasta el final
- Realización de ataques de ingeniería social
- Desarrollo de “puertas traseras”, transformar logs de auditoría, analizar infraestructuras, analizar y “esnifar” la red, analizar las tácticas y estrategias del departamento de Seguridad de la Información y generalmente explotar errores de configuración
- Diseño de estrategias de filtración, tácticas y extracción de información
- Alcanzar el objetivo
- Trabajo conjuntamente con los defensores para entrenarlos y hacerlos más resistentes



Red Team: Objetivos y Actividades

Objetivo: llevar a cabo un ataque real contra una entidad usando todas las habilidades y métodos que un atacante podría realizar

- Posibles tipos de ataque

Robo de información sensible
para la entidad, con el
propósito de uso o publicarlo

Espionaje industrial: robo
de información útil para la
competencia

**Robo de
activos**

Daño o destrucción de
la entidad a través de la
infraestructura crítica

- ¿Cómo?

Grupo altamente organizado
capaz de llevar a cabo ataques
planeados y coordinados

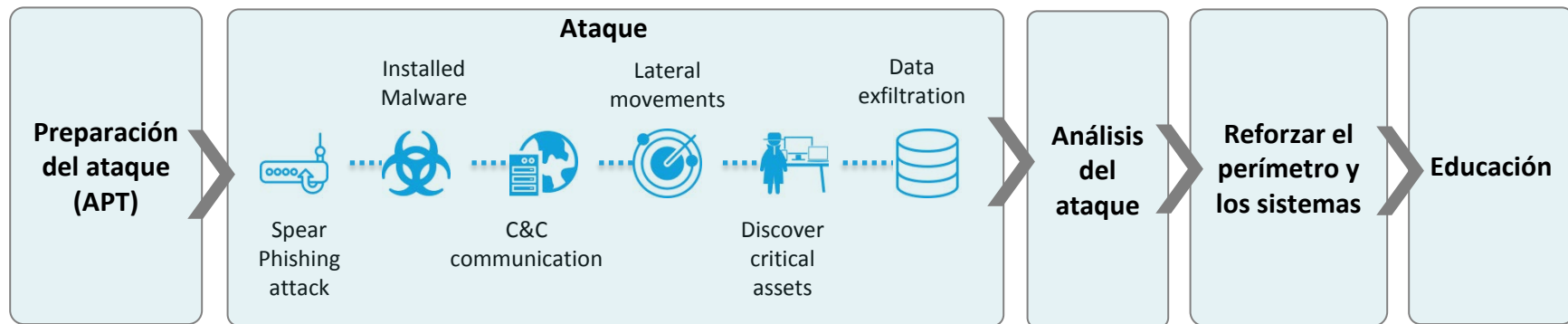
**Equipo
multidisciplinario**
con alto grado de
especialización

Características similares a las de un atacante real, no limitado a recursos clásicos. Cualquier técnica puede ser utilizada (dentro de las reglas del encargo) para alcanzar los objetivos.

Red Team: Metodología

No es un test de intrusión. Cambia el paradigma.

- Los sistemas de detección son testados en una situación real. La organización no sabe el objetivo del ataque.



- No es un test de intrusión:
 - Incluso cuando los responsables de la defensa no son notificados, un test de intrusión únicamente evalúa la red y las vulnerabilidades del sistema definidas en el alcance. Los recursos humanos y materiales están asignados para cada acción siendo limitados y predefinidos.
 - Un Red Team utiliza todos sus recursos para llevar a cabo las acciones más comprometidas



Red Team: Diferencias vs. test de intrusión

- No hay limitaciones predefinidas
- No está limitado en encontrar únicamente vulnerabilidades, va más lejos. De hecho, sólo está limitado por el líder del Red Team y por la ley
- Los atacantes actúan como “black hackers”, sin moral y sin paradigmas
- Filtración de información durante el ataque
- Test de intrusión es sólo una de las miles herramientas que un *Red Team* puede utilizar
- La compañía define los objetivos y deja actuar al *Red Team*, el cual utiliza todos los recursos sin limitaciones
- *Red Team* realiza acciones como: ingeniería social, espiar las infraestructuras... No sólo de forma electrónica, también físicamente: usando drones o cualquier método disponible
- La defensa no lo sabe, no lo espera, no interviene
- IT, infraestructura, CISO, operaciones, departamentos técnicos, nunca están involucrados
- *Red Team* puede atacar a cualquier dispositivo perteneciente a la organización



Red Team: atributos para su éxito

Cultura de la compañía

La organización tiene que ser capaz de aceptar la autocrítica

Debajo de la salvaguarda de la alta dirección

Objetivo, campo de acción, comunicación y reporte tiene que ser cubierto por la alta dirección

Externo del departamento de Seguridad de la Información

Seguridad Informática y aquellos que crean la defensa de la infraestructura de la compañía no tienen información privilegiada de los ataques

Selección inusualmente cuidadosa del equipo

Talento, inteligencia, imaginación, lealtad y confianza

Líder Red Team

debe dirigir y controlar con independencia. El líder tiene que formar parte de CaixaBank para fijar los límites

Técnicos de confianza

Esta confianza se basa en sus capacidades técnicas, la confidencialidad de sus acciones, la eficiencia de uso de los recursos, etc...

Uso continuo del Red Team

Red Team no debe actuar únicamente cuando hay un gran problema o emergencia, su trabajo debe ser continuado a pesar de no tener resultados satisfactorios inmediatamente



Red Team: Historias de Guerra

- Ataque Wi-Fi
- De LinkedIn a la Red Interna
- Ataque USB
- Exfiltración vía Escritorio Remoto

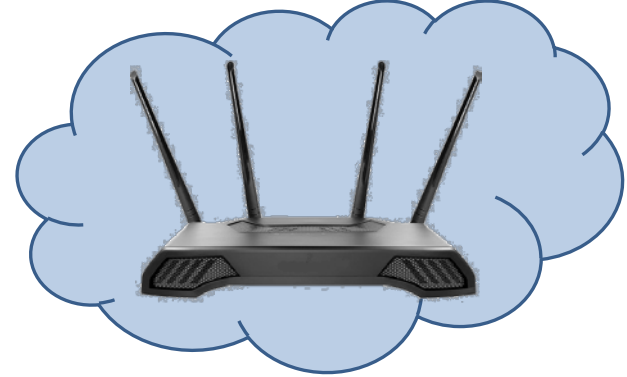


Historia de Guerra (I): Ataque Wi-Fi

OBJETIVO

“Vulnerar (de cualquier forma) la organización utilizando para ello tecnología inalámbrica”

Situación





Historia de guerra (I): Ataque Wi-Fi

¿Cómo colocar una infraestructura de ataque Wi-Fi en el rango del objetivo por el tiempo requerido para realizar ataques complejos?

Historia

¿Cómo colocar una infraestructura de ataque a un objetivo por el tiempo requerido para realizarlo?





Historia de guerra (I): Ataque Wi-Fi



¿Para de ataque Wi-Fi en el rango del
para realizar ataques complejos?

Historia de guerra (I): Ataque Wi-Fi

¿Cómo colocar una infraestructura de ataque Wi-Fi en el rango del objetivo por el tiempo requerido para realizar ataques complejos?





Historia de guerra (I): Ataque Wi-Fi

¿Cómo colocar una infraestructura de ataque Wi-Fi en el rango del objetivo por el tiempo requerido para realizar ataques complejos?



Historia de guerra (I): Ataque Wi-Fi

Red Team diseña, construye y controla remotamente la infraestructura



Historia de guerra (I): Ataque Wi-Fi

Red Team diseña, construye y controla remotamente la infraestructura





Historia de Guerra (II): de LinkedIn a la Red Interna

OBJETIVOS

Realizar una ataque dirigido con las siguientes premisas:

- vector de entrada *phishing* o similar
- intentar penetrar lo más posible en la Red del Objetivo
- no ser identificado como atacante

Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 1: Preparar infraestructura

Preparar infraestructura



**Comprar bitcoins
de forma
anónima**



Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 1: Preparar infraestructura

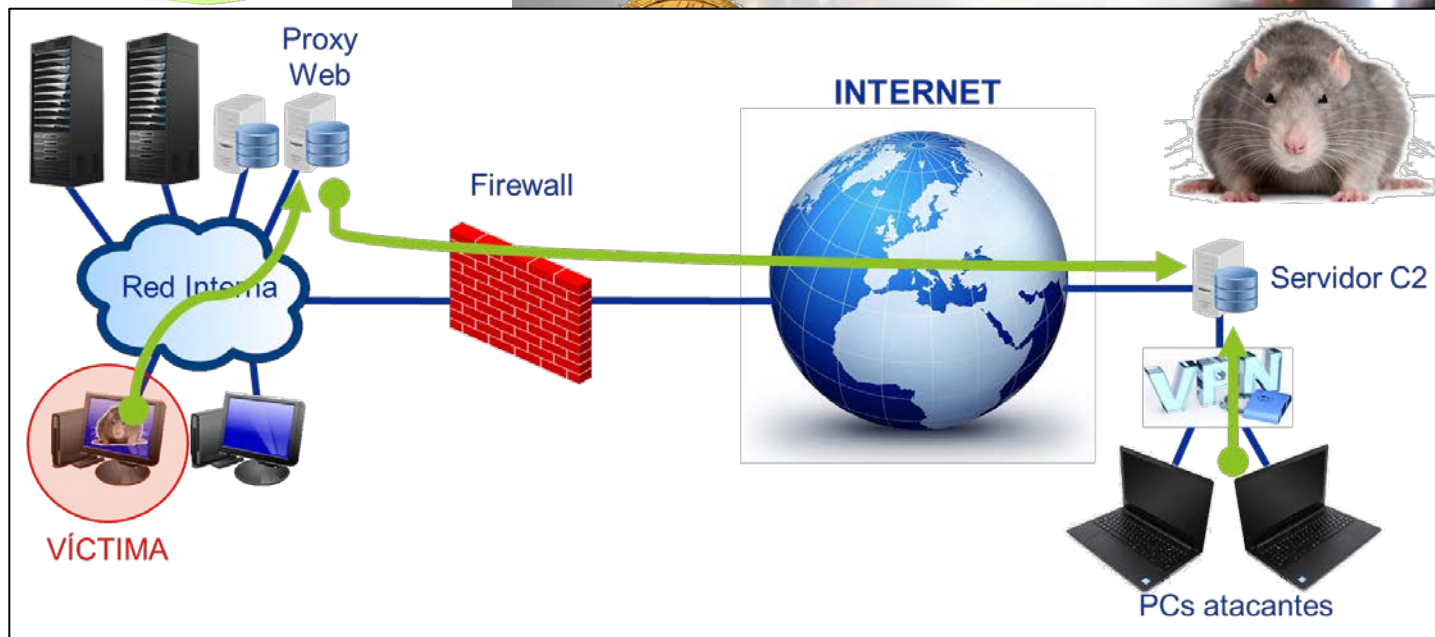
Preparar infraestructura



Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 1: Preparar infraestructura

Preparar infraestructura



Preparar
Troyano RAT
y C&C



Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 2: Construir el engaño

Preparar infraestructura

Construir el engaño

Crear su página web, maliciosa

Inventar empresa falsa



Crear perfiles de LinkedIn de sus empleados

Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 3: Seleccionar objetivos

Preparar infraestructura

Construir el engaño

Seleccionar objetivos



Localizar los perfiles adecuados de empleados de la compañía objetivo en LinkedIn

Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 4: Entrar

Preparar infraestructura

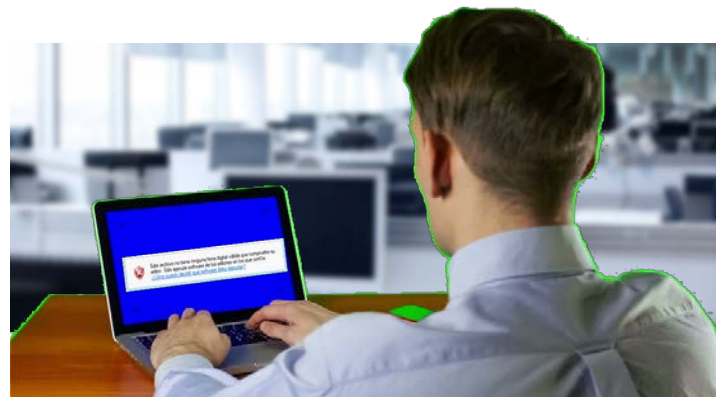
Construir el engaño

Seleccionar objetivos

Entrar



Enviar mensajes de contacto en
LinkedIn a los empleados



Esperar a engañar a un objetivo para
que acepte la instalación de un
Downloader en su PC, el cual acaba
instalando el RAT. El truco utilizado fue
desplegar un aviso de adobe muy
corriente usando Windows.



Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 5: Escalado de privilegios

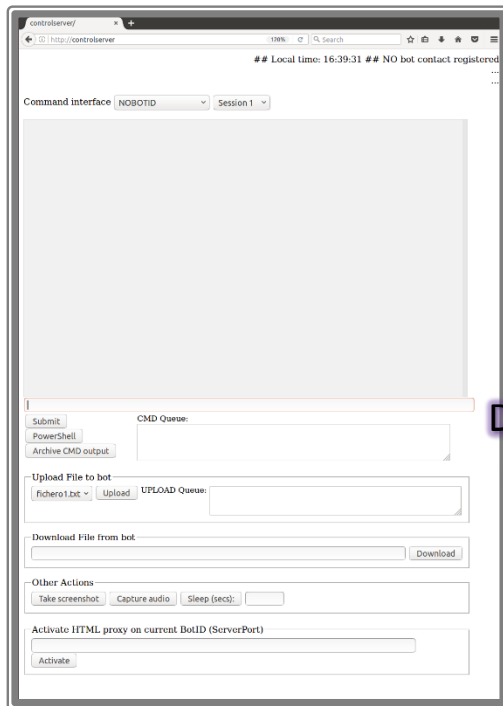
Preparar infraestructura

Construir el engaño

Seleccionar objetivos

Entrar

Escalar



Usar C&C para acceder RAT



Determinar el nivel de acceso de la víctima

Infección de otros sistemas internos y escalado de privilegios





Historia de Guerra (II): de LinkedIn a la Red Interna

PASO 6: Filtración de información

Preparar infraestructura

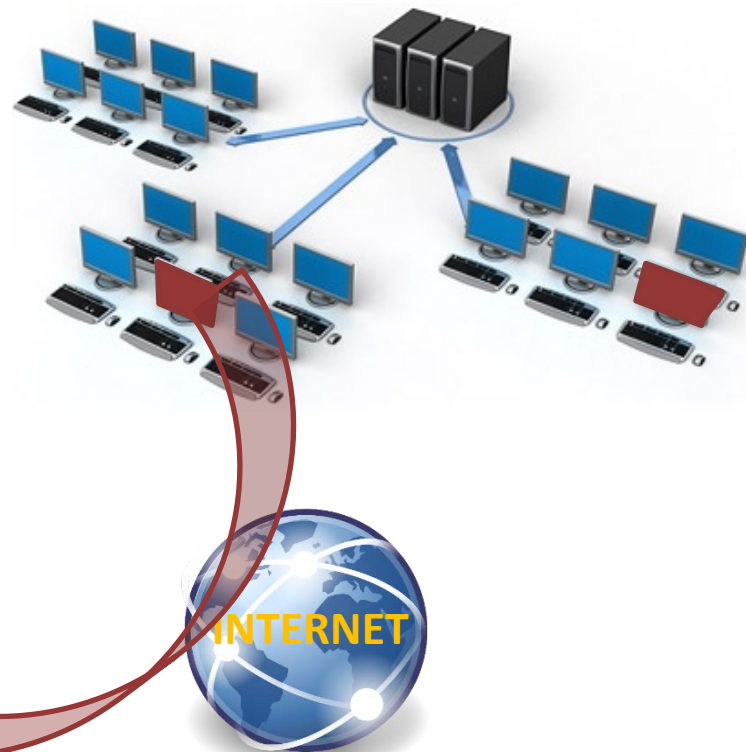
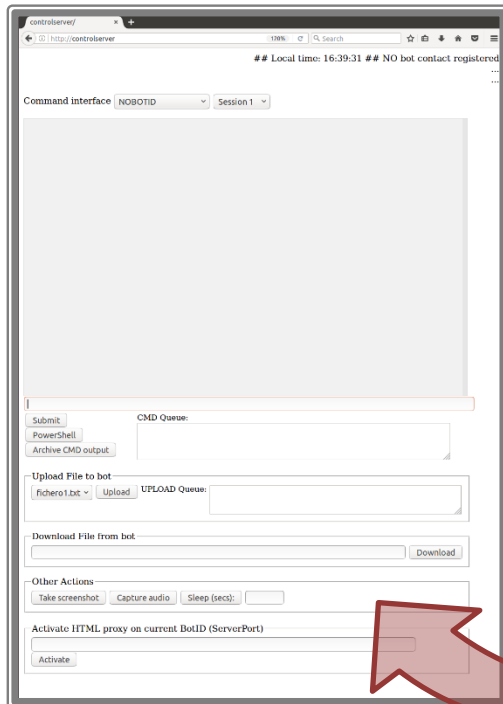
Construir el engaño

Seleccionar objetivos

Entrar

Escalar

Filtración



Filtración de información



Historia de Guerra (III): Ataque USB

OBJETIVO

“Infectar un PC expuesto al público”

Historia de Guerra (III): Ataque USB

Reconocimiento: Puertos USB expuestos



Foto: Evan Bench (<https://www.flickr.com/photos/austinevan/3225409596/>)



Historia de Guerra (III): Ataque USB

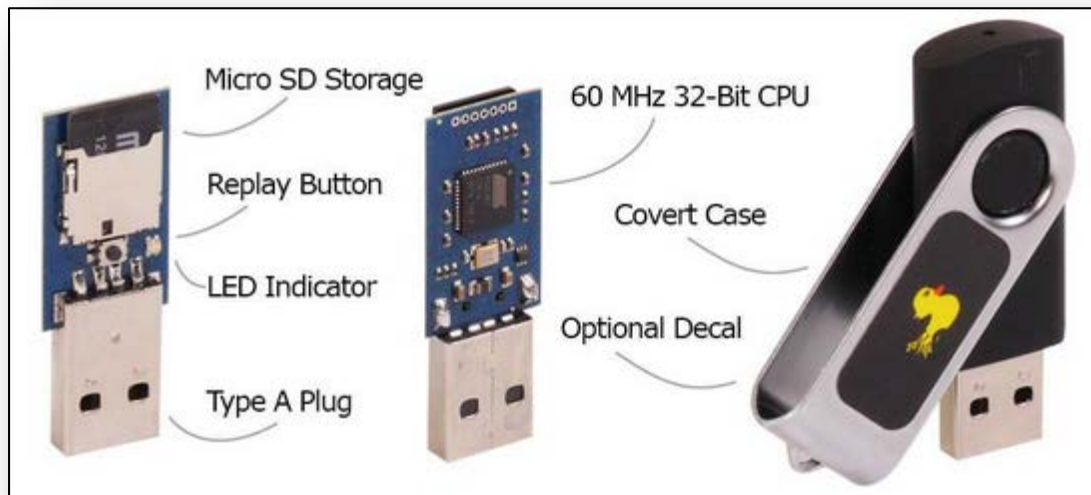
Preparación

- C2 : Command & Control
- RAT : Remote Access Trojan
- Downloader : Descarga el RAT
- Dispositivo USB malicioso: Instala el downloader

Historia de Guerra (III): Ataque USB

Preparación: Dispositivo USB malicioso

- Emulador de teclado, programable
- “USB RUBBER DUCKY” de HAK5 (alias “EL PATO”)

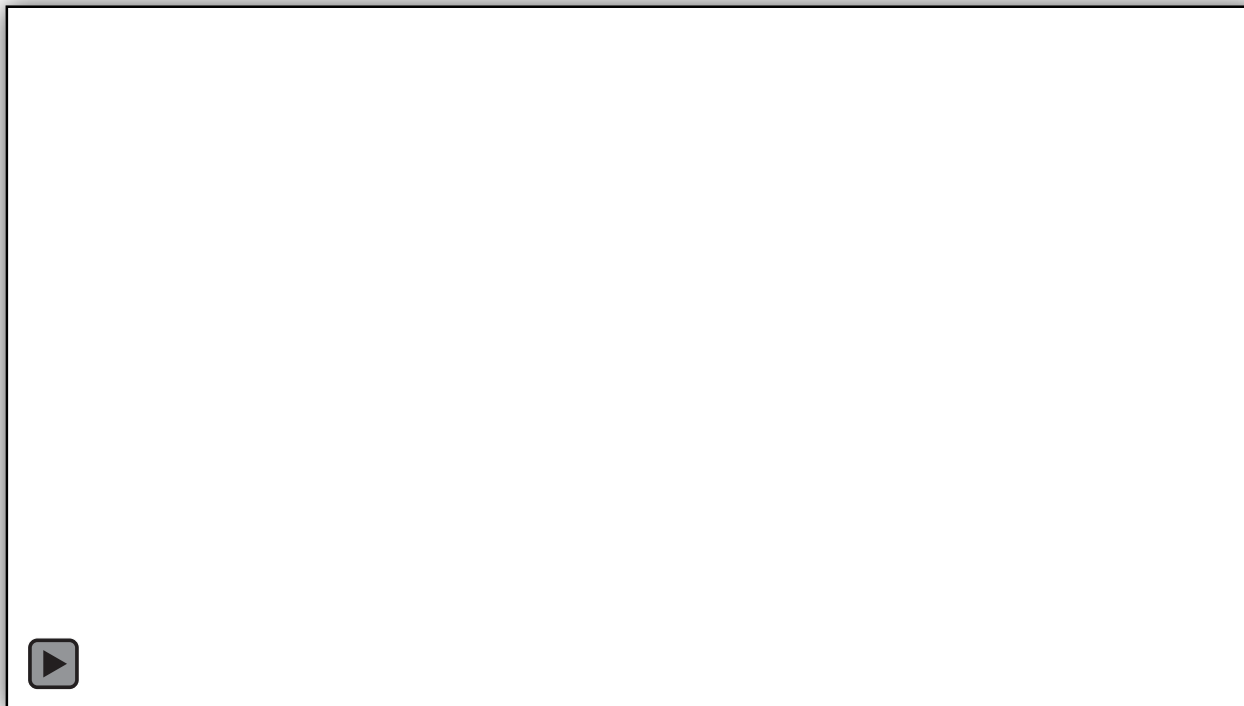


Ref: <https://hakshop.com/products/usb-rubber-ducky-deluxe>



Historia de Guerra (III): Ataque USB

Infección





Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

OBJETIVO

“Exfiltrar ficheros a través de una conexión Escritorio Remoto”



Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

Conexión Escritorio Remoto

- HTTPS
- Autenticación segura
- Aplicaciones virtualizadas: ejecutan en el servidor
- Explorador de archivos: copia hacia dentro, PERO NO HACIA FUERA
- Portapapeles: copia hacia dentro, PERO NO HACIA FUERA
- Navegador: SÓLO INTRANET

Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

Representación gráfica de datos: códigos QR (Quick Response)



Contenido de este código QR:

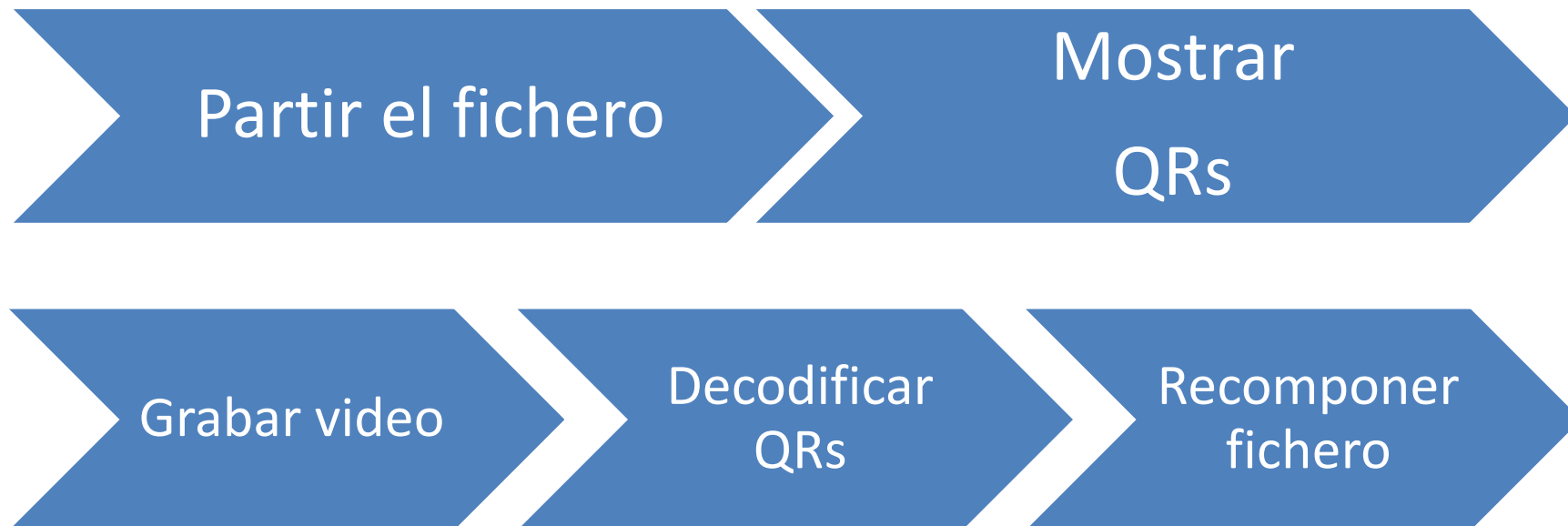
<http://en.m.wikipedia.org>

https://en.wikipedia.org/wiki/QR_code



Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

Proceso de exfiltración



Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

Posible método de ejecución: DLL





Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

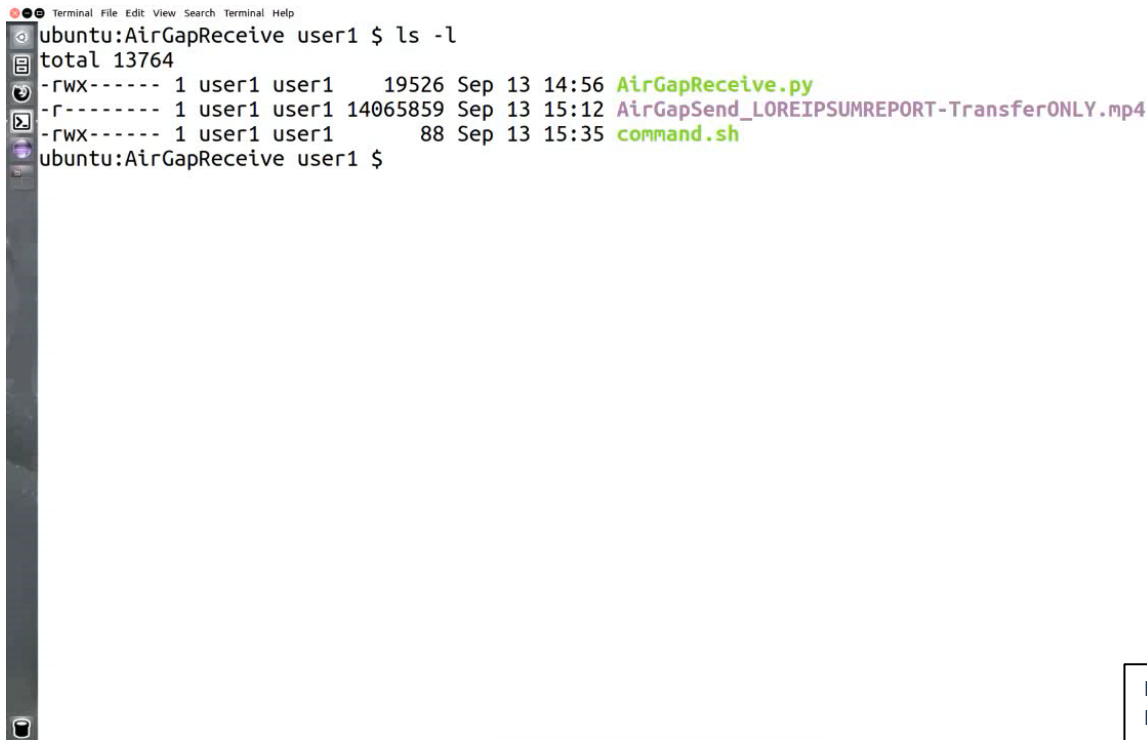
Envío





Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

Decodificación



```
ubuntu:AirGapReceive user1 $ ls -l
total 13764
-rwx----- 1 user1 user1   19526 Sep 13 14:56 AirGapReceive.py
-r----- 1 user1 user1 14065859 Sep 13 15:12 AirGapSend_LOREIPSUMREPORT-TransferONLY.mp4
-rwx----- 1 user1 user1     88 Sep 13 15:35 command.sh
ubuntu:AirGapReceive user1 $
```

Ref.: qr-data-reconstruct by Tudor Gheorghiu
Ref.: zbar.sourceforge.net

Historia de Guerra (IV): Exfiltración vía Escritorio Remoto

Velocidades conseguidas

- Envío: 0.3 GB/h (1 GB = 3,33 h)
- Decodificación: 0.15 GB/h (1 GB = 6,66 h)





Índice

1. *Red Team*: ¿Qué es, qué implica y cómo se gestiona?
2. *Red Team*: Historias de guerra

¡Muchas gracias!

XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- oc.ccn.cni.es

➤ Síguenos en

