

CASO DE USO

authUSB SafeDoor

Sector público



¿Cuál es la problemática específica de las administraciones públicas respecto al tráfico de Memorias USB?

Según la [Ley 39/2015, de 1 de octubre \(LA LEY 15010/2015\)](#) (BOE del 2), del Procedimiento Administrativo Común de las Administraciones Públicas **Las oficinas de asistencia en materia de registros han de recibir todo tipo de documentación** dirigida a ellos. La digitalización constituye el proceso para incorporar el documento presentado al expediente electrónico; pudiendo requerir previamente su escaneado para convertirlo en formato electrónico, o simplemente copiar dicho documento ya en formato electrónico para incorporarlo al expediente electrónico. Este último proceso puede darse cuando el documento se presenta presencialmente, es decir, no a través de la sede electrónica, pero en formato electrónico **contenido en un pen drive**. De acuerdo al [artículo 16.5 de la Ley 39/2015 \(LA LEY 15010/2015\)](#), si una norma determina la obligatoriedad de presentar documentos en un soporte específico no susceptible de digitalización, como un pen drive, éste tendrá que ser aceptado en la oficina en materia de registro».

Esto abre un abanico enorme de posibilidades para que se pueda producir un ciberataque de forma muy sencilla a través de Memorias USB, toda vez que la propia administración admite la

obligatoriedad de recoger la información de los ciudadanos personas físicas a través de este medio.

Independientemente del riesgo que suponen las memorias externas, existe también la posibilidad de que los dispositivos de memoria de carácter interno hayan sido modificados para provocar ataques a nivel Hardware, que serían indetectables (No hay nada que escanee el hardware de los equipos) y persistentes en el tiempo pudiendo estar “dormidos” el tiempo que el atacante desee, activándose de forma remota cuando él lo elija o Eléctrico.

¿Qué es SafeDoor?

SafeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando, analizando y deteniendo amenazas a tres niveles:

- Eléctrico: identificando y deteniendo ataques destructivos de sobretensión tipo UsbKiller.
- Hardware: detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc.
- Software: antivirus integrado que realiza un análisis previo a la descarga de cualquier contenido.

SafeDoor está certificado bajo la metodología Lince y dentro del catálogo CPSTIC del CCN-CERT.

¿Cómo encaja SafeDoor en nuestro esquema de trabajo?

SafeDoor es un dispositivo multiplataforma , integrable, pequeño y ligero lo que hace posible su despliegue en multitud de entornos.

CONTROL ARCOS DE ENTRADA:

Al igual que se efectúa un control de seguridad física en la entrada se implementaría un control de Memorias USB mediante SafeDoor en el control de acceso.

El objetivo es proteger dispositivos y redes de cualquier tipo de intrusión (HW, SW o Eléctrica (USB Killer)) que se produzca a través de dispositivos de almacenamiento USB que sean ajenos a la propia organización. La implementación de leds (rojo/verde) permite de forma visual e instantánea, saber si el dispositivo USB está infectado o no.

RECEPCIÓN EN REGISTROS Y MEMORIAS DE USO INTERNO:

Conectado en red el SafeDoor da servicio a varios puestos y a través de él se realizan los análisis de los dispositivos de almacenamiento USB que provengan del exterior o utilizados por el personal.

Aquí se realizaría el análisis Software, donde se detectarían las amenazas Malware y las particiones ocultas en los archivos que se alojan dentro de la Memoria USB.

Aunque los dispositivos se manejen siempre dentro de la organización, y no salgan al exterior, no implica que sean seguros, aún en el caso de que la información esté cifrada, ya que se pueden producir igualmente ataques a nivel Hardware y Eléctrico.

En todos los casos la implantación de Safe Door evita que se pueda extraer información interna de la organización a través de dispositivos de almacenamiento USB. Existe la posibilidad de permitirlo, bajo un estricto protocolo y con los permisos adecuados en cada organización y siempre auditando esta extracción a través de nuestra Consola Central.

PERSONAL EN MOVILIDAD

Existen puestos de trabajo (inspectores) cuya labor se efectúa fuera de las oficinas de la administración. El inicio del expediente sancionador se comunica de forma inmediata al sujeto. En caso de no existir conexión a internet, o que esta haya sido deshabilitada, la comunicación se llevará a cabo a través de Memoria USB del propio sancionado con lo que ello puede implicar no solamente para el terminal utilizado por el inspector, si no a la red a la que se conecta el mismo.

El tamaño y ligereza del SafeDoor permite su uso en movilidad y con el triple análisis automatizado, en unos minutos sabemos si esa memoria USB es apta o no.

RESPUESTAS A CUESTIONES FRECUENTEMENTE PLANTEADAS

1. Número máximo de antivirus a instalar en dispositivo

Safe Door soporta dos motores antivirus simultáneos.

2. Forma de actualización de los antivirus.

Existen tres métodos de actualización de firmas, en función del entorno:

- **Directa.** Si los safedoor disponen de salida a internet, ya sea directa o a través de proxy, se actualizan directamente contra el servidor del proveedor de antivirus.
- **Indirecta.** Si los safeDoor no disponen de salida a internet pero su consola central sí, utilizarán ésta como mirror para la actualización.
- **Offline.** Proporcionamos una herramienta (windows) a ejecutar desde un equipo con salida a internet que obtendrá las firmas y las volcará en una memoria USB. Esta memoria podrá ser conectada a cualquier safeDoor, que la utilizará como fuente de actualizaciones. También es posible utilizarla para volcar las firmas en la consola central (si ésta se encuentra en una red aislada) de forma que actúe como mirror para sus safeDoor asociados.

3. Niveles de escaneo a ejecutar (rápido, completo, selectivo,)

En cuanto se conecta una memoria a safeDoor, se lleva a cabo el análisis

hardware y eléctrico automáticamente. Este análisis es muy rápido, apenas dos segundos, aunque se sigue monitorizando continuamente hasta su extracción. En cuanto al análisis software (antivirus) existen dos modos de uso:

- **Manual:** Desde un navegador web, el usuario selecciona los archivos/carpetas a descargar. Sobre estos ficheros seleccionados se lleva a cabo el análisis por parte del antivirus (análisis selectivo)
- **Automático:** Los antivirus escanean todo el contenido de la memoria informando a través de Leds del progreso y resultado. No es necesario acceder a la interfaz web, el equipo es autónomo (análisis completo)

También es posible modificar los parámetros por defecto de los motores de antivirus (tamaño máximo, niveles de profundidad en archivos comprimidos, extensiones a analizar...)

4. Tiempo medio de escaneo por USB.

El tiempo de escaneo es similar al de un equipo de escritorio, ya que el cuello de botella está en la velocidad de lectura de la memoria USB. Con una memoria moderna se pueden alcanzar velocidades de lectura de unos 35 MB/s, mientras que con memorias publicitarias o degradadas por el uso la velocidad puede caer a los 15/20 MB/s.

5. Almacenamiento de logs: dispositivo, consola?

Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. En caso de pérdida de conectividad o equipos aislados estos informes se almacenarán en el dispositivo, siendo posible su descarga (firmado digitalmente) para su posterior carga en la consola central de forma manual a través de su interfaz web.

6. Número máximo de dispositivos a gestionar desde una consola central

Es escalable en función del hardware o configuración de la máquina virtual sobre el que corra. Con 2 núcleos /16GB RAM se soportan 50 dispositivos vinculados.

7. Pantallazos ejemplo consola central

authUSB console

Menú

Panel

Usuarios

Dispositivos

Dispositivos USB

Analisis

Analisis

usbBox	Archivo	Descripción	Dirección	Fecha
usbBox00040	sdhst.cfg	Clean	INPUT	2019/06/16 13:34:55
usbBox00040	ace.ir	Clean	INPUT	2019/06/16 13:34:55
usbBox00040	access.pcx	Clean	INPUT	2019/06/16 13:34:55
usbBox00040	sb.ir	Clean	INPUT	2019/06/16 13:34:55
usbBox00040	sa.ir	Clean	INPUT	2019/06/16 13:34:55
usbBox00040	1dx16.fnt	Clean	INPUT	2019/06/16 13:34:55
usbBox00039	gstreamer-1.0-devel-x86-1.12.4.msi	Clean	INPUT	2019/06/16 22:04:08

Detalles:

Dispositivo: USB/Disk 2.0
 Ruta: /gstreamer-1.0-devel-x86-1.12.4.msi
 SHA1: bba633b159ba36869002351c14d93a9c41d93
 SHA256: 6138a25383fc1918a3fbed46e590a65c00038d03a712921693b015ce9d80
 Tipo: Composite Document File V2 Document, Little Endian, OS: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: GStreamer 1.0 (Development Files), Author: GStreamer Project, Keywords: Installer, Comments: GStreamer 1.0, Template: Intel1033, Revision Number: [03304F06-9983-4A54-B96D-270E5E8D8240], Create Time/Date: Sat Dec 9 18:30:36 2017, Number of Pages: 100, Number of Words: 2, Name of Creating Application: Windows Installer XML (3.5.2519.0), Security: 2
 Tamaño: 12978556 bytes
 F. Creación: 2019/06/12 18:48:23
 F. Acceso: 2019/06/12 02:00:00
 F. Modificación: 2019/04/12 12:55:26

Resultado global del análisis:

AV: Global
 Cod. Resultado: 0
 Desc. Resultado: Clean

authUSB console

Menú

Panel

Usuarios

Dispositivos

Dispositivos USB

Analisis

Dispositivos USB

usbBox	Descripción	Dirección	Fecha
usbBox00037	authUSB Local Storage		2019/04/29 01:30:39
usbBox00037	Generic Mass Storage	928825D1	2019/04/29 01:28:19
usbBox00037	authUSB Local Storage		2019/04/29 01:04:56
usbBox00037	authUSB Local Storage		2019/04/29 00:48:27
usbBox00037	Generic Mass Storage	928825D1	2019/04/29 00:47:35
usbBox00037	authUSB Local Storage		2019/04/29 00:38:50
usbBox00030	Kingston DataTraveler 3.0	08609E686615F28087233886	2019/04/18 00:21:05
usbBox00030	No a storage device ATAMEL AVR	HEID Keyboard	2019/04/18 00:18:39
usbBox00030	Killer detected (USB2) USBKILL	USBKiller	0

Detalles:

Fabricante: USBKILL
 Cod. Fabricante: USBKILL
 Producto: USBKiller
 Cod. Producto: USBKiller
 Serial: 0

Particiones:

Etiqueta	Formato	Tamaño	Oculto
usbBox00030	authUSB	Local Storage	
usbBox00040	USB2.0	Flash Disk	2019/03/0710210562
usbBox00040	No a storage device	ATAMEL AVR	HEID Keyboard
usbBox00040	USB2.0	Flash Disk	2019/03/0710210562
usbBox00040	Killer detected (USB1) USBKILL	USBKiller	0

Mostrando registros del 76 al 90 de un total de 92 registros

Anterior 1 2 3 4 5 6 7 Siguiente

authUSB console

Menú

Panel

Usuarios

Dispositivos

Dispositivos USB

Analisis

Dispositivos USB

usbBox	Archivo	Descripción	Dirección	Fecha
usbBox00040	eicar.com	Infected	INPUT	2019/06/16 13:39:21
usbBox00039	eicar.com	Infected	INPUT	2019/06/15 22:02:46
usbBox00039	win32.exe	Infected	INPUT	2019/05/23 21:50:03
usbBox00039	warnacy.exe	Infected	INPUT	2019/05/23 21:50:03
usbBox00039	ArdamaxKeylogger	Infected	INPUT	2019/05/23 21:50:03
usbBox00039	eicar.com	Infected	INPUT	2019/05/23 21:50:03
usbBox00039	win32.exe	Infected	INPUT	2019/05/23 21:46:12
usbBox00039	e681e6b8c9eb5bba545ef4d01b5f1d71661840403969e5babe9e0e41aa.exe	Infected	INPUT	2019/05/23 21:46:12
usbBox00039	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18	Infected	INPUT	2019/05/23 21:46:12

Detalles:

Dispositivo: USB2.0/Flash Disk
 Ruta: /keylogger.Ardamax/ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18
 SHA1: 8f6ec9bc137822bc1d8f139c35edc3b847ce3fe
 SHA256: 6cd70e0c48b04ee1aaca1f0c63c8a2aaada8b37197708a703211238da8b6b75
 Tipo: PE32 executable (GUI) Intel 80386, for MS Windows
 Tamaño: 802724 bytes
 F. Creación: 2019/05/23 19:43:51
 F. Acceso: 2019/05/23 02:00:00
 F. Modificación: 2019/06/06 16:22:30

Resultado global del análisis:

AV: Global
 Cod. Resultado: 1
 Desc. Resultado: Infected
 Amenaza: Win32/KeyLogger.Ardamax.NBB.application

Copyright © 2019 authUSB

captura de fichero limpio, amenaza SW y amenaza HW

8. En caso de que se detecte Malware en un USB queda éste inutilizado?

El paso previo y obligatorio a la descarga es el análisis Software (antivirus). En caso de detección de amenaza en alguno de los ficheros, en ningún caso el usuario podrá descargar ese concretamente, si el resto de ficheros están libres de amenazas podrán descargarse.