CASO DE USO

authUSB SafeDoor para Sector Bancario

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

La banca y el sector financiero son sectores objetivo de ciberataques dirigidos y la motivación de estos ataques es siempre económica.
En el sector financiero 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 en cuenta, dada la confidencialidad de los datos que se manejan, los casos de extracción de datos por parte de actores internos . En algunos casos esto se debe a negligencias o descuidos internos y en otros a un intento de uso en nuevo trabajo o para su venta.
Los analistas financieros necesitan mover información crítica tanto de forma interna como hacia el exterior, sin olvidar la necesidad de mantenerla protegida y bajo control.

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.

Tanto en los servicios centrales 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 es SafeDoor?

SafeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando 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.

¿Cómo encaja SafeDoor en nuestro esquema de trabajo?

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.

DEPARTAMENTOS CENTRALES ADMINISTRATIVOS Y OFICINAS:

Conectado en red el 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 del Safe door los análisis de los USB gestionados por el personal, tanto internos como externos, convirtiéndose en el único punto de entrada de las memorias USB .

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.

RESPUESTAS A CUESTIONES ESPECÍFICAS 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.

   Safe Door soporta dos motores antivirus simultáneos.

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...)

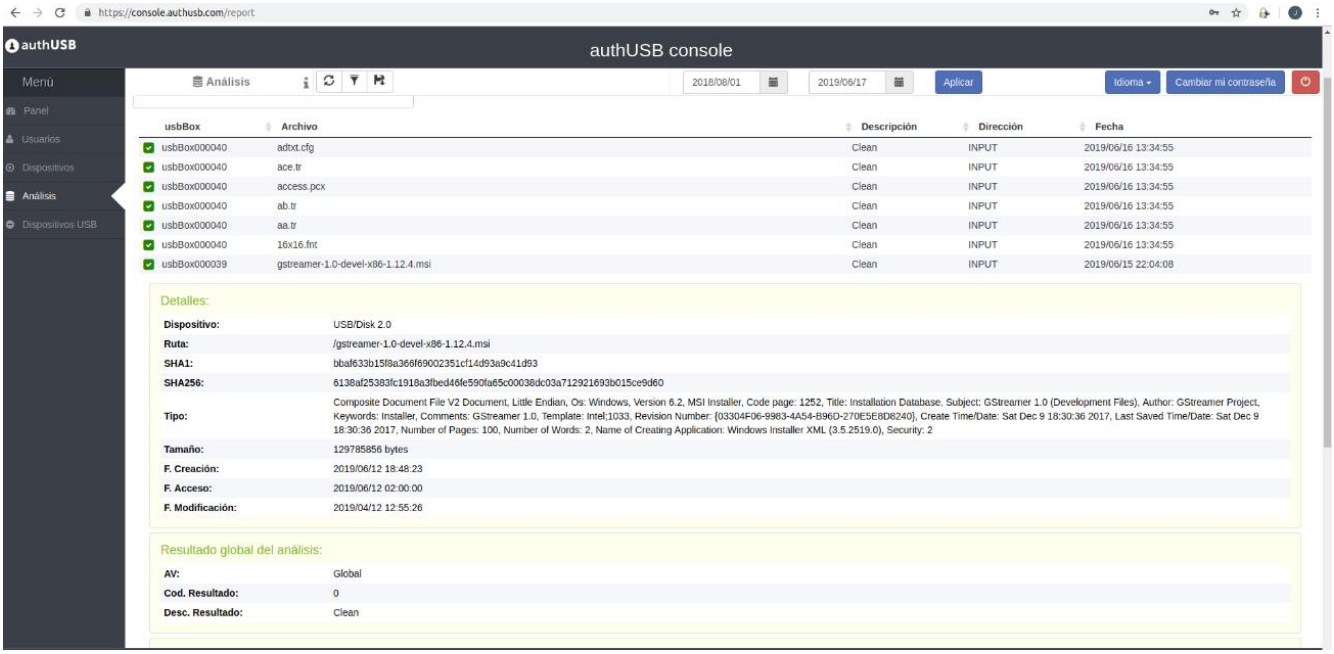
4. **Tiempo medio de escaneo por USB.**

   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.

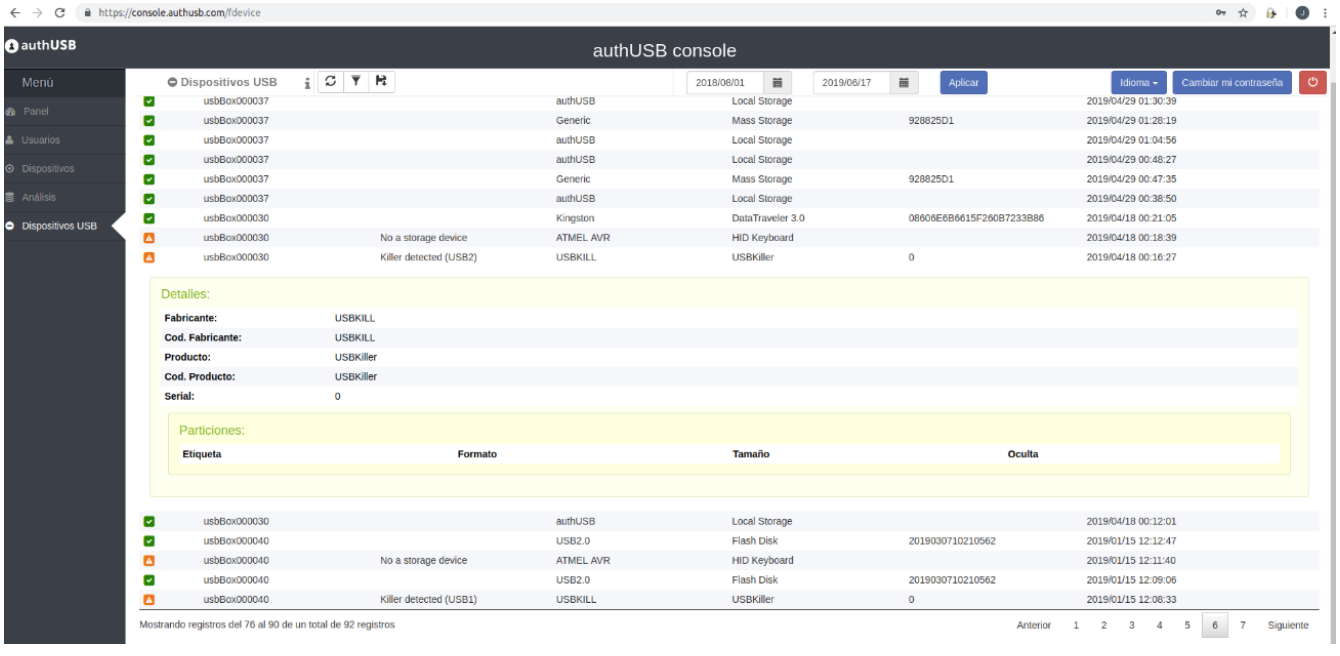
5. **Almacenamiento de logs: dispositivo,consola?**

   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.

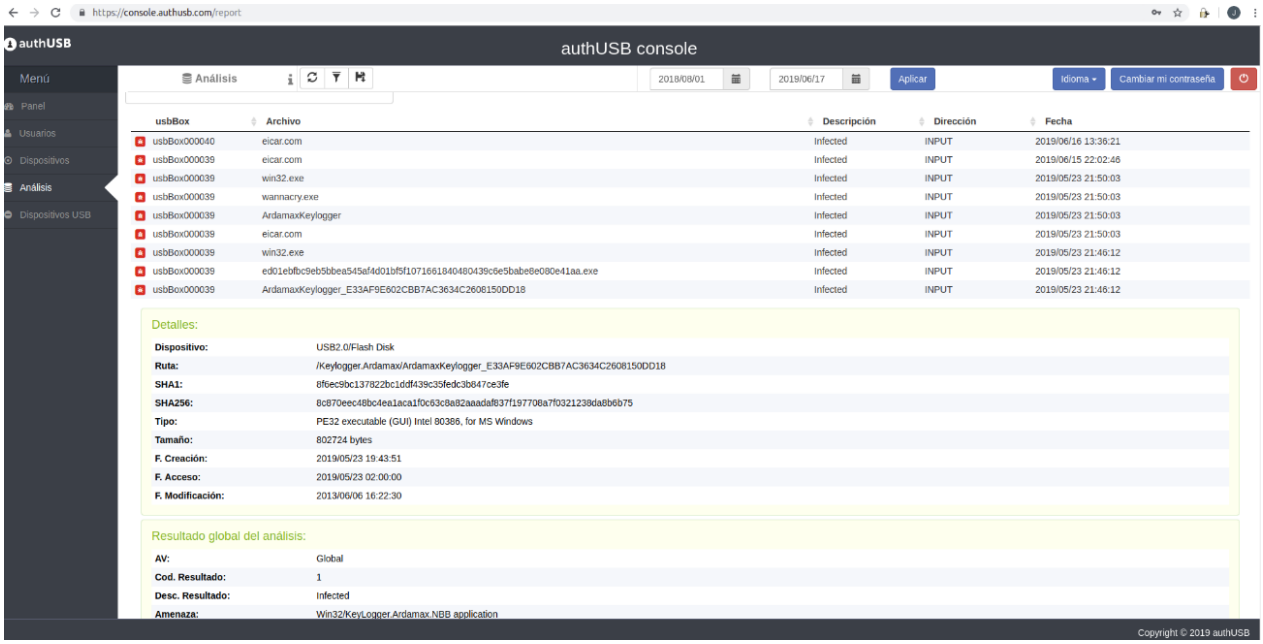
6. **Número máximo de dispositivos a gestionar desde una consola central**
   Es escalable en función del hardware o configuración de la máquina virtual sobre el que corra. Con 2 núcleos /16GB RAM se soportan 50 dispositivos vinculados.
7. **Pantallazos consola central**



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 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.