

CASO DE USO

authUSB SafeDoor

Infraestructuras críticas



¿Cuál es la problemática específica de este tipo de estructuras respecto al tráfico de Memorias USB?

Según la propia definición que realiza el CNPIC las Infraestructuras Críticas son las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Las redes aisladas suponen la utilización tanto para los procesos propios como de terceros (actualizaciones etc.) de Memorias USB. Dentro de estas IICC este uso está regulado y controlado utilizándose en la actualidad en los accesos a las mismas kioskos de sanitización (equipo frontera/aduana), Firewalls y otros elementos que se dedican a escanear las memorias USB en busca de amenazas Malware , a nivel software.

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 frontera de la instalación anulando la posibilidad de generación, a través de éste, del pendrive autorizado y permitir así la entrada de un dispositivo no autorizado que contendría una amenaza Hardware en su interior.

¿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.

¿Cómo encaja SafeDoor en nuestro esquema de trabajo?

EQUIPOS EN 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 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 ESPECÍFICAS PLANTEADAS

1. Número máximo de antivirus a instalar en dispositivo (Mcafee, Symantec,.)

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 consola central

authUSB console

2018/06/01 2019/06/17 Aplicar Idioma Cambiar mi contraseña

usbBox	Archivo	Descripción	Dirección	Fecha
usbBox00040	subnt.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	ab.r	Clean	INPUT	2019/06/16 13:34:55
usbBox00040	aa.r	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: bba633b15f9a3686902351c14d93a9c41d93
 SHA256: 6138a25383fc1918a3fbed46e590a85c00038d03a712921693b015ce9d80
 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: 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

2018/06/01 2019/06/17 Aplicar Idioma Cambiar mi contraseña

usbBox	Dispositivos USB	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	ATMEL AVR		2019/04/18 00:18:39	
usbBox00030	Killer detected (USB2)	USBKILL	USBKiller	0	2019/04/18 00:16:27

Detalles:

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

Particiones:

Etiqueta	Formato	Tamaño	Oculto		
usbBox00030	authUSB	Local Storage		2019/04/18 00:12:01	
usbBox00040	USB2.0	Flash Disk	2019030710210562	2019/04/15 12:12:47	
usbBox00040	No a storage device	ATMEL AVR		2019/04/15 12:11:40	
usbBox00040	USB2.0	Flash Disk	2019030710210562	2019/04/15 12:09:06	
usbBox00040	Killer detected (USB1)	USBKILL	USBKiller	0	2019/04/15 12:06:33

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

authUSB console

2018/06/01 2019/06/17 Aplicar Idioma Cambiar mi contraseña

usbBox	Archivo	Descripción	Dirección	Fecha
usbBox00040	eicar.com	Infected	INPUT	2019/06/16 13:38:21
usbBox00039	eicar.com	Infected	INPUT	2019/06/15 22:02:46
usbBox00039	win32.exe	Infected	INPUT	2019/05/23 21:50:03
usbBox00039	warnacry.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	e861e6b0c9b5bba545ef4d01b5f1d716618404804396e5babe9e0e41aa.exe	Infected	INPUT	2019/05/23 21:46:12
usbBox00039	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2606150DD18	Infected	INPUT	2019/05/23 21:46:12

Detalles:

Dispositivo: USB2.0/Flash Disk
 Ruta: /keylogger.Ardamax/ArdamaxKeylogger_E33AF9E602CBB7AC3634C2606150DD18
 SHA1: 8f6ec9bc137822bc1d4f139c35edc3b847ce3fe
 SHA256: 6cd70e0c48b04ee1aaca1f0c63c8a2aaada8377197708a703211238da886b75
 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

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.

