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.

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.

Además la apertura cada vez más frecuente entre las redes IT y OT provocan 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 separadas..

Los ataques al Hardware (BadUSB) realizados a través de memorias USB, son muy específicos, dirigidos. 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 es SafeDoor*?

SafeDoor es un dispositivo Hw con Sw embebido que actúa como barrera entre las memorias USB y los equipos de una organización analizando,bloqueando, informando, auditando y gestionando las 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.
  En este tipo de ataques, el escaneo que SafeDoor realiza del dispositivo se basa en el comportamiento del propio dispositivo, no en patrones de ataque, lo que consigue que, aunque las amenazas evolucionen, SafeDoor siempre las detectará. Esta detección se efectúa de forma continua y en tiempo real .
- Software: Con los hasta dos antivirus integrados, safeDoor realiza un análisis previo a la descarga de cualquier contenido.

SafeDoor permite así la protocolización en la utilización de dispositivos USB dentro de las organizaciones

SafeDoor está certificado bajo la metodología Lince y dentro del catálogo CPSTIC del CCN-CERT.
*protegido bajo patente

¿Cómo encaja SafeDoor en nuestro esquema de trabajo y de ciberseguridad?

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 contínua de las memorias USB externas o internas y cuya información queremos volcar a un nuevo Pendrive de forma segura. (Equipo frontera)

Puerto 2- Prendrive 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 efectua 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.Este 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 zación 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 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**. 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.**

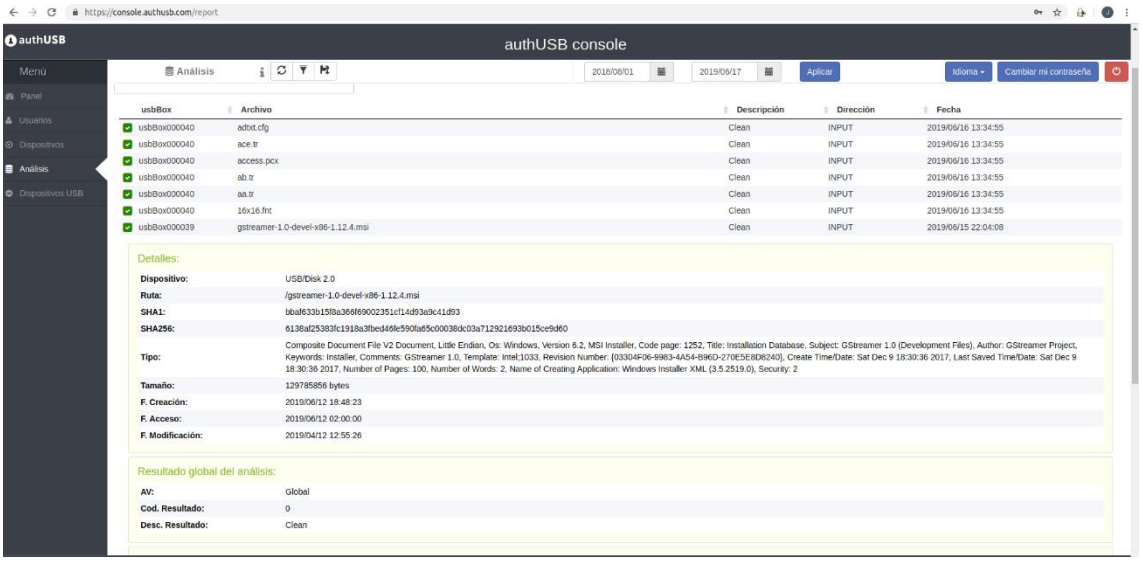
   El tiempo de escaneo es similar al de un equipo de escritorio, ya que el cuello de botella está en la velocidad de lectura de la memoria USB. Con una memoria moderna se pueden alcanzar velocidades de lectura de unos 35 MB/s, mientras que con memorias publicitarias o degradadas por el uso la velocidad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

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

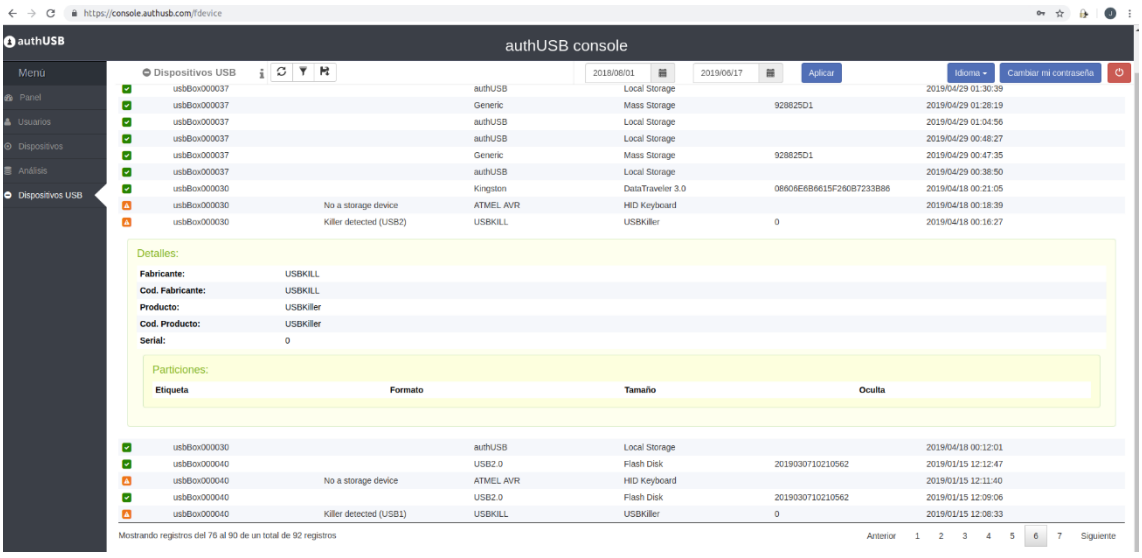
   Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. En caso de pérdida de conectividad o equipos aislados estos informes se almacenarán en el dispositivo, siendo posible su descarga (firmado digitalmente) para su posterior carga en la consola central de forma manual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

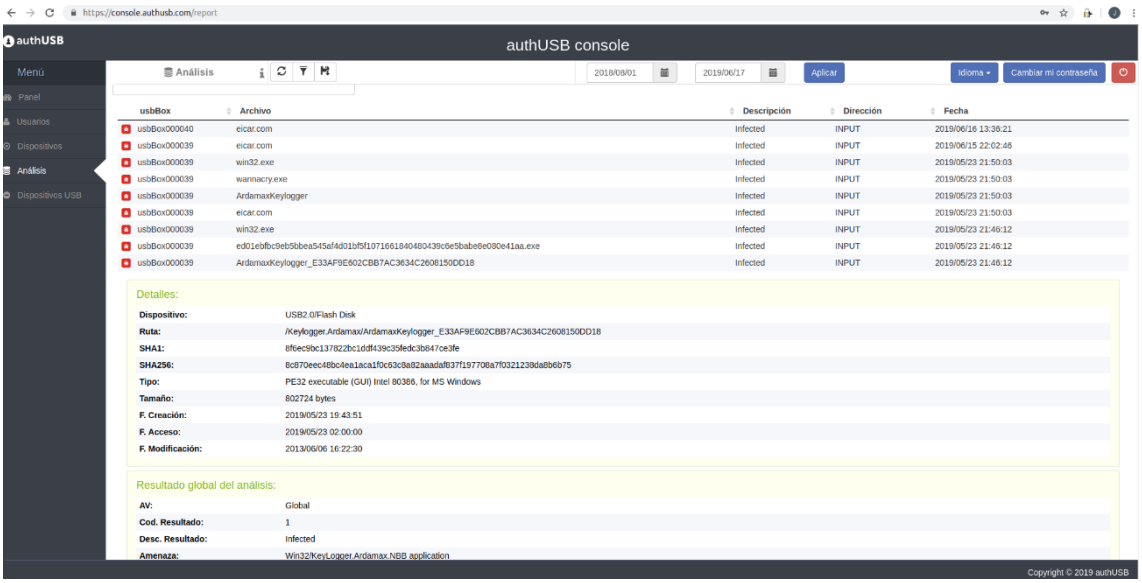
7. Pantallazos consola central



captura de fichero limpio



amenaza SW



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.