Configuración ESET anti-ransomware

Más seguridad contra el secuestro de información

ENJOY SAFER TECHNOLOGY™

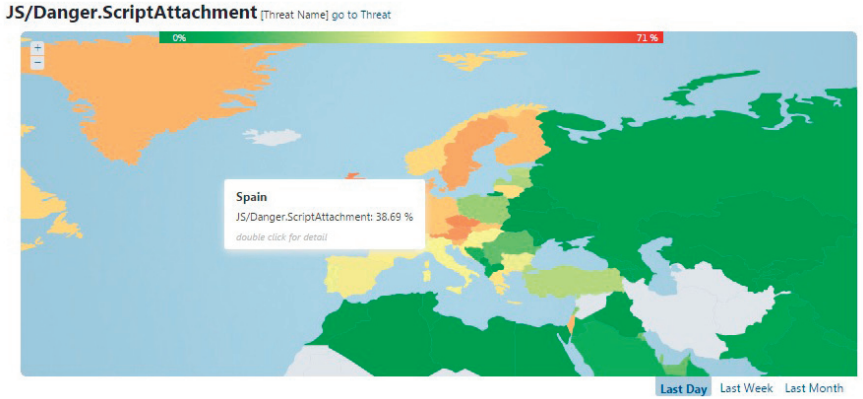
ÍNDICE

OBJETIVOS DE ESTE MANUAL TÉCNICO

En este manual técnico describimos la configuración óptima de los productos de seguridad ESET contra las diferentes variantes actuales de ransomware. El objetivo es mejorar la protección de nuestros clientes contra cualquier brote de ransomware para evitar que la información de la empresa sea cifrada por extorsionadores (generalmente los ciberdelincuentes piden una recompensa por liberar los archivos, algo que ESET desaconseja en cualquier caso).

¿POR QUÉ ESTA CONFIGURACIÓN ADICIONAL?

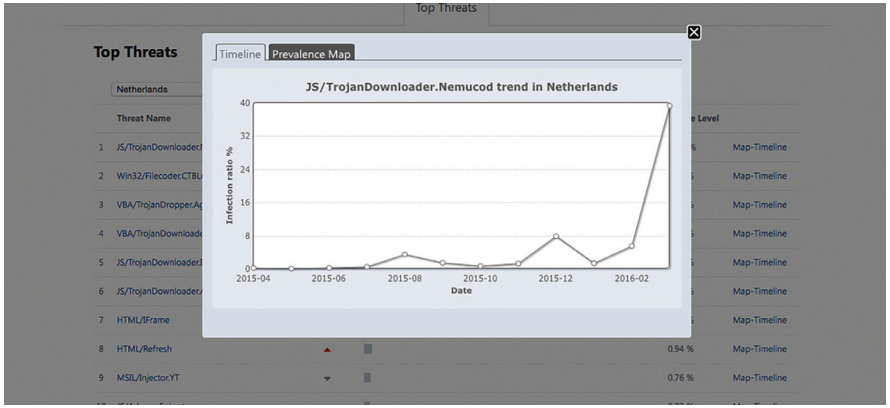
Porque casi el 40% de las amenazas detectadas hoy en España pueden suponer una infección por ransomware.



Los ataques actuales de ransomware utilizan técnicas de infección avanzadas que permiten que el software malicioso infecte los dispositivos. Los ciberdelincuentes convencen a los usuarios para que ejecuten un archivo que a su vez descargará el código malicioso para empezar el proceso de cifrado. Adjuntando este ejecutable a un correo electrónico, los cibercriminales intentan evitar la detección cuando llega a la bandeja de entrada. En la mayoría de casos se utiliza un correo de phishing elaborado correctamente con un archivo ZIP como documento adjunto. Este archivo ZIP contiene en la mayoría de los casos un JavaScript con extensión .js.

Debido a que el código JavaScript es utilizado en numerosas páginas web, es imposible bloquearlo en el navegador. Además, Windows también ejecuta código JavaScript directamente.

El código JavaScript causante de la descarga del malware se encuentra altamente ofuscado, y es modificado por los cibercriminales continuamente para evitar su detección. Influyendo en la ejecución de códigos potencialmente maliciosos, podremos bloquear las infecciones por ransomware, utilizando diversos módulos de seguridad. En adelante, te explicamos cómo hacerlo.



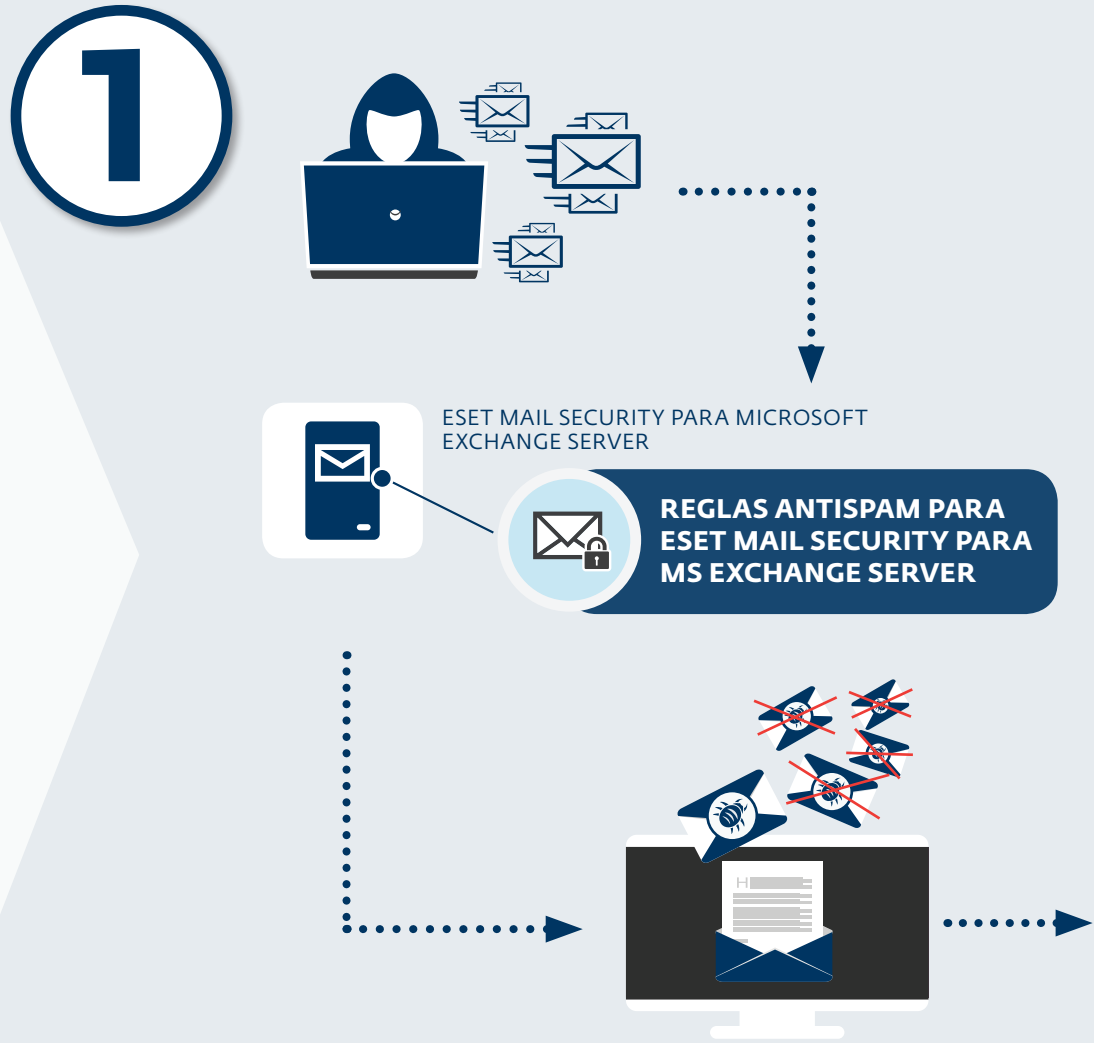
Limitación de responsabilidad:

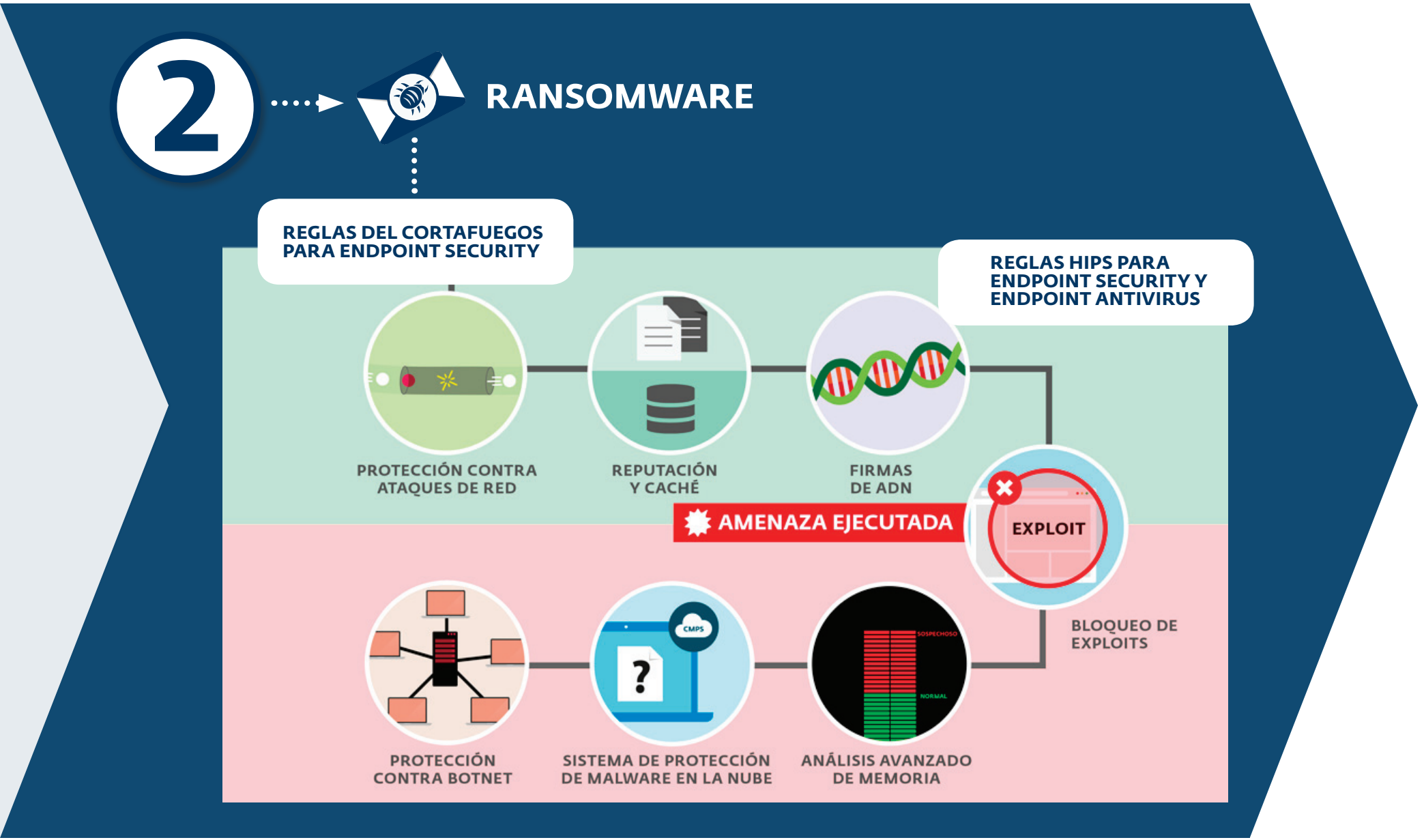
La configuración y políticas ESET anti-ransomware han sido creadas de forma genérica y pueden variar según la zona geográfica. Recomendamos comprobar la configuración para cada instalación en un entorno cliente antes de implementarla completamente.

CONFIGURACIÓN ESET ANTI-RANSOMWARE PARA EMPRESAS

La configuración adicional de ESET anti-ransomware evita que empiece la descarga del código malicioso, causante de las infecciones por este malware (que utiliza JavaScript). A continuación, explicamos esta configuración adicional con más detalle a través de una serie de políticas que puedes descargar e implementar utilizando ESET Remote Administrator o directamente sobre un equipo cliente con ESET Endpoint instalado.

DESCARGA TU CONFIGURACIÓN AQUÍ



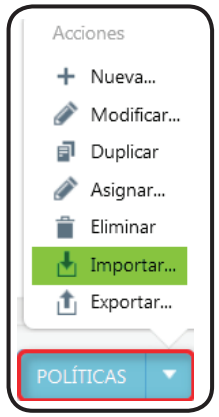

2
RANSOMWARE
REGLAS DEL CORTAFUEGOS PARA ENDPOINT SECURITY
REGLAS HIPS PARA ENDPOINT SECURITY Y ENDPOINT ANTIVIRUS
PROTECCIÓN CONTRA ATAQUES DE RED
REPUTACIÓN Y CACHÉ
FIRMAS DE ADN
AMENAZA EJECUTADA
EXPLOIT
BLOQUEO DE EXPLOITS
PROTECCIÓN CONTRA BOTNET
SISTEMA DE PROTECCIÓN DE MALWARE EN LA NUBE
ANÁLISIS AVANZADO DE MEMORIA
CMPS
SOSPECHOSO
NORMAL

REGLAS ANTISPAM PARA ESET MAIL SECURITY PARA MS EXCHANGE SERVER

Si utilizamos las reglas antispam correctas, los correos entrantes no deseados serán filtrados en el propio servidor de correo. Esto garantiza que el documento adjunto que contiene el malware no se entregue al usuario final y no haya opción de que se ejecute el ransomware.

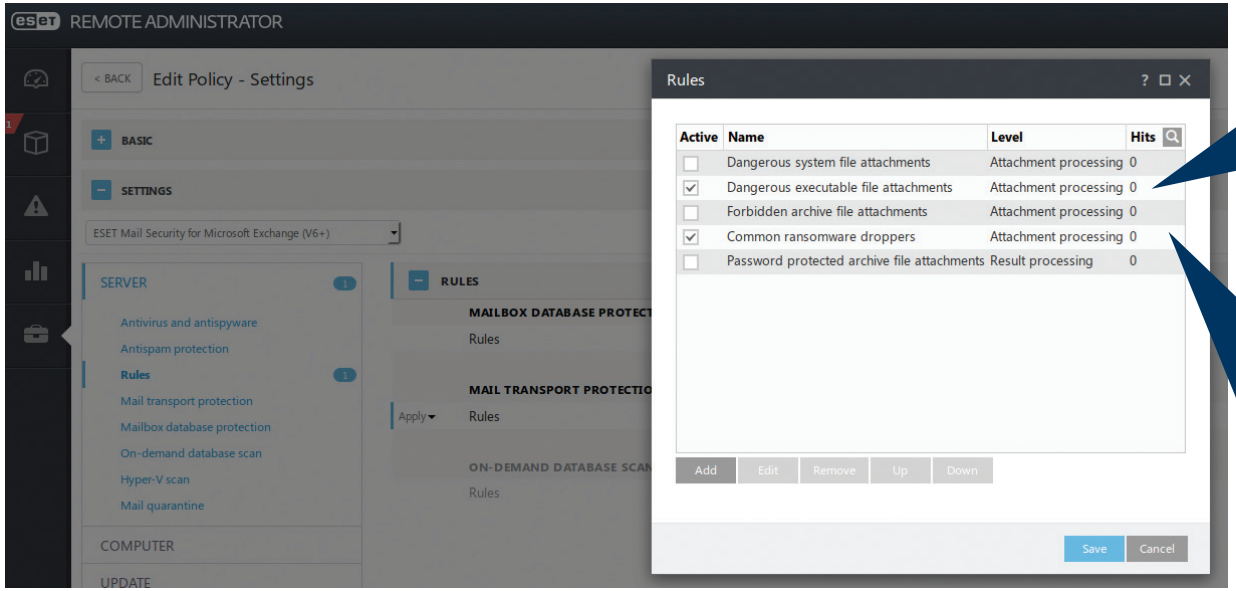
Cómo importar y aplicar las políticas*

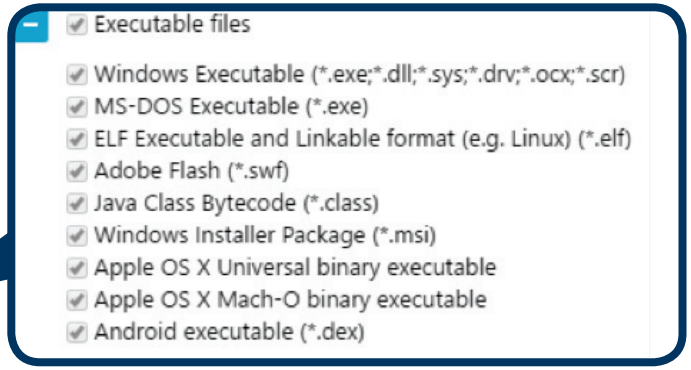
1. Inicia sesión en la consola web de ERA 6
2. Accede a ADMIN > Políticas
3. Accede a "Políticas" y después "Importar"
4. Importa las políticas de una en una
5. Asigna las políticas a *un grupo* o *cliente*



***No se necesita la repetición con otras configuraciones.**

Importante:
Actualiza ESET Mail Security para Microsoft Exchange Server a la última versión 6.3.x o superior para garantizar el funcionamiento de las reglas de filtrado.





Los adjuntos más comunes que descargan ransomware tienen las siguientes extensiones:

*.js
*.hta
*.docm
*.xlsm
*.pptm
*.vbs
*.bat

* En este caso los archivos de **Microsoft Office con Macros también se bloquearán (docm, xlsm, y pptm).** Cuando se usan este tipo de archivos, esta regla tiene que ser ajustada o deshabilitada.

REGLAS DEL CORTAFUEGOS PARA ENDPOINT SECURITY

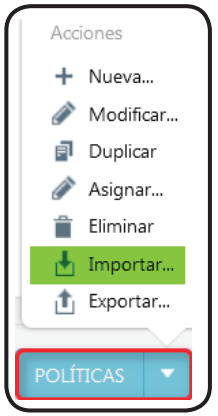
En caso de que se ejecute el archivo malicioso adjunto, ESET Endpoint Security evitará la descarga de malware gracias al cortafuegos integrado.

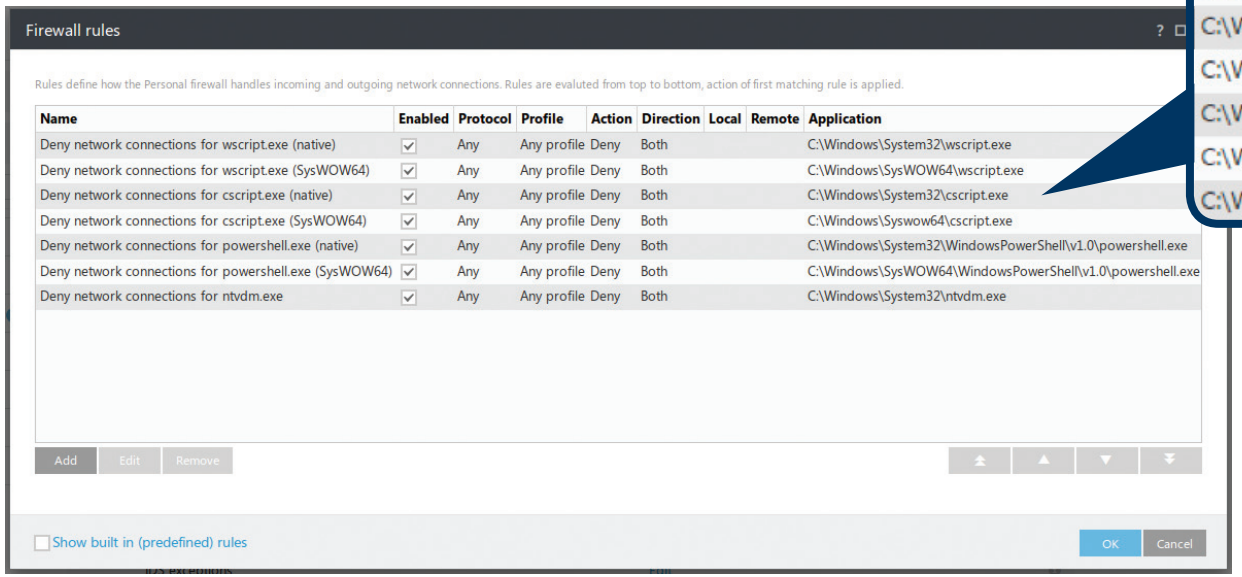
Aplicando estas reglas del cortafuegos, ESET Endpoint Security bloqueará la descarga del malware y denegará el acceso de otros scripts a Internet.

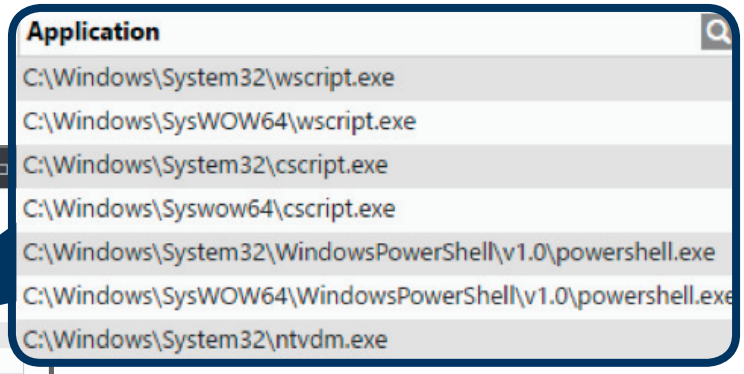
Cómo importar y aplicar las políticas

1. Inicia sesión en la consola web de ERA 6
2. Accede a ADMIN > Políticas
3. Accede a "Políticas" y después "Importar"
4. Importa las políticas de una en una
5. Asigna las políticas a *un grupo* o *cliente*

Por favor, ten en cuenta que al importar las Reglas del cortafuegos pueden sobrescribirse otras reglas.







IMPORTANTE

- Esta política solo funciona en combinación con ESET Endpoint Security debido a que esta configuración únicamente afecta al cortafuegos integrado en este producto.
- Para estas reglas, también se aplica que las aplicaciones legítimas puedan usar este tipo de ejecutables. Recomendamos, por tanto, que se pruebe antes de aplicar completamente la política en tu entorno.

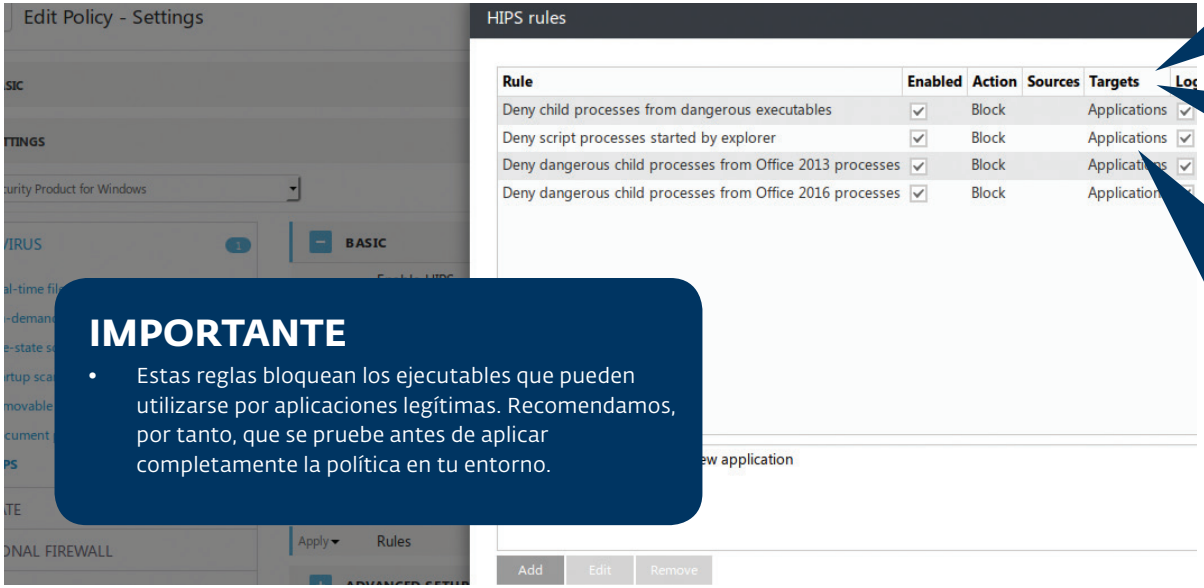
REGLAS HIPS PARA ENDPOINT SECURITY Y ENDPOINT ANTIVIRUS

El sistema de prevención de intrusiones (HIPS) defiende el sistema desde dentro y puede interrumpir acciones no autorizadas para ciertos procesos antes de su ejecución. Al prohibir la ejecución de JavaScript y otros scripts, el ransomware no tiene posibilidad de ejecutar códigos maliciosos, tan solo permite descargarlos.

Nuestro módulo HIPS también forma parte de ESET File Security para Windows Server, lo cual permite también proteger los servidores. Por favor, ten en cuenta que el HIPS no distinguirá los scripts legítimos que se inician en entornos de producción.

Cómo importar y aplicar las políticas

1. Inicia sesión en la consola web de ERA 6
2. Accede a ADMIN > Políticas
3. Selecciona "Políticas" y después "Importar"
4. Importa las políticas de una en una
5. Asigna las políticas a *un grupo* o *cliente*



Denegar el proceso hijo de los ejecutables peligrosos

Application
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\Syswow64\cscript.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\ntvdm.exe

Denegar los procesos script iniciados por el explorador

C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe

Denegar los procesos hijos peligrosos de Office 201x

C:\Windows\System32\cmd.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\System32\wscript.exe
C:\Windows\SysWOW64\wscript.exe
C:\Windows\System32\cscript.exe
C:\Windows\SysWOW64\cscript.exe
C:\Windows\System32\ntvdm.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

IMPORTANTE

- Estas reglas bloquean los ejecutables que pueden utilizarse por aplicaciones legítimas. Recomendamos, por tanto, que se pruebe antes de aplicar completamente la política en tu entorno.

RESULTADOS DEL ANÁLISIS DE LA CONFIGURACIÓN ESET ANTI-RANSOMWARE

Con una configuración ESET anti-ransomware completa en los servidores de correo, equipos e incluso en servidores de archivos, los correos electrónicos que contienen ransomware en documentos adjuntos ya se pueden filtrar antes de ser detectados como código malicioso o ransomware. Además, hemos llevado a cabo varios análisis en los equipos con esta configuración reforzada, donde desactivamos todas las capas de detección de nuestras soluciones de seguridad ESET, demostrando que este tipo de ransomware no tiene ninguna posibilidad de cifrar el propio sistema y otras ubicaciones de la red corporativa.

Como vemos, la configuración ESET anti-ransomware contribuye a reforzar las soluciones de seguridad ESET y minimiza el riesgo de infección por ransomware, evitando con ello el cifrado de la información corporativa.