CASO DE USO

authUSB SafeDoor

Sectores Estratégicos y Esenciales

¿Cuál es la problemática específica de los Servicios Estratégicos y Esenciales respecto al tráfico de Memorias USB?

Los Servicios estratégicos, según los define el CNPIC, los componen cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporcionan un servicio esencial o que garantizan el ejercicio de la autoridad del Estado o de la seguridad del país. En la normativa española hay doce identificados.

Servicio esencial: Es el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

http://www.cnpic.es/Biblioteca/Noticias/listado_servicios_esenciales.pdf

Por tanto y como en este listado se recoge, los sectores son diversos, pero tienen en común que cualquier tipo de ciberataque, en lo que a nosotros atañe, a través de Memorias USB, utilizados tanto internamente como por terceros derivarían en un daño no solamente de carácter económico si no que se podrían ver afectados factores extremadamente dañinos para la ciudadanía.

Estamos ante servicios especialmente golosos, por los datos que en ellos se manejan, para un ciberataque. El tipo de amenazas que aquí se dan son siempre dirigidos y perfectamente preparados.

Controlar el acceso de este tipo de Memorias USB a las instalaciones de estos servicios es básico.

La inutilización de puertos USB por parte de este tipo de Servicios estratégicos, además de ser inviable en la mayoría de los casos, no suponen que no se pueda producir igualmente un ciberataque a través de ellos. Los ataques Hw y Electricos son igualmente viables en este caso. Este tipo de amenazas son además indetectables, persistentes en el tiempo y en la mayoría de las ocasiones irreversibles.

¿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, 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?

Dada la gran variedad de casuísticas que se pueden dar en los diferentes sectores que componen estos Sectores estratégicos los dividiremos en dos bloques tratando de exponer en cada uno de ellos donde poner el foco en la utilización de SafeDoor.

I. **SECTORES SIN RED PRODUCTIVA**

1. IMPLEMENTACIÓN EN ALTA DIRECCIÓN:

SafeDoor conectado directamente a equipos informáticos de Alta Dirección, ejerciendo de único punto de entrada de cualquier dispositivo de almacenamiento USB. Impide además que se pueda extraer por este medio cualquier tipo de información sin que exista una autorización previa. En este caso se audita, a través de la Consola Central esta extracción, consignando quién, como, cuando y donde se produce.

2. DEPARTAMENTOS ADMINISTRATIVOS Y OFICINAS:

Conectado en red SafeDoor da servicio a cada departamento, compuesto por 5-6 puestos/oficina y a través de él se realizan los análisis de los dispositivos de almacenamiento USB utilizados por el personal.

En el caso de la Oficinas, al igual que en los departamentos de los servicios centrales, se efectúan a través de SafeDoor los análisis de los USB gestionados por el personal, tanto internos como externos, convirtiéndose en el único punto de entrada de las memorias USB a la organización.

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 con los permisos adecuados en cada organización y siempre auditando esta extracción a través de nuestra Consola Central.

II. SECTORES CON RED PRODUCTIVA

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 efectúa 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. Éste 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 PREGUNTAS FRECUENTES SOBRE SAFEDOOR

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 análidis 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.

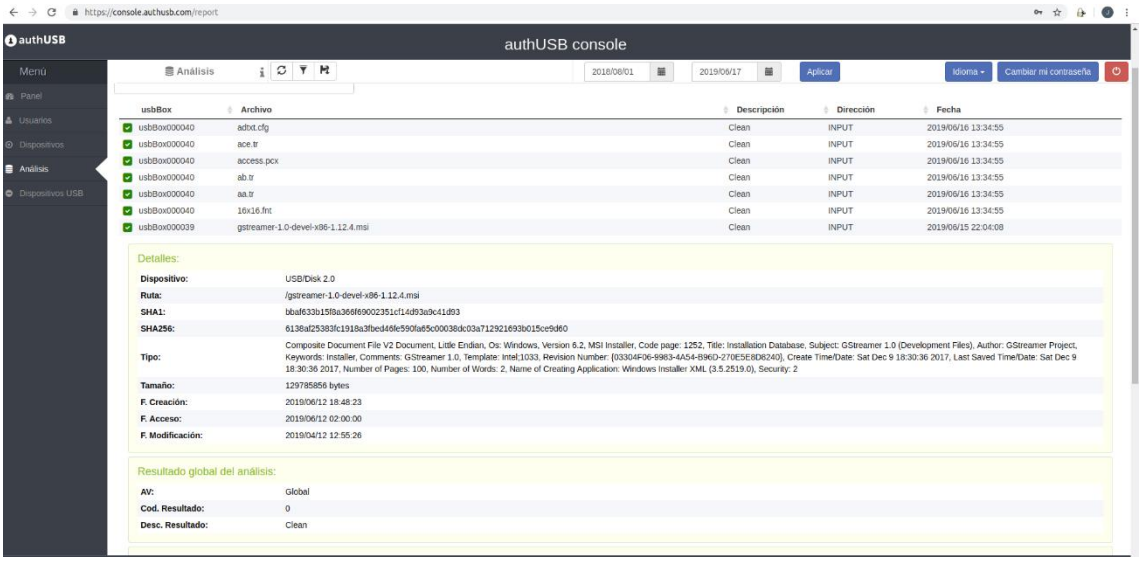
5. **Almacenamiento de logs: dispositivo, consola?**

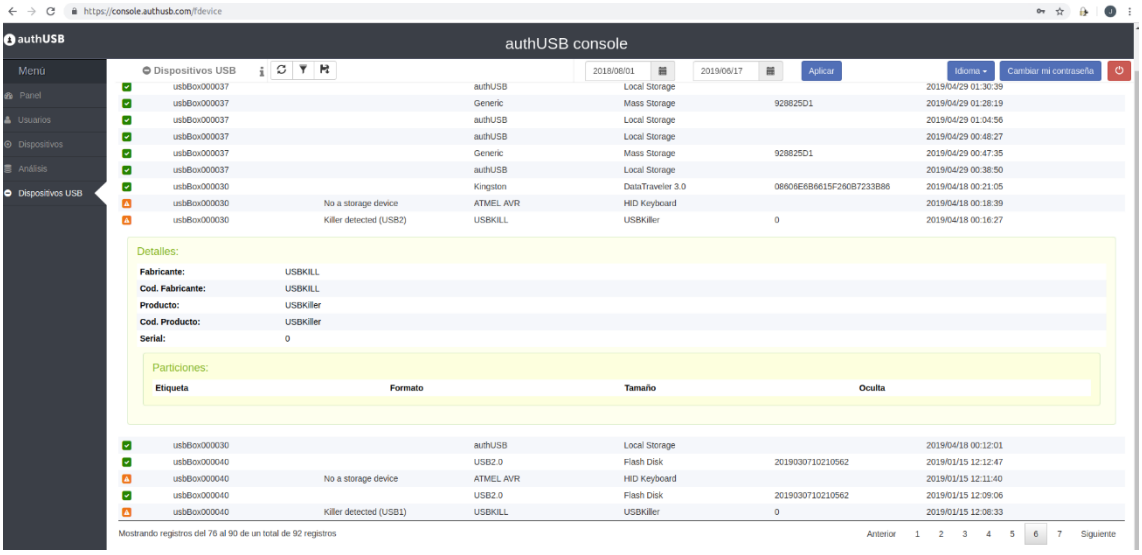
   Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. En caso de pérdida de conectividad o equipos aislados estos informes se almacenarán en el dispositivo, siendo posible su descarga (firmado digitalmente) para su posterior carga en la consola central de forma manual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

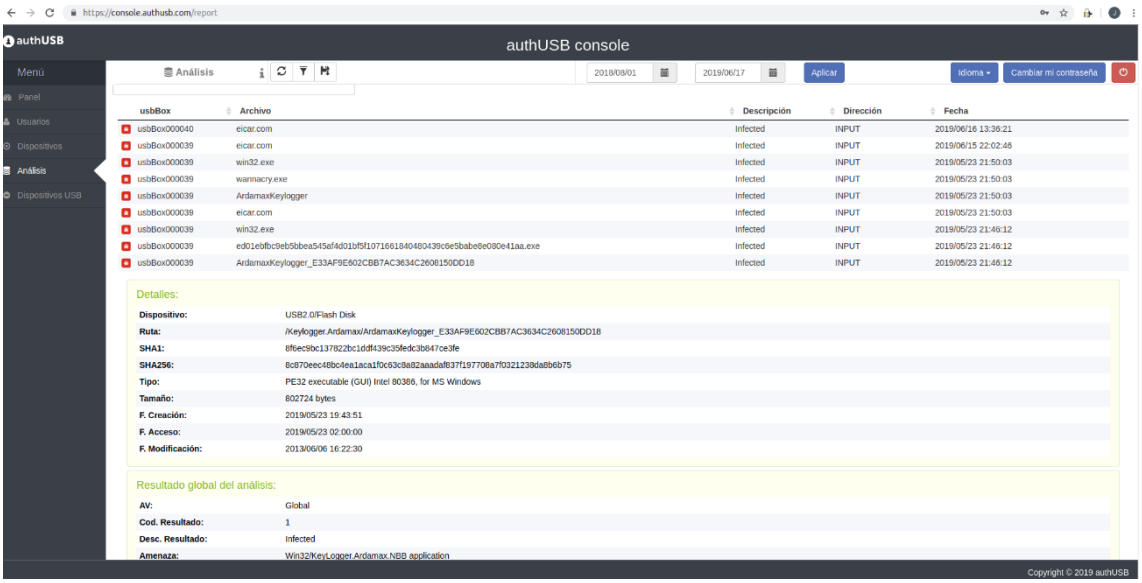
6. **Número máximo de dispositivos a gestionar desde una consola central**
   Es escalable en función del hardware o configuración de la máquina virtual

sobre el que corra. Con 2 núcleos /16GB RAM se soportan 50 dispositivos vinculados.

7. Pantallazos consola central







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.