Nuevas víctimas de ransomware en España – Ryuk

Cómo protegerse con soluciones Stormshield

Índice

Contexto

Nuevas víctimas de ransomware en España

Tras la campaña masiva de ransomware en España a principios de noviembre, la compañía de seguridad Prosegur también ha sufrido un ataque de ransomware que le ha obligado a parar su red para mitigar la infección.

¿Un nuevo caso de ataque de ramsomware dirigido?

El ransomware Ryuk que ha infectado a Prosegur se conoce desde agosto de 2018. Según algunos análisis de la comunidad de ciberseguridad, Ryuk se ha utilizado exclusivamente en ataques dirigidos, y ha impactado ya a más de 100 organizaciones en todo el mundo.

Una prueba más de que el ransomware reciente tiende a enfocarse en grandes organizaciones más que en intentar causar el mayor número de víctimas posible.

Cómo protegerse

Stormshield Endpoint Security

Basándonos en nuestro análisis de las versiones conocidas del malware, Stormshield Endpoint Security (SES) puede protegerle de distintas maneras.

Active Honey Pot Protection (HPP)

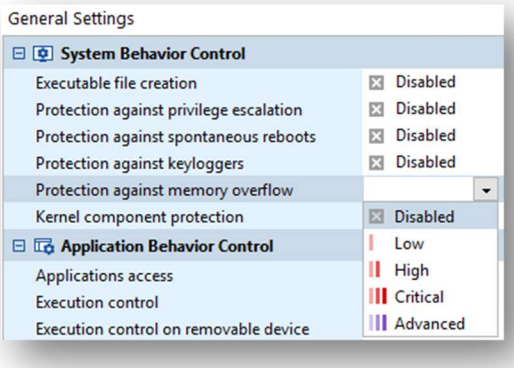
Muchas muestras conocidas de ransomware, incluyendo algunas de Ryuk, son «ficheros empaquetados» que también utilizan técnicas de ofuscación para evitar la detección. La protección "HoneyPot Memory Overflow" de SES 7.2 puede detectar esas técnicas y bloquear la amenaza.

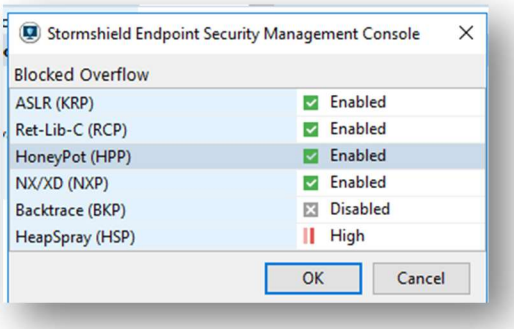
Hay varias maneras de habilitar la protección "HoneyPot Memory Overflow" en SES 7.2:

Desde la consola, abra la Política de Seguridad, seleccione la pestaña **System Behavior**.

La protección HoneyPot Protection (HPP) quedará habilitada si se fija el nivel de **Protection Against Memory Overflow** en «Low» o superior.

Como alternativa, se puede habilitar específicamente la protección HPP seleccionando «**Advanced**» y después habilitando **HoneyPot (HPP)**.

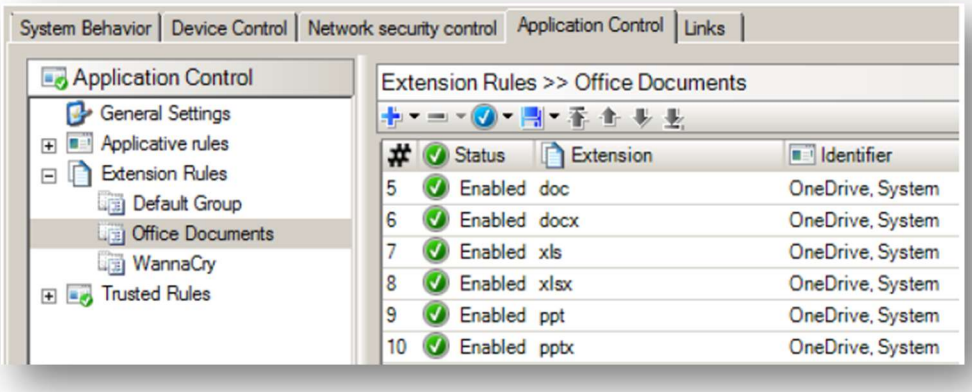




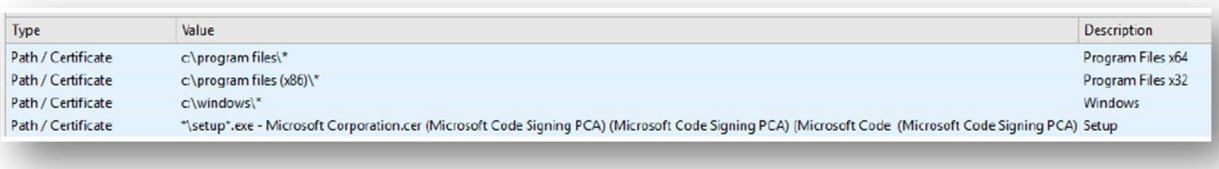
Restrinja el acceso a extensiones de fichero conocidas (especialmente ficheros de Microsoft Office)

Como recordatorio, una protección eficaz contra la mayoría de ransomware: utilice el Control de Aplicaciones de SES para permitir sólo a aplicaciones específicas el acceso a extensiones de ficheros conocidas.

Por ejemplo, para prevenir el acceso de procesos anormales a documentos Microsoft Office, permita sólo a aplicaciones específicas el acceso a documentos Office:



El identificador corresponde a las aplicaciones que están autorizadas a acceder a los archivos con estas extensiones. En este ejemplo, "System" ID corresponde a los siguientes archivos:



Esto puede realizarse por ejemplo para todas las aplicaciones.

NOTA
Estos parámetros deben probarse en su entorno para asegurarse de que no tienen impacto en aplicaciones legítimas.

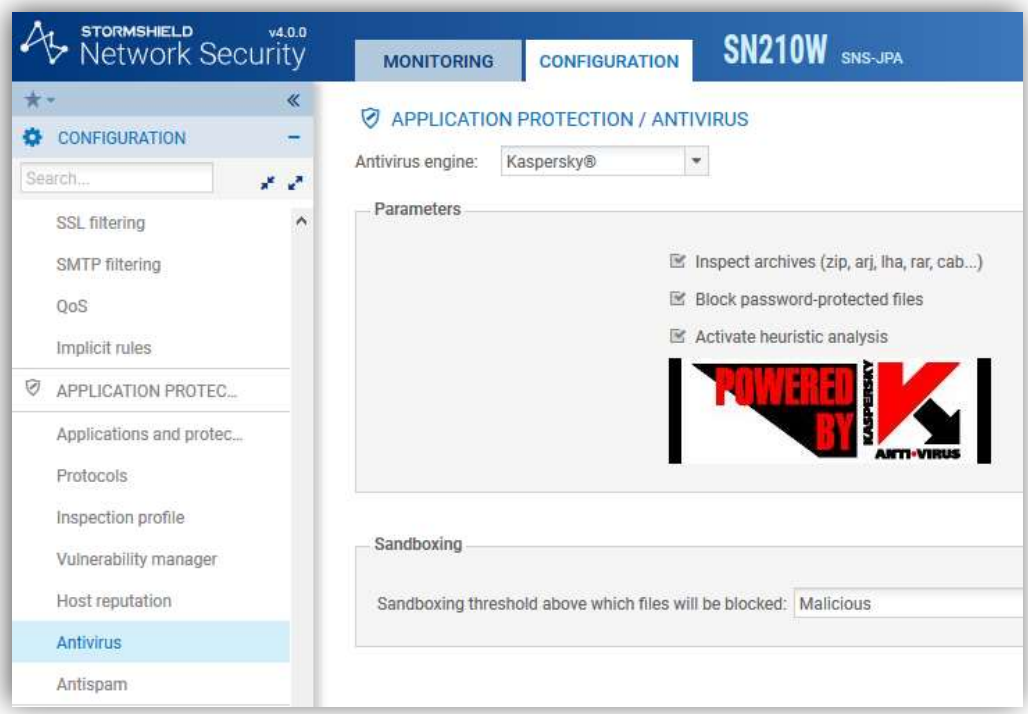
Stormshield Network Security

Breach Fighter sandboxing

Todas las muestras conocidas que han sido analizadas por nuestro equipo de Seguridad son detectadas por Breach Fighter, la solución de sandboxing de Stormshield Network Security:

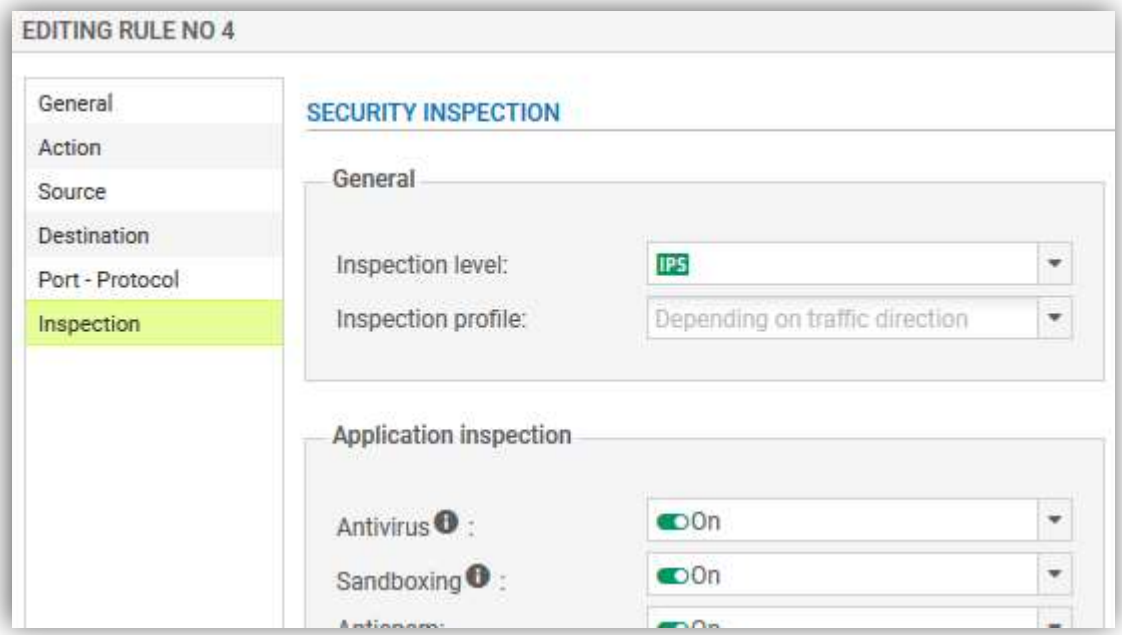
- *https://breachfighter.stormshieldcs.eu/0b1008d91459937c9d103a900d8e134461db27c602a6db5e082ab9139670ccb6*
- *https://breachfighter.stormshieldcs.eu/e75622957decf1594c2cbe726ff0aaba4a509dab7b77721d3db16977f224ae4a*
- *https://breachfighter.stormshieldcs.eu/487d4698c6c938ca3e9251827a5813ddd21e26584b3459d768e457ddd4e8c4d4*
- *https://breachfighter.stormshieldcs.eu/dd0691992d947366f1b9caf2acc1fec951f761a39ca3863e81bc2c3fb5efd415*
- *https://breachfighter.stormshieldcs.eu/fe55650d8b1b78d5cdb4ad94c0d7ba7052351630be9e8c273cc135ad3fa81a75*

Para beneficiarse del análisis de Breach Fighter en su firewall SNS habilite Sandboxing en Application Protection > Antivirus.



El sandboxing está disponible solo cuando el antivirus Kaspersky está habilitado, y debe ser adquirido como un servicio de seguridad adicional.

También compruebe que el análisis de Antivirus y Sandboxing están habilitados en las reglas de seguridad autorizando tráfico de email y web.


EDITING RULE NO 4
General
Action
Source
Destination
Port - Protocol
Inspection
SECURITY INSPECTION
General
Inspection level:
IPS
Inspection profile:
Depending on traffic direction
Application inspection
Antivirus :
On
Sandboxing :
On