

CASO DE USO

authUSB SafeDoor en entornos industriales



¿Cuál es la problemática específica de los entornos industriales respecto al tráfico de Memorias USB?

Las redes aisladas OT suponen la utilización tanto para los procesos propios como de terceros (actualizaciones etc.) de Memorias USB. Dentro de estas infraestructuras, este uso debe estar regulado y controlado, habitualmente este control se efectúa a través de Firewalls y otros elementos que se dedican a escanear las memorias USB y el tráfico de la red aislada en busca de amenazas Malware, a nivel software.

La conexión cada vez más frecuente entre las redes IT y OT provocan que cualquier vulnerabilidad, a través de dispositivos USB, que se produzca repercute de forma inmediata en la seguridad de las plantas.

Los ataques al Hardware (BadUSB) realizados a través de memorias USB, son muy específicos, dirigidos. El atacante conoce bien el sistema que se dispone a vulnerar. Este tipo de amenazas son además indetectables, persistentes en el tiempo y en la mayoría de las ocasiones irreversibles.

Por último existe además la amenaza Eléctrica (USB Killer) con él se inutilizaría el equipo dedicado de la red con el objetivo de detener la producción. Esto supondría un perjuicio económico brutal.

El control a todos los niveles de estos dispositivos de almacenamiento es vital para la seguridad y funcionamiento de la cadena industrial.

¿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. *patentado

¿Cómo encaja SafeDoor en nuestro esquema de trabajo y de ciberseguridad?

EQUIPOS EN RECEPCIÓN Y ACCESOS:

1. EQUIPOS FRONTERA Y ADUANA

El dispositivo SafeDoor se puede dedicar como equipo frontera y aduana.

Dispositivo 1- Análisis y Monitorización continua de las memorias USB externas o internas y cuya información queremos volcar a un nuevo Pendrive de forma segura. (Equipo frontera)

Dispositivo 2- Pendrive donde vamos a volcar esta información. Se efectúa un borrado seguro previo a la introducción de la misma. Con esto conseguimos asegurarnos de que, tanto la información contenida en él, como el propio hardware no contienen amenazas de ningún tipo. (Equipo aduana)

Se puede, si ello fuese necesario, establecer un protocolo de utilización de whitelists/blacklists para las memorias utilizadas. Este protocolo podría eliminarse ya que con los pasos previos que hemos señalado tendríamos ya la certeza de que las memorias están libres de cualquier tipo de amenaza.

Se incluye la posibilidad de utilización de firma digital del fichero que se descarga para garantizar su integridad.

La trazabilidad del proceso es total.

2. INTÉRNAMENTE

Cualquier dispositivo USB que entre o salga y se utilice, se analiza previamente con SafeDoor y nunca se conectará directamente en dispositivos corporativos. Esto evita que las diferentes

redes y la comunicación que se pueda producir entre ellas, se vean afectadas por ataques Hw, Eléctricos o Sw.

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 siempre auditando esta extracción a través de nuestra Consola Central.

RESPUESTAS A CUESTIONES FRECUENTEMENTE PLANTEADAS

1. Número máximo de antivirus a instalar en dispositivo

Safe Door soporta hasta 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.

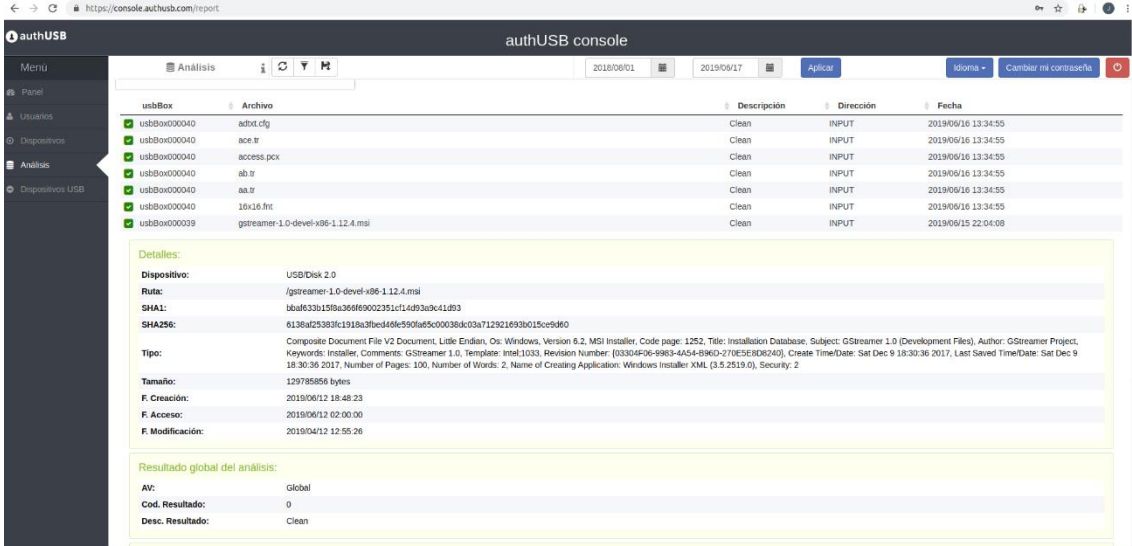
5. Almacenamiento de logs: dispositivo, consola?

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 consola central



The screenshot displays the 'authUSB console' web interface. The main area shows a table of scanned files with columns for 'usbBox', 'Archivo', 'Descripción', 'Dirección', and 'Fecha'. Below the table, a 'Detalles:' section provides information for a selected file, including device type, file name, hashes, and metadata.

usbBox	Archivo	Descripción	Dirección	Fecha
usbBox000040	adrot.ctg	Clean	INPUT	2019/06/16 13:34:55
usbBox000040	ace.tr	Clean	INPUT	2019/06/16 13:34:55
usbBox000040	access.pcx	Clean	INPUT	2019/06/16 13:34:55
usbBox000040	ab.tr	Clean	INPUT	2019/06/16 13:34:55
usbBox000040	aa.tr	Clean	INPUT	2019/06/16 13:34:55
usbBox000040	16x16.fnt	Clean	INPUT	2019/06/16 13:34:55
usbBox000039	gstreamer-1.0-devel-x86-1.12.4.msi	Clean	INPUT	2019/06/15 22:04:08

Detalles:

Dispositivo: USB/Disk 2.0
Ruta: /gstreamer-1.0-devel-x86-1.12.4.msi
SHA1: 1b4f633b159a3666902351c14493a9c411893
SHA256: 6136a25383fc1918a3bed468e990a65c000384d03a712921693b015ce940
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: Intel:1033, Revision Number: {03304D6-6983-4A54-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: 129785856 bytes
F. Creación: 2018/06/12 18:48:23
F. Acceso: 2018/06/12 02:00:00
F. Modificación: 2018/04/12 12:55:26

Resultado global del análisis:

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

authUSB console

Dispositivos USB	id	Fecha	Aplicar	Idioma	Cambiar mi contraseña
usb8x000037	authUSB	2019/06/17			
usb8x000037	Generic	2019/06/17	92882501		
usb8x000037	authUSB	2019/04/29 01:30:39			
usb8x000037	Generic	2019/04/29 01:28:19			
usb8x000037	authUSB	2019/04/29 01:14:56			
usb8x000037	Generic	2019/04/29 00:46:27			
usb8x000037	authUSB	2019/04/29 00:47:35	92882501		
usb8x000030	authUSB	2019/04/29 00:38:50			
usb8x000030	Kingston	2019/04/18 00:21:05	06606E6B6615F260B723B866		
usb8x000030	No a storage device	2019/04/18 00:18:39			
usb8x000030	ATMEL AVR	2019/04/18 00:18:39			
usb8x000030	USBKILL	2019/04/18 00:16:27	0		

Detalles:

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

Particiones:

Etiqueta	Formato	Tamaño	Oculto

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

authUSB console

Análisis

usb8x000039	Archivo	Descripción	Dirección	Fecha
usb8x000040	eicar.com	Infected	INPUT	2019/06/16 13:38:21
usb8x000039	eicar.com	Infected	INPUT	2019/06/15 22:02:46
usb8x000039	win32.exe	Infected	INPUT	2019/05/23 21:50:03
usb8x000039	warmacy.exe	Infected	INPUT	2019/05/23 21:50:03
usb8x000039	ArdamaxKeylogger	Infected	INPUT	2019/05/23 21:50:03
usb8x000039	eicar.com	Infected	INPUT	2019/05/23 21:50:03
usb8x000039	win32.exe	Infected	INPUT	2019/05/23 21:46:12
usb8x000039	ed01ebfbc9eb5bbea545ef4d01b5f1071661840480439c6e5babe0e00e41aa.exe	Infected	INPUT	2019/05/23 21:46:12
usb8x000039	ArdamaxKeylogger_E33AF9E602CB7AC3634C2606150DD18	Infected	INPUT	2019/05/23 21:46:12

Detalles:

Dispositivo: USB2.0/Flash Disk
 Ruta: /Keylogger/Ardamax/ArdamaxKeylogger_E33AF9E602CB7AC3634C2606150DD18
 SHA1: 8f6ec9c137822bc1d8f439c3fedc3b47ce3fe
 SHA256: 6c870eac48b0ea1aca1f0c3c9a82aaad8b37f197706a70321239da0b6b75
 Tipo: PE32 executable (GUI) Intel 80386, for MS Windows
 Tamaño: 602724 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

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.

