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 aporta SafeDoor*?

El sistema SafeDoor es una solución de análisis, protección y detección de ciber amenazas efectuadas a través de dispositivos de almacenamiento USB, actuando como barrera entre éstas y los equipos de una organización, frente a los tres vectores de ataque:

▪ Eléctrico: Monitoriza continuamente el comportamiento de la memoria USB a nivel eléctrico, identificando y deteniendo ataques de sobretensión tipo usbKiller

▪ Hardware: Monitoriza continuamente el comportamiento de la memoria USB a nivel hardware, detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc.

▪ Software: Dispone de motor/res antivirus completo/s integrado/s (compatible con varios fabricantes) con el/los que realiza un análisis previo a la descarga o transferencia de cualquier contenido.

El comportamiento de la memoria USB es monitorizado continuamente hasta la extracción evitando de esta manera ataques activados por tiempo o número de conexiones, que pasarían inadvertidos en un análisis inicial. Por esta razón, entre otras un dispositivo USB ajeno nunca debe ser conectado directamente a un equipo de la organización.

Además de la protección el sistema ofrece auditoría y trazabilidad de todos los dispositivos conectados y archivos analizados.

SafeDoor está certificado bajo la metodología Lince y dentro del catálogo CPSTIC del CCN. Posee además una calificación de Alta con respecto al ENS.
https://oc.ccn.cni.es/index.php/es/catalogo-productos-stic/listado-productos-cualificados/441-authusb-safedoor-2-0-0-8
*Producto bajo patente, Marcado CE y FCC

¿Cómo encaja SafeDoor en nuestro esquema de trabajo?

La configuración estándar de SafeDoor permite un uso inmediato, multiplataforma y sin provisionamiento previo ya que el usuario únicamente necesita un navegador web para acceder a la interfaz web del dispositivo y no es necesaria la instalación de software o drivers en su equipo cliente.

El usuario conecta las memorias USB al dispositivo y navega su contenido, seleccionando los ficheros o carpetas de interés para su descarga en el equipo cliente, en una carpeta de red previamente configurada o en un dispositivo USB de confianza, previo escaneo de amenazas.

1. **Usuarios en movilidad / Uso individual**

Es la configuración más sencilla, el usuario navega el contenido de los dispositivos USB conectados a SafeDoor a través de su navegador web seleccionando los archivos o carpetas a descargar, tras escaneo por parte del motor antivirus

2. **Uso compartido / Oficinas de registro**

Es la forma de uso habitual para el sector público. Instalación de SafeDoor en todas las oficinas de registro y en cada departamento, esto permite:

- Establecimiento de protocolos. SafeDoor proporciona las herramientas necesarias para implantar de forma sencilla metodologías específicas en toda o parte de la organización, en función de las características y requisitos de cada unidad:
- Obligatoriedad de análisis por antivirus de cualquier archivo previo a su introducción
- Trazabilidad automática de cualquier fichero entrante o saliente a través de memorias USB
- Gestión de roles. Define quién puede descargar/ acceder a memorias USB y quién además puede copiar información a éstas (lectura/escritura). Soporta LDAP/Directorio activo.
- Simplificación y automatización de procesos para su uso por parte de personal no especializado.

RESPUESTAS A CUESTIONES FRECUENTEMENTE PLANTEADAS

1. **Número máximo de antivirus a instalar en dispositivo**
   SafeDoor embebe simultaneamente dos* maquinas antivirus completas
   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**.
- **Indirecta**.
- **Offline**.

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...)

3. **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.

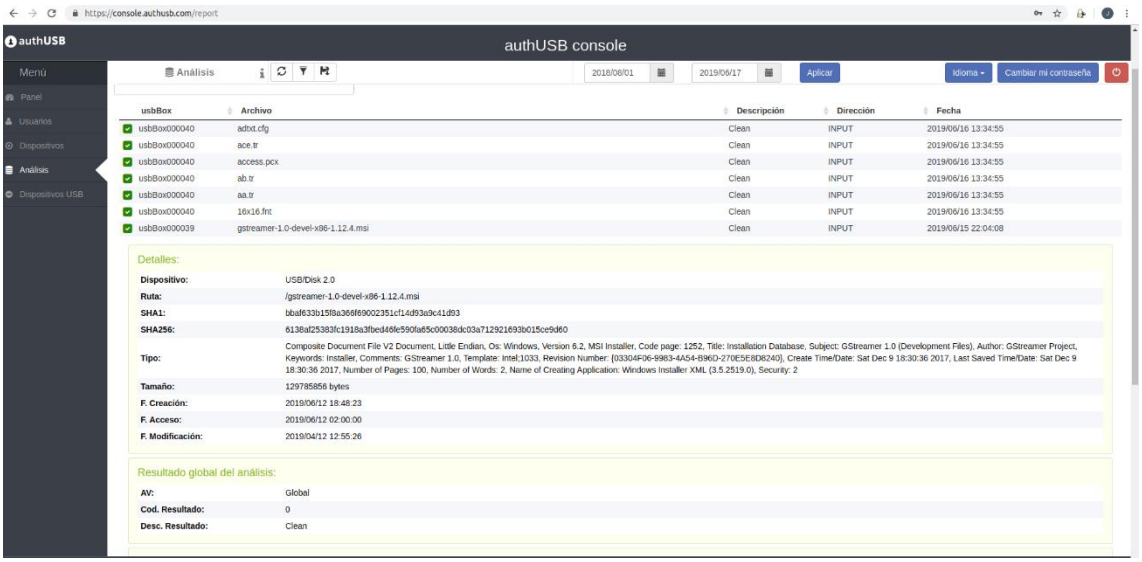
4. **Almacenamiento de logs: dispositivo, consola?**

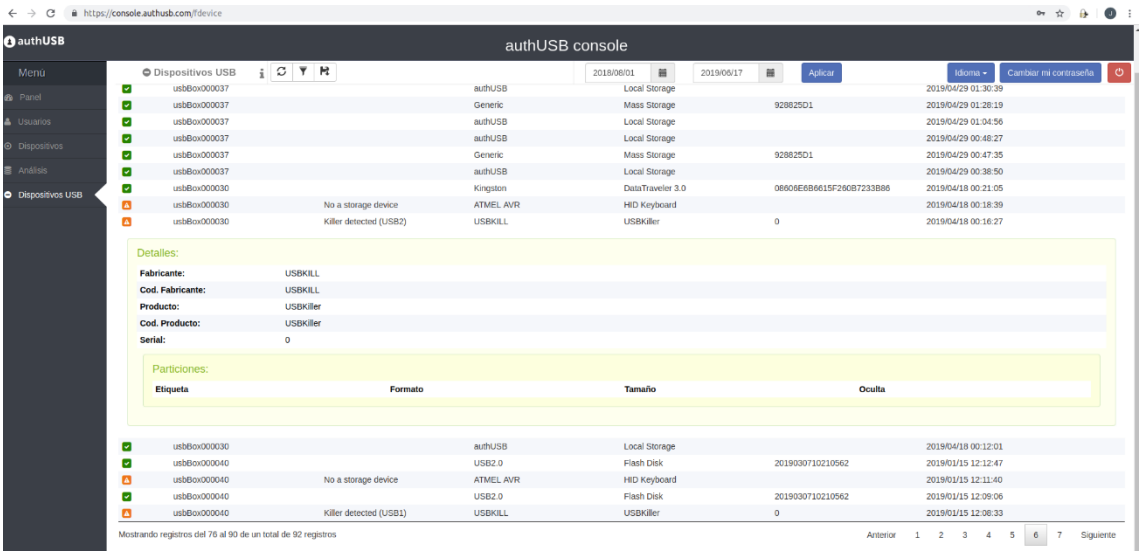
Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. Recibe los informes de auditoría (registro detallado de los dispositivos y archivos analizados) firmados digitalmente desde los dispositivos SafeDoor.

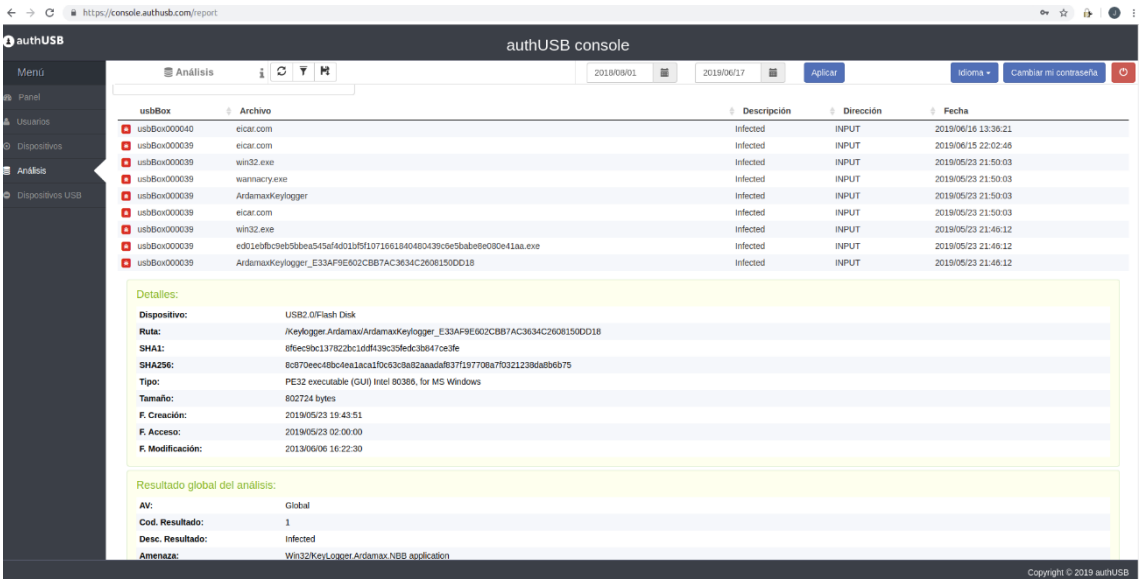
- Por el mismo canal proporciona actualizaciones de firmware y configuración de forma automática a los SafeDoors. En caso necesario también puede actuar como mirror de las actualizaciones de firmas de antivirus (HTTP)
- Integrable con SIEM externo vía syslog
- Ofrece una interfaz web a los administradores para interactuar con el sistema

5. **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.

6. **Pantallazos ejemplo consola central**







captura de fichero limpio, amenaza SW y amenaza HW

7. 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.