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 aporta SafeDoor*?

El sistema SafeDoor es una solución de análisis, protección y detección de ciberamenazas 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?

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.

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 u oficina y a través de él se realizan los análisis de los dispositivos de almacenamiento USB tanto los del propio personal como aquellos externos. Esto supone que cualquier dispositivo USB utilizado no se conecte directamente a ningún puerto USB dentro de la organización. SafeDoor permite así la protocolización en la entrada de este tipo de dispositivos.

Para su uso compartido por parte de distintos usuarios, el sistema soporta la reserva explícita de cada uno de los puertos de forma que se garantiza la confidencialidad de los contenidos.

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, siempre quedado este movimiento auditado en la Consola Central.

SECTORES CON RED PRODUCTIVA

EQUIPOS EN RECEPCIÓN Y ACCESOS:

1. ARCOS DE ENTRADA, CONTROLES DE ACCESO

Instalación autónoma y automatizada de SafeDoor (Sólo conectado a la red eléctrica) A través de los leds incorporados en él, nos indica si el USB conectado está libre de amenazas realizando el escaneo a los tres niveles de ataques (eléctrico, Hw y Sw)

2. EQUIPOS FRONTERA Y FRONTERA /ADUANA

FRONTERA:

Este modelo permite volcar el contenido de una memoria externa no confiable en una interna confiable e inventariada, autorizada para su posterior conexión a los equipos internos de la organización garantizando de esta manera que no existen amenazas HW o eléctricas y que el contenido ha sido analizado por antivirus, proporcionando a su vez trazabilidad de todos los archivos intercambiados por USB.
Se pueden dar dos tipos diferentes de dedicación como equipo Frontera:

-Automatizado: se efectúa el escaneo de modo totalmente automático, tanto del firmware como de la totalidad de los archivos contenidos en el dispositivo USB.

-Interactivo: Se efectúa la comprobación a nivel Hw y Eléctrico y, a través de la consola web de SafeDoor, podemos elegir aquellos archivos que queramos analizar previos a su descarga.

En este punto aconsejamos de manera insistente que estos dispositivos sean cifrados a nivel HW . SafeDoor soporta los dispositivos de Data Locker y Iron Key.SafeDoor soporta también memorias cifradas con Bitlocker y Luks.

FRONTERA/ADUANA:

Este modelo permite respetar el Airgap entre redes IT/OT o con distintos niveles de clasificación de seguridad a la vez que mantiene la trazabilidad de los ficheros introducidos en la red interna.

El equipo SafeDoor situado en la red interna solamente aceptará dispositivos USB inventariados que previamente deberán haber sido escaneados por el SafeDoor externo. Éste generará en el dispositivo USB inventariado un fichero firmado digitalmente con la lista de archivos escaneados y autorizados, garantizando el SafeDoor interno, previa verificación de la firma digital, que solamente estos archivos sean transferidos. Con este modelo se evita la necesidad de mantener actualizado el antivirus del SafeDoor interno (proceso siempre laborioso en redes aisladas) al no ser necesario, incluso al intercambiar información entre redes situadas en distintos emplazamientos.

La trazabilidad del proceso es total.

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.Permite la integración del directorio activo de la organización.(LDAP)

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 PREGUNTAS FRECUENTES SOBRE SAFEDOOR

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 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...)

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.

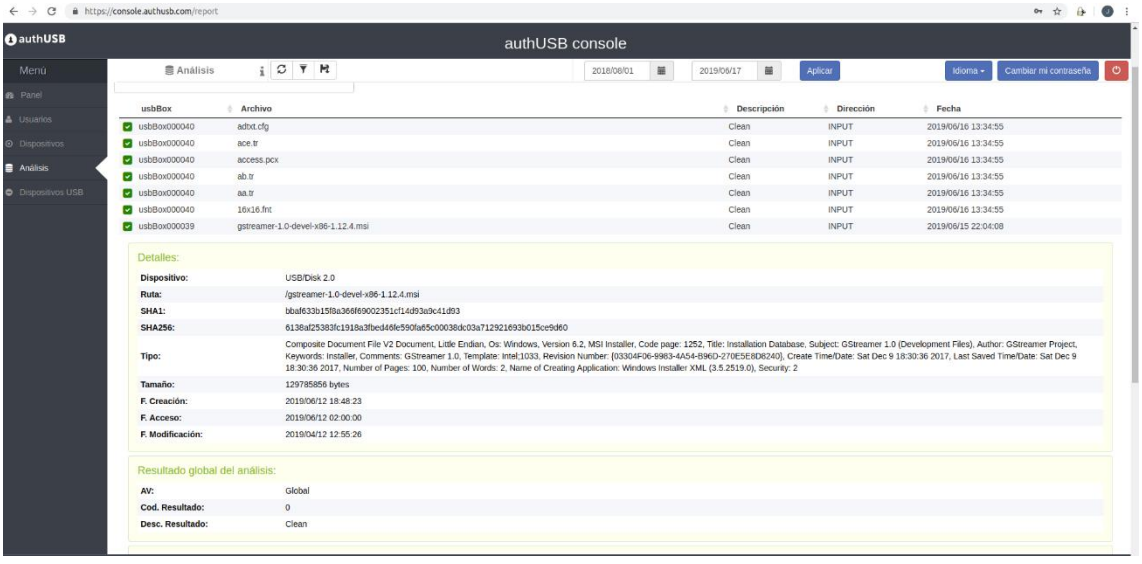
4. Almacenamiento de logs: dispositivo, consola?

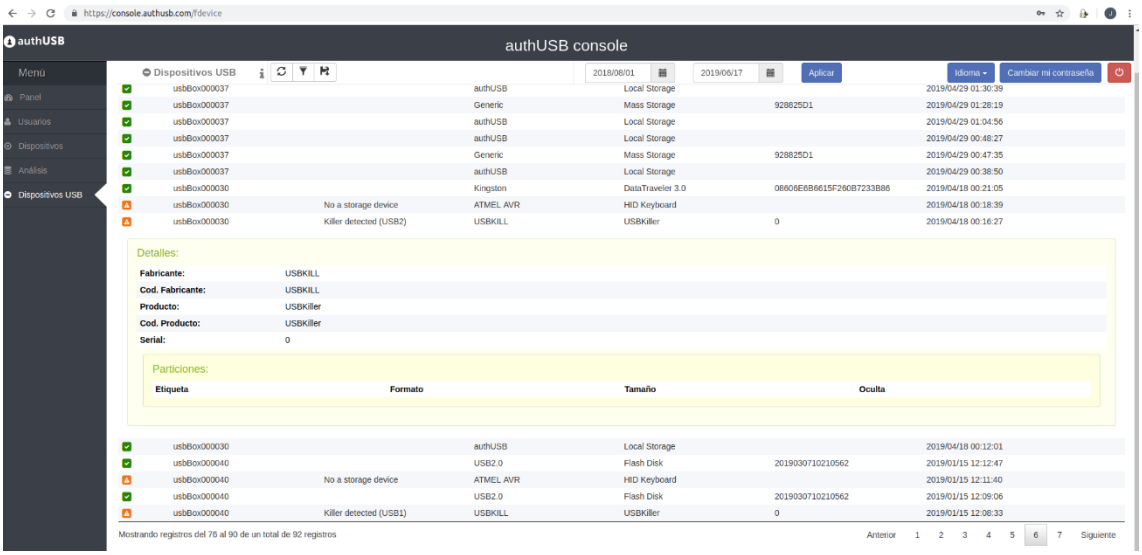
Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. Recibe los informes de auditoría (registro detallado de los dispositivos y archivos analizados) firmados digitalmente desde los dispositivos SafeDoor.

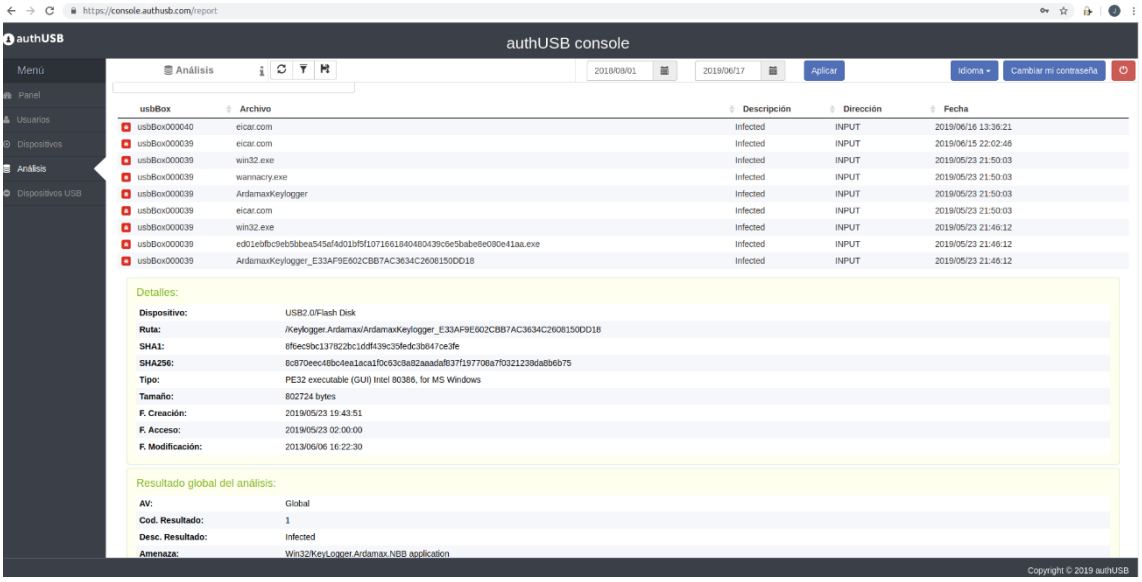
- Por el mismo canal proporciona actualizaciones de firmware y configuración de forma automática a los SafeDoors. En caso necesario también puede actuar como mirror de las actualizaciones de firmas de antivirus (HTTP)
- Integrable con SIEM externo vía syslog
- Ofrece una interfaz web a los administradores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