
# MEDIOS EXTRAÍBLES EN ENTORNOS INDUSTRIALES

authUSB
MOVE FIRST & CROWN THE GAME

&

HackRTU
INDUSTRIAL SECURITY

2025

# 1

# INTRODUCCIÓN

# 1. / INTRODUCCIÓN /

El presente documento nace de la colaboración entre el fabricante de soluciones especializadas en ciberseguridad authUSB y el proveedor de servicios especializados en ciberseguridad industrial HackRTU.

## 1.1 OBJETIVOS Y ALCANCE

Este whitepaper tiene el objetivo de presentar a la comunidad una solución especializada, como es el SafeDoor de authUSB, para el uso seguro de medios extraíbles, focalizando sus funcionalidades en entornos industriales. La detección de incidentes que utilizan como vector de ataques los medios extraíbles y el potencial impacto de estos en un entorno industrial, crean una necesidad fácil de solventar con tecnologías específicas como la que propone authUSB.

A lo largo del whitepaper, se presentará la solución SafeDoor, se repasarán las capacidades de esta solución para la defensa activa ante diferentes vectores de ataques (hardware, software, eléctrico), se valorarán las bondades del dispositivo frente a las recomendaciones detalladas en las guías de referencia como la NIST SP 1335 (2025) o la familia de estándares IEC 62443 y, por último, se incluirán diferentes escenarios simulados de ataques mediante memorias USB. En cada caso expuesto, se detallará la forma óptima para detectar, bloquear y auditar los ataques gracias a SafeDoor.

## 1.2 PROPÓSITO DEL DOCUMENTO

authUSB es una compañía española especializada en el desarrollo de soluciones certificadas que permiten el uso seguro de dispositivos USB en cualquier entorno mediante su dispositivo SafeDoor y también el borrado seguro de información mediante la herramienta Olvido. En este documento, el foco, como bien se ha mencionado anteriormente, estará en el uso seguro de los dispositivos USB en los entornos industriales concretamente, servicio en el que authUSB es especialista, permitiendo a las organizaciones en las que se imple-

mente su solución, controlar todo lo relacionado con la seguridad de los dispositivos USB y la transmisión de información.

Por otro lado, HackRTU, es un proveedor de servicios especializados en ciberseguridad industrial. Con sede en León (España), sus servicios profesionales van desde la asesoría a empresas en materia de ciberseguridad industrial, hasta el análisis de plantas o de dispositivos industriales. Con foco en la seguridad ofensiva, su equipo posee un alto conocimiento a nivel técnico sin dejar de lado todo el trabajo más consultivo. Todos los trabajos ejecutados son respaldados tanto a nivel normativo como técnico ofreciendo a los clientes una visión concreta de la ciberseguridad industrial con resultados profesionales y realistas.

## 1.3 DEFINICIONES CLAVE

**Autorun (malicioso):** Funcionalidad de un malware que utiliza el archivo autorun.inf para ejecutarse automáticamente al conectar memorias USB. Aunque está limitado en sistemas modernos, aún funciona en entornos antiguos o mal configurados como los entornos industriales.

**BadUSB:** Ataque que aprovecha la manipulación del firmware de un dispositivo USB (pendrive, teclado, adaptador de red, etc.), permitiendo a potenciales atacantes asumir funciones maliciosas no visibles para sus víctimas.

**Baiting:** Estrategia de manipulación (ingeniería social) en la que se dejan memorias USB infectadas en lugares estratégicos esperando que alguien las conecte por curiosidad.

**Juice Jacking:** Técnica basada en la manipulación de puertos de carga o adaptadores USB públicos para extraer información o instalar malware en los dispositivos conectados.

**Keylogger:** Funcionalidad concreta dentro de un malware o, directamente un dispositivo, que permite registrar pulsaciones de teclado.

# 1. / INTRODUCCIÓN /

Los keyloggers pueden ser tanto físicos si se utilizan entre la conexión que posee un teclado y un host, como software por la implementación de funcionalidades en una pieza malware.

**Sandboxing:** Técnica de análisis que ejecuta archivos sospechosos en un entorno aislado y controlado para observar su comportamiento antes de permitir su ejecución en el sistema final.

**USB Killer:** Dispositivo USB diseñado para emitir descargas eléctricas de alto voltaje hacia el equipo al que se conecta, destruyendo puertos y placas base. Es un ataque físico más que lógico.

# 2

# HISTORIA DE LOS USB Y SU PROTAGONISMO A NIVEL OT

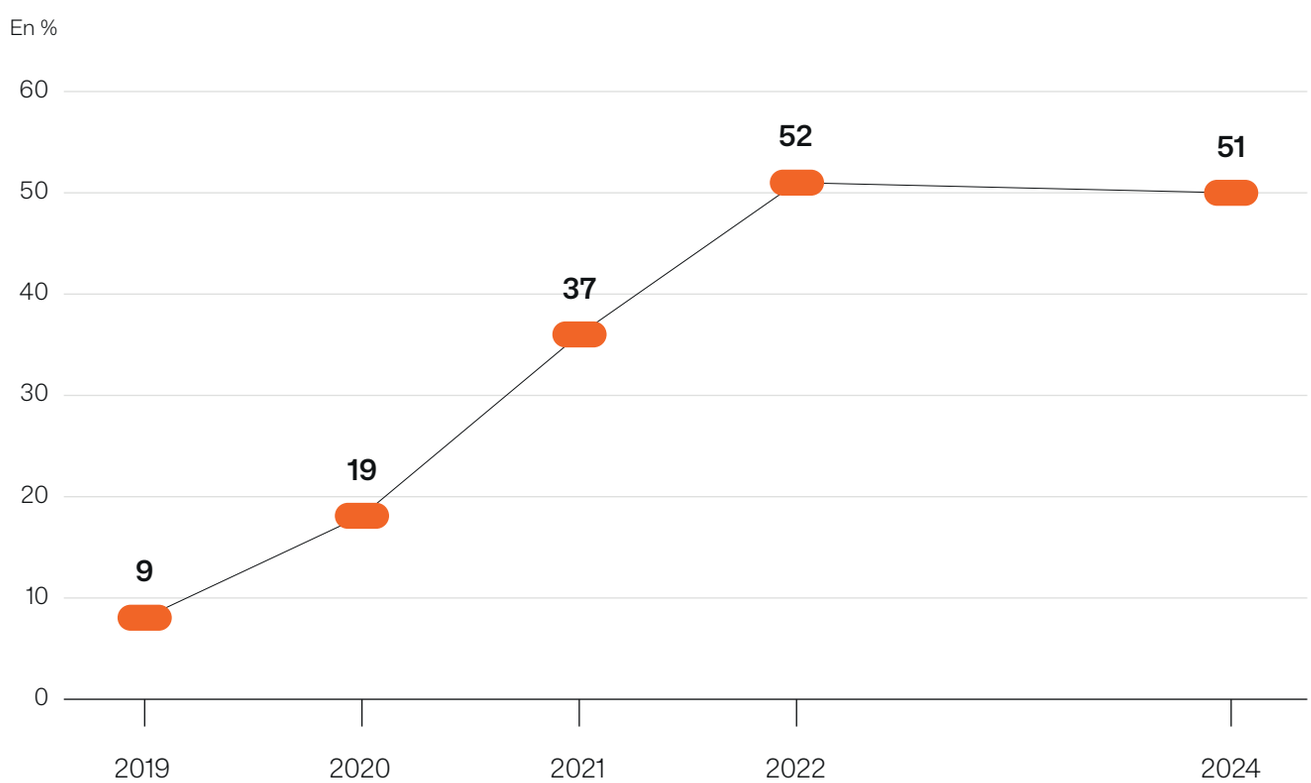
## 2. / HISTORIA DE LOS USB Y SU PROTAGONISMO A NIVEL OT /

En la actualidad, los medios extraíbles siguen siendo un vector crítico de ataque para los entornos industriales.

Desde hace años, los entornos *Operation Technologies* (OT) ya no se encuentran tan aislados como en el pasado, la interoperabilidad entre sistemas y la Industria 4.0 ha generado un mayor número de interconexiones entre la parte OT y la parte IT *(Information Technology)*, lo que ha supuesto también un aumento de los ataques mediante dispositivos USB, siendo uno de los primeros, el famoso Stuxnet en el año 2010. Un gusano introducido por USB que saboteo las centrifugadoras de una planta nuclear.

Desde entonces, se ha podido ver una tendencia al alza en el diseño de malware para propagarse vía USB en los Sistemas de Control Industrial *(ICS - Industrial Control Systems en inglés)*. Destacable es que aproxi-

Aumento del porcentaje de malware industrial que usa USB como vector



madamente solo el 9% del malware estaba diseñado para propagarse a través de memorias USB en el año 2019, pero en el año 2022, ya se registró que el 52% de las amenazas analizadas estaban diseñadas para utilizar los USB como vector de ataque. Esta tendencia se ha estabilizado en los últimos años ya que en el año 2024 aproximadamente el 51% de los ataques implicaban el uso de un medio extraíble como vector inicial para tratar de acceder a redes industriales.

Esto supone que los USB se utilizan como medio de ataque 6 veces más que en el año 2019, lo que se puede catalogar como un crecimiento explosivo. Este crecimiento puede relacionarse, entre otros argumentos, por la mejora tecnológica que se está desplegando en las empresas. Las mejoras en el despliegue de cortafuegos, switches con mayor capacidad de ciberseguridad, uso de comunicaciones VPN, monitorizaciones de red, etc. hacen que los vectores de ataque más asequibles por los criminales empiecen por el uso de memorias USB.

En cuanto a los tipos específicos de ataques de malware utilizando USB, los análisis realizados han demostrado que su foco principal es el de lograr la persistencia o realizar movimientos laterales en las redes industriales. En su mayoría, el malware tenía el objetivo de mantener siempre una puerta trasera abierta para los atacantes, lo que confirma que los USB se han utilizado y se utilizan como vector inicial para lograr establecer una conectividad remota persistente que permita a los atacantes exfiltrar datos, para posteriormente, como objetivo principal, causar la pérdida de control o visibilidad de los procesos industriales.

# 3

# SAFEDOOR DE AUTHUSB

# 3. / SAFEDOOR DE AUTHUSB /

SafeDoor es un dispositivo hardware que actúa como barrera entre los medios de almacenamiento USB y los ordenadores de la organización. El dispositivo se diseñó originalmente para Defensa y como medio de interconexión de redes clasificadas utilizando dispositivos USB. Después de consolidarse en Defensa, se expandió al sector industrial dado que las necesidades eran similares respecto a la interconexión de redes IT/OT, incluyendo mejoras para automatizar y simplificar procesos, evitando la necesidad de cualificar operarios para tareas específicas y asegurar la trazabilidad de los datos.

Las principales características son:

- Analiza tanto el contenido como el continente del USB conectado.
- Bloquea las amenazas basándose en el comportamiento del USB.
- Permite la gestión del dato delegando los permisos a usuarios locales o mediante la integración con LDAP.

## Características

### Analiza

*Realiza el análisis de los dispositivos de almacenamiento USB a los tres niveles: Eléctrico, Hardware y Software.*

### Bloquea

*Bloquea el acceso a los dispositivos en caso de ataque HW y Eléctrico o a los archivos infectados (malware). No permite la extracción de información.*

### Gestiona

*Control de Gestión Total: en usuarios específicos o perfiles, delega la gestión del usuario/perfil en el Directorio Activo de la Organización (LDAP).*

### Informa

*Genera informes de auditoría de uso de cada dispositivo e información sobre los archivos analizados.*

### Audita

*Auditoría del dispositivo USB y análisis de su contenido. Todo a través de la Consola Central.*

### Actualiza

*Actualizaciones de firmware y Firma AV totalmente automáticas, locales (para dispositivos sin acceso a Internet), offline desde un dispositivo de almacenamiento USB.*

- Genera informes detallados del uso de USB dentro de la organización permitiéndonos auditar cada una de las conexiones de estos dispositivos y cada una de las transferencias.
- Está certificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC), cualificado y aprobado para su uso en sistemas bajo el alcance del ENS.
- Facilita el cumplimiento de las medidas de seguridad para superar la Certificación de Conformidad con el ENS y la acreditación de sistemas clasificados.

# 4

# MARCOS DE PROTECCIÓN

# 4. / MARCOS DE PROTECCIÓN /

En el mundo industrial y, concretamente dentro del mundo de la ciberseguridad industrial, existen diferentes guías de buenas prácticas y estándares que permiten a las organizaciones revisar y mejorar el nivel de seguridad de sus infraestructuras.

En este whitepaper se quiere destacar una de las últimas publicaciones del NIST, la publicación *NIST SP 1334 (2025) "Reducing The Cybersecurity Risks Of Portable Storage Media In Ot Environments"*, la cual hace referencia a una serie de recomendaciones para el control de los medios extraíbles en entornos OT. Así mismo, también mencionaremos la familia de estándares de la IEC 62443 y algunos de sus controles específicos para el uso de medios extraíbles en entornos industriales.

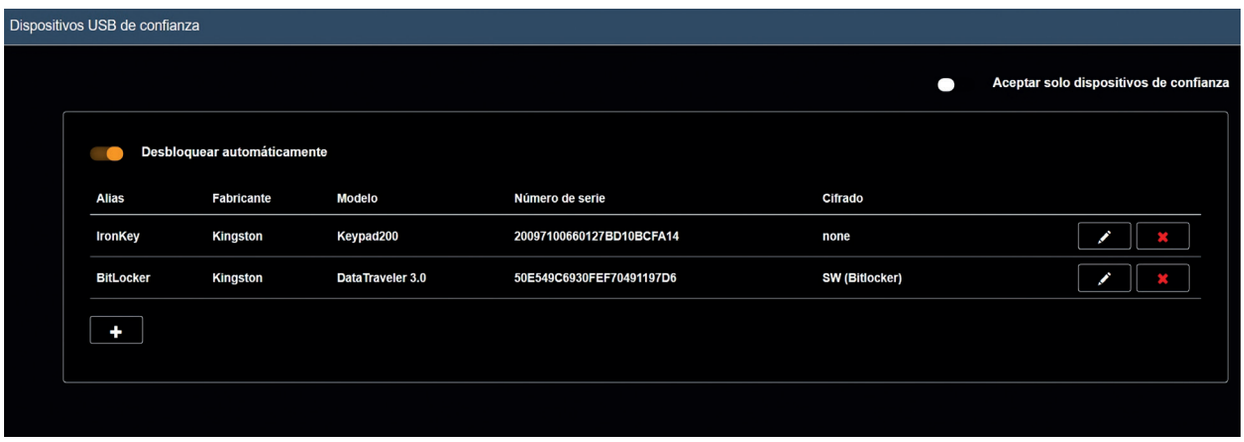
A continuación, se analiza cada tipo de control en entornos industriales (manufactura, energía, petróleo/gas, defensa, etc.), incluyendo cómo un dispositivo como el **SafeDoor** de **AuthUSB** ayuda a cumplir con los diferentes requisitos y recomendaciones.

## 4.1 POLÍTICAS Y CONTROLES PROCEDIMENTALES

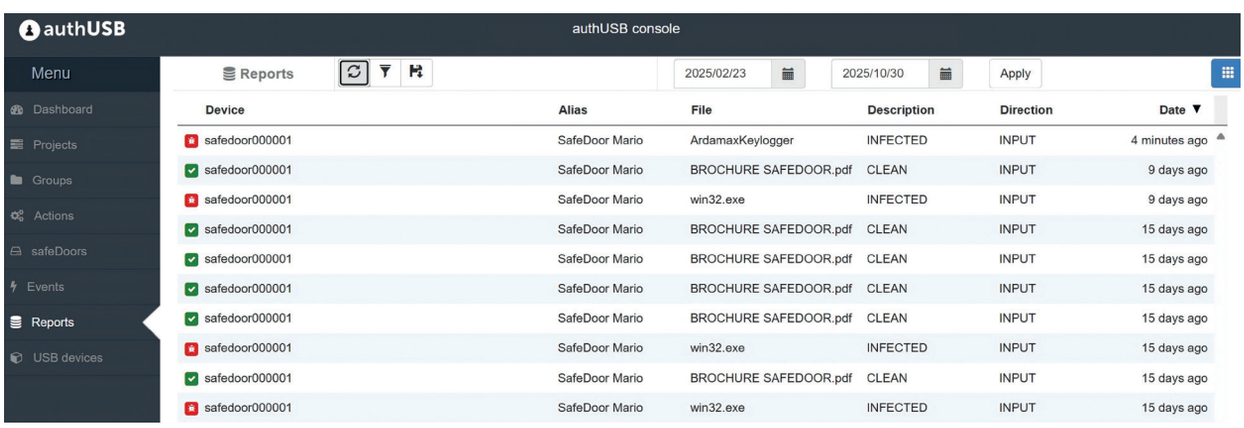
La publicación especial del NIST, el NIST SP 1334, hace referencia a la necesidad de establecer políticas estrictas que limiten y gestionen el uso de los medios extraíbles en entornos industriales. En el documento, hace hincapié en los siguientes aspectos:

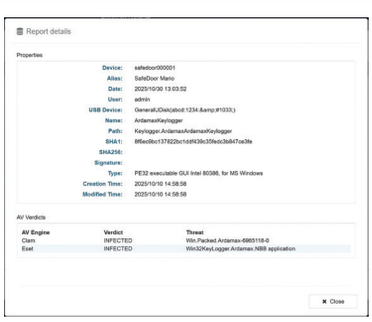
**Uso autorizado y gestión de los dispositivos:** Limitar el uso de los dispositivos USB únicamente a aquellos gestionados o proporcionados por la organización considerando como no seguros/confiables el resto de los dispositivos fuera de dicha lista blanca.

Un ejemplo claro en los entornos industriales es garantizar que la actualización de firmware por parte de un proveedor sobre un dispositivo industrial como un PLC, se realice utilizando únicamente dispositivos USB corporativos y controlados por la empresa.




**Registro y trazabilidad:** El análisis de los dispositivos analizados, junto con los posibles eventos asociados a los USB, ha de registrarse capturando tanto la identidad del usuario, el número de serie del dispositivo, fecha y hora, archivos transferidos, etc.



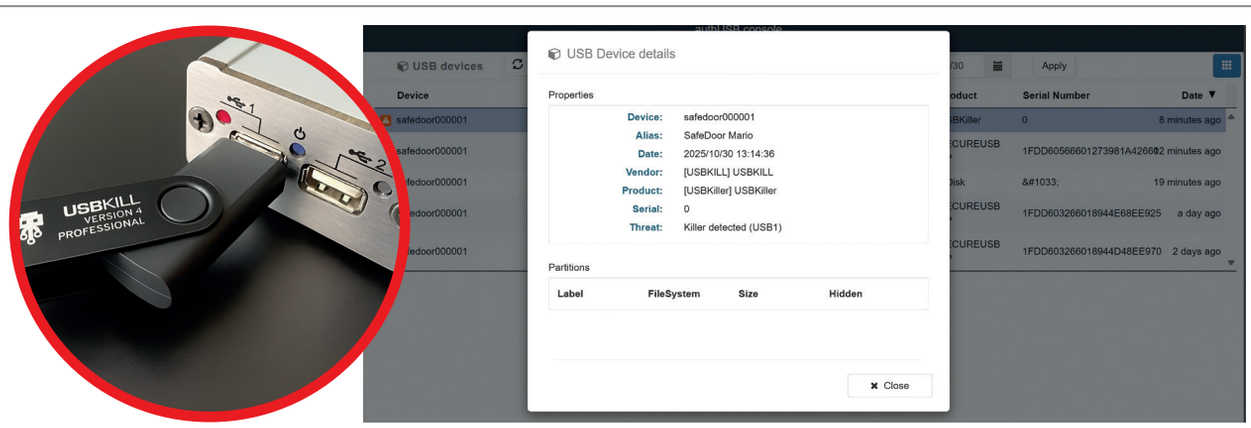

**Esta trazabilidad es crucial en entornos industriales y SafeDoor permite realizarla ya que comprueba, analiza y recopila toda la información de los USB que se utilizan a través de su dispositivo.**

Toda esta información deberá ir contenida en diferentes políticas, procedimientos e incluso listas de instrucciones que garanticen a todos los empleados de la organización y a proveedores como utilizar y gestionar el uso de los medios extraíbles en los entornos industriales. El SafeDoor de authUSB mediante su **consola de gestión centralizada** permite cumplir con diferentes recomendaciones o controles de tanto el NIST SP 1334 como de la familia de estándares IEC 62443.

## 4.2 CONTROLES A NIVEL FÍSICO

La protección física de los USB posiblemente es de los controles menos implementados ya que cuando uno habla de ciberseguridad, siempre hace referencia al plano lógico. En este caso, la implementación de estas medidas tiene un impacto del medio físico al lógico. Por esta razón, documentos como el generado por la NIST hacen referencia a protecciones específicas como:

- Uso de llaves (hardware port locks) para introducir en ranuras USB dispositivos externos.
- Bloqueadores de puertos (port blockers/locks).
- Protecciones frente a subidas de tensión (USBKiller).
- Etc.



En resumen, toda protección que evite ataques derivados de la conexión físicos en los puertos USB y su manipulación.

## 4.3 CONTROLES TÉCNICOS

Posiblemente estos controles sean de los más aplicados por las organizaciones a nivel de ciberseguridad para controlar el uso de medios extraíbles en las organizaciones.

Los cambios socioculturales, impulsados por nuevas formas de trabajo en remoto, hacen que aplicar unas políticas para restringir el uso de memorias USB sea prácticamente obligatorio. Pero ¿en los entornos industriales se puede restringir así de fácil? No existe una respuesta inmediata ya que cada sector industrial y cada organización tiene su manera de funcionar. Por ejemplo, empresas donde se utilizan máquinas con gran inteligencia para la fabricación de piezas, suele ser normal el uso de medios extraíbles que contienen ficheros específicos para modificar en este tipo de máquinas que tienen un ordenador incorporado. Algunas de estas máquinas están aisladas de las redes y su único vector de ataque serían los USB.

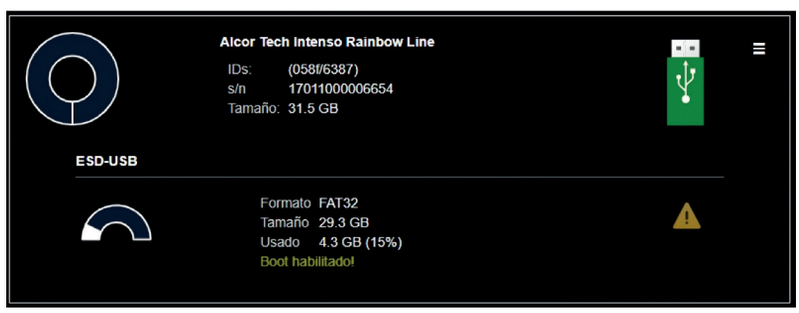
Por otro lado, empresas del sector manufactura o alimentación donde se utilizan sistemas ERP (Enterprise Resource Planning) para la gestión de producto, pueden utilizar escritorios remotos en las máquinas físicas para la protección de las acciones que ejecutan los operadores. Estos equipos suelen estar desplegados en planta cerca del proceso industrial con el que tienen relación y, en muchos casos, tienen acceso directo a dispositivos de campo por la configuración de red. Dada esta situación, puede darse el caso en el que no tengan una protección aplicada para los puertos USB y una infección, dependiendo de la red que posea la organización, podría ser devastadora.

En ambos ejemplos, el uso de SafeDoor proporcionaría una protección extra focalizada en las memorias USB y permitiría centralizar el uso de estos dispositivos con un control mucho más profundo a nivel técnico.

Algunos de los controles que pueden implementarse por SafeDoor como protección principal por la imposibilidad de aplicar políticas para restringir los USB o limitaciones tecnológicas de sistemas legacy son:

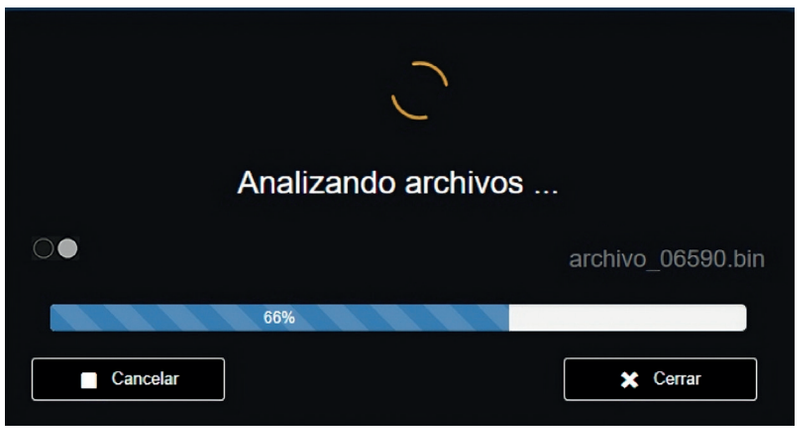
### DETECCIÓN DE AUTORUN

La solución SafeDoor permite la detección de AutoRun en las memorias USB. Este es uno de los primeros síntomas de que, si la memoria USB se conecta a un ordenador y este no posee las medidas de ciberseguridad correctas, en caso de que la memoria contenga una pieza malware que se activa a través del *AutoRun*, el host será infectado..




### USO DEL PROPIO DISPOSITIVO COMO BARRERA FRENTE A VECTORES DE ATAQUE VÍA MEMORIAS USB

La revisión por firmas que posee SafeDoor, sumado a otras características de protección y a que este dispositivo no tiene conexión directa con el host, sino que funcionaría como un quiosco de análisis inicial, a modo de sandbox. Permite un gran filtro inicial a nivel técnico sin la necesidad de aplicar políticas concretas en los ordenadores de campo o luchas complejas contra sistemas legacy que no permiten la incorporación de algunos controles. Además, como no es necesaria la aplicación de configuraciones en el sistema final donde se utilizará la memoria USB tras su revisión con SafeDoor, las luchas con integradores o fabricantes desaparecen y, aunque se siga con una "caja negra" funcionando en el proceso, al menos las memorias USB están controladas.




## BORRADO DE MEMORIAS EXTRAÍBLES

Ya sea por privacidad de los datos manejados en las memorias USB o para asegurar un borrado tras su uso, se considera una buena práctica realizar borrados en ciertos momentos. Por ejemplo, realizar borrados tras el uso de las memorias en sistemas *"aislados"* evitando así propagar un posible malware que contenga la memoria USB y no tengamos conocimiento de que está infectada.

## 4.4 CONTROLES PARA EL USO COMPARTIDO DE MEMORIAS USB

En el punto anterior ya se ejemplificaron algunas de las situaciones cotidianas dentro de las organizaciones, pero ¿qué pasa cuando la memoria USB sale hasta de la organización? Muchas empresas poseen políticas frente al uso de dispositivos externos a la organización (BYOD - Bring Your Own Device) o el uso de material de la organización fuera de sus instalaciones. Como en ocasiones estas políticas no se siguen al pie de la letra por situaciones concretas que se dan en el día a día de los trabajadores, el uso de SafeDoor proporciona cierta tranquilidad. Dada su facilidad de uso, los empleados no necesitan poseer grandes conocimientos a nivel de ciberseguridad y hasta ellos se sentirán más tranquilos si todo se revisa previamente a un uso en producción.

Algunos de los controles que pueden aplicarse derivados de las funcionalidades que posee SafeDoor para el uso compartido de memorias USB son::

- **Creación de hashes** sobre los ficheros analizados para trazabilidad de estos.
- **Borrado completo** para evitar propagaciones de malware.
- **Control de escritura y lectura** sobre las memorias USB.
- **Creación de lista blanca** para controlar las memorias USB confiables.
- **Reserva de puertos** que permite añadir una capa de privacidad a los datos de una memoria USB, en caso de dispositivos SafeDoor compartidos en la red con varios usuarios.

# 5

# ATAQUES ESPECÍFICOS MEDIANTE USB A ENTORNOS INDUSTRIALES

# 5. / ATAQUES ESPECÍFICOS MEDIANTE USB A ENTORNOS INDUSTRIALES/

A lo largo de los últimos años, se han detectado varios ataques de relevancia a diferentes sistemas y equipos industriales. Todo realmente comenzó en el año 2010 con Stuxnet, pero, anteriormente ya existieron ataques mediante USB.

Las infraestructuras han cambiado, han mejorado, la concienciación es un aspecto crítico para las empresas y más aún para las empresas dedicadas a algún sector industrial, pero los ataques con USB continúan existiendo y siendo eficaces.

Los ataques específicos mediante USB han mutado y han pasado a otro nivel, por ello, ahora se realiza una revisión de tres ataques en separados por varios años en los que claramente se puede apreciar como cada vez, los ataques al mundo industrial mediante USB han sido más sofisticados.

Cronología de ataques de relevancia detectados a diferentes sistemas y equipos industriales


**Agent.BTZ** Gusano introducido en redes del Departamento de Defensa de EE. UU. mediante un USB infectado; millones de equipos comprometidos. / **Botnet Mariposa** Botnet global que se propagó por USB y otros medios; infectó millones de equipos. / **Stuxnet** Gusano altamente sofisticado que se propagaba por USB para sabotear controladores PLC de Siemens en instalaciones iraníes. / **Raspberry Robin** Gusano que se propaga por USB mediante accesos directos (.LNK) y enlaza con redes de pre-ransomware. / **Raspberry Robin** Gusano que se instala desde un USB para abrir backdoors y descargar cargas secundarias. / **WispRider - Mustang Panda** Amenaza china que distribuyó backdoors USB; detectada en campañas de espionaje globales. / **SNOWYDRIVE** Malware que se instala desde USB para abrir backdoors y descargar cargas adicionales. / **SOGU** Campaña paralela a SNOWYDRIVE que usó USB como vector inicial en múltiples sectores. / **Infraestructura de distribución en Irán** Atribuido a Predatory Sparrow, que usó USB para paralizar gasolineras y sistemas de distribución.

## 5.1 BOTNET MARIPOSA (2008) – SECTOR ELÉCTRICO

En el año 2008, durante una formación a empleados de una compañía eléctrica, un formador distribuyó en una memoria USB infectada el contenido del curso a los alumnos, trabajadores de una compañía del sector eléctrico. Uno de los empleados conectó el USB a su equipo de trabajo e introdujo el malware a la red corporativa.

La botnet Mariposa propagó código malicioso a diferentes sistemas empresariales y aunque no se ha confirmado totalmente dada la delicadeza de la información, se cree que hubo una afectación sobre los equipos industriales de la compañía eléctrica.

Este fue uno de los primeros ataques registrados y aunque no fue confirmado al 100% fue incluso previo a Stuxnet de ahí que se haya querido resaltar y mostrar como algo tan simple como un formador descontento, fue capaz de infectar toda una compañía eléctrica con un USB.

Ataque específico mediante USB a entorno industrial

**BOTNET MARIPOSA 2008**

1. "Drop" del USB a usuarios en la empresa del sector eléctrico.
2. Conexión a un equipo de la red corporativa de la organización.
3. Propagación del malware y posible afectación a equipos industriales.

**USB DROP**

Sector eléctrico

**TA0108 - INITIAL ACCESS**
T0847 - Replication Through Removable

MITRE ATT&CK™

Acceso inicial a sistemas aislados mediante malware en medios extraíbles (p.ej., USB) introducidos sin saberlo por terceros de confianza –proveedores o contratistas–, comprometiendo equipos que no se conectan a redes externas, pero sí son físicamente accesibles.

# 5. / ATAQUES ESPECÍFICOS MEDIANTE USB A ENTORNOS INDUSTRIALES/

## CAPACIDADES Y PREVENCIÓN UTILIZANDO EL SAFEDOOR DE AUTHUSB Y CONTROLES TEÓRICOS A APLICAR

Este ataque, aunque básico, fue uno de los primeros y, por lo tanto, un claro ejemplo de cómo se podría haber evitado utilizando el dispositivo SafeDoor de authUSB.

El usuario que infectó a la red corporativa y que posteriormente afectaría supuestamente a la red industrial, debería haber seguido una serie de pautas teóricas marcadas en base a la familia de estándares IEC 62443 y a las buenas prácticas indicadas en las guías NIST SP 800-82 (Guide to Operational Technology (OT) Security), NIST SP 800-53 (Guide to Security and Privacy Controls for Information Systems and Organizations), NIST SP 800-83 (Guidelines for media Sanitation) y la última publicación especial específica de USB del NIST titulada NIST SP 1334.

**¿Qué controles y por qué se deberían haber estado implementado? Y lo más importante, ¿Habría la implantación de estos controles evitado el problema de seguridad?**

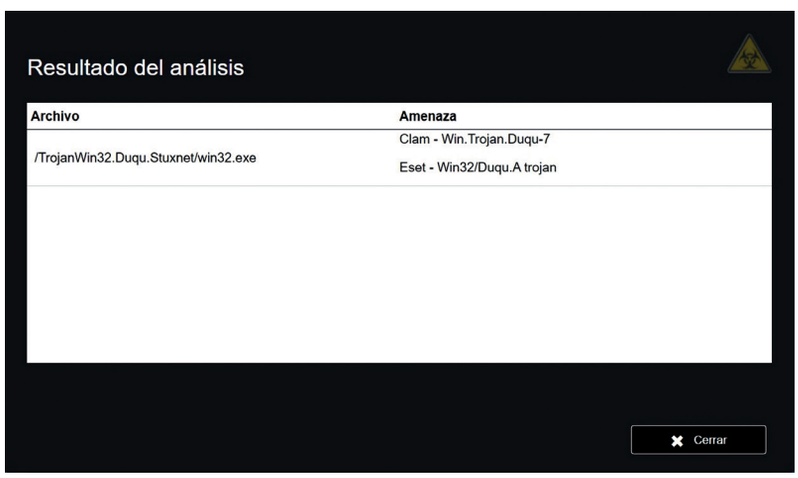
**SÍ, podría haberse evitado**

Veamos los controles relacionados con los estándares anteriormente mencionados y las guías de buenas prácticas y que controles se estarían validando con el uso del SafeDoor de AuthUSB.

### DETECCIÓN DEL VECTOR DEL USB

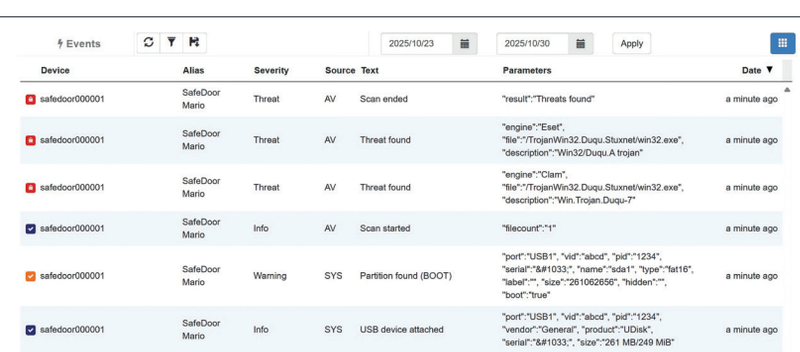
Aplicando las políticas y procedimientos base estipulados en los estándares y guías de referencia, el usuario debería haber escaneado la memoria USB externa antes de utilizarla en el portátil de la empresa

lo que habría permitido evitar la expansión de la botnet ya que el SafeDoor realizar un análisis a nivel de software (mediante el motor de antivirus interno certificado). Una vez detectado el malware el SafeDoor habría bloqueado el dispositivo impidiendo la copia de archivos infectados **(IEC 62443-3-3 SR 3.2 Malicious Code Protection)**.




## TRAZABILIDAD Y CONTROL DE USO

El SafeDoor tiene la capacidad de registrar cada evento de conexión del USB, el usuario y el equipo en el que se hace. Esta auditoría completa del dispositivo USB esta alineada con varios controles de la IEC 62243-3-3 y del NIST SP 800-153 en cuanto a tener capacidad de respuesta, trazabilidad y monitorización continua del uso de los USB. **(IEC 62443-3-3 SR 2.8 Auditable Events y IEC 62443-3-3 SR 6.2 Continuous Monitoring).**



### POLÍTICA DE EMPLEO BASADO EN PERFILES DE CONFIANZA

Aparte de servir de analizador para todas las memorias USB externas que lleguen a la organización, SafeDoor permite implementar una serie de políticas que garantizan que solo los USB corporativos estén autorizados para su uso, es decir, están registrados como memorias de confianza. Ya que en el caso de la Botnet Mariposa, el USB provenía de un externo, el SafeDoor lo habría marcado directamente como dispositivo no confiable bloqueando totalmente su uso. **(IEC 62443-3-3 SR 1.2 Software/Device Authentication y NIST SP 800-153 mediante su recomendación de que todos los USB estén marcados como NO confiables).**

## 5.2 CAMPAÑA DE FIN7 “BADUSB” (2021-2022)

Entre los años 2021 y 2022, el grupo FIN7 (famoso por ataques de ransomware) inició una campaña de ingeniería social enviando miles de memorias USB “BadUSB” en paquetes postales como regalos corporativos.

Dichos dispositivos eran dispositivos de la marca LilyGO modificados para comportarse como HID (Human Interface Device), lo que provocaba que, al conectarlos, los sistemas los reconocían como teclado y les permitía escribir una serie de comandos preconfigurados (Ataque BadUSB) permitiendo así al grupo FIN7 lograr implementar accesos remotos para, posteriormente, a través del uso de herramientas como Metasploit, Cobal Strike o Carkanak, realizar movimientos laterales en la red gracias a las explotaciones realizadas para finalmente ejecutar un ransomware en los activos críticos detectados en las redes, afectando tanto a sistemas IT como a sistemas OT directamente y exfiltrando a su vez datos críticos e información sensible para extorsionar a las víctimas, técnica conocida como ransomware de doble extorsión.

## Ataque específico mediante USB a entorno industrial

**BadUSB FIN7 2021 - 2022**

1. Envío masivo de BadUSB en campaña de phising a través del correo postal.
2. Emulación del teclado mediante una ejecución “invisible” de comandos para lograr acceso remoto.
3. Uso de exploits específicos C&C, herramientas específicas, para pivotar en las redes del dispositivo afectado.
4. Finalmente, ransomware de doble extorsión, cifrado de datos IT y OT y exfiltración de datos para extorsión.

**BadUSB**

Campaña de phising masiva

**TA0108 - INITIAL ACCESS**
T0847 - Replication Through Removable Media
T0864 - Transient Cyber Asset

**TA0111- LATERAL MOVEMENT**
T0866 - Exploitation of Remote Services
T0859 - Valid Accounts

**TA0101 - COMMAND AND CONTROL**
T0885 - Commonly Used Port

MITRE ATT&CK™

**TA0104 - EXECUTION**
T0807 - Command-Line Interface
T0853 - Scripting (PowerShell)

**TA0105 - IMPACT**
T0826 - Loss of Availability
T0828 - Loss of Productivity and Revenue

## CAPACIDADES Y PREVENCIÓN UTILIZANDO EL SAFEDOOR DE AUTHUSB Y CONTROLES TEÓRICOS A APLICAR

Este ataque, en comparación con la Botnet Mariposa, tiene una mayor complejidad, pero el vector inicial sigue siendo el uso de una memoria USB infectada, en este caso, tras el envío masivo de memorias BadUSB.

**¿Qué controles y por qué se deberían haber estado implementado? Y lo más importante, ¿Habría la implantación de estos controles evitado el problema de seguridad?**

# 5. / ATAQUES ESPECÍFICOS MEDIANTE USB A ENTORNOS INDUSTRIALES/

La implantación del SafeDoor como “aduana física y lógica” para cualquier USB externo, junto con las políticas y procedimientos alineados con los controles de la familia de estándares de la IEC 62443 y NIST habría evitado que se hubiesen alcanzado estaciones del entorno industrial.

A continuación, se pueden ver los controles relacionados con los estándares anteriormente mencionados y las guías de buenas prácticas y que controles se estarían validando con el uso del SafeDoor de authUSB:

## ANÁLISIS INICIAL Y PUNTO DE CONTROL DEL USB

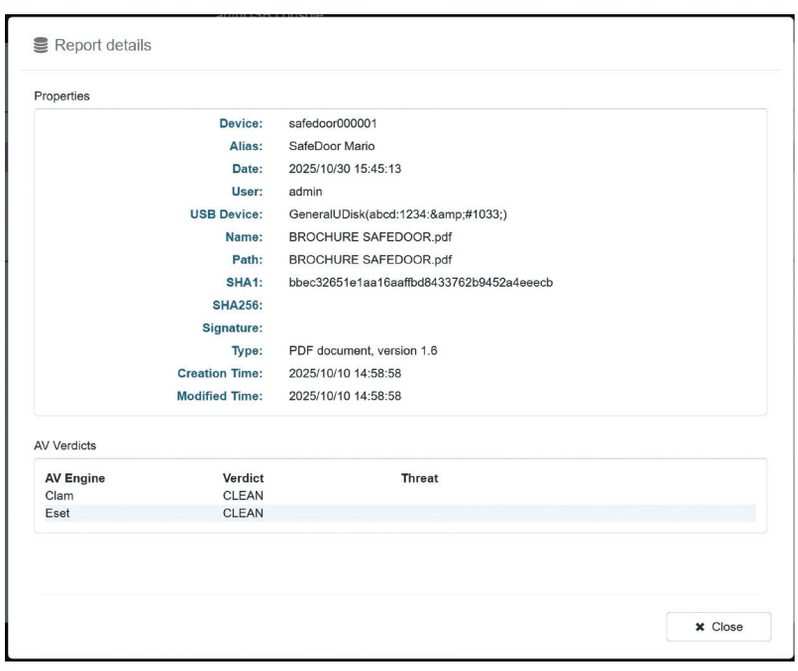
El SafeDoor proporciona no solo una revisión a nivel de AV/Sandbox de los ficheros, sino que también tiene la capacidad para bloquear scripts, deshabilitar el AutoRun y bloquear a nivel eléctrico cualquier tipo de ataque. Además, el SafeDoor inspecciona los medios extraíbles a un tercer nivel, al nivel de hardware/firmware. Este análisis es el que habría bloqueado el uso de los BadUSB ya que habría un bloqueo por “allow-list” para ese dispositivo implementando la política de bloquear cualquier USB externo a la organización. **(IEC 62443-3-3 SR 1.2 – Software Process and Device Identification and Authentication, IEC 62443-3-3 SR 2.1 – Authorization Enforcement, IEC 62443-3-3 SR 3.2 – Malicious Code Protection, IEC 62443-2-1 – Establish, implement and maintain IACS security policies, SP 800-53: MP-7 Media Use, CM-7 Least Functionality, NIST SP 1334** con principios de no confianza por defecto).

Teniendo en cuenta que FIN7 emulaba el teclado mediante el BadUSB, la implementación del SafeDoor habría neutralizado esta posibilidad y por lo tanto la inyección de PowerShell sobre el dispositivo final.

## TRAZABILIDAD Y CONTROL DEL USO EXTREMO-EXTREMO

SafeDoor, es capaz de registrar cada uso de un USB (dispositivo, usuario, host, hora, archivos, hashes, etc) y exportar toda la información a un SIEM o permitir al administrador ver toda la información en una consola centralizada **(NIST SP 1334 Comprehensive Audit & Telemetry para todos los eventos, NIST SP 1334 Real-time Alerting, IEC 62443-3-3 SR 6.1 – Audit Log Accessibility, IEC 62443-3-3 SR 6.2 – Continuous Monitoring, IEC 62443-2-1 – Security program & incident response processes, SP 800-53: AC-6 Least Privilege, CM-7 Least Functionality, MP-5/MP-7).**

En el caso de la campaña de FIN7, se habría detectado el uso del BadUSB, dicho intento habría quedado auditado y habría generado una alerta habilitando la capacidad de implementar una respuesta y probablemente habiendo evitado el ataque (Respuesta temprana y threat hunting).



### NEUTRALIZACIÓN DE LA FASE DE SCRIPTING/POWERSHELL

Dentro de las capacidades que proporciona el SafeDoor, existen diferentes políticas que permiten bloquear archivos en base a sus extensiones (.ps1, .vbs, .js, .hta, .lnk, **MSI** no firmados, **EXE/DLL** no firmados, etc) o analizar archivos (firmware, proyectos, etc) en base a su firma y hash. (Dentro del **NIST SP 1334 cript/Interpreter Blocking at Media Gateway, Content Policy Enforcement or Pre-Transfer, IEC 62443-3-3 SR 3.2 – Malicious Code Protection, IEC 62443-3-3 SR 3.3 – Security Function Verification, IEC 62443-3-3 SR 3.4 – Software and Information Integrity).**

Todo esto permite bloquear cualquier “dropper” que se pueda transmitir a través del USB.

## 5.3 CAMPAÑA SNOWYDRIVE (ORIENTE MEDIO) (2023) – GAS Y PETRÓLEO

En 2023, existió una campaña focalizada en el sector “Oil and Gas” en Oriente Medio. Esta campaña se conoce por la distribución de unidades USB con dropper alojando en el sistema objetivo múltiples ejecutables señuelos, DLL maliciosas para la ejecución de DLL Sideloading y desplegando el backdoor SNOWYDRIVE. La autoría de esta campaña la tiene el actor UNC4698.

La campaña comenzó con el uso de un pendrive “rearmado” conectándose a un dispositivo de la red corporativa por parte de un usuario, el cual ejecutó un falso ejecutable en la raíz del sistema (name.exe) el cual actuó como dropper depositando .exe legítimos y DLL maliciosas para ejecutar un DLL sideloading junto con el despliegue del backdoor SNOWYDRIVE en memoria, así mismo, el instalador ejecutado por la víctima creó claves de arranque y otros componentes auxiliares ocultándolo en carpetas cifradas para posteriormente replicarse a otros medios extraíbles conectados en el equipo.

En una segunda fase, el backdoor estableció un *Command & Control* (C2), abriendo una shell remota y enumerando diferentes archivos para su posterior exfiltración.

Ataque específico mediante USB a entorno industrial

**UNC4698 SNOWYDRIVE 2023**

1. USB con dropper y múltiples recursos cifrados.
2. El dropper despliega el backdoor SNOWYDRIVE y otros artefactos en el disco del equipo objetivo.
3. Shell inversa, operaciones de ficheros y enumeración de otras unidades e información del equipo y la red objetivo.
4. Propagación mediante copias a otras unidades USB para la realización de movimientos laterales tras su uso en otros equipos.
5. Command and Control (C2). Conexión con dominio y protocolo binario sobre TCP. Exfiltración de información.

**SNOWYDRIVE**

Sector
Oil & Gas

**TA0108 - INITIAL ACCESS**
T0847 - Replication Through Removable

**TA0101 - COMMAND AND CONTROL**
T0885 - Commonly Used Port

**TA0110 - PERSISTENCE**
T0889 - Modify Program
T0846 - Remote System Discovery (Enterprise)
T0861 - Point & Tag Identification (Enterprise)
T0801 - Monitor Process State (Enterprise)

MITRE ATT&CK™

**TA0104 - EXECUTION**
T0863 - User Execution
T0871 - Execution Through API

**TA0103 - EVASION**
T0849 - Masquerading

**TA0111 - LATERAL MOVEMENT**
T0867 - Lateral Tool Transfer

**TA0105 - IMPACT**
T0826 - Loss of Availability
T0828 - Loss of Productivity and Revenue

# 5. / ATAQUES ESPECÍFICOS MEDIANTE USB A ENTORNOS INDUSTRIALES/

## CAPACIDADES Y PREVENCIÓN UTILIZANDO EL SAFEDOOR DE AUTHUSB Y CONTROLES TEÓRICOS A APLICAR

Este ataque fue muy complejo, requería de diferentes pasos y de la interactuación de un usuario, aun así, el paso inicial para el éxito del ataque es la mencionada interacción del usuario con el USB en un equipo corporativo.

**¿Qué controles y por qué se deberían haber estado implementado? Y lo más importante, ¿Habría la implantación de estos controles evitado el problema de seguridad?**

La integración del SafeDoor de authUSB como aduana física y lógica para cualquier USB externo permitiría detectar la carga maliciosa del USB. A continuación, se pueden observar las funcionalidades que ofrece SafeDoor y que habrían permitido detener el ataque y que controles relacionados con normativas, estándares y guías de buenas prácticas se estarían cumpliendo.

### DETECCIÓN DE USB “REARMADOS”

SafeDoor, tiene la capacidad de detectar ejecutables ocultos u otras rutas señuelo dentro del USB. Esta detección generaría una alerta y, además, el dispositivo pasaría a cuarentena. **(NIST SP 1334 Default-Deny on Removable Media, Mandatory Pre-Use Inspection, Anomaly Patterns on Media Layout, No AutoMount; IEC 62443-3-3 SR 1.2 – Software Process and Device Identification and Authentication, IEC 62443-3-3 SR 2.1 – Authorization Enforcement, IEC 62443-3-3 SR 3.2 – Malicious Code Protection).**

### BLOQUEO DE EJECUTABLES/TRANSFERENCIA DE ARCHIVOS EXE EN RAÍZ

SafeDoor permite la implementación de políticas que bloqueen la transferencia de archivos ejecutables o la auto ejecución de los mismos. **(NIST SP 1334 Executable Governance at Media Gateway, Root-Path Execution Ban, Name-Based Heuristic; IEC 62443-3-3 SR 3.3 – Security Function Verification, IEC 62443-3-3 SR 3.4 – Software and Information Integrity).**

### CONTROL DE LA TRANSFERENCIA DE ARCHIVOS

Las funcionalidades del SafeDoor permiten integrar reglas para limitar las transferencias de archivos desde y hacia memorias USB lo que garantiza el control de la información. En el caso de la campaña SNOWYDRIVE, se podría haber evitado la transferencia de algunos tipos de archivos hacia el equipo infectado y también la transferencia de archivos exfiltrados hacia la memoria USB. **(NIST SP 1334 Directional Transfer Controls, Post-Use Re-Evaluation & Mandatory Sanitization, Least Data Movement; IEC 62443-3-3 SR 5.2 – Zone Boundary Protection, IEC 62443-2-1 – Media handling procedures).**

### MONITORIZACIÓN DE ACTIVIDADES Y ANÁLISIS DE IOC

Mediante la consola central, el operario del SafeDoor de authUSB tienen una visión completa de los análisis realizados sobre las memorias USB. Este tipo de control podría haber alertado al equipo de seguridad de la compañía afectada por el ataque. Además, SafeDoor permite el bloqueo por IOC de dispositivo (VID/PID/Serial). **(NIST SP 1334 Comprehensive Audit & Telemetry, Real-time Response Hooks, IOC-based Device and Artifact Blocking; IEC 62443-3-3 SR 6.1 – Audit Log Accessibility, IEC 62443-3-3 SR 6.2 – Continuous Monitoring, IEC 62443-3-3 FR-7 – Resource Availability).**

# 6

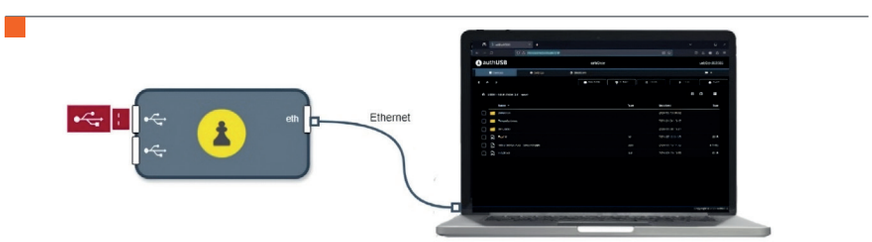
# RECOMENDACIONES DE IMPLEMENTACIÓN Y BUENAS PRÁCTICAS (CONCLUSIONES)

# 6. / RECOMENDACIONES DE IMPLEMENTACIÓN Y BUENAS PRÁCTICAS (CONCLUSIONES)

El dispositivo SafeDoor se ha diseñado y producido para ofrecer una solución óptima para todo tipo de entornos. La filosofía que hay detrás del dispositivo es la de bloquear todos los puertos USB de nuestro entorno para solo permitir el uso de esos equipos a través de SafeDoor. Esta filosofía nos lleva a tener múltiples casos de uso orientados a satisfacer las necesidades de entornos empresariales tanto en IT como en OT y entornos militarizados. En este documento, estamos focalizados a los casos de uso de industria y como resumen, tenemos una explicación de algunos de los casos más utilizados.

## OPERATIVA “CONEXIÓN DIRECTA RED OT”

Esta operativa permite la conexión de memorias USB de forma segura a equipos aislados que típicamente solo admiten la entrada y salida de información a través de estos medios. Con este caso de uso, podemos conectar el dispositivo SafeDoor directamente a estas máquinas desconectadas o legacy mediante el uso de un cable de red gracias al cual rompemos el protocolo de transferencia. Básicamente esta operativa convierte a SafeDoor en un punto de acceso para USB con una capa de seguridad con vigilancia efectiva en ataques eléctricos, ataques hardware y ataques malware.




## OPERATIVA “CONEXIÓN COMPARTIDA” EN REDES IT Y OT

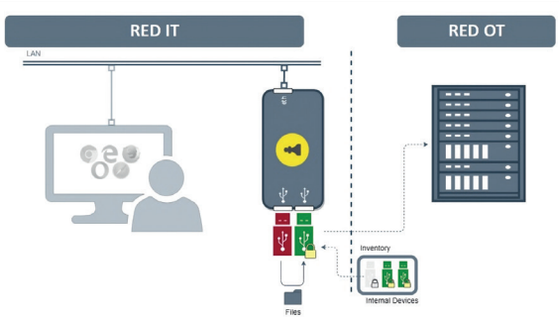
Esta operativa nos permite convertir nuestro SafeDoor en un punto de acceso conectado a toda la línea productiva. Las limitaciones de este modelo residen únicamente en la comunicación a través de la red. En este caso de uso, nuestro planteamiento consiste en disponer de uno o varios dispositivos desplegados según conveniencia en

puntos clave de nuestra red. El proceso permite el servicio a múltiples puestos de trabajo y o máquinas industriales apoyándose en todo momento de la transferencia por red interna.


## OPERATIVA “FRONTERA” ENTRE REDES IT Y OT

Existen entornos donde nos vemos obligados a continuar la operativa con un USB, o bien nuestra máquina no admite otro soporte de datos que no sea el anterior citado o nuestra propia operativa no permite la conexión entre máquinas. Para estos casos, hemos diseñado el modelo de uso “Frontera”. Esta configuración nos permite utilizar únicamente USB que pertenezcan a un listado. Dicho de otra manera, todo USB que se requiera conectar a una máquina, debe ser reconocido por el SafeDoor.

Los únicos USB registrados serán internos. Unos USB que tenemos segurizados, inventariados y registrados en el sistema SafeDoor. Este método nos permite hacer un análisis y posterior transferencia de los datos que llegan a nuestra factoría en un USB externo o desconocido hacía un USB seguro.



# 6. / RECOMENDACIONES DE IMPLEMENTACIÓN Y BUENAS PRÁCTICAS (CONCLUSIONES)

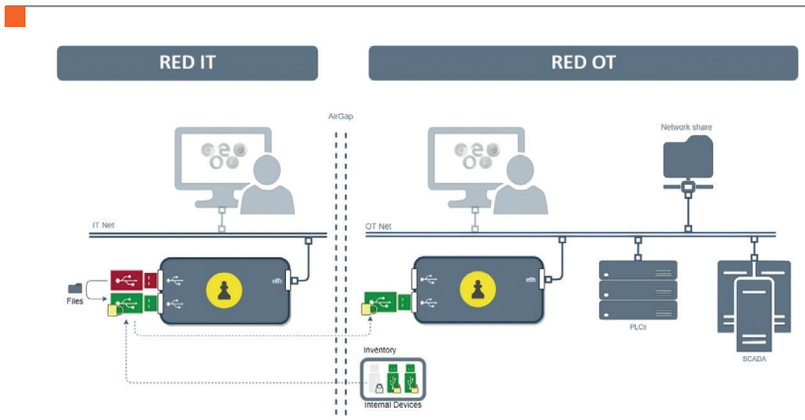
## OPERATIVA “FRONTERA – ADUANA” ENTRE REDES IT Y OT

Esta operativa está diseñada para ser utilizada en todo entorno donde tenemos que respetar un AirGap temporal o espacial que nos obliga a hacer una segunda comprobación para verificar que todo lo analizado sigue siendo correcto.

Nuestro planteamiento implica la utilización de dos o más SafeDoor desconectados entre sí, pero que igualmente comparten configuración para trabajar en parejas.

Al igual que en el modelo anterior, trabajamos con memorias USB segurizadas, inventariadas y registradas en sendos dispositivos. Estos dispositivos, idealmente estarán cifrados por hardware o por software imposibilitando así el acceso por parte de terceros. Estas memorias cifradas, en su debido momento, serán descifradas automáticamente por el dispositivo ya que parte de su registro implica en el almacenamiento de las claves.

Con el escenario descrito; dos SafeDoor con al menos una memoria cifrada registrada, uno en IT y otro en OT. Requieren transferir datos de una red a la otra haciendo en el primero el análisis de la memoria desconocida y la transferencia a la memoria registrada siendo esta la que viajará a la red aislada para ser recibida por el segundo SafeDoor que a su vez hará el análisis del dato comprobando así que todo el proceso queda ajeno a amenazas y accesos no deseados.



# 7

# REFERENCIAS

# 7. / REFERENCIAS /


**MANUAL DE USO SEGURO SAFEDOOR (CCN)**
*https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/4146-ccn-stic-1201-procedimiento-de-empleo-seguro-de-authusb-safedoor/file.html*

**MANUALES INTERNOS AUTHUSB**

**SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS**
*https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final*

**REDUCING THE CYBERSECURITY RISKS OF PORTABLE STORAGE MEDIA IN OT ENVIRONMENTS**
*https://csrc.nist.gov/pubs/sp/1334/final*

**IEC 62443-3-3:2020**
*https://www.incibe.es/incibe-cert/blog/el-proceso-de-certificacion-en-iec62443-3-3*

**IEC 62443-2-1:2024**
*https://webstore.iec.ch/en/publication/62883*

**AUTHUSB**
*https://www.authusb.net/*

**SAFEDOOR AUTHUSB**
*https://www.authusb.net/en/safedoor/*

**HACKRTU**
*https://www.hackrtu.com/*

8

# ABREVIATURAS

# 8. / ABREVIATURAS /

- **CPSTIC:** Catálogo de Productos y Servicios de Tecnologías de la Información y Comunicación de Seguridad (gestión del Centro Criptológico Nacional, CCN).
- **DLL:** *Dynamic Link Library* (Biblioteca de enlace dinámico).
- **ENS:** Esquema Nacional de Seguridad.
- **ERP:** *Enterprise Resource Planning* (Planificación de Recursos Empresariales).
- **EXE:** *Executable* (Archivo ejecutable).
- **HID:** *Human Interface Device* (Dispositivo de Interfaz Humana).
- **ICS:** *Industrial Control Systems* (Sistemas de Control Industrial).
- **IEC:** *International Electrotechnical Commission* (Comisión Electrotécnica Internacional).
- **IOC:** *Indicator of Compromise* (Indicador de Compromiso).
- **IT:** *Information Technology* (Tecnologia de la Información).
- **LDAP:** *Lightweight Directory Access Protocol* (Protocolo Ligero de Acceso a Directorios).
- **MSI:** *Microsoft Installer* (Instalador de Microsoft).
- **NIST:** *National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología de Estados Unidos).
- **OT:** *Operational Technology* (Tecnología Operacional).
- **SIEM:** *Security Information and Event Management* (Gestión de Información y Eventos de Seguridad).
- **SP:** *Special Publication* (Publicación Especial).
- **USB:** *Universal Serial Bus*.
- **VPN:** *Virtual Private Network* (Red Privada Virtual).

# MEDIOS EXTRAÍBLES EN ENTORNOS INDUSTRIALES

authUSB
MOVE FIRST & CROWN THE GAME

&

HackRTU
INDUSTRIAL SECURITY

2025