CASO DE USO

authUSB SafeDoor para Sector Bancario y afines.

¿Cuál es la problemática específica del Sector Bancario respecto al tráfico de Memorias USB?

La banca , el sector financiero y asegurador son cada vez más sectores objetivo de ciberataques dirigidos
En estos sectores es crítico el cumplimiento de regulaciones específicas, como PCI-DSS, así como otro tipo más transversal y que afectan a cualquier sector como la GDPR.
Es muy importante tener controlados y auditados, dada la confidencialidad de los datos que se manejan, los casos de extracción de datos por parte de actores internos.
En algunos casos estas extracciones se deben a negligencias o descuidos internos y en otros a un intento de uso en un nuevo trabajo o para su venta.
La necesidad de mover información crítica ,tanto de forma interna como hacia el exterior, hace que la necesidad de mantenerla protegida y bajo control sea prioritaria.

En este sector existen tipos de información altamente confidencial o sensible, que es crítico mantener bajo control. Algunos ejemplos de ellos son:

- **Datos de clientes:** Los clientes de servicios financiero dan por supuesto que su información confidencial está segura en manos de las firmas financieras. Cualquier filtración de esta información puede dañar de forma grave el cliente.
- **Información regulada:** Datos que deben ser auditados de forma obligatoria por PCI-DSS.
- **Informes internos, análisis financieros confidenciales** de carácter estratégico para la organización.
- **Documentación de Dirección, Consejo Ejecutivo** que está restringida a un colectivo específico dentro de la organización.
- **Información relacionada con blanqueo de capitales** de alta criticidad y cuyo acceso debe ser controlado de manera exhaustiva.
- **Información de datos confidenciales**

Tanto en los SSCC como en las oficinas bancarias, existe un tráfico de dispositivos USB, tanto internos como externos, que no está protocolizado ni regulado. En muchas ocasiones en estas organizaciones se toma la decisión de deshabilitar la Bios de los puertos USB, creyendo erróneamente que, al haber sido deshabilitados los clips de datos de los puertos, las amenazas por esta vía desaparecen. Nada más lejos de la realidad.

Las amenazas a nivel HW y Eléctrico siguen vigentes.

¿Qué aporta SafeDoor?

SafeDoor es una solución de análisis, protección y detección de ataques por medio de dispositivos de almacenamiento USB, actuando como barrera entre éstas y los equipos de una organización actuando 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,bombas de tiempo etc.

▪ Software: Dispone de motor/es antivirus completo/s integrado/s (compatible con varios fabricantes) con el 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 ofrece dos conectores hembra tipo A para la introducción de memorias USB a analizar y un puerto ethernet para su conexión a la red o punto a punto directamente a un ordenador. A través de esta conexión de red ofrece una interfaz web para la interacción con el usuario.

¿Cómo encaja SafeDoor en nuestro esquema de trabajo?

IMPLEMENTACIÓN EN PUESTOS DE DIRECCIÓN:

SafeDoor conectado directamente a equipos informáticos de 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 del administrador del sistema. En este caso se audita, a través de la Consola Central esta extracción, consignando quién, como, cuando y donde se produce.

DEPARTAMENTOS CENTRALES 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 que puedan entregar los clientes.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.

RESPUESTAS A CUESTIONES ESPECÍFICAS PLANTEADAS

1. **Número máximo* de antivirus a instalar en dispositivo**

SafeDoor embebe simultáneamente 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 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...)

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?

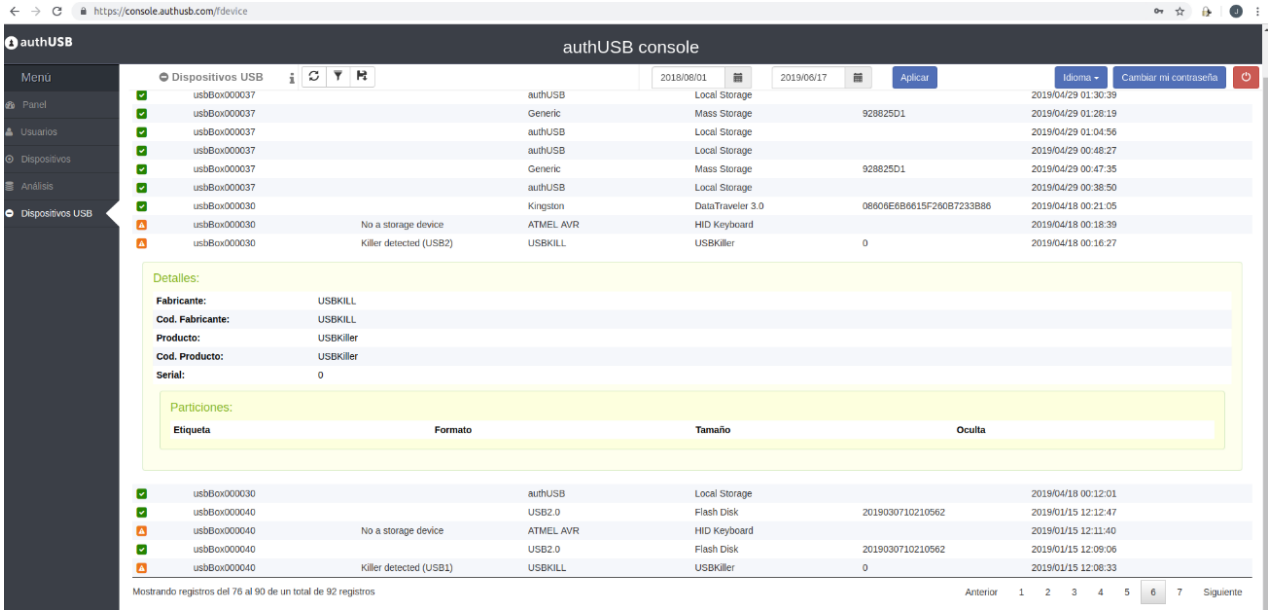
Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. Recibe los informes de auditoría (registro detallado de los dispositivos y archivos analizados) firmados digitalmente desde los dispositivos SafeDoor.

- 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

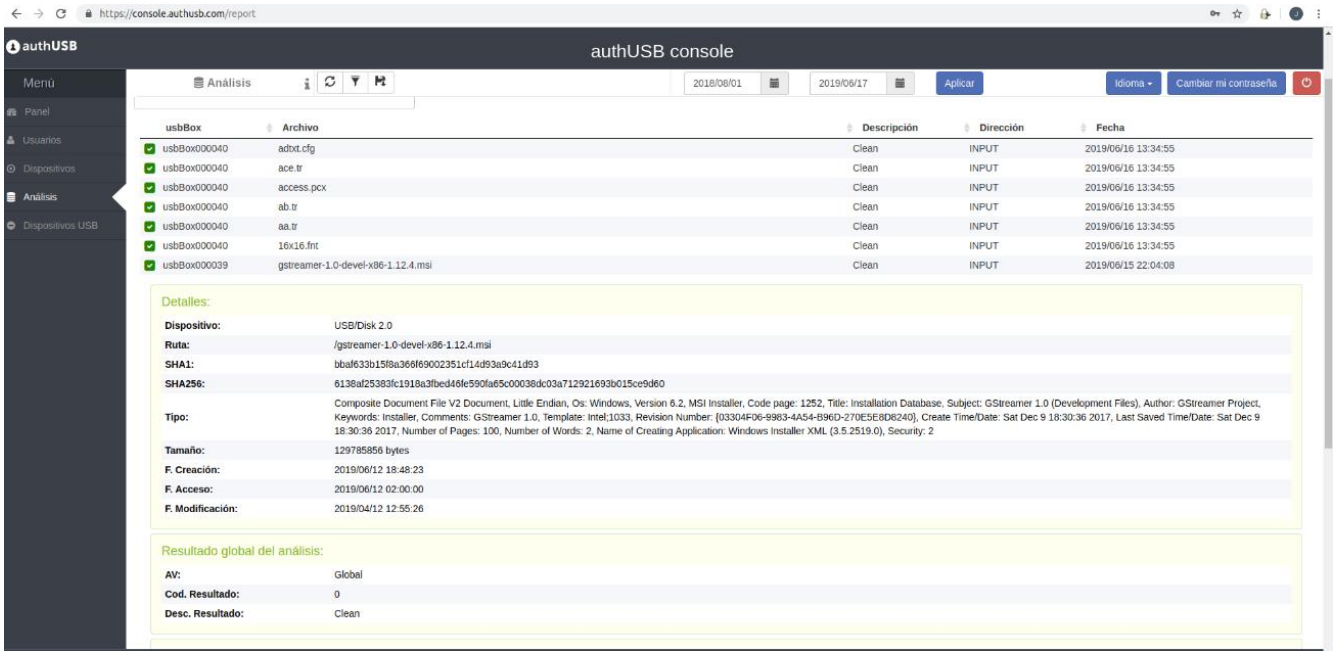
5.-Número máximo de dispositivos a gestionar desde una consola central

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.

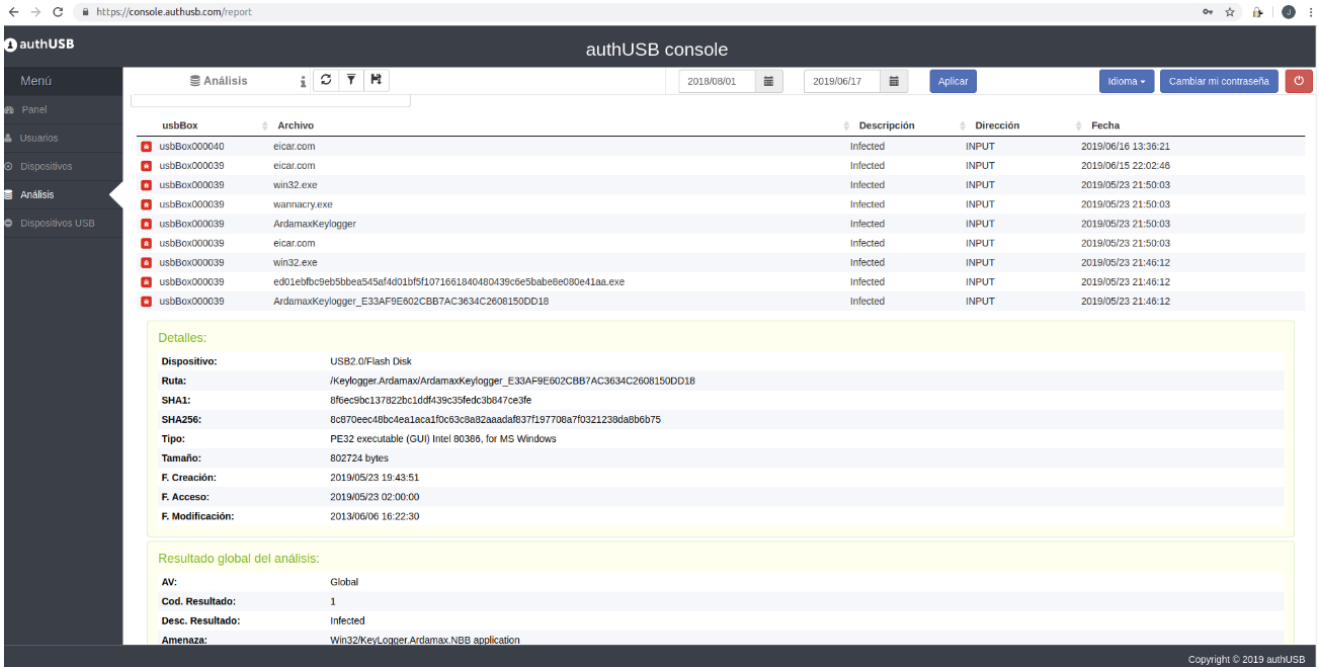
6.-Pantallazos consola central



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 a los tres niveles. Electrico, Hw y SW (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.