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

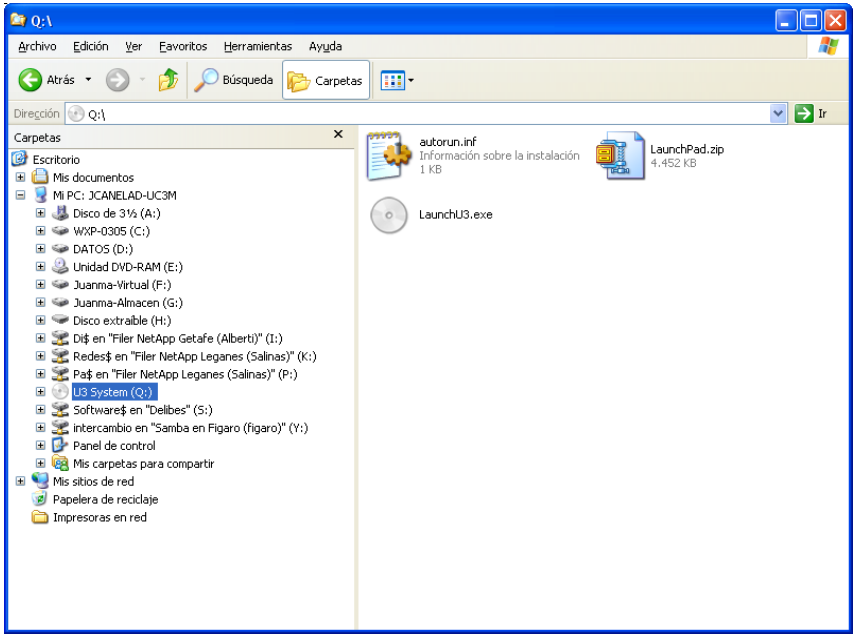
http://www.nopuedocreer.com/quelohayaninventado/1356/memoria-usb-perrito-caliente/

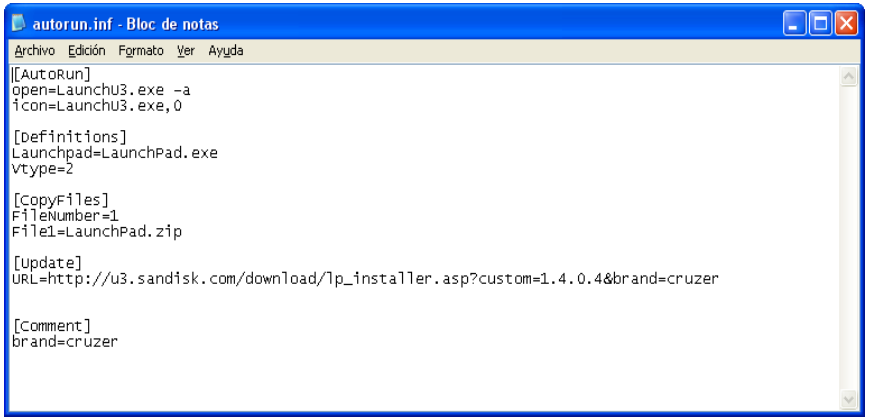
Tecnología U3

- 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





Tecnología U3 (III)

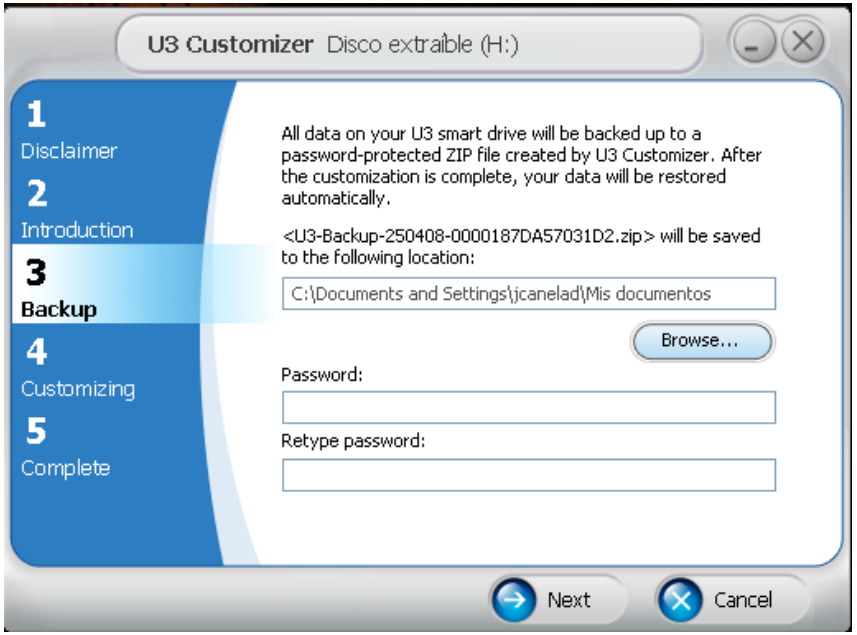
- Hasta aquí todo bien pero …
- **¡¡ DEMO !!**
- ¿Qué pasa si somos malos?
  - USBDumper

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!!

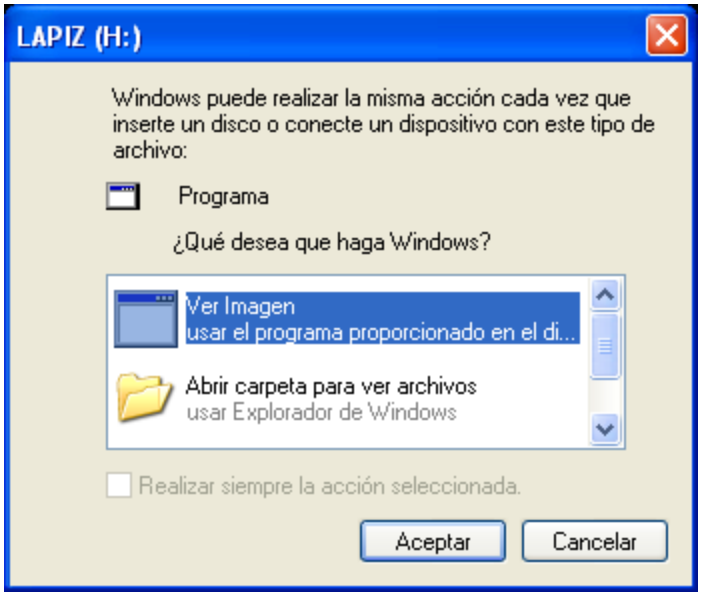
Payloads (II)

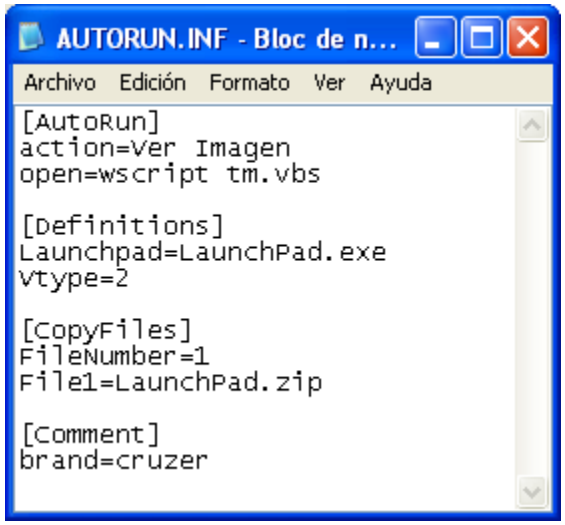
- **Universal Customizer**
  - Permite modificar el payload
  - Imágenes ISO
  - Copia de seguridad del launcher original

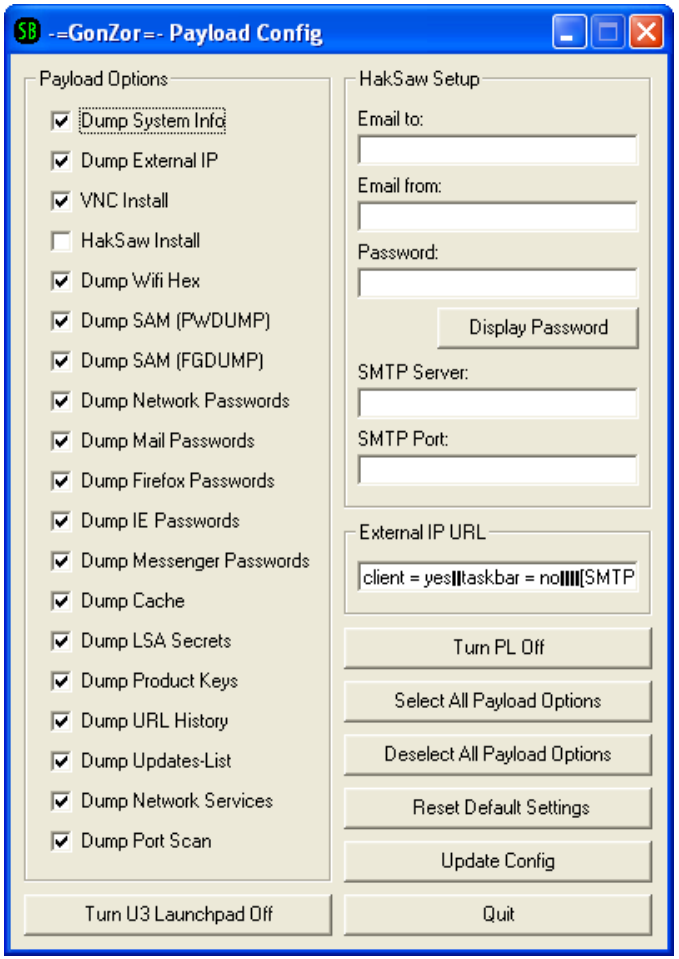


http://www.u3community.com/viewtopic.php?t=434

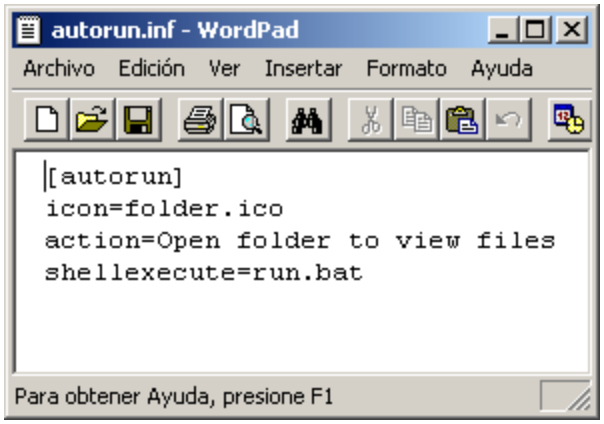
Payloads (III)

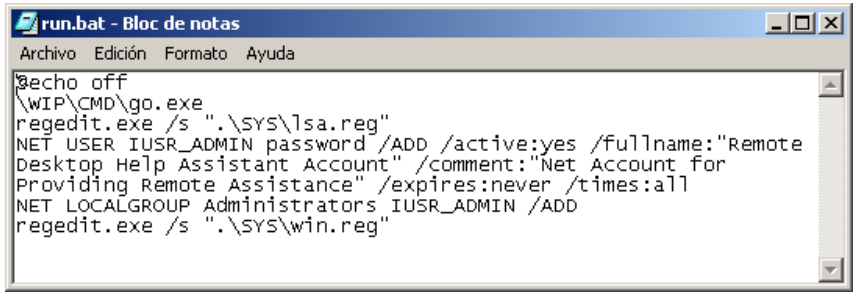


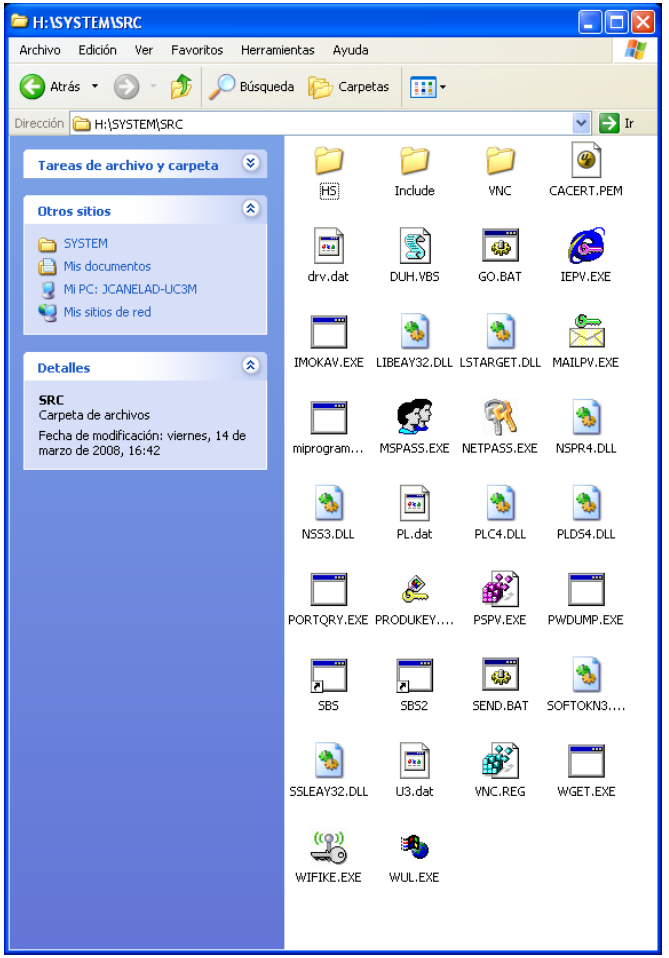




Payloads (IV)







¡¡ **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

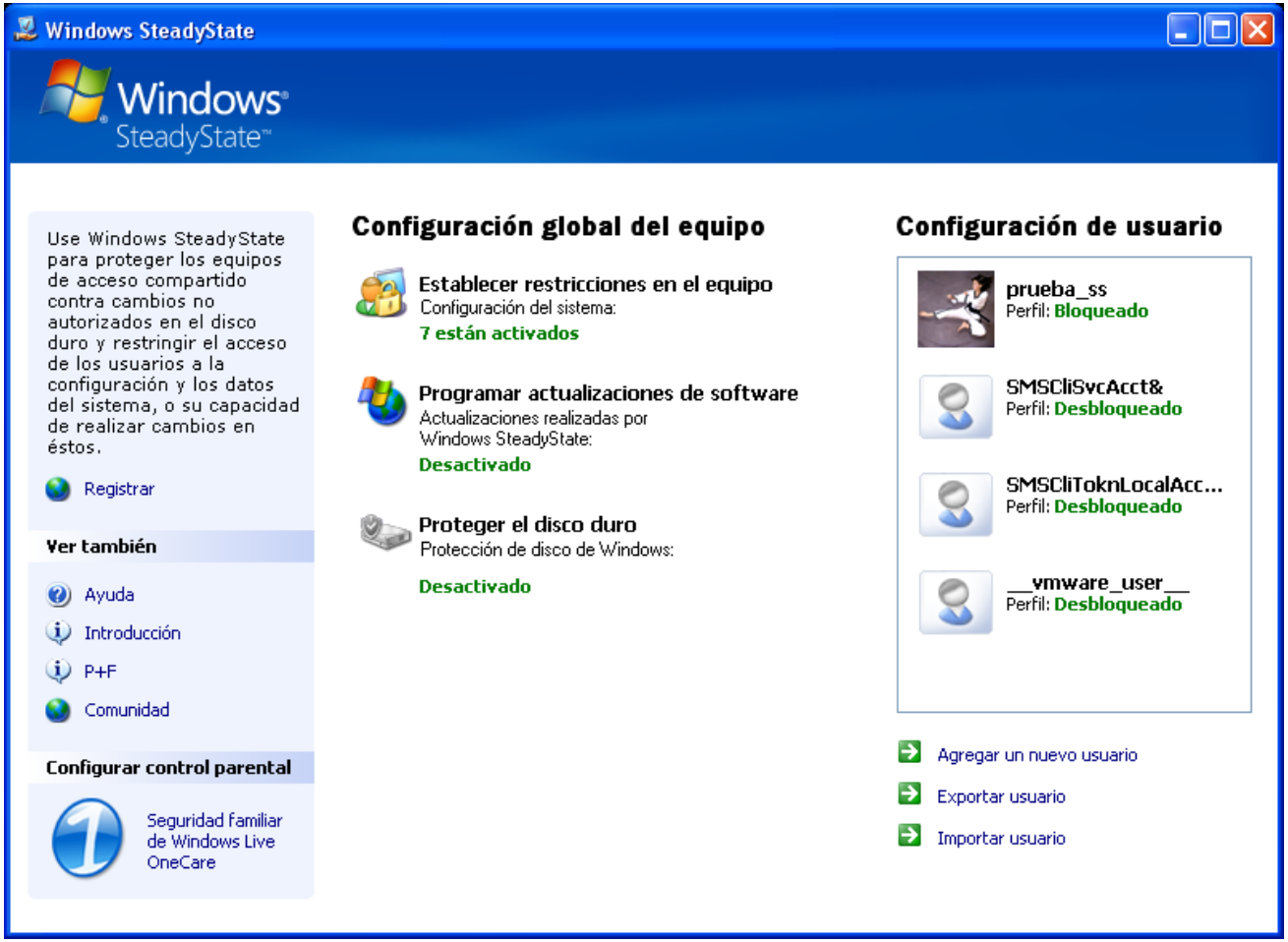
- GFI EndPointSecurity

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

- CenterTools DriveLock

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

Windows SteadyState



¿Preguntas?

Muchas Gracias por su atención