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 con software embebido,que actúa como barrera entre las memorias USB y los equipos de una organización, analizando, bloqueando, informando, auditando y posteriormente gestionando las amenazas, que se producen a través de dispositivos USB, 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 multi plataforma, integrable, pequeño y ligero lo que hace posible su despliegue en multitud de entornos.

EQUIPOS EN RECEPCIÓN Y ACCESOS:

1. ARCOS DE ENTRADA, CONTROLES DE ACCESO

   Instalación de forma totalmente autónoma de SafeDoor (Sólo conectado a la red eléctrica) A través de los leds incorporados nos indica si el dispositivo conectado es seguro o no, realizando el escaneo de los tres tipos de amenazas.

2. EQUIPOS FRONTERA Y ADUANA

   SafeDoor se puede dedicar como equipo frontera y aduana.

Puerto 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)

Puerto 2- Pendrive donde vamos a volcar la información. Se efectúa un escaneo de esta memoria confiable. Con esto conseguimos asegurarnos de que, tanto la información contenida en él, como el propio hardware no contienen amenazas de ningún tipo. (Equipo aduana)

Todo el proceso de transferencia de la información se efectua de forma SEGURA dentro del dispositivo SafeDoor.

SafeDoor soporta memorias encriptadas tipo Bitlocker, Ironkey y similares.

Se puede, si ello fuese necesario, establecer un protocolo de utilización de dispositivos confiables para las memorias utilizadas dentro de la organización. 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.

La inclusión de utilización de firma digital del fichero que se descarga garantiza su integridad.

La trazabilidad del proceso es total.

3. RED INTERNA

Cualquier dispositivo USB que entre o salga y se utilice en la organización, 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 SafeDoor 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**
   SafeDoor embebe simultaneamente dos* maquinas antivirus. Podemos además integrarlo con un Metadefender o enviar los archivos a una Sandbox.
   Podemos integrar más por especificación del cliente.

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.**

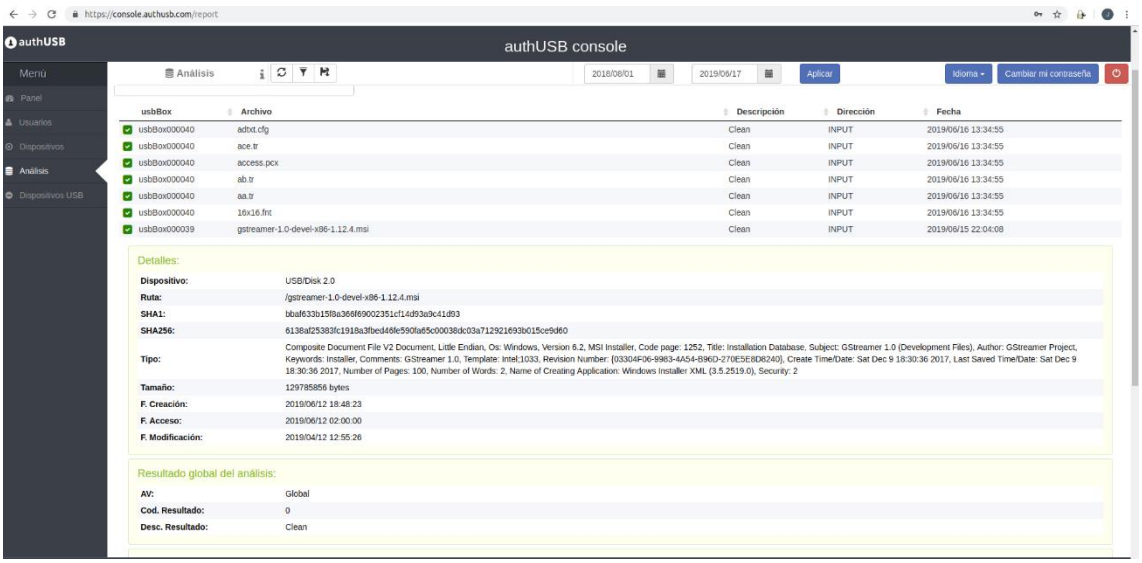
El tiempo de escaneo es similar al de un equipo de escritorio, ya que el cuello de botella está en la velocidad de lectura de la memoria USB. Con una memoria moderna se pueden alcanzar velocidades de lectura de unos 35 MB/s, mientras que con memorias publicitarias o degradadas por el uso la velocidad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

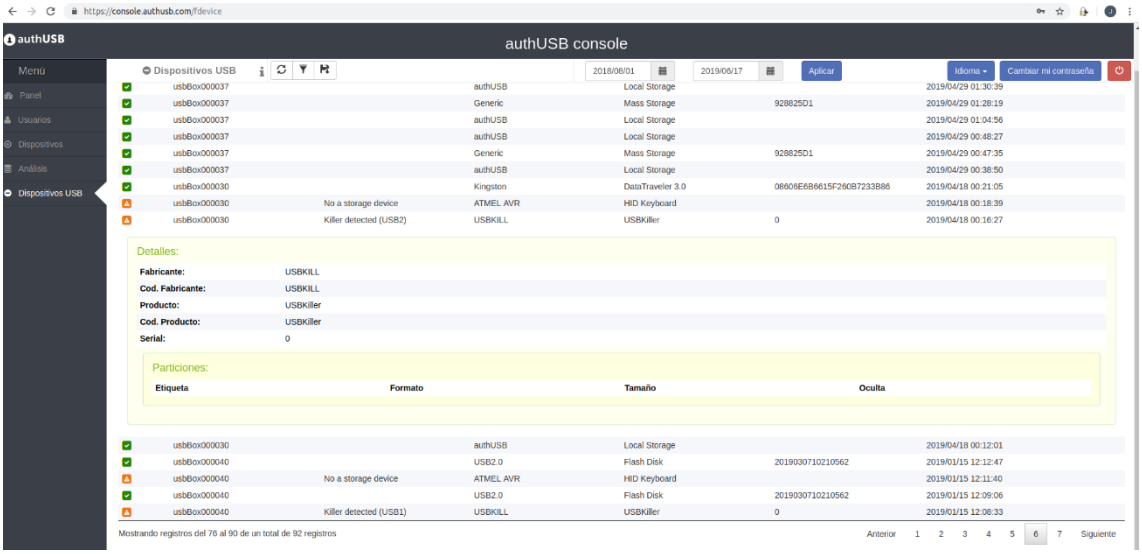
5. **Almacenamiento de logs: dispositivo, consola?**

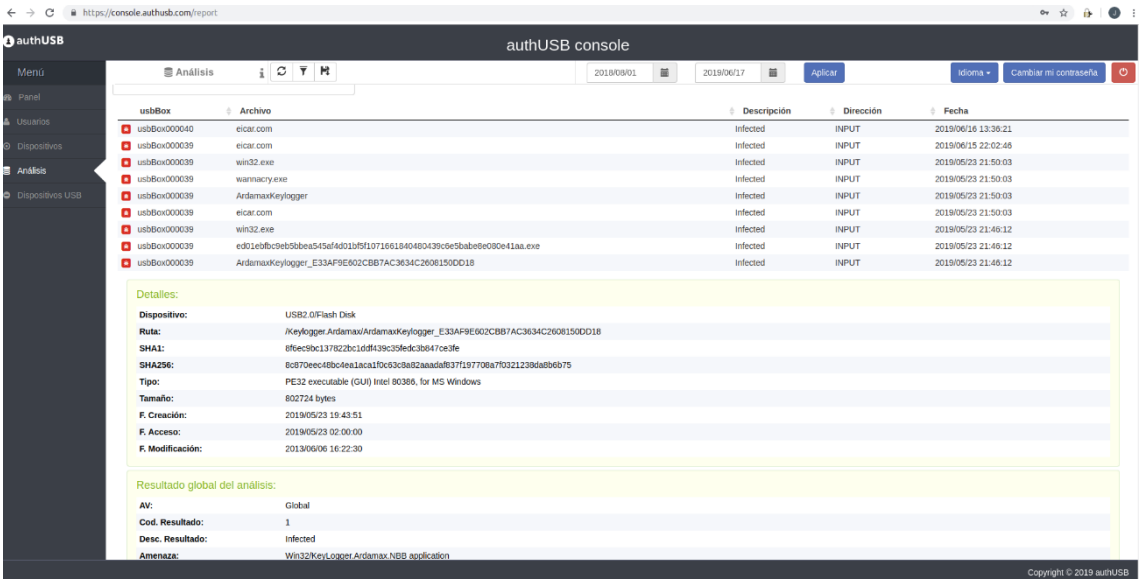
Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. En caso de pérdida de conectividad o equipos aislados estos informes se almacenarán en el dispositivo, siendo posible su descarga (firmado digitalmente) para su posterior carga en la consola central de forma manual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


https://console.authusb.com/report
authUSB
authUSB console
Menú
Panel
Usuarios
Dispositivos
Análisis
Dispositivos USB
Análisis
2018/06/01
2019/06/17
Aplicar
Idioma
Cambiar mi contraseña
usbBox
Archivo
Descripción
Dirección
Fecha
usbBox000040 adxt.cfg 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: bbaf633b15f8a366f69002351cf14d93a9c41d93
SHA256: 6138af25383fc1918a3fbed46fe590fa65c00038dc03a712921693b015ce9d60
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: {03304F06-9983-4A54-B96D-270E5E8D8240}, Create Time/Date: Sat Dec 9 18:30:36 2017, Last Saved 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: 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


https://console.authusb.com/fdevice
authUSB
authUSB console
Menú
Panel
Usuarios
Dispositivos
Análisis
Dispositivos USB
Dispositivos USB
2018/06/01
2019/06/17
Aplicar
Idioma
Cambiar mi contraseña
usbBox000037 authUSB Local Storage 2019/04/29 01:30:39
usbBox000037 Generic Mass Storage 928825D1 2019/04/29 01:28:19
usbBox000037 authUSB Local Storage 2019/04/29 01:04:56
usbBox000037 authUSB Local Storage 2019/04/29 00:48:27
usbBox000037 Generic Mass Storage 928825D1 2019/04/29 00:47:35
usbBox000037 authUSB Local Storage 2019/04/29 00:38:50
usbBox000030 Kingston DataTraveler 3.0 08606E6B6615F260B7233B86 2019/04/18 00:21:05
usbBox000030 No a storage device ATMEL AVR HID Keyboard 2019/04/18 00:18:39
usbBox000030 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
Oculta
usbBox000030 authUSB Local Storage 2019/04/18 00:12:01
usbBox000040 USB2.0 Flash Disk 2019030710210562 2019/01/15 12:12:47
usbBox000040 No a storage device ATMEL AVR HID Keyboard 2019/01/15 12:11:40
usbBox000040 USB2.0 Flash Disk 2019030710210562 2019/01/15 12:09:06
usbBox000040 Killer detected (USB1) USBKILL USBKiller 0 2019/01/15 12:08:33
Mostrando registros del 76 al 90 de un total de 92 registros
Anterior 1 2 3 4 5 6 7 Siguiente



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.