CASO DE USO

authUSB SafeDoor

Infraestructuras críticas

¿Cuál es la problemática específica de este tipo de estructuras respecto al tráfico de Memorias USB?

Según la propia definición que realiza el CNPIC las Infraestructuras Críticas son las infraestructuras estratégicas, que proporcionan servicios esenciales y cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Las redes aisladas suponen la utilización tanto para los procesos propios como de terceros (actualizaciones etc.) de Memorias USB.Dentro de estas IICC este uso está regulado y controlado utilizándose en la actualidad en los accesos a las mismas kioskos de sanitización (equipo frontera/aduana), Firewalls y otros elementos que se dedican a escanear las memorias USB en busca de amenazas Malware , a nivel software.

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 además la amenaza Eléctrica (USB Killer) con él se inutilizaría el equipo frontera de la instalación anulando la posibilidad de generación,a través de éste, del pendrive autorizado y permitir así la entrada de un dispositivo no autorizado que contendría una amenaza Hardware en su interior.

¿Qué es SafeDoor?

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

EQUIPOS EN ACCESOS:

1. EQUIPOS FRONTERA Y ADUANA

El dispositivo SafeDoor se puede dedicar como equipo frontera y aduana.

Dispositivo 1- Análisis y Monitorización continua de las memorias USB externas o internas y cuya información queremos volcar a un nuevo Pendrive de forma segura. (Equipo frontera)

Dispositivo 2- Prendrive donde vamos a volcar esta información. Se efectúa un borrado seguro previo a la introducción de la misma. Con esto conseguimos asegurarnos de que,tanto la información contenida en él, como el propio hardware no contienen amenazas de ningún tipo. (Equipo aduana)

Se puede, si ello fuese necesario, establecer un protocolo de utilización de whitelists/blacklists para las memorias utilizadas.Este protocolo podría eliminarse ya que con los pasos previos que hemos señalado tendríamos la certeza de que las memorias están libres de cualquier tipo de amenaza.

Se incluye la posibilidad de utilización de firma digital del fichero que se descarga para garantizar su integridad.

La trazabilidad del proceso es total.

2. INTÉRNAMENTE

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.

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 ESPECÍFICAS PLANTEADAS

1. **Número máximo de antivirus a instalar en dispositivo (Mcafee, Symantec,.)**

   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.

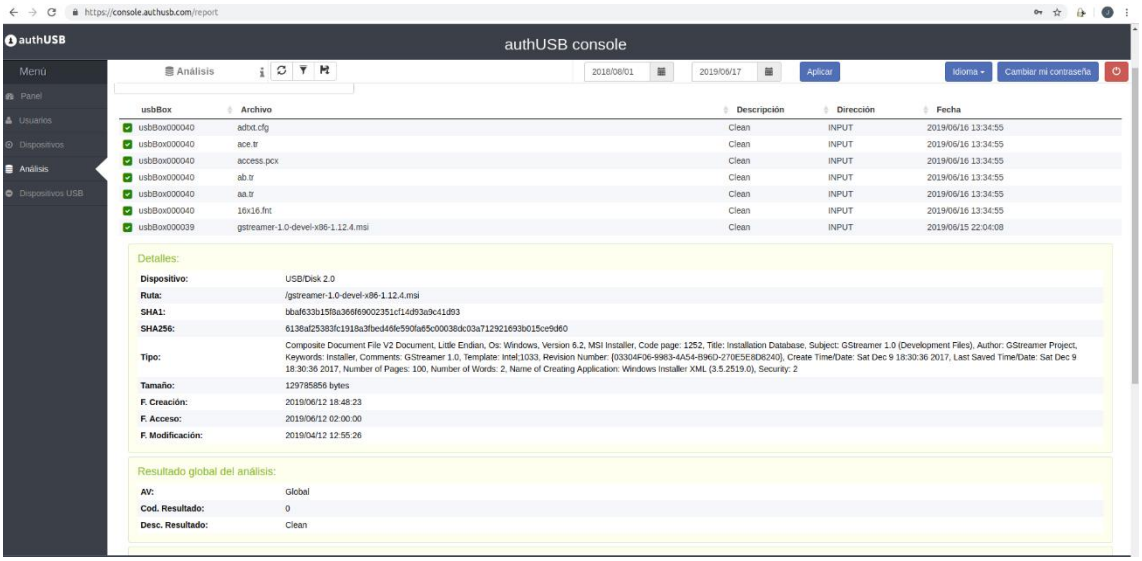
El tiempo de escaneo es similar al de un equipo de escritorio, ya que el cuello de botella está en la velocidad de lectura de la memoria USB. Con una memoria moderna se pueden alcanzar velocidades de lectura de unos 35 MB/s, mientras que con memorias publicitarias o degradadas por el uso la velocidad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

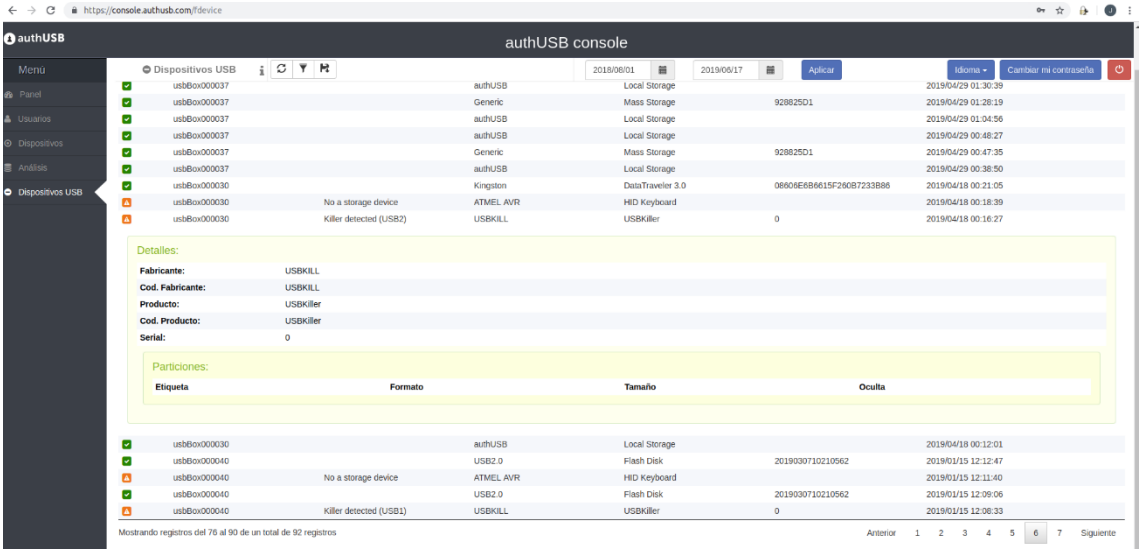
5. Almacenamiento de logs: dispositivo, consola?

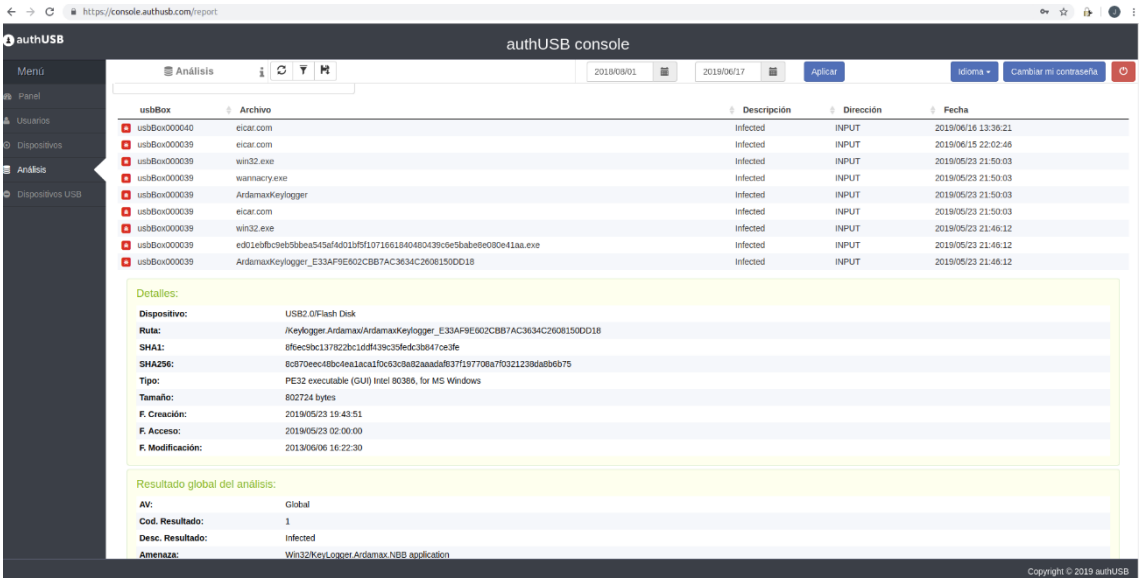
Cada acción llevada a cabo en cada safeDoor se vuelca en tiempo real en la consola central. En caso de pérdida de conectividad o equipos aislados estos informes se almacenarán en el dispositivo, siendo posible su descarga (firmado digitalmente) para su posterior carga en la consola central de forma manual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







captura de fichero limpio, amenaza SW y 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.