ESA FAQ: Los filtros/brote de virus del brote filtran (VOF) el FAQ

Contenido

Introducción

Este documento describe y contesta a algunas de las más preguntas frecuentes con respecto los filtros del brote, o al brote de virus filtra, en el dispositivo de seguridad del correo electrónico (ESA).

¿Cuáles son filtros del brote, o el brote de virus filtra (VOF)?

Los filtros del brote protegen su red contra los brotes de virus en grande y ataques más pequeños, NON-virales, tales como timos del phishing y distribución del malware, pues ocurren. A diferencia de la mayoría del software anti-malware de la Seguridad, que no puede detectar los nuevos brotes hasta que se recojan los datos y se publica una actualización de software, datos de los frunces de Cisco sobre los brotes como separan y envían la información actualizada a su ESA en el tiempo real para evitar que estos mensajes alcancen a sus usuarios.

Cisco utiliza los modelos de tráfico global para desarrollar las reglas que determinan si un mensaje entrante es seguro o parte de un brote. Los mensajes que pueden ser parte de al brote quarantined hasta que se determinen para ser caja fuerte basada en la información actualizada del brote de Cisco o nuevas definiciones del contra virus son publicados por Sophos y el McAfee.

Los mensajes usados en los ataques a escala reducida, NON-virales utilizan un diseño de legítimo-mirada, la información del beneficiario, y la aduana URL que señalan a los sitios web del phishing y del malware que han estado en línea solamente por un período corto y son desconocidos a los Servicios de seguridad de la red. Los filtros del brote analizan un contenido de mensaje y buscan para que los links URL detecten este tipo de ataque NON-viral. Los filtros del

brote pueden reescribir los URL para reorientar el tráfico a los sitios web potencialmente dañinos con un proxy de la Seguridad de la red, que cualquier advierte a los usuarios que el sitio web que están intentando acceder puede ser malévolo o bloquea el sitio web totalmente.

¿Puedo utilizar los filtros del brote incluso si no estoy funcionando con Sophos o el contra virus del McAfee en mi ESA?

Cisco recomienda que usted permite a Sophos o al contra virus del McAfee además de los filtros del brote de virus para aumentar su defensa contra los virus. Sin embargo, VOF puede actuar independientemente sin requerir Sophos o el contra virus del McAfee que se habilitará.

¿Cuándo los filtros del brote quarantine los mensajes?

Un mensaje quarantined cuando contiene el archivo adjunto que encuentra o excede las reglas actuales del brote y por correo a los administradores fijados los umbrales. Cisco publica las reglas actuales del brote a cada ESA que tenga las teclas de función válidas, y en nuestro portal del soporte. Los mensajes que pueden ser parte de al brote quarantined hasta que se determinen para ser caja fuerte basada en la información actualizada del brote de Cisco o nuevas definiciones del contra virus son publicados por Sophos y el McAfee.

La información sobre los brotes de virus actuales se puede encontrar en SenderBase

El sitio web de las operaciones de inteligencia del Cisco Security (SIO) proporciona una lista de amenazas NON-virales actuales, incluyendo el Spam, phishing, y la distribución del malware intenta.

¿Qué sucede cuando la cuarentena del brote se llena?

Cuando una cuarentena excede el espacio máximo afectado un aparato a ella, o si un mensaje excede la configuración del tiempo máximo, los mensajes se podan automáticamente de la cuarentena para guardarla dentro de los límites. Los mensajes se quitan en un primero en entrar, base del primero en salir ((Primero en Entrar, Primero en Salir FIFO)). Es decir los más viejos mensajes se borran primero. Usted puede configurar una cuarentena a la versión (es decir, entregue) o borrar un mensaje que se deba podar de una cuarentena. Si usted elige a los mensajes release, usted puede elegir para tener el asunto marcado con etiqueta con el texto que usted especifica cuál alertará al beneficiario que el mensaje era forzado fuera de una cuarentena.

La versión de siguiente de la cuarentena del brote, los mensajes es pre-explorada por el módulo del contra virus, y medidas se toman según la directiva antivirus. Dependiendo de esta directiva, un mensaje se puede entregar, borrar, o entregar con las conexiones virales eliminadas. Se espera que los virus sean encontrados a menudo durante la pre-exploración después de la versión de la cuarentena del brote. Los mail_logs ESA o Seguimiento de mensajes se pueden consultar para determinar si un mensaje individual que fue observado en la cuarentena fueron

encontrados para ser viral, y si y cómo él fue entregado.

Antes de que una cuarentena del sistema se llene, se envía una alerta cuando la cuarentena alcanza el 75% lleno, y se envía otra alerta cuando alcanza el 95% lleno. La cuarentena del brote tiene una función de administración adicional que permita que usted borre o que libere todos los mensajes que hagan juego un nivel determinado de la amenaza del virus (VTL). Esto permite el claro fácil de la cuarentena después de que se reciba una actualización del contra virus que dirige una amenaza determinada del virus.

¿Cuál es el significado de la amenaza llana para una regla del brote?

Los filtros del brote actúan bajo niveles de la amenaza entre 0 y 5. El nivel de la amenaza valora la probabilidad de un brote viral. De acuerdo con el riesgo de un brote viral, el nivel de la amenaza influencia quarantining de los archivos sospechosos. El nivel de la amenaza es basado en varios factores, incluyendo pero no sólo el tráfico de la red, la actividad de archivo sospechosa, la entrada de los vendedores del contra virus, y el análisis por el centro de operaciones de la amenaza de Cisco. Además, los filtros del brote permiten que los administradores del correo aumenten o disminuyan el impacto de los niveles de la amenaza para sus redes.

'Nivel'	Riesgo	Significado
0	Ninguno	No hay riesgo que el mensaje es una amenaza.
1	Bajo	El riesgo que el mensaje es una amenaza es bajo.
2	Bajo/media	El riesgo que el mensaje es una amenaza es bajo al media. ¿Es a? ¿sospechado? amenaza.
3	Medio	O el mensaje es parte de al brote confirmado o hay un media al riesgo grande de su contenido que es una amenaza.
4	Alto	O el mensaje se confirma para ser parte de al brote del gran escala o su contenido es peligroso.
5	Extremo	¿El mensaje? el contenido s se confirma a la parte de un brote que sea extremadamer gran escala o gran escala y extremadamente peligroso.

¿Cómo puedo ser alertado cuando ocurre un brote de virus?

Cuando la red de SenderBase eleva un VTL para un tipo determinado de perfil del mensaje, usted puede ser alertado vía un correo electrónico enviado a su dirección de correo electrónico alerta configurada. Cuando un VTL baja debajo de su umbral configurado, se envía otra alerta. Usted puede monitorear así el progreso del virus. Para asegurarle recibirá estas alertas, verifica la dirección de correo electrónico que las alertas estén enviadas en al CLI usando el comando del **alertconfig**.

Para configurar, o confirugation del reivew

- GUI: Los Servicios de seguridad > los filtros del brote y revisan la configuración bajo **configuraciones globales del editar…**
- CLI: **outbreakconfig > puesto**

Ex.

```
> outbreakconfig

Outbreak Filters: Enabled

Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.
- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.
[]> setup

Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above
or back down below), meaning that new messages of certain types could be quarantined
or will no longer be
quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]> y

What is the largest size message Outbreak Filters should scan?
[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system. You must use the
'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable
Outbreak Filters for the desired Incoming and Outgoing Mail Policies.
```

Un nuevo brote de virus primero será detectado por SenderBase y VTL será elevado. Usted recibirá una alerta si el VTL resuelve o excede su umbral configurado VTL. Las alertas de Sophos seguirán como se identifica y se captura el virus, y cuando el nuevo virus que identifica las firmas está disponible.

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems