

Mejores prácticas para combatir una amenaza Ransomware

Qué es un Ransomware

Un Ransomware es un malware que se instala en estaciones de trabajo y servidores, sin que los usuarios se den cuenta, ejecutando un ataque criptoviológico que encripta o cifra la información y exigiendo un pago de rescate al usuario para restaurarlo y recuperar sus datos.

El Ransomware puede cifrar desde el Master File Table (MFT) o el disco rígido completo hasta unidades de disco externo o pendrives, conectados a la estación de trabajo. Por lo tanto, impide que los usuarios tengan acceso a los archivos ya que resulta imposible descifrarlos sin una clave. Los ataques Ransomware se llevan a cabo usando un troyano disfrazado como un archivo legítimo.

Cómo ingresa un Ransomware

El Ransomware puede llegar a estaciones de trabajo o servidores de dos formas:

- **A través de la ejecución de los archivos adjuntos en correos electrónicos:** Estos correos electrónicos maliciosos pueden aparentar tener documentos adjuntos legítimos, pero una vez abiertos, el equipo está en riesgo de infectarse con malware.
- **A través de ciertos sitios web:** estos pueden ser sitios web maliciosos, creados por los delincuentes con el único propósito de infectar a cualquier persona que visita el sitio, o pueden ser sitios web legítimos que han sido comprometidos por los cibercriminales y que se utilizan para propagar malware.

Cómo evitar un ataque Ransomware

- **Mantenga actualizado:**
 - **El sistema antivirus:** Si bien no todas las variantes del Ransomware son detectadas por los antivirus, mantener el antivirus actualizado se considera una buena práctica ya que se van incorporando la mayoría de las variantes conocidas dentro de la categoría de Ransomware.





- **Los parches de seguridad de sistemas operativos:** Mantener los sistemas operativos con los últimos parches de seguridad actualizados permite minimizar los riesgos de ataques sobre vulnerabilidades detectadas. De acuerdo a lo expresado por Microsoft, están trabajando periódicamente en actualizaciones que minimizan los riesgos relacionados con este tipo de malware.
- **La herramienta AntiSpam:** La primera barrera de defensa es el sistema de AntiSpam. Cuentan con herramientas que analizan la “Reputación de URL”, mediante el análisis del contenido de los sitios web de destino, detectando el origen de la amenaza para bloquear software malicioso.
- **Realice campañas de concientización en su empresa:** Es fundamental que los empleados de su organización estén al tanto de cómo funciona y cómo actúa esta amenaza.

El Ransomware ataca en base a dos puntos fundamentales:

1. La mayor parte de los usuarios abren los archivos adjuntos que llegan a su cuenta de mail.
2. Muy pocos usuarios guardan copias de seguridad recientes de sus documentos.

Algunos consejos a tener en cuenta:

- Lea atentamente los mensajes antes de dar OK, ya que es donde se valida la instalación del malware.
 - No acceda a sitios o páginas de internet a través de URLs que se encuentren contenidas en correos electrónicos.
 - Desconfiar de correos sospechosos. Si no son mails que esperamos, no abrir los archivos adjuntos por ninguna razón.
- **Prevenga la ejecución de archivos por políticas (GPO):** Una de las mejores practicas recomendadas, no solo para evitar ransomware, sino también para evitar la infección de otros malwares o virus es la creación de políticas para bloqueo y ejecución de archivos en carpetas de sistemas. Microsoft permite de manera centralizada verificar la ejecución y aplicación de las políticas definidas en cada uno de los recursos. Reporte conocido como “Resultant Set of Policy”.





- **Mantenga un cronograma de backup periódico:** Mantener un esquema de backup periódico nos garantiza poder recuperar la información a un punto en el tiempo anterior a la infección. Teniendo en cuenta que el sistema de encriptación utilizado es de 1024 bits, técnicamente es imposible recuperar los archivos encriptados a su estado original en un tiempo razonable si no hay backup.
- **Cuente con soporte profesional del proveedor de seguridad:** Comuníquese con el soporte técnico de NextVision por cualquier duda o consulta a soporte@nextvision.com.

Cómo puede Symantec Endpoint Protection y el equipo de soporte de NV ayudar a prevenir el ingreso de esta amenaza

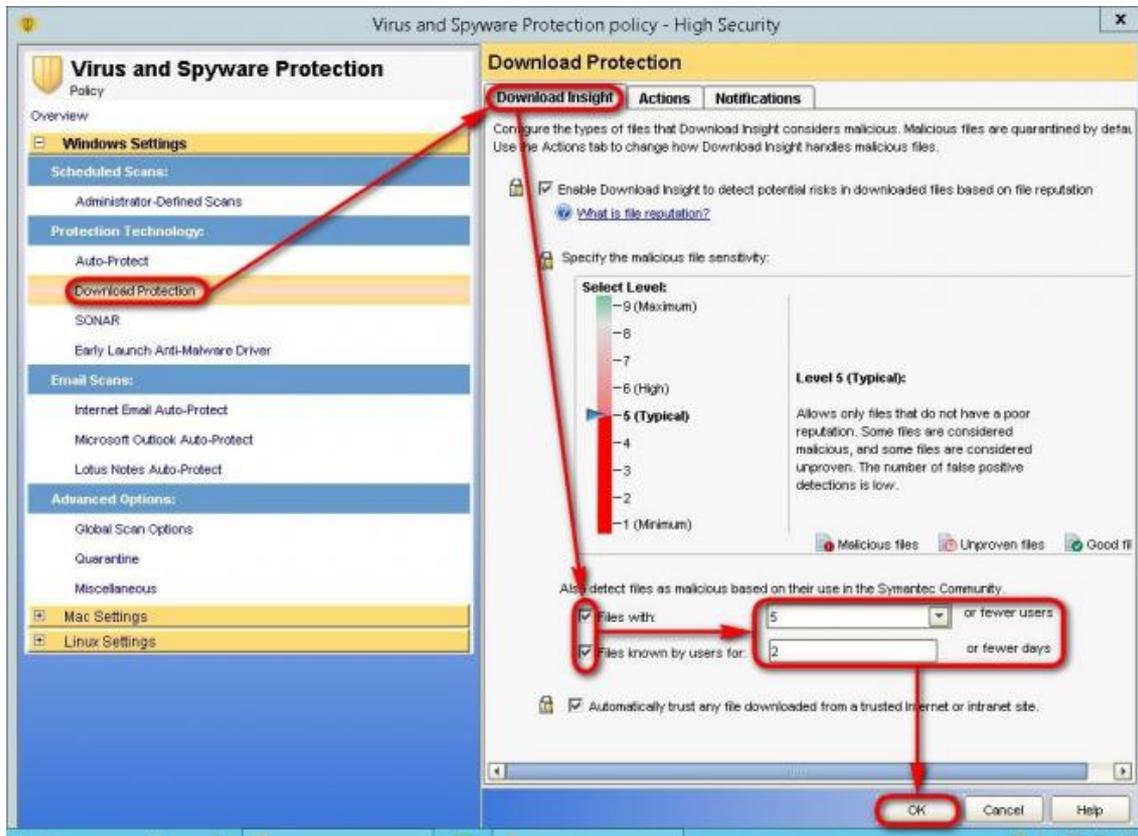
Implemente y habilite las siguientes protecciones:

DOWNLOAD INSIGHT

Para una protección adicional de las nuevas variantes Ransomware, la política de "alta seguridad" puede ser editada y la característica Download Protection puede ser modificada para actuar sobre los archivos que la base de clientes de Symantec aún no ha probado que sean seguros.

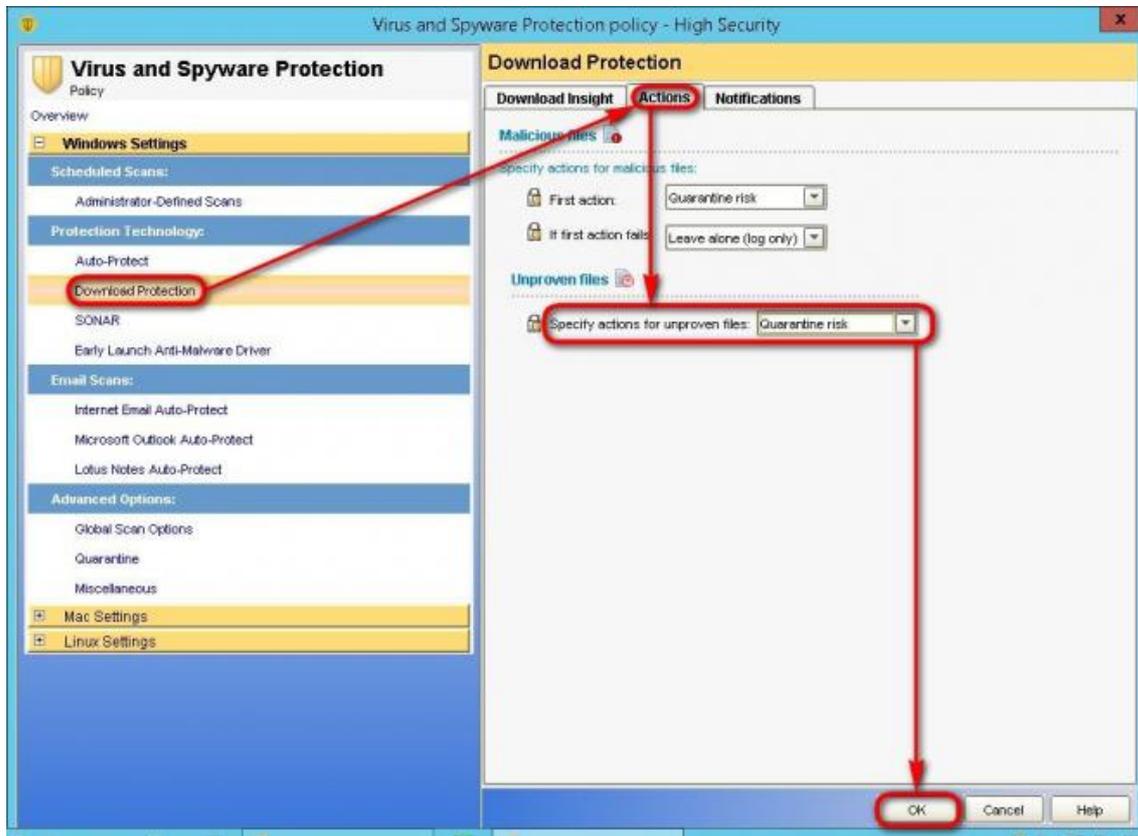
Las opciones que tendrían que ser configuradas se encuentran en "Download Protection" - "Download Insight" - también detecta archivos maliciosos en función de su uso en la Comunidad Symantec. Activación de las dos casillas de verificación junto a "Files with" y "Files known by users for:" y el uso de los valores por defecto de 5 y 2, respectivamente, obligará al cliente SEP a tratar cualquier archivo que no ha sido reportado a Symantec por más de 5 usuarios o han sido reportados durante menos de 2 días para ser tratados como archivos no comprobados.





El manejo de estos archivos se encuentra en la pestaña "Actions" en "Unproven Files" y el ajuste de "Specify actions for unproven files:" debe ser modificado en "Quarantine risk".





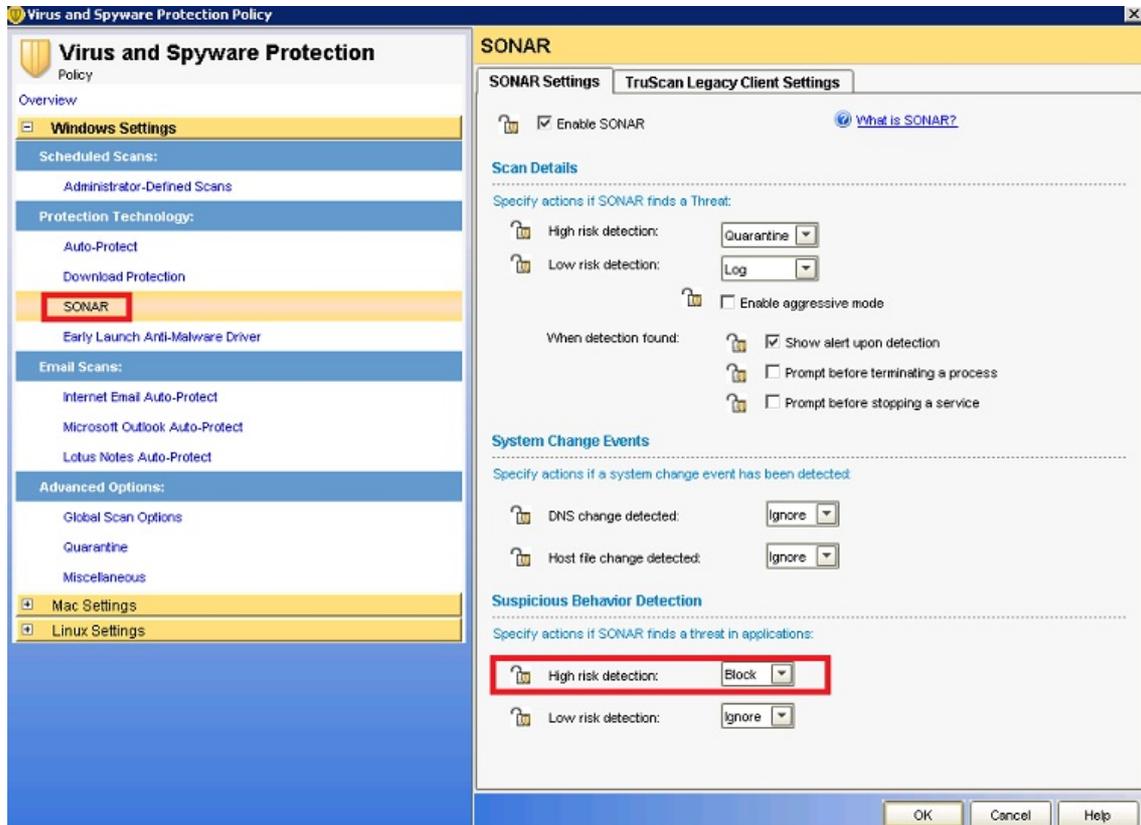
SONAR

SONAR es una protección en tiempo real que detecta aplicaciones potencialmente maliciosas cuando se ejecutan en los equipos. Ofrece protección "**día cero**", ya que detecta las amenazas antes que se hayan creado las definiciones de virus para hacer frente a las amenazas.

Esta protección utiliza la heurística, así como los datos de reputación para detectar amenazas emergentes y desconocidas. Proporciona un nivel adicional de protección en los equipos cliente y complementa al antivirus existente, protección contra programas espía, prevención de intrusiones y protección de firewall.

Recomendamos configurar **SONAR** para que bloquee amenazas detectadas en aplicaciones.





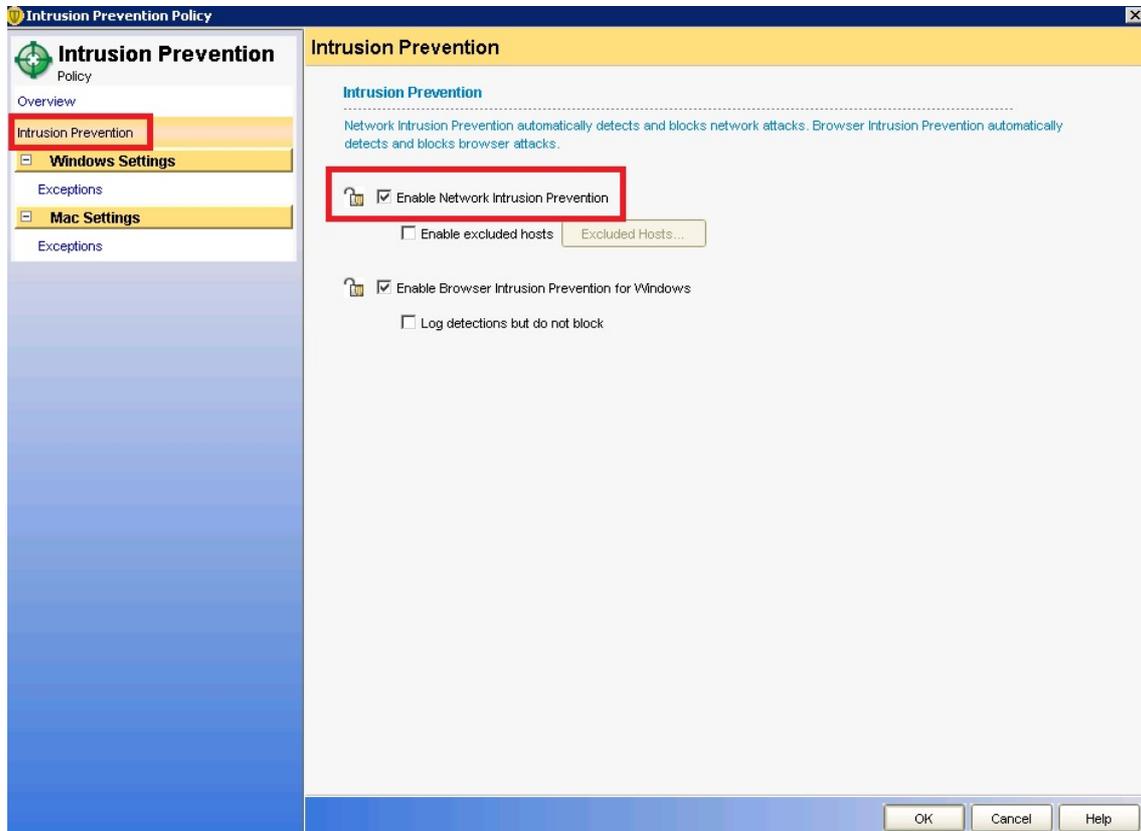
APPLICATION AND DEVICE CONTROL

Los usuarios de Symantec Endpoint Protection pueden aprovechar políticas de Application and Device Control para evitar que los archivos se ejecuten en la raíz y / o subcarpetas del directorio de los usuarios %AppData%. La política impide intentos de ejecución de archivos que han sido extraídos de los formatos de compresión, de ejecución automática, el acceso a los archivos de comandos y la ejecución de archivos de volúmenes extraíbles.

INTRUSION PREVENTION SYSTEM

IPS bloquea algunas amenazas que las definiciones de virus tradicionales por sí solas no pueden parar. IPS es la mejor defensa contra las descargas no autorizadas, que se producen cuando el software se descarga involuntariamente de Internet. Los atacantes a menudo usan paquetes de exploits para entregar un ataque basado en la web a través de una descarga dirigida.





El Departamento Técnico de NextVision cuenta con políticas creadas que podrán encontrar una política de Antivirus y una de Application and Device Control preparadas para combatir un Ransomware. Las mismas pueden ser importadas a su consola administradora y ser aplicadas a los grupos que se desee. Para solicitar estas políticas, envíe un mail a sosporte@nextvision.com

NOTA: En ningún caso deben ser utilizadas en producción sin un previo testeo en ambiente de laboratorio ya que dependiendo de las aplicaciones que cada cliente utiliza pueden generar un bloqueo no deseado.





¿Cómo eliminar un Ransomware?

No hay herramienta de eliminación de ransomware. Si sus equipos se infectan y sus datos se cifran, siga estos pasos:

1. **No pague el rescate.**

Si paga el rescate:

- No hay garantía de que el atacante vaya a suministrar un método para desbloquear su equipo o para descifrar sus archivos.
- El atacante usa el dinero del rescate para financiar ataques adicionales contra otros usuarios.

2. **Aísle el equipo infectado antes de que el ransomware pueda atacar las unidades de red a las cuales tiene acceso.**

3. **Utilice Symantec Endpoint Protection Manager para actualizar las definiciones de virus y analizar los equipos cliente.**

Las nuevas definiciones pueden detectar y reparar los ransomlockers. Las definiciones de virus de Symantec Endpoint Protection Manager descargan automáticamente definiciones de virus al cliente, siempre que el cliente esté administrado y conectado a Symantec Endpoint Protection Manager.

En Symantec Endpoint Protection Manager, haga clic en **Clientes**, haga clic con el botón derecho en el grupo y haga clic en **Ejecutar un comando en el grupo > Actualizar contenido y analizar**.

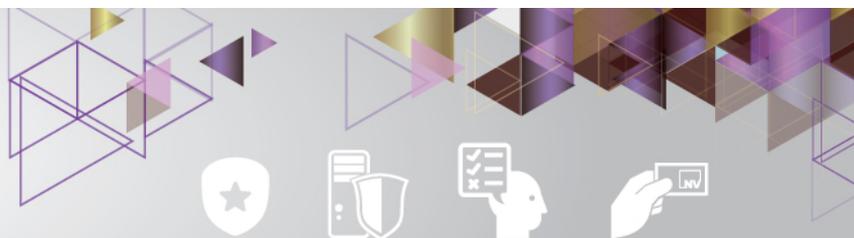
4. **Restablezca archivos dañados de una copia de seguridad de buena reputación**

Como otros productos de seguridad, Symantec Endpoint Protection no puede descifrar los archivos que los ransomlockers han saboteado.

5. **Envíe el software malicioso a NextVision.**

Si puede identificar el correo electrónico o el archivo ejecutable malicioso, envíelo a nuestro equipo de soporte. Nuestra comunicación directa con el soporte de Symantec permiten crear nuevas firmas y mejorar las defensas contra el Ransomware.





Tecnología que integramos:



Acerca de NextVision: Desde 1990 integramos Seguridad con soluciones de Tecnología, mediante servicios profesionales especializados, para que la información de nuestros clientes esté siempre protegida y disponible. Desarrollamos proyectos en diferentes mercados – como Banca y Finanzas, telecomunicaciones, Oil & Gas y Servicios, entre otros – y para diversas organizaciones de gobierno, tanto en Argentina como en América Latina y Europa. Para más información, ingresar a www.nextvision.com

