CASO DE USO

authUSB SafeDoor en Entornos Industriales

¿Cuál es la problemática específica de los entornos industriales respecto al tráfico de Memorias USB?

Las redes aisladas OT suponen la utilización tanto para los procesos propios como de terceros (actualizaciones etc.) de memorias USB. Dentro de estas infraestructuras, este uso debe estár regulado y controlado. Habitualmente este control se efectua a través de Firewalls y otros elementos que se dedican a escanear las memorias USB y el tráfico de la red aislada, en busca de amenazas Malware, a nivel software.

A este problema especifico, se une la apertura cada vez más frecuente entre las redes IT y OT lo que provoca que cualquier vulnerabilidad , a través de dispositivos USB ,que se produzca repercuta de forma inmediata en la seguridad de las plantas hasta este momento perfectamente aisladas.

Los ciberataques que se producen en entornos industriales no son de carácter aleatorio, si no que están perfectamente pensados y dirigidos. Conocen perfectamente el entorno donde se va a llevar a cabo.

Las soluciones actuales, Firewalls, AV,Kioskos de sanitización escanean los dispositivos USB a dos niveles Sw y Hw

A nivel SW se realiza un **escaneo estático** de los dispositivos USB, es decir si la memoria USB contiene una amenaza con retardo, no serían capaces de detenerla.

Por otra parte las amenazas a nivel HW que son detectadas por estas soluciones están basadas siempre en Listas Blancas (Whitelists). Cualquier amenaza nueva no serían capaces de detectarla

En este entorno son especialmente significativos los ataques Hardware (BadUSB) realizados a través de memorias USB, El atacante conoce bien el sistema que se dispone a vulnerar. Este tipo de amenazas son además indetectables, persistentes en el tiempo y en la mayoría de las ocasiones irreversibles.

Por último existe la amenaza Eléctrica (USB Killer).Esta amenaza lo que pretende es derribar la primera capa de seguridad física de la organización y evitar así que se pueda protocolizar la utilización de dispositivos USB que tengan que acceder a la red.Normalmente este paso previo de derribo se da como parte de un ataque combinado.Se inutilizaría el equipo dedicado de la red con el objetivo de efectuar un posterior ataque a nivel Hw.Este sería persistente en el tiempo y lo que es más grave indetectable. Nada escanea el Hw del equipo.

El control a todos los niveles de estos dispositivos es vital para la seguridad y funcionamiento de la cadena industrial.

¿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 y de ciberseguridad?

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 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**.
- **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?

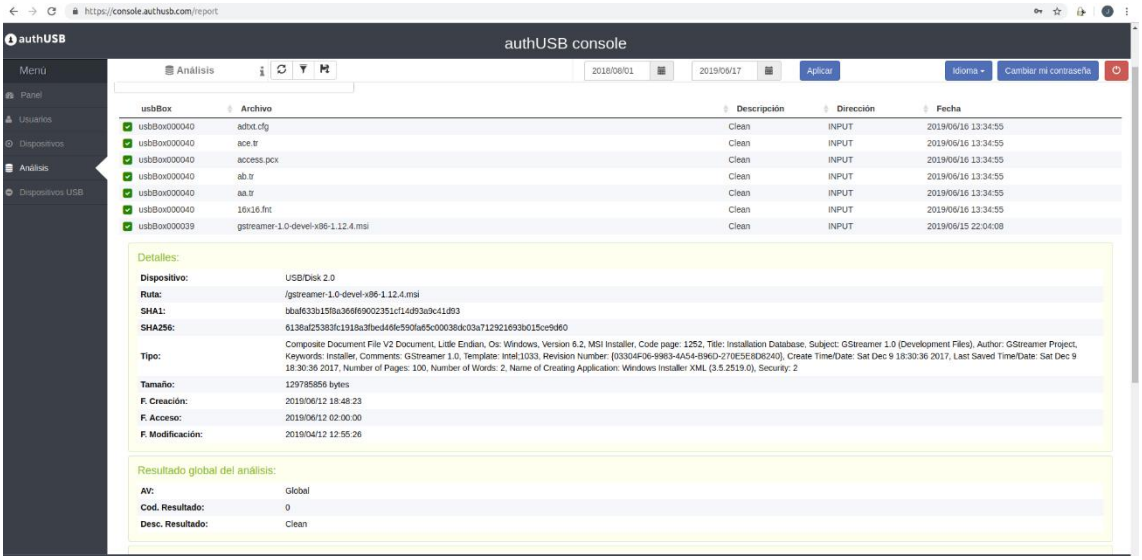
Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. Recibe los informes de auditoría (registro detallado de los dispositivos y archivos analizados) firmados digitalmente desde los dispositivos SafeDoor.

- 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

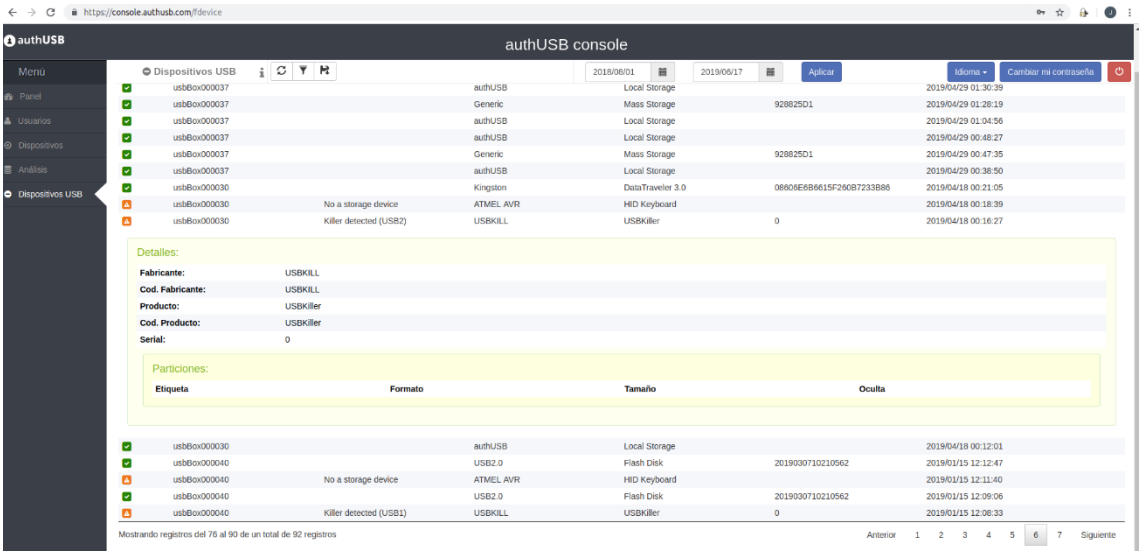
5. Número máximo de dispositivos a gestionar desde una consola central

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.

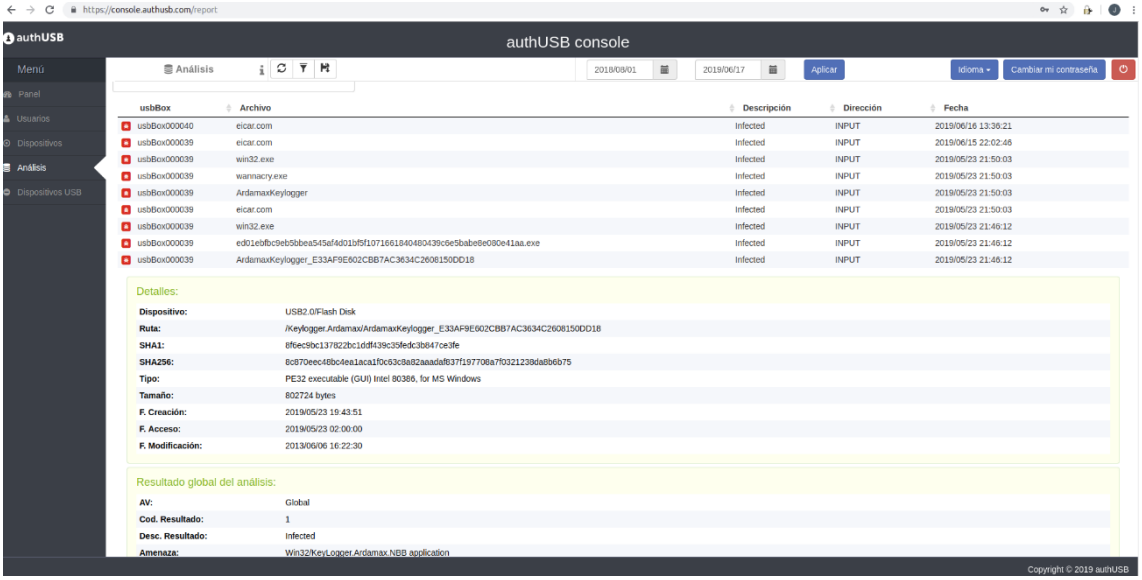
6. Pantallazos consola central



captura de fichero limpio



amenaza SW



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.