

# Exploiting relevant enterprises software for fun and profit



[kub0x@elhacker.net](mailto:kub0x@elhacker.net)

# Sobre mí


- Autodidacta apasionado por la seguridad de sistemas, programación e ingeniería inversa.
- Investigador de seguridad de aplicaciones web y escritorio.
- Programador de malware y exploits.
- Usuario activo de la comunidad [elhacker.net](http://elhacker.net)




# HACKER

**You keep using that word... I do not think it means what you think it means.**

# Personajes: h4x0rs

olaa... oies se que eres un GRAN HACKER, me encantaria serlo, se que hay una forma de hackear un msn, hay muchas pero solo esta conozco... Mandar un troyano mata procesos por medio de ingenieria social, el KEYLOGGER y asi... pero no se si tuu me podrias mandar un consejo... TE LO AGRADECERIA demasiado ñ\_ñ 

Señor por favor enseñeme como obtener una contraseña de Facebook. Se que me podrian decir lammer, pero es que entonces como lo pido? no lo quiero para novias, enemigos ni cosas asi, primero por que no tengo enemigos ni novia, no me interesa, solo quiero aprender, hacer algo por mi mismo, quiero aprender como obtener una direccion de Facebook en un mes como maximo, incluso un mes seria demasiado, pero aun asi, es el tiempo limite. Necesito que me ayude, dejeme ser su aprendiz por favor señor 

Estas tío :S necesito un favor quiero hackear a uno pero cuando descargo cualquier programa para crear servers y eso mi antivirus lo borra me recomiendas algun programa?

Te explico lo que quiero hacer.

Quiero crear un keylogger con un dwonloader de esos subirlo que me cree un link y que cuando la gente se meta en ese lo descargue automaticamente

# Personajes: Cornudos

gracias de nuevo amigo de verdad gracias cambiare como me has dicho todo, pero mira yo tenia una cuenta la cual no usaba con ella la creee para poder recabar informacion sobre este tema y tambien aberiguo claves y entro en ella, no se como pero lo hizo, incluso me dijo la contraseña que habia puesto, ya vez puse hijadeputa de contraseña y ella lo sabia, no se como lo pudo hacer, por que yo cuando entro en opciones y me pone contraseña salen \*\*\*\*\* estos asteriscos y sin embargo ella sabia que la contraseña era hijadeputa no te parece raro???

y la verdad es que el tema es serio , sabes ella lo tiene facil sola toda el mes salvo 2 fines de semana que bajo yo a ver a mis hijoas, y ella hace y desace como quiere, ella usa el telefono movil para hablar por el facebook y yo no puedo hacer nada se que habla con tios y se esconde para hacerlo, quiero saber quien cojones son y por que ella lo hace , s es que ellos le ofrecen algo que yo no le he dado, o si simplemente es una hijade puta que lo unico que busca es un polvo facil, por eso pedia ayuda para poder acceder a su msn y facebook,

**kub0x #~011011~#** <voskater15@gmail.com>

para luloma 

Buenas, yo en tu caso buscaría un consejero matrimonial y/o un abogado. Poner "hijadeputa" de contraseña no es muy fiable si tienes problemas de pareja.

# Objetivo de la ponencia

- Explicar ciertos fallos de seguridad encontrados a lo largo de mi experiencia.
- Desmitificar mediante la explotación la idea de las aplicaciones seguras.
- Proveer herramientas seguras que previenen diversos ataques de explotación.
- Concienciar a los usuarios del peligro al que están expuestos.

# Contenido (I)

- Hacking Mozilla Firefox
  - Firefox user stored passwords decryption.
- Hacking Euskaltel ISP & Cisco
  - Router Cisco ECP3825:
    - Remote Access Vulnerability.
    - Remote DoS Vulnerability.

# Contenido (II)

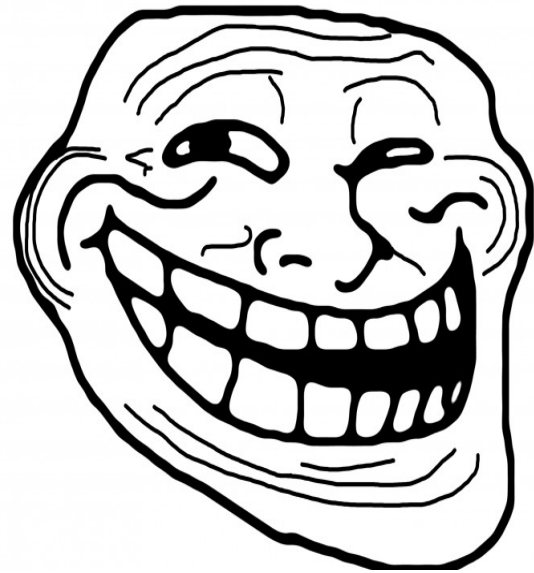
- Hacking EHU/UPV
  - Gaur:
    - Full access to students profile.
- Hacking Microsoft
  - Windows (Vista/7/8/8.1):
    - Thread Token Local Privilege Escalation.
    - COM Elevation Moniker Local Privilege Escalation.



# Estado de las vulnerabilidades

- Mozilla “parcheó” hace varios meses la vulnerabilidad. Fácilmente bypassable.
- Euskaltel sólo parcheó la vulnerabilidad de acceso remoto. Incompetencia al poder.
- EHU/UPV parcheó todas las vulnerabilidades relacionadas con GAUR. ¡Bravo!
- Microsoft parcheará en un futuro ambas vulnerabilidades (Windows 10 maybe).

EMPECEMOS



# Bypassing new FireFox stored passwords protection

- Anteriormente → signons.sqlite
- Ahora → logins.json
- Usuario y Contraseña cifradas con Triple-DES y codificadas con BASE64.
- Por defecto → !password maestra → default password's used.

# DEMO TIME!





# Contra medidas

- Mozilla → obligar al usuario a establecer una contraseña maestra. No seguir vendiendo humo.
- Utilizar una contraseña maestra:
  - El delincuente debe de descifrar/conocer dicha contraseña.

euskaltel



# Cisco ECP3825: Remote Access Vulnerability

- Vulnerabilidad hallada en su Firmware.
- Permitía el acceso remoto aunque éste estuviera deshabilitado.
- Me enviaron un técnico que verificó la vulnerabilidad.
- Estuvieron expuestos durante 3 semanas.
- No paré de recibir llamadas (ಠ\_ಠ)



# Cisco ECP3825: Remote Access Vulnerability (II)

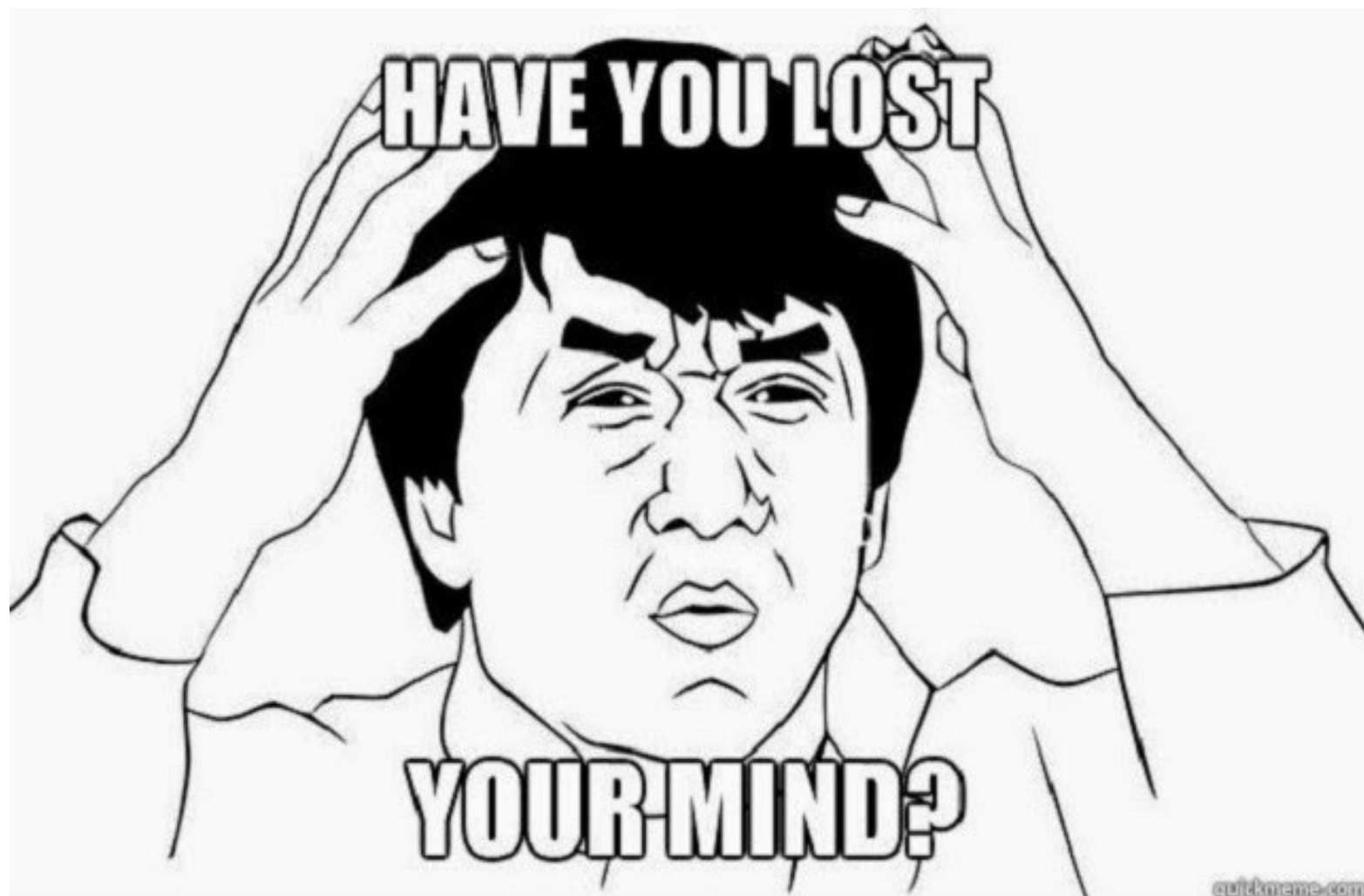
- Implementé una Prueba de concepto (PoC)
  - Escanee varios rangos de IPs de Euskaltel.
  - En un rango de 4096 routers → 990 vulnerables.
  - DNS Spoofing → your data is mine.
  - Have fun!

# Cisco ECP3825: Remote Access Vulnerability (II)

- Implementé una Prueba de concepto (PoC)
  - Escanee varios rangos de IPs de Euskaltel.
  - En un rango de 4096 routers → 990 vulnerables.
  - DNS Spoofing → your data is mine.
  - Have fun!

```
Scanning      ..
[1]           1: Proxy Detected! ;>
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
[1]           1: Proxy Detected! ;>
Scanning
[1]           1: Proxy Detected! ;>
[1]           1: Proxy Detected! ;>
Scanning
Scanning
Scanning
Scanning
Scanning
Scanning
[1]           1: Proxy Detected! ;>
```

[illegible]



# Router Cisco ECP3825: Remote DoS Vulnerability

- Vulnerabilidad en su panel de administración.
  - Basada en inyección HTML.
  - No valida correctamente los parámetros enviados.
  - Denegación de servicio (DoS): El router se reinicia.
  - Cientos de clientes se quedarón sin servicio durante días (no fui yo... :D).
  - Les avisé y quisieron escuchar, por lo que hoy día sigue activa.

eman ta zabal zazu



Universidad  
del País Vasco

Euskal Herriko  
Unibertsitatea



# Gaur: Full access to students profile

- Acceso al expediente del alumnado.
- Acceso a la matriculación de todos los años del alumnado y sus becas.
- Acceso a las fotografías de toda la institución (profesores, colaboradores, alumnado, directivos...)
- Big brother's watching at you!

# Gaur: análisis de las vulnerabilidades

- Expediente:
  - HTTP POST
  - Parámetro nº de alumno & expediente
- Fotos:
  - HTTP GET
  - [https://gestion-alumnos.ehu.es/pls/entrada/svu\\_captura\\_imagenes.htm\\_descarga\\_imagen?p\\_sesion=\[SESSION\]&p\\_proceso=expw0020&p\\_idp=\[ID\\_USUARIO\\_GAUR\]](https://gestion-alumnos.ehu.es/pls/entrada/svu_captura_imagenes.htm_descarga_imagen?p_sesion=[SESSION]&p_proceso=expw0020&p_idp=[ID_USUARIO_GAUR])
- Matrículas:
  - Parámetro de nº de expediente.
  - HTTP GET.



## Asignaturas

Asignatura	Año acad.	Grupo	Tipo	Créd.	Calificacion	Nota	Fecha calif.	Conv.	Renun.
Ciclo Indiferente, Curso Primero									
<a href="#">27303 - Álgebra Lineal</a>	2012/13	61	Básica de rama	9.0	Aprobado	5.00	3/6/2013	1	0
<a href="#">27304 - Ampliación de Física</a>	2013/14	16	Obligatoria	6.0				2	0
<a href="#">27307 - Ampliación de Gráficos de Ingeniería</a>	2012/13	01	Obligatoria	6.0	Aprobado	5.00	19/6/2013	1	0
<a href="#">25971 - Cálculo</a>	2013/14	16	Básica de rama	12.0				2	0
<a href="#">27414 - Física</a>	2012/13	01	Básica de rama	9.0	Notable	7.20	18/6/2013	1	0
<a href="#">27306 - Gráficos de Ingeniería</a>	2012/13	01	Básica de rama	6.0	Aprobado	5.00	12/7/2013	2	0
<a href="#">26570 - Informática</a>	2012/13	01	Básica de rama	6.0	Aprobado	5.00	17/6/2013	1	0
<a href="#">26571 - Química</a>	2012/13	01	Básica de rama	6.0	Aprobado	5.90	22/7/2013	2	0
Ciclo Indiferente, Curso Segundo									
<a href="#">27313 - Ampliación de Ecuaciones Diferenciales</a>	2013/14	02	Obligatoria	6.0				0	0
<a href="#">27309 - Ampliación de Matemáticas</a>	2013/14	02	Obligatoria	6.0				0	0
<a href="#">26144 - Economía</a>	2013/14	02	Básica de rama	6.0				0	0
<a href="#">27310 - Electrotecnia</a>	2013/14	02	Obligatoria	6.0				0	0
<a href="#">25110 - Estadística</a>	2013/14	02	Básica de rama	6.0				0	0
<a href="#">27308 - Fundamentos de Ciencia de Materiales</a>	2013/14	02	Obligatoria	6.0				0	0
<a href="#">26058 - Mecánica</a>	2013/14	02	Obligatoria	6.0				0	0
<a href="#">27314 - Mecánica Aplicada</a>	2013/14	02	Obligatoria	6.0				0	0
<a href="#">27311 - Mecánica Fluidos</a>	2013/14	02	Obligatoria	6.0				0	0
<a href="#">27312 - Termodinámica</a>	2013/14	02	Obligatoria	6.0				0	0



**KEEP  
CALM  
AND BE A  
GOOD  
STUDENT**



897



898



899



900



901



903



904



905



906



907



908



909



910



911



912



913



914



915



916



922



923



924



925



926



927



928



929



931



932



933



934



935



936



937



938



940



941



942



943



944



946



947



948



949



950



951



952



954



955



956



957



958



959



960



961



962



963



964



966



967



968



969



970



971



972



973



974



975



976



977



978



979



980



981



983



984



986



987



988



989



990



992



993



994



995



996



997



998



999



1001



1002



# Security Fail



**██████████ ENEKO**

**Grado en Ingeniería Informática**

**Facultad de Informática**

Tipo de Matrícula Ordinaria

Tipo de Pago Domiciliación

Forma de Pago DOMICILIACIÓN 1 PLAZO

El importe de su matrícula asciende a **██████████ euros**, que corresponde a :

Por asignaturas 1ª matrícula	██████████	2 euros
Seguro escolar (grado)	██████████	euros
Tarjeta universitaria (grado)	██████████	euros

Que abonará por **DOMICILIACIÓN 1 PLAZO** en las siguientes fechas :

Plazo 1º	██████████	2013	██████████ euros
----------	------------	------	------------------

Importe Total Pagado	██████████ euros	Importe Pendiente de Pago	0,00 euros
----------------------	------------------	---------------------------	------------

Cuenta Corriente **██████████ 56300**

## Tasas asociadas a la matrícula

██████████ ENEKO

Grado en Ingeniería Informática

Facultad de Informática

Tipo de Matrícula

Ordinaria

Tipo de Pago

Domiciliación

Forma de Pago

DOMICILIACIÓN 1 PLAZO

El importe de su matrícula asciende a ██████████ euros, que corresponde a :

Por asignaturas 1ª matrícula

██████████ euros

Por convalidaciones

██████████ 4 euros

Por reconocimientos

██████████ euros

Seguro escolar (grado)

██████████ euros

Tarjeta universitaria (grado)

██████████ euros

Apertura de expediente académico (grado)

██████████ euros

Adaptación, Convalidación, Reconocimiento univ. estatal o UPV

██████████ 12 euros

Que abonará por **DOMICILIACIÓN 1 PLAZO** en las siguientes fechas :

Plazo 1º

██████████ 2012

██████████ euros

Importe Total Pagado

██████████ euros

Importe Pendiente de Pago

0,00 euros

Cuenta Corriente

██████████ 56300

Cerrar

## Tasas asociadas a la matrícula

IMANOL

Grado en Ingeniería en Tecnología Industrial

Escuela Técnica Superior de Ingeniería de Bilbao

Tipo de Matrícula	Ordinaria
Tipo de Pago	Domiciliación
Forma de Pago	DOMICILIACIÓN 1 PLAZO

El importe de su matrícula asciende a [REDACTED] que corresponde a :

Por asignaturas 2ª matrícula	[REDACTED] 4 euros
Seguro escolar (grado)	[REDACTED] euros
Tarjeta universitaria (grado)	[REDACTED] euros

Que abonará por **DOMICILIACIÓN 1 PLAZO** en las siguientes fechas :

Plazo 1º	[REDACTED] 2013	[REDACTED] euros
----------	-----------------	------------------

Importe Total Pagado	[REDACTED] euros	Importe Pendiente de Pago	0,00 euros
----------------------	------------------	---------------------------	------------

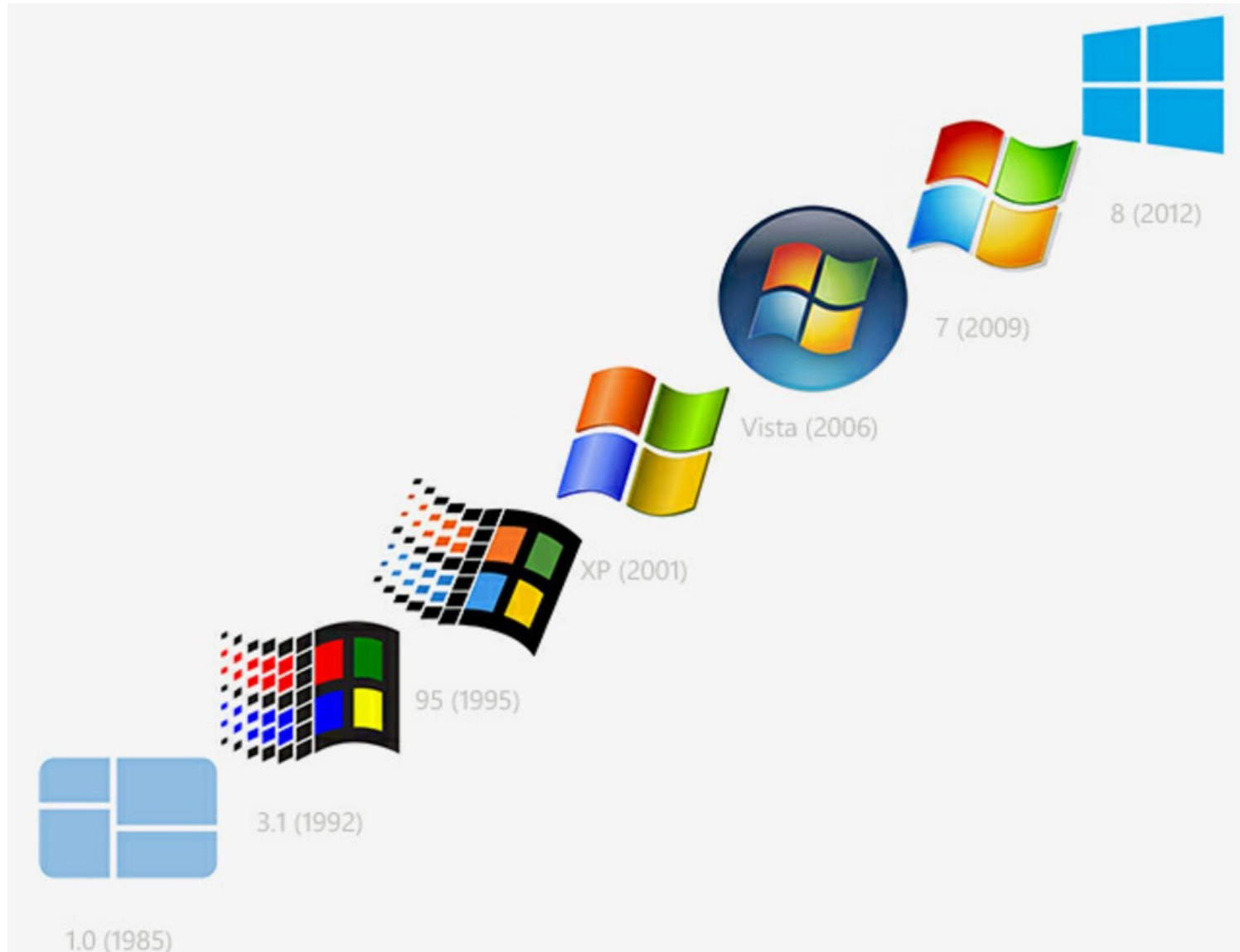
Cuenta Corriente	[REDACTED] 00285
------------------	------------------

Cerrar





# Microsoft Windows: Years full of fails!



# Thread Token Local Privilege Escalation: Conceptos previos (I)

- Thread = Hilo = Subproceso.
- Token = Privilegios del proceso.
- Una aplicación se divide en subprocesos.
- Cada proceso y subproceso tiene un Token de acceso.
- Windows controla el acceso de los usuarios mediante UAC (User Access Control).

# Thread Token Local Privilege Escalation: Conceptos previos (II)

- Si conseguimos un Token con privilegios y lo suplantamos → actuamos con el mismo nivel de privilegios que el Token obtenido.
- Proceso auto-elevado → proceso iniciado con privilegios de administrador → UAC no salta.
- Windows utiliza Tokens de acceso para definir su sistema de seguridad de aplicaciones.

# Thread Token LPE: Conceptos previos (III)

- Si tratamos de obtener un identificador de proceso con privilegios mayores → ERROR.
- Funciones interesantes de la WIN32 API:
  - OpenProcessToken()
  - DuplicateTokenEx()
  - SetTokenInformation()
  - SetThreadToken()
  - RevertToSelf()

# Lista de procesos auto-elevados: Windows 8.1 Pro x64

```
C:\Windows\system32>strings -s *.exe | findstr "autoElevate"
C:\Windows\system32\BitLockerWizardElev.exe:      <autoElevate xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</autoElevate>
C:\Windows\system32\bthudtask.exe:                <autoElevate>true</autoElevate>
C:\Windows\system32\chkntfs.exe:                  <autoElevate>false</autoElevate>
C:\Windows\system32\cleanmgr.exe:                 <autoElevate xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</autoElevate>
C:\Windows\system32\cliconfg.exe:                 <autoElevate>true</autoElevate>
C:\Windows\system32\CompMgmtLauncher.exe:         <autoElevate>true</autoElevate>
C:\Windows\system32\ComputerDefaults.exe:         <autoElevate>true</autoElevate>
C:\Windows\system32\dccw.exe:                     <autoElevate>true</autoElevate>
C:\Windows\system32\dcomcnfg.exe:                 <autoElevate>true</autoElevate>
C:\Windows\system32\DeviceEject.exe:             <autoElevate>true</autoElevate>
```

# Objetivos

- Obtener privilegios SYSTEM.
- El usuario no debe percibir ningún diálogo de UAC.
- Explotar el sistema y tomar el control.

# Where's the fault? (I)

- `BOOL ShellExecuteEx(  
    _Inout_ SHELLEXECUTEINFO *pExecInfo  
);`
- `typedef struct _SHELLEXECUTEINFO {  
    [...]  
    ULONG      fMask;  
    HANDLE     hProcess;  
    [...]`

`SEE_MASK_NOCLOSEPROCESS` (0x00000040)

Use to indicate that the **hProcess** member receives the process handle.

# Where's the fault? (II)

- ShellExecuteEx(procesoElevado) → obtenemos el HANDLE al proceso elevado.
- Duplicamos su token.
- Modificamos el token del proceso actual.
- Desencadenamos acciones como SYSTEM.
- Cambiamos el token suplantado por el original.



**DEMO TIME!**



# Contra medidas

- UAC → “Notificar siempre”:
  - Aun siendo administrador pedirá credenciales.
- Utilizar una cuenta estándar sin privilegios de administrador:
  - Al abrir un proceso auto-elevado pedirá las credenciales del administrador del sistema.

# COM Elevation Moniker Local Privilege Escalation

- “Parcheado” en 2009.
- Solución basada en Whitelisting dentro del manifest de la aplicación.
- Sigue siendo vulnerable → DLL Hijacking dentro de un Trusted Folder.
- Además encontré otra forma más que pasaron por alto.

# COM Elevation Moniker LPE: Conceptos previos

- DLL Hijacking:
  - Aprovechar el fallo de diseño del árbol de búsqueda de librerías.
- Elevation Moniker → Permite que la librería ejecute código en modo administrador:
- COM → Component Object Model
  - Librerías registradas en el registry de Windows.
  - Utilizadas por aplicaciones corrientes y del sistema.

# DEMO TIME!

- Copiamos nuestra DLL maliciosa en el directorio del ejecutable auto-elevado.
- El proceso auto-elevado ejecutará nuestra DLL.
- El whitelist fallará pues la DLL no está en su lista.
- El code de nuestra DLL correrá como admin.
- ¡Tenemos el control!



# Contra medidas

- Windows → evitar DLL Hijacking + proceso auto-elevado. !WhiteListing → Registry is OK.
- UAC → “Notificar siempre”:
  - Aun siendo administrador pedirá credenciales.
- Utilizar una cuenta estándar sin privilegios de administrador:
  - Al abrir un proceso auto-elevado pedirá las credenciales del administrador del sistema.



# Microsoft: Estado actual de las vulnerabilidades.

- Notifiqué a Microsoft a mediados de Octubre.
- COM Elevation Moniker LPE sigue abierto.
- Thread Token LPE cerrado:
  - No ofrecen parche de seguridad.
  - Rediseñarán la API y el acceso a Tokens (Win10?).

# Alternativas

- Utilizar cuentas sin privilegios de administrador.
- Software → última version. Windows Updates...
- Usar el sentido común a la hora de instalar software.
- Kits de anti-explotación en tiempo real.
  - EMET.
- Software antivirus:
  - IDS, Firewall.

# Referencias interesantes

- [http://foro.elhacker.net/analisis\\_y\\_diseno\\_de\\_malware/uac\\_task\\_manager-t416652.0.html;msg1949263](http://foro.elhacker.net/analisis_y_diseno_de_malware/uac_task_manager-t416652.0.html;msg1949263)
- [http://foro.elhacker.net/hacking\\_wireless/vulnerabilidad\\_administracion\\_remota\\_cisco\\_epc3825\\_euskaltel-t381008.0.html](http://foro.elhacker.net/hacking_wireless/vulnerabilidad_administracion_remota_cisco_epc3825_euskaltel-t381008.0.html)
- [http://en.wikipedia.org/wiki/User\\_Account\\_Control](http://en.wikipedia.org/wiki/User_Account_Control)
- <http://msdn.microsoft.com/en-us/library/windows/desktop/ms679687%28v=vs.85%29.aspx>
- <http://freejaus.com/>
- <https://github.com/FreeJaus/gea-PRISM/tree/master/Documentation>



**THANK  
YOU  
for  
LISTENING  
ANY QUESTIONS?**