Configuración de ESET Anti-Ransomware

Seguridad en múltiples capas contra el cifrado

Versión del documento:
1.1

Autores:
Michael van der Vaart, Chief Technology Officer | ESET Holanda
Donny Maasland, Head of Cybersecurity Services and Research | ESET Holanda

CONTENIDO

Propósito del presente informe técnico 3

¿Por qué se agregaron estas configuraciones adicionales? 3

Configuración de ESET Anti-Ransomware para empresas 4

- Reglas de antispam para ESET Mail Security para MS Exchange . 6
- Reglas de firewall para Endpoint Security 7
- Reglas de HIPS para Endpoint Security y Endpoint Antivirus . . . 8
- Resultados de las pruebas de configuración de ESET Anti-Ransomware 9

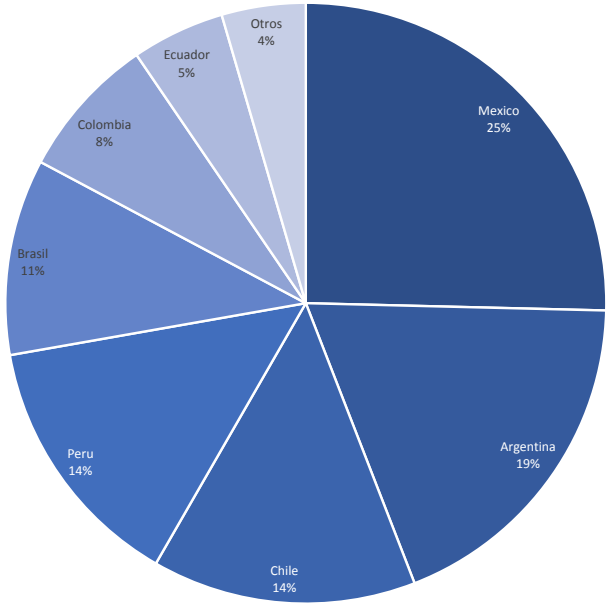
PROPÓSITO DEL PRESENTE INFORME TÉCNICO

En este informe técnico describimos la configuración óptima de las soluciones de seguridad de ESET para combatir los tipos actuales de ransomware y los escenarios de infección más comunes. El objetivo es mejorar la protección de nuestros clientes contra el nuevo brote de ransomware, que cifra o secuestra los datos importantes de los usuarios y pide el pago de un rescate para liberarlos.

¿POR QUÉ SE AGREGARON ESTAS CONFIGURACIONES ADICIONALES?

El ransomware es un tipo de amenaza que llegó para quedarse, un claro ejemplo de esto es la cantidad de variantes que hemos analizado con respecto al año 2015. Hasta septiembre del 2016 vemos que la cantidad de variantes se ha duplicado con respecto al año anterior.

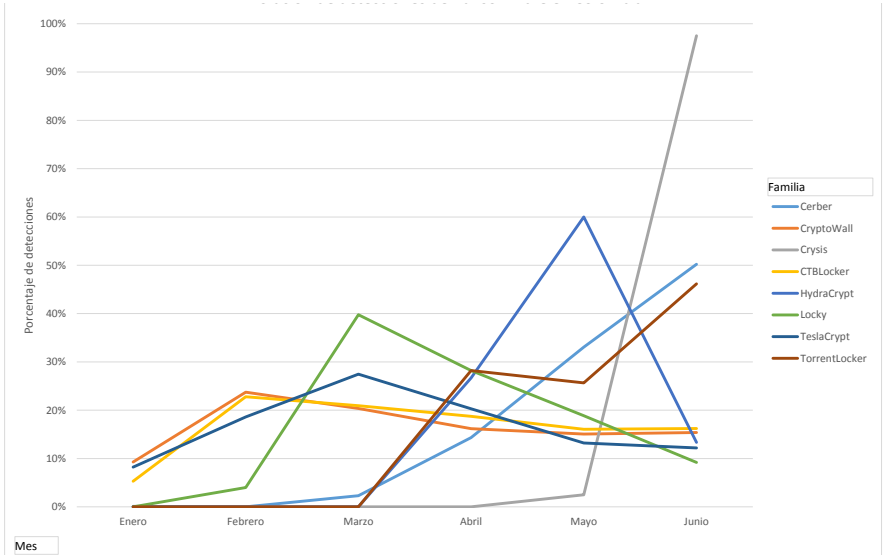
Porcentajes de detección por país:



Los ataques de ransomware en la actualidad utilizan técnicas avanzadas de infección que le permiten al malware infectar los dispositivos de las víctimas. Convencen a los usuarios de ejecutar un archivo conocido como dropper, que a su vez descarga el payload malicioso para iniciar el proceso de cifrado. Con el objetivo de evitar la detección al ingresar al equipo, los cibercriminales adjuntan el dropper a un correo electrónico. En la mayoría de los casos, se usa un correo de phishing creado específicamente con un ZIP como archivo adjunto. Este archivo ZIP en general contiene un archivo de JavaScript con extensión .JS.

Como son muchos los sitios Web que utilizan JavaScript, es imposible bloquearlo en el navegador. Por otra parte, Windows también ejecuta JavaScript directamente. Además, el código JavaScript del dropper está fuertemente ofuscado y se modifica continuamente con el fin de evitar la detección. Esto nos da la oportunidad de interceder en la ejecución de código potencialmente malicioso a través de procesos estándar, mediante el uso de diversos módulos de seguridad.

Deteccion de las variantes de ransomware mas detectadas entre Enero y Junio:



Aviso:

La configuración y las políticas de ESET Anti-Ransomware fueron trazadas en forma genérica y pueden variar según el área. Recomendamos probar la configuración para cada implementación en un grupo reducido de clientes antes de implementarla plenamente.

MANTENGA ACTUALIZADA SU SOLUCION DE SEGURIDAD

Lo primero que hay que saber es con qué versión de las soluciones de ESET se cuenta instalada en los equipos. Para realizar esto, se debe acceder al Menú de Ayuda de los productos haciendo clic en "Acerca de", o bien, se pueden seguir las instrucciones presentadas en este artículo de la Base de Conocimiento de ESET: http://soporte.eset-la.com/kb3040/

Además, dentro del Menú de Ayuda de los productos incluso se podrá buscar actualizaciones de forma directa desde los servidores de ESET.

Es ideal que luego de esta prueba se pueda comprobar que se cuenta con la última versión disponible en el mercado (6.x).

MAXIMIZAR LOS NIVELES DE PROTECCION

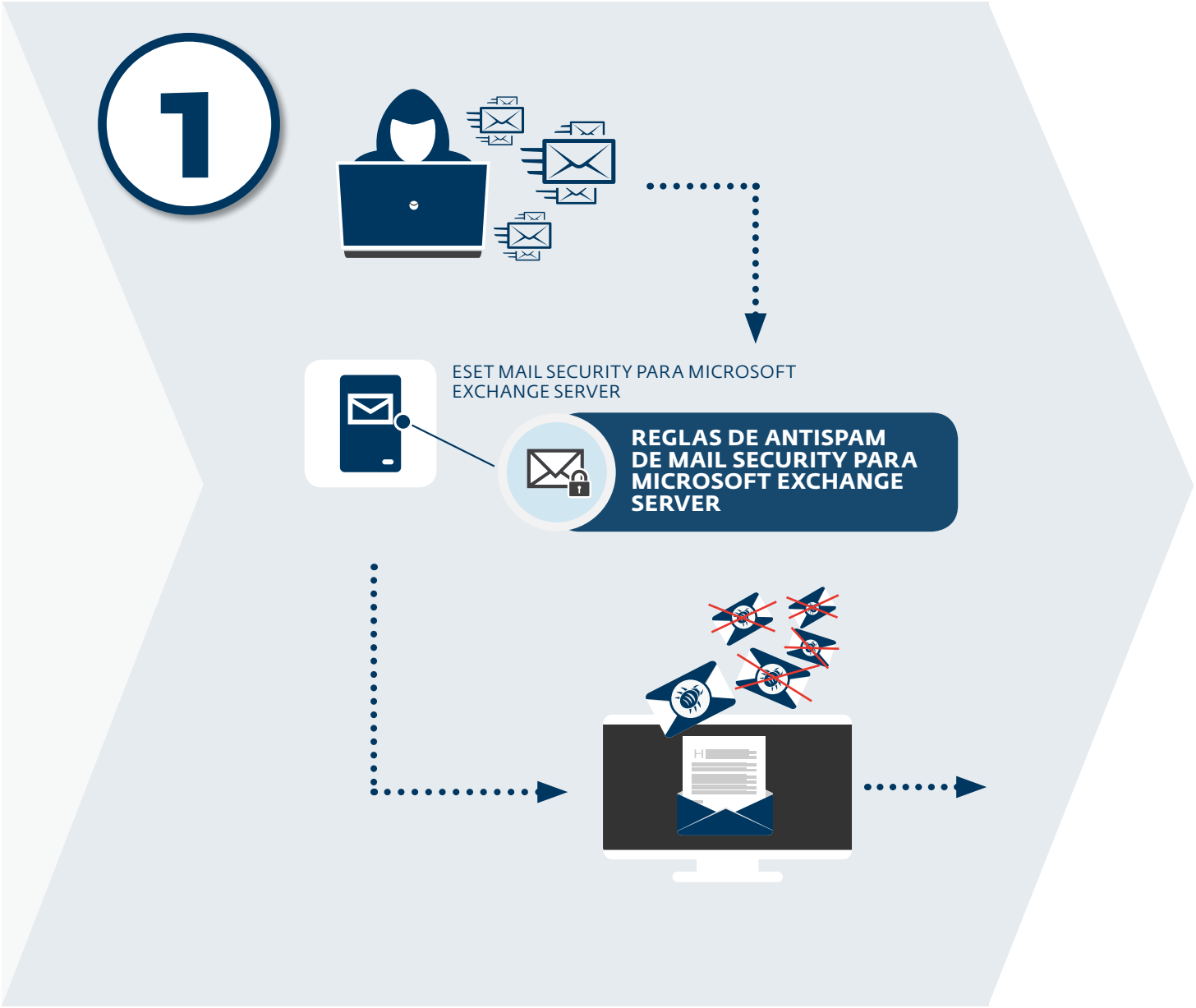
A continuación se listarán una serie de opciones o estados a revisar para asegurarse que se tiene la mejor configuración posible:

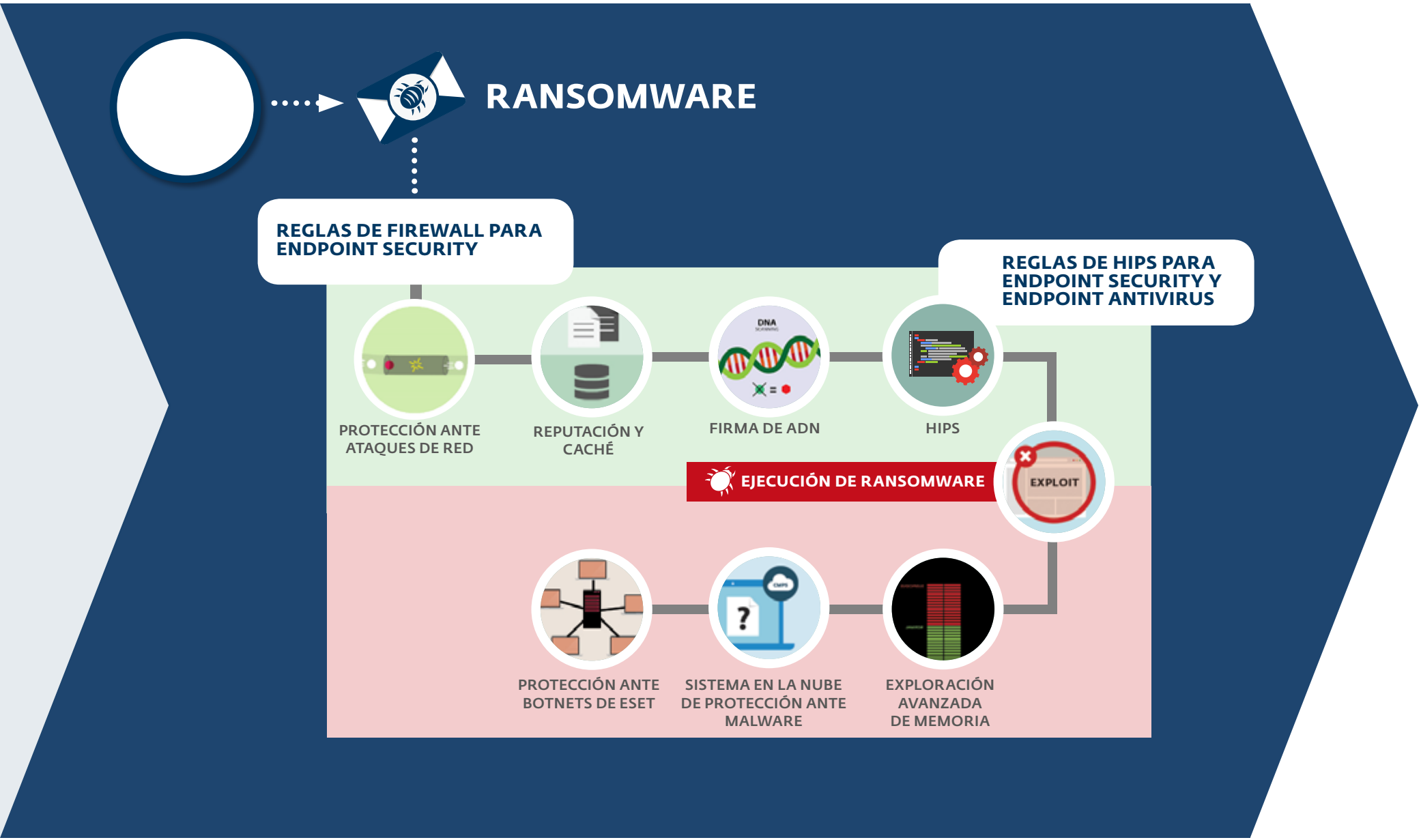
- Asegurarse que se encuentra la última base de firmas instalada y que se están realizando las actualizaciones correctamente.
- Asegurarse que esté activo el módulo Advance Memory Scanner dentro de la configuración del producto.
- Asegurarse que esté activo y funcional ESET LiveGrid, ya que las soluciones de ESET utilizan esta funcionalidad para realizar algunos análisis comparando de forma inmediata con la base de malware de ESET en la nube y, de esta manera, se mejora la protección ante el malware nuevo hasta que sea incluido en la próxima base de firmas de virus. Con ESET LiveGrid se puede reducir a minutos la protección ante códigos maliciosos desconocidos, mientras que con la base de firmas tradicional se tardaría algunas horas.
- Una vez que ESET LiveGrid esté activo, también se recomienda asegurarse que la detección mediante Heurística Avanzada también se encuentre activa.
- Asegurarse que no hay ningún tipo de exclusión de archivos o sitios web dentro del producto. Idealmente no se recomienda utilizar exclusiones salvo que sea alguna excepción puntual y necesaria, y que también se encuentre muy bien documentada.
- Asegurarse que los productos cuenten con una protección con contraseña, con el objetivo de que los usuarios no puedan modificar ninguna configuración del producto.

CONFIGURACIÓN DE ESET ANTI-RANSOMWARE PARA EMPRESAS

Al bloquear el método de infección del ransomware (utilizando un dropper de JavaScript), los ajustes adicionales de nuestra configuración de ESET Anti-Ransomware evitan que el malware inicie la descarga. Como este enfoque demostró ser muy eficiente, decidimos explicar los ajustes adicionales en detalle en este informe técnico y ofrecerlos como una configuración de políticas que usted podrá descargar e implementar con nuestro sistema ESET Remote Administrator.

DESCARGUE LA CONFIGURACIÓN DESDE AQUÍ


1
ESET MAIL SECURITY PARA MICROSOFT EXCHANGE SERVER
REGLAS DE ANTISPAM DE MAIL SECURITY PARA MICROSOFT EXCHANGE SERVER

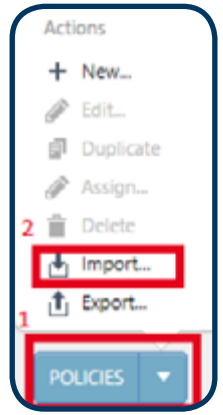

RANSOMWARE
REGLAS DE FIREWALL PARA ENDPOINT SECURITY
REGLAS DE HIPS PARA ENDPOINT SECURITY Y ENDPOINT ANTIVIRUS
PROTECCIÓN ANTE ATAQUES DE RED
REPUTACIÓN Y CACHÉ
DNA
FIRMA DE ADN
HIPS
EJECUCIÓN DE RANSOMWARE
EXPLOIT
PROTECCIÓN ANTE BOTNETS DE ESET
SISTEMA EN LA NUBE DE PROTECCIÓN ANTE MALWARE
EXPLORACIÓN AVANZADA DE MEMORIA

REGLAS DE ANTISPAM PARA ESET MAIL SECURITY PARA MS EXCHANGE SERVER

Al utilizar las reglas correctas de antispam, los mensajes entrantes de correo electrónico ya se están filtrando en el mismo servidor de correo. Esto garantiza que el archivo adjunto con el dropper malicioso no se entregará en el buzón del usuario final y que el ransomware no tendrá oportunidad de ejecutarse.

Cómo importar y aplicar las políticas*

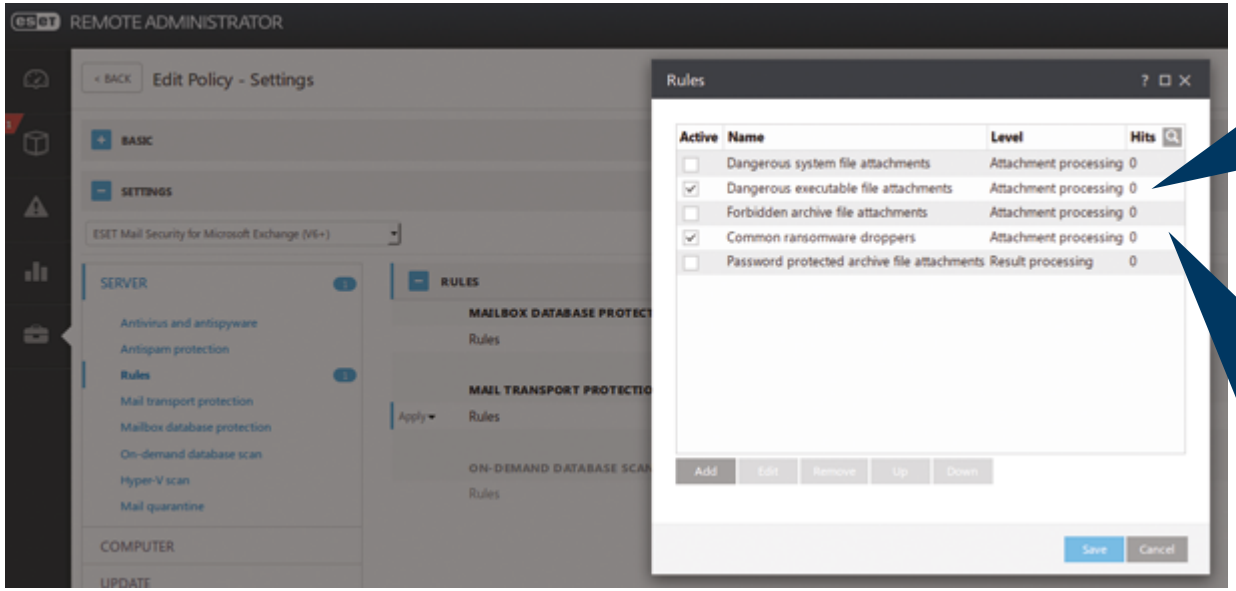
1. Inicie sesión en la Consola Web ERA 6
2. Vaya a Administrador > Políticas
3. A continuación, elija "Políticas" y luego "Importar"
4. Importe las políticas de a una por vez
5. Configure las políticas para un *grupo* o *cliente*

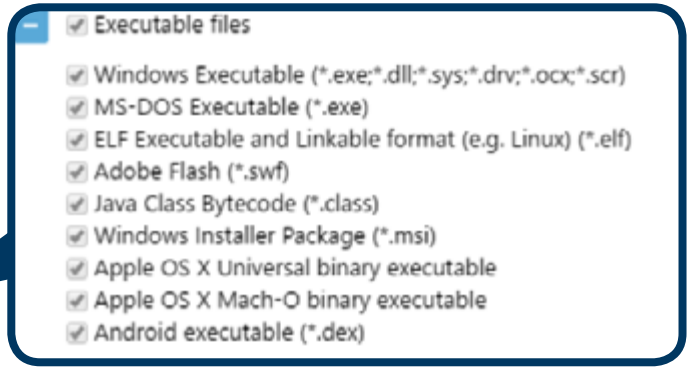


*** No es necesario repetir para otras configuraciones.**

Importante:

Actualice ESET Mail Security para Microsoft Exchange Server a la última compilación disponible 6.3.x o posterior para asegurar el funcionamiento correcto de las reglas de filtrado.





Droppers comunes de ransomware que bloequean las siguientes extensiones*:

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

* En este caso **también se bloquearán los archivos de Microsoft Office con Macros (docm, xlsm, pptm)**. Si en su área se utilizan estos tipos de archivo, será necesario ajustar la configuración de la regla o desactivarla

REGLAS DE FIREWALL PARA ENDPOINT SECURITY

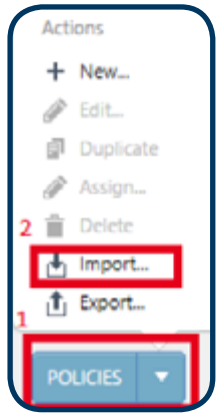
Aunque se llegue a ejecutar el dropper con código malicioso, ESET Endpoint Security igualmente impedirá la descarga de malware debido al firewall integrado.

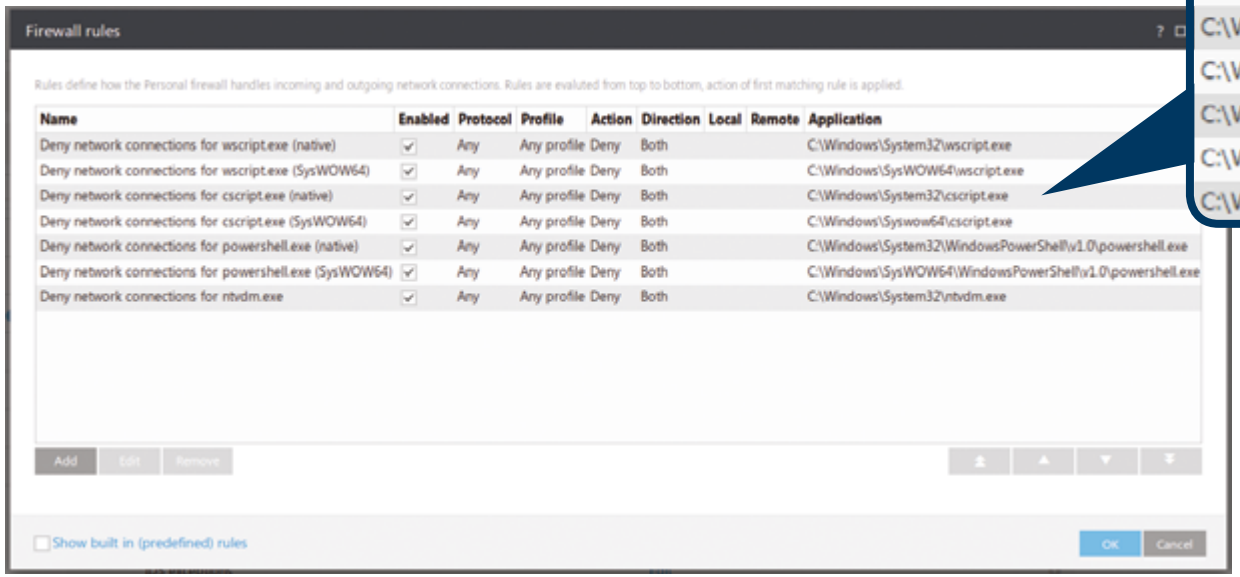
Al aplicar estas reglas de firewall, ESET Endpoint Security bloqueará la descarga de payloads maliciosos y denegará cualquier otro acceso de comandos de script a Internet.

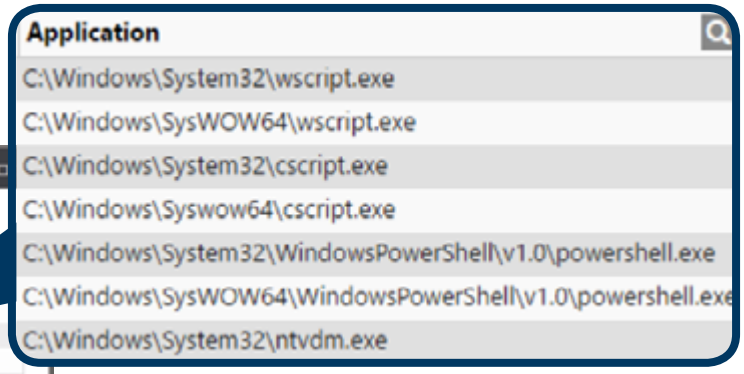
Cómo importar y aplicar las políticas

1. Inicie sesión en la Consola Web ERA 6
2. Vaya a Administrador > Políticas
3. A continuación, elija "Políticas" y luego "Importar"
4. Importe las políticas de a una por vez
5. Configure las políticas para un grupo o cliente

Recuerde que, al importar las reglas de firewall, se pueden sobrescribir otras reglas.







IMPORTANTE

- Esta política solo funciona en combinación con ESET Endpoint Security por el módulo de firewall integrado.
- Sin embargo, hay que tener en cuenta que algunas aplicaciones legítimas pueden usar los ejecutables. Por ello, recomendamos que pruebe la política antes de implementarla plenamente en su área.

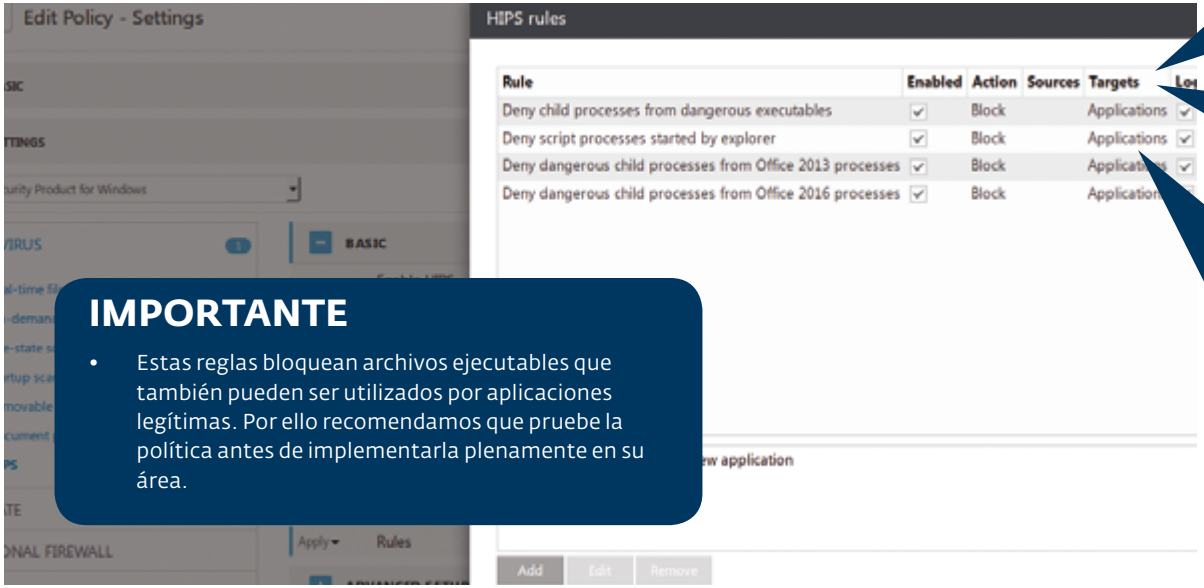
REGLAS DE HIPS PARA ENDPOINT SECURITY Y ENDPOINT ANTIVIRUS

Nuestro Sistema de prevención de intrusiones basado en host (HIPS) defiende el sistema desde dentro y es capaz de interrumpir las acciones no autorizadas en los procesos antes de que se lleguen a ejecutar. Al prohibir la ejecución estándar de JavaScript y de otros scripts, el ransomware no tiene ninguna oportunidad de ejecutar malware, menos aún de descargarlo.

Nuestro sistema HIPS también es parte de ESET File Security para Windows Server, por lo que es aplicable a los servidores. Tenga en cuenta que el sistema HIPS no distingue los scripts legítimos que se inician en áreas de producción.

Cómo importar y aplicar las políticas

1. Inicie sesión en la Consola Web ERA 6
2. Vaya a Administrador > Políticas
3. A continuación, elija "Políticas" y luego "Importar"
4. Importe las políticas de a una por vez
5. Configure las políticas para un *grupo* o *cliente*



Denegar procesos secundarios provenientes de 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 procesos de script iniciados por Explorer.

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

Denegar procesos secundarios peligrosos provenientes 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 archivos ejecutables que también pueden ser utilizados por aplicaciones legítimas. Por ello recomendamos que pruebe la política antes de implementarla plenamente en su área.

RESULTADOS DE LAS PRUEBAS DE CONFIGURACIÓN DE ESET ANTI-RANSOMWARE

Con una configuración completa de ESET Anti-Ransomware desde el servidor de correo electrónico hasta las endpoints e incluso los servidores, los correos electrónicos de ransomware con droppers en archivos adjuntos quedarán excluidos por los filtros antes de que se detecten como código malicioso o ransomware. Además, en las endpoints donde se aplicaron estos ajustes reforzados, hemos llevado a cabo varias pruebas en las que desactivamos todas las capas de detección de las soluciones de seguridad de ESET, lo que demuestra que estos tipos de ransomware no tienen ninguna posibilidad de cifrar el sistema ni la red.

Como conclusión, podemos decir que esta configuración de ESET Anti-Ransomware para fortalecer las soluciones de seguridad de ESET reduce al mínimo el riesgo de infección con ransomware así como el cifrado de los datos corporativos valiosos.