Soluciones antimalware off-line y whitelisting de aplicaciones para la protección de servidores/clientes SCADA/Historian/OPC en redes OT (Operation Technology)

Las soluciones antimalware son programas que pueden ser instalados tanto en hosts, servidores o en firewalls, que detectan virus y malware comparando los archivos almacenados en estos equipos con una base de datos de firmas (que se actualiza en muchas ocasiones horariamente) en la que se recogen todos los virus y malware conocidos. Además de detectar, estos sistemas proceden a la eliminación y/o puesta en cuarentena de los archivos infectados.

¿Qué ocurre cuando queremos utilizar este tipo de tecnologías en los sistemas de gestión en tiempo real que se utilizan para optimizar los procesos de producción asociados a los entornos OT?

Que debemos ser conscientes de la idiosincrasia de estos entornos, para que la incorporación de estas soluciones no afecte a la disponibilidad y óptimo funcionamiento del proceso productivo. En particular, hay que considerar que en los entornos OT existen sistemas en los que:

- No es posible instalar ningún tipo de agente porque el fabricante del SCADA, HMI, Historian, etc. no lo recomienda y/o soporta.
- Los sistemas operativos utilizados han quedado obsoletos y ya no disponen de soporte por parte del fabricante del antimalware.
- No pueden pararse (no es posible degradar el rendimiento del sistema) ni reiniciarse para realizar actualizaciones ya que son críticos.
- No pueden llevarse a cabo actualizaciones de firmas a través de la red por estar aislados.

La pregunta que surge es: **¿Existen soluciones antimalware no invasivas y que no degraden el rendimiento de los sistemas críticos?** La respuesta es afirmativa.

En aquellos equipos en los que por razones de seguridad no puedan conectarse a Internet (ni si quiera a través de un servidor ubicado en una zona desmilitarizada en el que se descarguen las firmas actualizadas); no esté permitida la instalación de software anti-malware porque el SO ya no está soportado (recordemos que en los entornos OT el SO más extendido es XP sin soporte por parte de Microsoft) o porque el propio fabricante del sistema HMI, SCADA, OPCServer, Historian, MES desaconseja su instalación, la solución pasa por realizar **una protección en modo off-line**. Dentro de este tipo de protección, existen entre otras, las dos siguientes soluciones:

La utilización de herramientas de escaneo de malware realizada de forma manual y no invasiva (sin instalar agentes)

La instalación de software específico que permita realizar "whitelisting" o "lockdown" de aplicaciones

Para la primera de las soluciones, **Trend Micro, con su aplicación Portable Security** proporcionan la posibilidad de realizar el escaneo de diferentes equipos, utilizando para ello un "antimalware portable". Este antimalware se encuentra instalado en una Scanning Tool que utiliza el puerto USB de PCs y servidores para realizar el escaneo y limpieza de malware, sin instalar ningún tipo de librería o archivo. En la figura 1, se recrea este escenario.

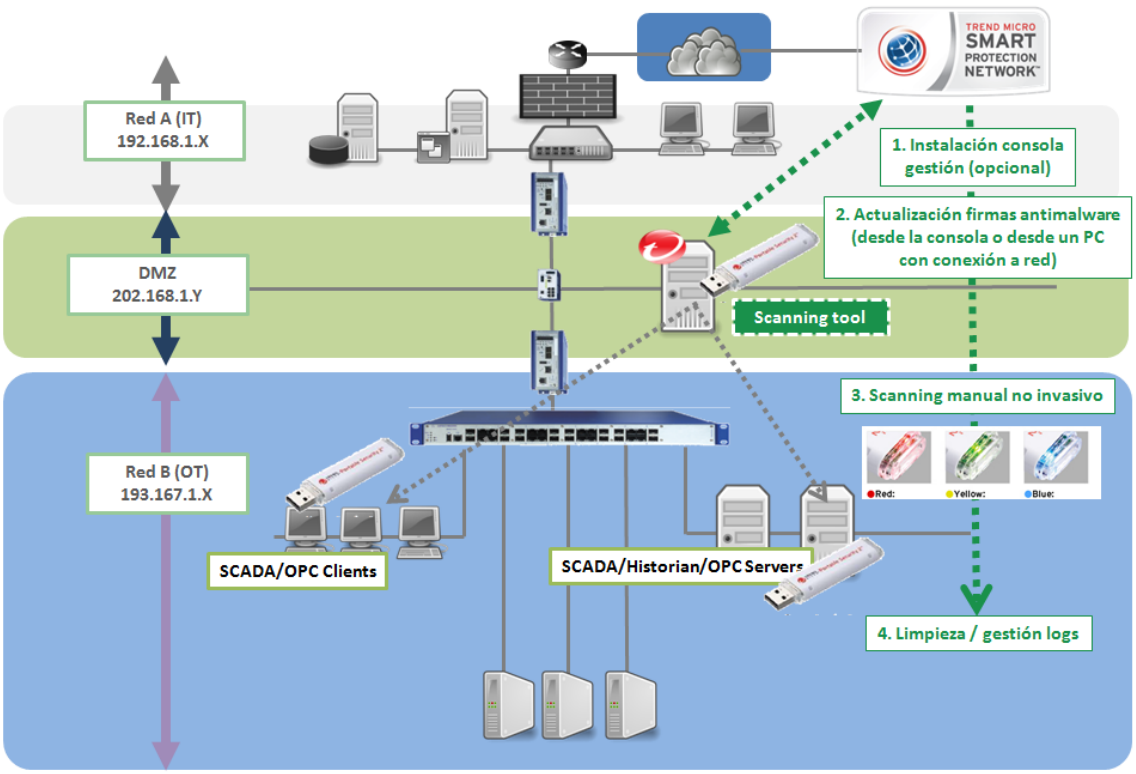

Figura 1. Proceso de escaneo y limpieza de malware off-line a través de "scanning tool"

Puede observarse que existen tres segmentos físicos de red:

- La red A (IT) con un rango de direcciones IP 192.168.1.X.
- La red B (OT) con un rango de direcciones IP 193.167.1.X, en la que se encuentran los PC clientes SCADA y OPC y servidores SCADA/Historian u OPC
- La zona desmilitarizada o DMZ[1] con su propio rango de direcciones IP 202.168.1.Y.2

Los equipos que se encuentran en la red OT se hallan bajo alguna de las circunstancias antes descritas que requieren de la instalación de soluciones antimalware off-line. En este caso, el proceso de escaneo y desinfección se realiza de la siguiente manera:

1. **En la zona desmilitarizada de encuentra un servidor en el que se ha instalado la consola central que permite: la actualización de firmas del antimalware (que se encuentra embebido en la "scanning tool") y la gestión de logs. La instalación de esta consola es opcional.**

2. **Se realiza el proceso de actualización del antimalware. Este proceso se realiza desde la consola o se podría realizar desde cualquier PC, ubicado tanto en la DMZ como en la red IT. Debe existir conexión a través de Internet para actualizar la base de datos de firma.**

3. **Manualmente, se realiza el escaneo en los dispositivos seleccionados. Es imprescindible que los equipos dispongan de un puerto USB libre. Este es el punto clave, ya que dicho escaneo (que se realiza sobre todos los ficheros o sobre aquellos que el administrador seleccione) se lleva a cabo sin instalar ningún tipo de agente (software, .dll, .exe) en el PC o en el servidor (Figuras 2, 3 y 4). Una vez que se ha producido el escaneo, la scanning tool proporciona visualmente los resultados obtenidos:**

    - **Rojo: escaneo de malware realizado, malware detectado y en espera de ser limpiado.**
    - **Amarillo: escaneo de malware realizado, malware detectado y limpieza realizada.**
    - **Azul: escaneo de malware realizado y malware no detectado.**

4. **Por último, los logs que la "scanning tool" ha recogido, pueden ser borrados o introducidos en la consola de gestión para su análisis.**

[1] Una DMZ se define como una red intermedia que se crea entre dos redes principales a través de dos firewalls (habitualmente de diferente fabricante para dificultar aún más el éxito de un posible ataque). La finalidad de esta red intermedia es que la información/aplicación que quiera ser compartida por los usuarios de las redes principales se ubique en dicha red intermedia, permitiendo por un lado dicho acceso, pero evitando el tráfico y acceso directo entre las dos redes principales.

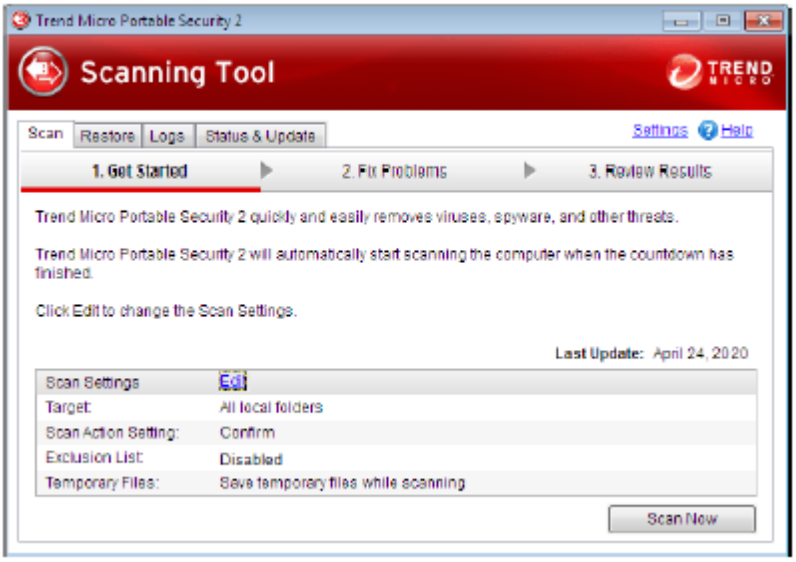

Figura 2. La “scanning tool” está preparada para realizar el escaneo sin haber instalado ningún agente

Figura 3. Detección de un virus que va a ser limpiado

Figura 4. Resultados del escaneo manual en la “scanning tool”

La segunda opción para realizar esta protección off-line es la instalación de agentes que permitan llevar a cabo lo que se conoce como "whitelisting" de aplicaciones, o "lockdown". En este caso, **Trend Micro proporciona la solución Safe Lock** y el proceso se realiza de la siguiente manera:

1. El agente que ha sido instalado en el PC o en el servidor mapea todos los ejecutables existentes en un determinado equipo (.exe, .dll, etc…).

2. Se determinan que estos son los programas que pueden lanzarse/ejecutarse desde este equipo (Figura 5).

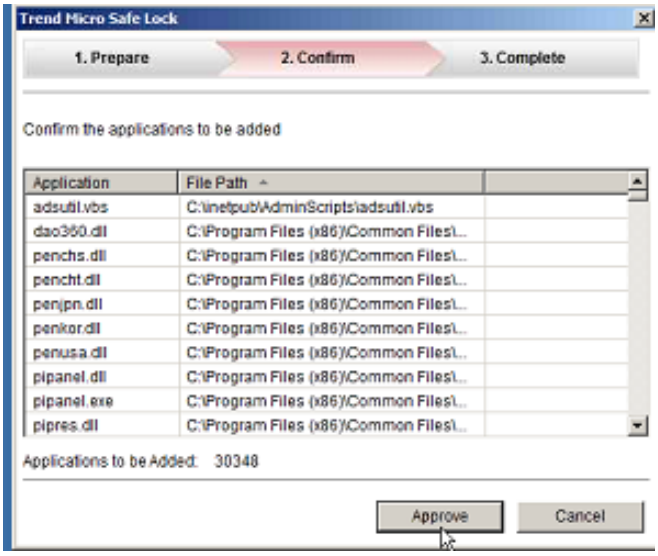

Figura 5. Programas seleccionados que podrán ser ejecutados desde la máquina

3. Se realiza el bloqueo o "lockdown", de manera que cualquier aplicación que quiera instalarse o cualquier ejecutable malicioso que quiera desplegarse no podrá hacerlo, ya que es una aplicación no autorizada para hacerlo (Figura 6).

Figura 7. Lockdowns de aplicaciones realizado

Para finalizar y a modo de conclusiones

- La seguridad de los entornos OT asociados a la industria química puede verse afectada por el efecto de distintos tipos de malware y de APTs.

- Es recomendable llevar a cabo políticas, procedimientos y estándares que ayuden a mitigar, minimizar y si es posible eliminar estas amenazas y apoyarse en tecnologías específicas que tengan en cuenta la idiosincrasia de la industria química (determinismo, disponibilidad, no degradación del rendimiento del sistema).

- La utilización de soluciones antimalware off-line en estos entornos es posible a través de la realización de escaneos manuales no invasivos (utilizando scanning tolos) y la realización de whitelisting de aplicaciones o “lockdowns”.

Dr. Fernando Sevillano | fernando.sevillano@logitek.es | Industrial Cybersecurity Manager