

# Seguridad Preventiva en Internet - Parte 1

...

¡Defiéndete ante las nuevas amenazas!

# ~\$ whoami

- Raúl Caro Teixidó
- Analista Red Team en BlackArrow (Tarlogic)
- OSCP
- Staff de Bitup Alicante
- Creador de Mística
- Ponente en BlackHat USA 2020



@secu\_x11



@secu77



# Overview

Este curso se ha preparado para dar a conocer las amenazas que existen hoy en día en Internet, cómo detectarlas, y cómo evitar que nos afecten.

La seguridad informática no es cosa: ni de edad, ni de profesiones ni nada parecido.

TODOS estamos implicados, una vez que coges un móvil, que creas un perfil en una red social, que consigues un trabajo, te conviertes en una posible víctima del cibercrimen.

Y es por ello que es muy importante conocer las amenazas, para trabajar en una buena defensa.

# ¿Qué veremos en este curso?

(con explicaciones y demostraciones)

- Phishing y estafas online
- Malwares
- Contraseñas y buenas prácticas
- Privacidad y seguridad en internet

---

# ¿Qué es el PHISHING?

El phishing es una técnica para conseguir, mediante el engaño, comprometer a un usuario.

Y... ¿cómo es este compromiso?

- Obtención de contraseñas
- Información personal o privada
- Acceso a uno o varios equipos
- Realizar una acción no intencionada



# SPEARPHISHING LINK

El Spearphishing Link es el phishing más habitual de encontrar. Consiste en engañar a un usuario para que proporcione información, forzar a descargar



Emirates giving free tickets to 500 people to celebrate its Anniversary .

Get yours at <http://www.emirates.com-freetickets.club>

16:53

# CREAR BUQUE LINK (demo)

Inform


← → ↻ 🏠


⚠ No es seguro | 194.179.98.71:18080/?rid=Ufr6Z3n

🔗 ☆

MU

Para: Isaac





Universidad  
Rey Juan Carlos

Introduzca su email y su contraseña

Iniciar sesión

Estudiante de cursos anteriores al 2019/2020 (incluido): puedes acceder a tu **antiguo buzón** (ahora @old-alumnos.urjc.es) [aquí](#).

Dispones de guías para mover tus contenidos [aquí](#).

[Inicio](#) [Aviso Legal](#) [Ayuda](#)

# ¿CÓMO EVITARLO?

1. Validar el remitente del correo/mensaje/etc

¿es un remitente válido? ¿es el canal de comunicación habitual o esperado?

1. Verificar el motivo/contenido del mensaje

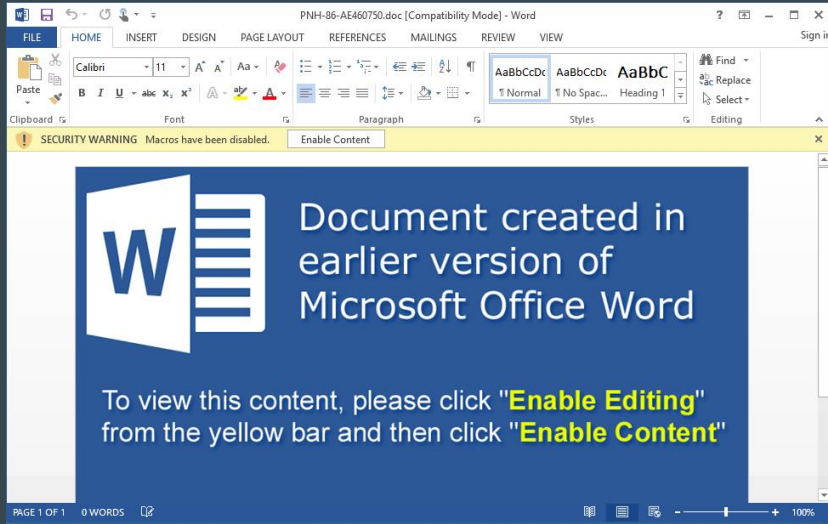
¿tiene sentido que esa persona o empresa nos envíe la información que envía?

1. Comprobar que el sitio al que nos lleva el link, es el sitio de confianza

¿el dominio es el real? ¿Esta bien puesto el certificado? ¿Cómo es la url?



# SPEARPHISHING ATTACHMENT



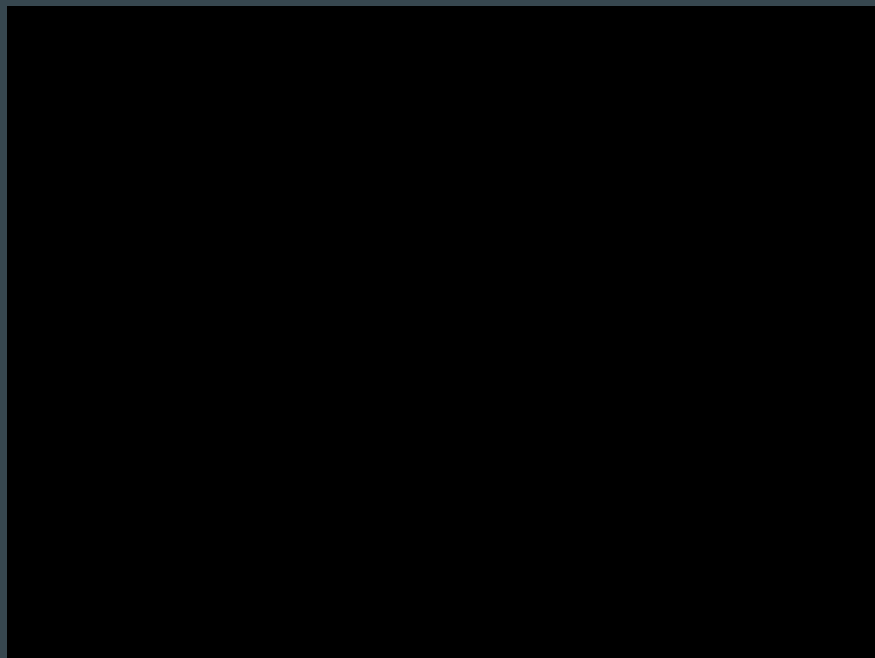
El Spearphishing Attachment, a diferencia del Spearphishing Link, se utiliza un archivo adjunto.

Con este archivo, malicioso, se busca conseguir comprometer o robar información del equipo del usuario víctima.



# SPEARPHISHING ATTACHMENT (demo)

Demo: documento ofimático con macro maliciosa que infecta el equipo.



# ¿CÓMO EVITARLO?

1. Validar el remitente del correo/mensaje/etc

¿es un remitente válido? ¿es el canal de comunicación habitual o esperado?

1. Verificar el motivo/contenido del mensaje

¿tiene sentido que esa persona o empresa nos envíe la información que envía?

1. Comprobar el adjunto del mensaje

¿qué tipo de archivo es? ¿puede ser potencialmente malicioso?

# SMISHING (SMS PHISHING)

El SMISHING

Habitualmente  
solicita algún ti

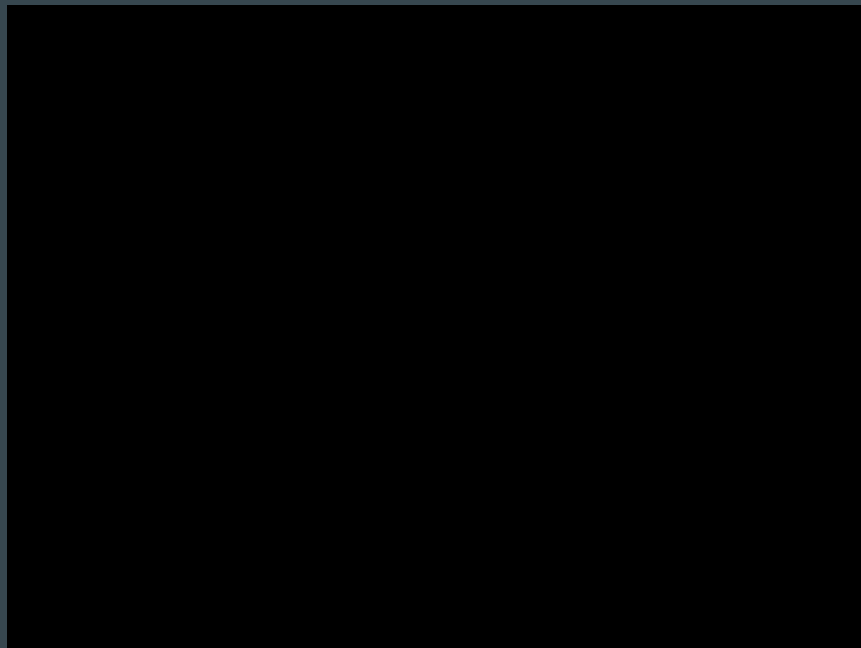
de SMS.

conocida que



# SMISHING (demo)

Demo: smishing suplantando a entidad bancaria y a contacto de familiar cercano.



# ¿CÓMO EVITARLO?

1. Validar el remitente del mensaje

¿es un remitente válido? ¿es el canal de comunicación habitual o esperado?

1. Verificar el motivo/contenido del mensaje

¿tiene sentido que esa persona o empresa nos envíe la información que envía?

1. Comprobar qué se está pidiendo

¿nos pide que cambiemos una contraseña? ¿que iniciemos sesión en algún lado?

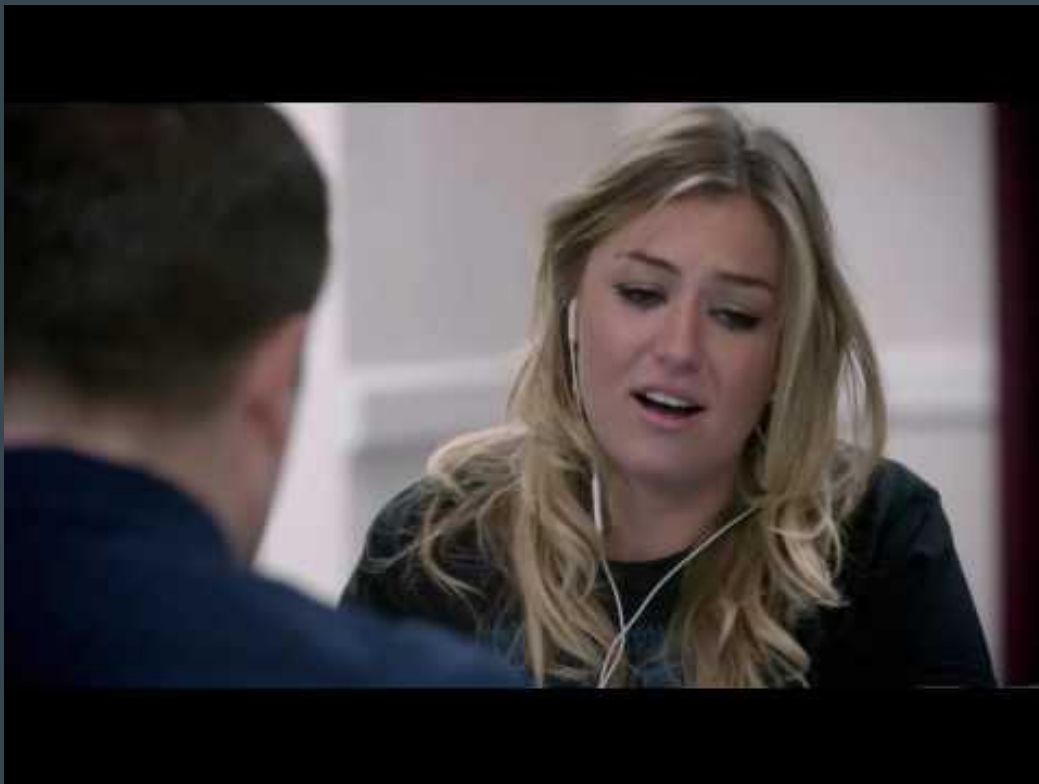
# VISHING (VOICE PHISHING)

Y, el vishing, se trata de un tipo engaño que se realiza a través de una **llamada telefónica**. Se suplanta la identidad de una empresa o persona para:

- Conseguir Información
- Obtener Acceso a un equipo
- Forzar a realizar una acción no-intencionada



# VISHING (demo)





# ¿CÓMO EVITARLO?

1. Confirmar la identidad del locutor

¿estás seguro que es quién dice ser? en caso afirmativo, ¿tiene sentido que esa persona te llame por teléfono?

1. Desconfía por naturaleza

¿qué información te está pidiendo? ¿Puedes validarlo con otra persona?



# SCAM (estafas)

Un scam, se le conoce como “una estafa digital”, pues la estafa se produce a través de Internet e utilizando los recursos disponibles en Internet.

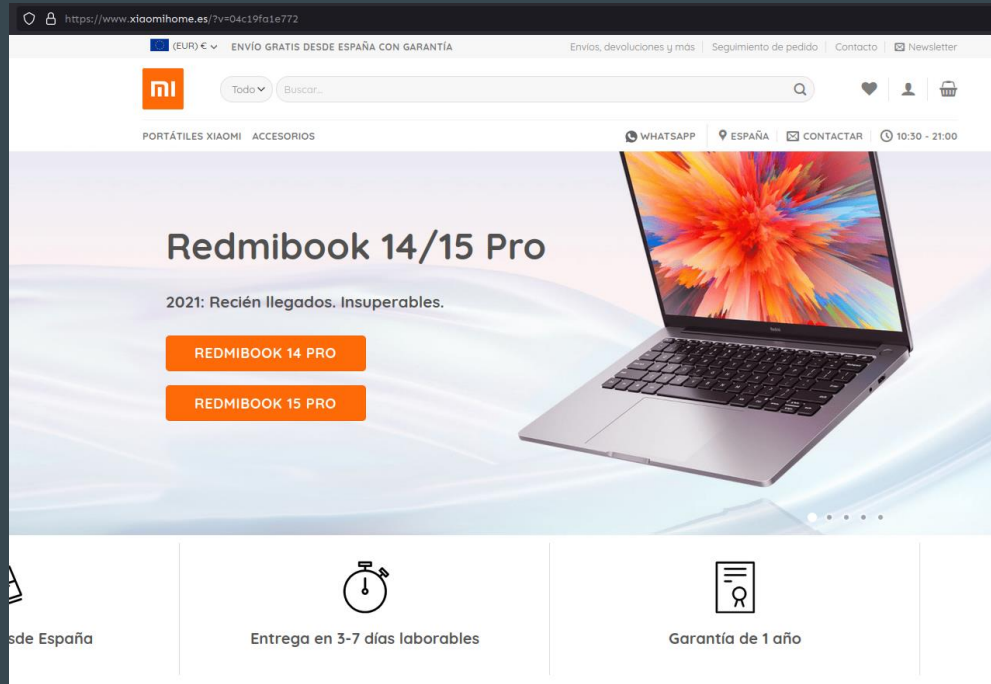
Objetivos que buscan los scammers:

- Robar datos bancarios (tarjetas de crédito, etc)
- Robar información personal (dni y otros docs)
- Comprometer sistemas (ordenadores y móviles)
- Robar accesos a correos y otras cuentas.



# SCAM (demo)

Practical Case: posible scam en [www.xiaomihome.es](https://www.xiaomihome.es)



# CONSEJOS PARA NO PICAR

1. Confirmar la identidad del sitio

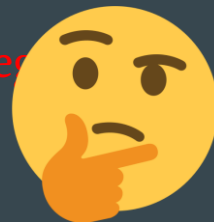
¿es un sitio oficial? ¿el dominio es el correcto?

1. Desconfía por naturaleza

los chollos no existen, o rara vez existen -> Desconfía

1. Servicios como ScamDoc pueden ser de ayuda
2. Verifica con un vendedor oficial

Si tienes la posibilidad, contacta antes con un vendedor oficial y asegúrate



¿Preguntas?



# Malware



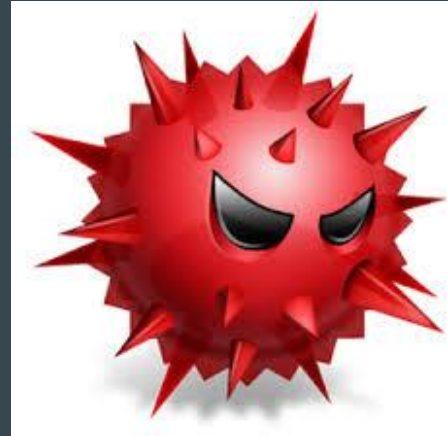
# ¿Qué es el **MALWARE**?

El Malware, o más comúnmente conocido como “virus”, es un programa que se utiliza con fines maliciosos para comprometer un sistema o información ajena.

En multitud de ocasiones el software no se desarrolló con ese fin sino que, al final, son las personas las que le dan ese uso malicioso.

Debido a esto, es imprescindible:

- Conocer los tipos de malware que existen
- Qué medios utilizan para infectar equipos
- Cúal es el objetivo de cada uno



# Tipos de **MALWARE**

- Troyanos: habilidad de camuflarse y parece inofensivos.
- Gusanos: capacidad de propagarse e infectar a otros sistemas.
- Keyloggers: monitorización de todo lo que escribes
- Stealers: especialistas en robar tus contraseñas y archivos.
- Adware: expertos en bombardearte a publicidad y anuncios.
- Minners: maestros en hacer dinero con los recursos de tu sistema.



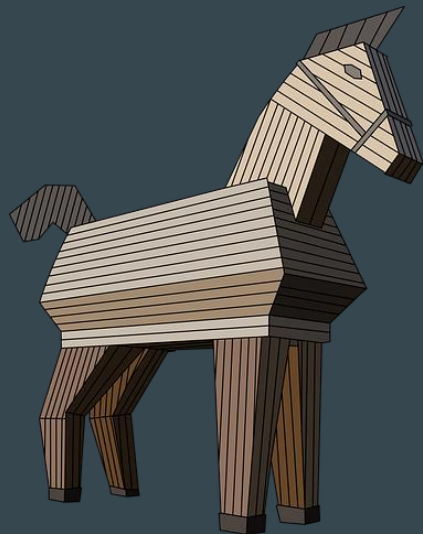


# TROJAN

Un troyano se trata de un tipo de malware que se **camufla** para evitar ser detectado y conseguir infectar al equipo. En ocasiones, este malware, no contiene acciones maliciosas, sino que te utiliza como "**transportador**" para ejecutar el verdadero programa malicioso (dropper).

¿Dónde podemos encontrar troyanos?

- Documentos ofimáticos maliciosos
- Cracks, keygens o cualquier software de pago troyanizado
- Ejecutables, aplicaciones y/o scripts
- Otros archivos que se pueden "mal-utilizar"



# ¿CÓMO EVITARLO?

1. No te descargues software de páginas como Softonic o sitios desconocidos.
2. Respecto a documentos/archivos descargados: **piénsalo dos veces** antes de abrir o ejecutar cualquier cosa en tu equipo.
3. Un buen antivirus siempre ayuda, pero **NO ES SUFICIENTE**.
4. Si alguna vez dudas, nunca está de más subir el archivo a **VirusTotal**

No obstante, recuerda siempre:

**“Si algo es gratis, es que tú eres el producto”**

# STEALER

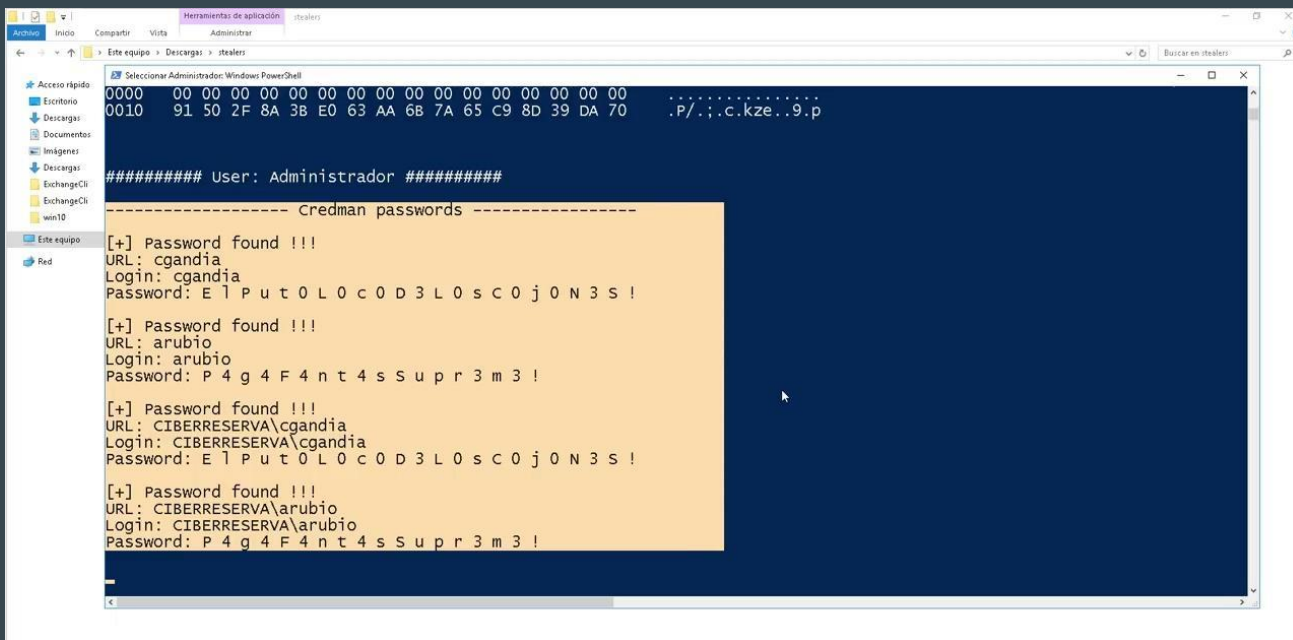
Un Stealer es un tipo de malware cuyo objetivo es encontrar **credenciales o información privada** y en un equipo comprometido y enviarlas al atacante.

Información comprometida:

- Contraseñas guardadas en los Navegadores (Chrome, Firefox, Edge, etc)
- Contraseñas en archivos del sistema (en notas, archivos excel, etc)
- Documentos privados o sensibles (imágenes, correos, etc)

# STEALER (demo)

Demo: stealer que roba las credenciales de Chrome, archivos del sistema y Wi-Fi.



```
0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0010 91 50 2F 8A 3B E0 63 AA 6B 7A 65 C9 8D 39 DA 70 .P/.;.c.kze..9.p

##### User: Administrador #####

----- Credman passwords -----

[+] Password found !!!
URL: cgandia
Login: cgandia
Password: E l P u t o L o c o D 3 L o s c o j o N 3 s !

[+] Password found !!!
URL: arubio
Login: arubio
Password: P 4 g 4 F 4 n t 4 s s u p r 3 m 3 !

[+] Password found !!!
URL: CIBERRESERVA\cgandia
Login: CIBERRESERVA\cgandia
Password: E l P u t o L o c o D 3 L o s c o j o N 3 s !

[+] Password found !!!
URL: CIBERRESERVA\arubio
Login: CIBERRESERVA\arubio
Password: P 4 g 4 F 4 n t 4 s s u p r 3 m 3 !
```

# ¿CÓMO EVITARLO?

1. Respecto a los USB: antes de conectar un USB a tu equipo, **asegúrate que es un dispositivo confiable.**
2. Respecto a documentos/archivos descargados: **piénsalo dos veces** antes de abrir o ejecutar cualquier cosa en tu equipo.
3. Guarda tus contraseñas en un **gestor de contraseñas** como Keepass.
4. No guardes las contraseñas en tu navegador (Chrome, Firefox, etc) ni tampoco en archivos de texto (**sin cifrar**) o similar.
5. **Protege la información sensible** de tu equipo y ten siempre copias de seguridad.



## Ooops, your files have been encrypted!

### What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

**S**ure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)

You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

*You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.*

### How Do I Pay?

Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28

Your files will be lost on

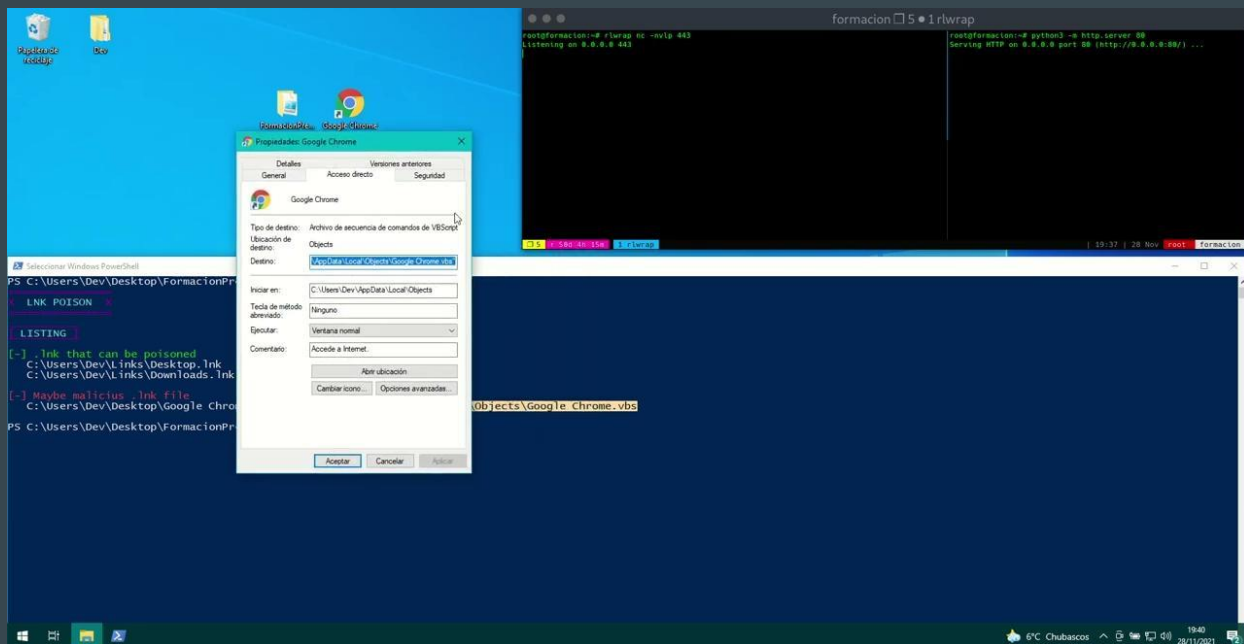
5/19/2017 16:25:02

Time Left

06:23:58:28

# Worm (demo)

Demo: gusano que infecta LNK's y deja una persistencia en el equipo.

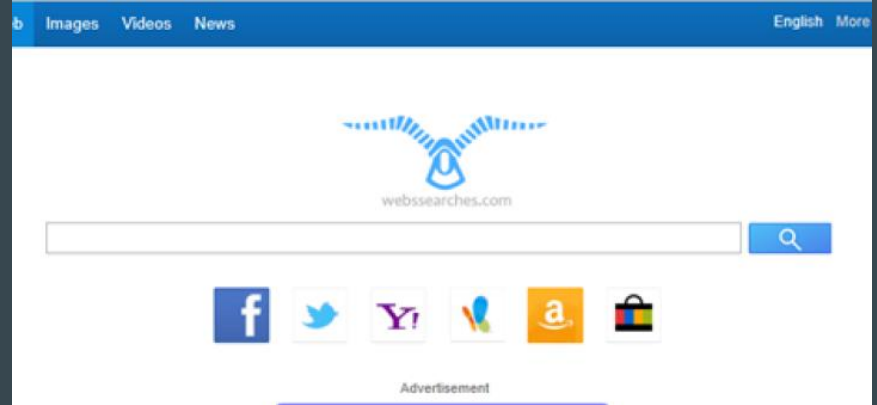


# Adware

El Adware es un tipo de malware enfocado a **distribuir anuncios o contenido malicioso** a través de la publicidad.

El atacante genera beneficios mediante:

- El robo de información
- Abuso de anuncios
- Código de referencia





# ¿Cómo combatirlo?

Para combatir el Adware se pueden seguir las siguientes pautas:

- Utilizar un **bloqueador de publicidad** como Ublocker o Adblocker.
- **No** descargar programas de sitios como **Softonic** o similar.
- Disponer de un **antivirus** instalado en el equipo
- **No** instalar programas **piratas, cracks, activadores** o similar.
- En caso de ser infectado con Adware, utilizar la herramienta **AdwCleaner**.



# Minners

Un **Minner** es un programa que está diseñado para utilizar los recursos del equipo para minar criptomonedas.

¿Por qué lo utilizan los cibercriminales? -> Para rentabilizar el compromiso

Problemas:

- Se ralentiza el equipo (debido al proceso de minado).
- Puede llegar a causar un problema en el hardware.



¿Preguntas?

# ¿Qué veremos mañana?

¡A recargar las pilas!

- ~~Phishing y estafas online~~
- ~~Malwares~~
- Contraseñas y buenas prácticas
- Privacidad y seguridad en internet

---