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.

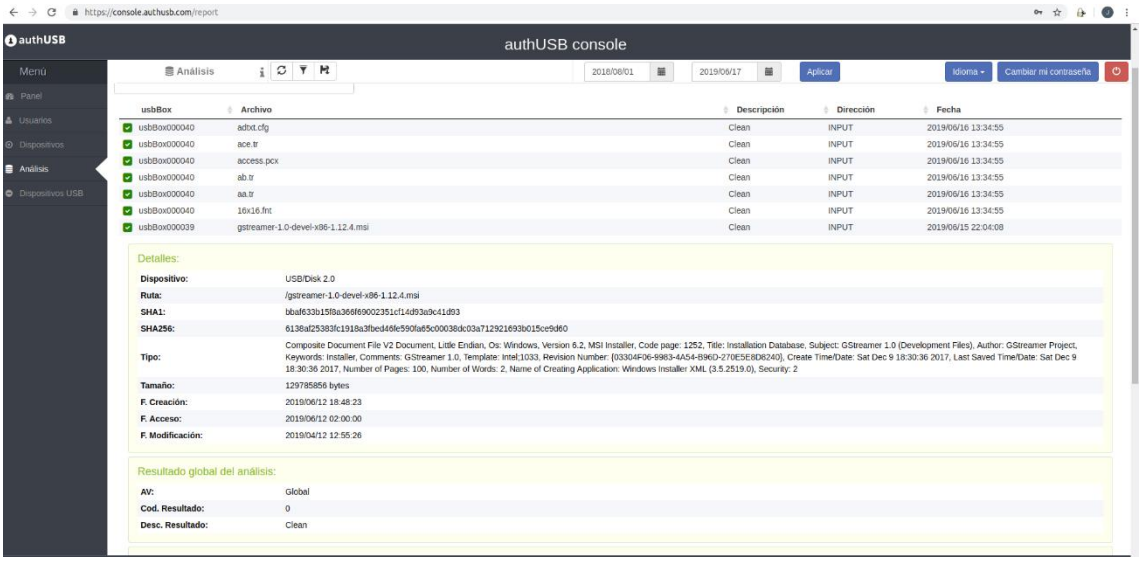
El tiempo de escaneo es similar al de un equipo de escritorio, ya que el cuello de botella está en la velocidad de lectura de la memoria USB. Con una memoria moderna se pueden alcanzar velocidades de lectura de unos 35 MB/s, mientras que con memorias publicitarias o degradadas por el uso la velocidad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

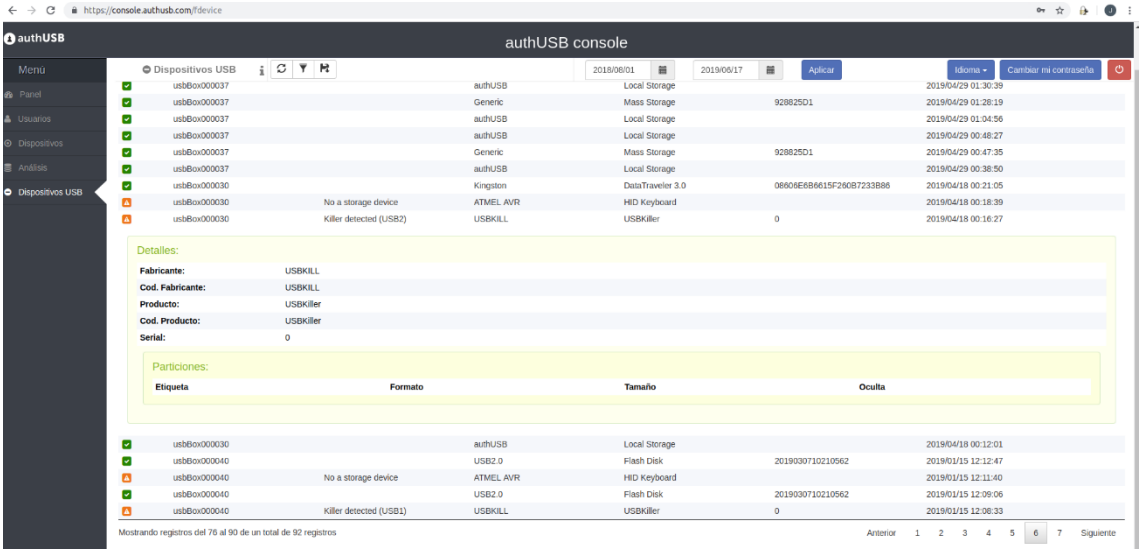
5. Almacenamiento de logs: dispositivo, consola?

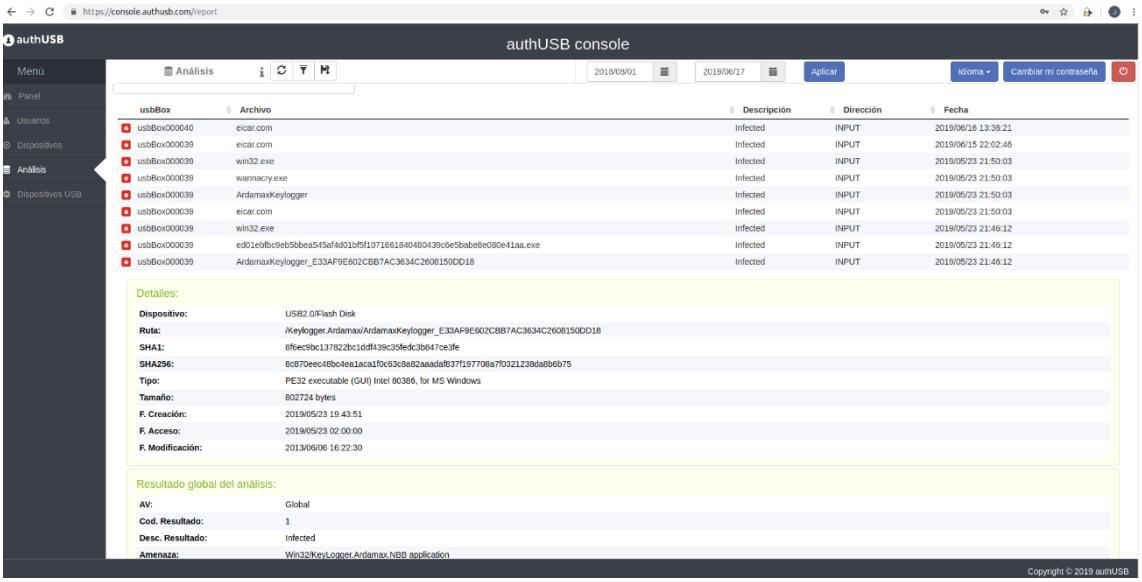
Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. En caso de pérdida de conectividad o equipos aislados estos informes se almacenarán en el dispositivo, siendo posible su descarga (firmado digitalmente) para su posterior carga en la consola central de forma manual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







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.