ESA FAQ: A manifestação dos filtros/vírus da manifestação filtra (VOF) o FAQ

Índice

Introdução

Este documento descreve e responde a algumas de mais perguntas mais frequentes em relação aos filtros da manifestação, ou aos filtros da manifestação do vírus, na ferramenta de segurança do email (ESA).

Que são filtros da manifestação, ou a manifestação do vírus filtra (VOF)?

Os filtros da manifestação protegem sua rede das manifestações em grande escala do vírus e menores, NON-viral atacam, como embustes do phishing e distribuição do malware, porque ocorrem. Ao contrário da maioria de software de segurança do anti-malware, que não pode detectar manifestações novas até que os dados estiverem recolhidos e uma atualização de software estiver publicada, dados dos recolhimentos de Cisco em manifestações como espalham e enviam a informação atualizadas a seu ESA no tempo real impedir que estas mensagens alcancem seus usuários.

Cisco usa testes padrões de tráfego global para desenvolver as regras que determinam se um mensagem recebida é seguro ou parte de uma manifestação. As mensagens que podem ser parte de uma manifestação quarantined até que estejam determinadas ser cofre forte baseado na informação actualizado da manifestação de Cisco ou definições anti-vírus novas são publicadas por Sophos e pela McAfee.

As mensagens usadas nos ataques em escala reduzida, NON-virais usam um projeto devista, a informação do receptor, e o costume URL que apontam aos Web site do phishing e do malware

que foram em linha somente por um curto período de tempo e são desconhecidos aos Serviços de segurança da Web. Os filtros da manifestação analisam um índice de mensagem e procuram-no pelos links URL para detectar este tipo de ataque NON-viral. Os filtros da manifestação podem reescrever URL para reorientar o tráfego aos Web site potencialmente nocivos com um proxy da Segurança da Web, que um ou outro advirta os usuários que o Web site que estão tentando alcançar pode ser malicioso ou obstrua o Web site completamente.

Posso eu usar filtros da manifestação mesmo se eu não estou executando Sophos ou a McAfee anti-vírus em meu ESA?

Cisco recomenda que você permite Sophos ou a McAfee anti-vírus além do que filtros da manifestação do vírus de aumentar sua defesa contra vírus. Contudo, VOF pode operar-se independentemente sem exigir Sophos ou a McAfee anti-vírus ser permitido.

Quando os filtros da manifestação quarantine mensagens?

Uma mensagem quarantined quando contém o anexo de arquivos que encontra ou excede as regras atuais da manifestação e pelo correio os administradores ajustados pontos iniciais. Cisco publica regras atuais da manifestação a cada ESA que tem uma chave de recurso válida, e em nosso portal do apoio. As mensagens que podem ser parte de uma manifestação quarantined até que estejam determinadas ser cofre forte baseado na informação actualizado da manifestação de Cisco ou definições anti-vírus novas são publicadas por Sophos e pela McAfee.

A informação sobre manifestações atuais do vírus pode ser encontrada em SenderBase

O Web site das operações secretas do Cisco Security (SIO) fornece uma lista de ameaças NON-virais atuais, incluindo o Spam, phishing, e a distribuição do malware tenta.

Que acontece quando a quarentena da manifestação se enche acima?

Quando uma quarentena excede o espaço máximo atribuído a ela, ou se uma mensagem excede o ajuste do tempo máximo, as mensagens estão podadas automaticamente da quarentena para mantê-la dentro dos limites. As mensagens são removidas em um first in, base do first-out (FIFO, primeiro a entrar, primeiro a sair) (FIFO). Ou seja as mensagens as mais velhas são suprimidas primeiramente. Você pode configurar uma quarentena à liberação (isto é, entregue) ou suprimir de uma mensagem que deva ser podada de uma quarentena. Se você escolhe aos mensagens release, você pode eleger para ter a linha de assunto etiquetada com o texto que você especifica qual alertará o receptor que a mensagem era forçada fora de uma quarentena.

A liberação de seguimento da quarentena da manifestação, mensagens é tornada a varrer pelo módulo anti-vírus, e a ação é tomada de acordo com a política anti-vírus. Segundo esta política, uma mensagem pode ser entregada, suprimido, ou entregado com os acessórios virais descascados. Espera-se que os vírus estarão encontrados frequentemente durante a nova

varredura após a liberação da quarentena da manifestação. Os mail_logs ou o rastreamento de mensagem ESA podem ser consultados para determinar se uma mensagem individual que seja notada na quarentena foram encontrados para ser viral, e se e como ele foi entregado.

Antes que uma quarentena do sistema se encha acima, um alerta está enviado quando a quarentena alcança 75% completo, e um outro alerta está enviado quando alcança 95% completo. A quarentena da manifestação tem uns recursos de gerenciamento adicionais que permitam que você suprima ou libere de todas as mensagens que combinam um nível particular da ameaça do vírus (VTL). Isto permite o esclarecimento fácil da quarentena depois que uma atualização anti-vírus é recebida que enderece uma ameaça particular do vírus.

Que é o significado da ameaça em nível para uma regra da manifestação?

Os filtros da manifestação atuam sob níveis da ameaça entre 0 e 5. O nível da ameaça avalia a probabilidade de uma manifestação viral. Baseado no risco de uma manifestação viral, o nível da ameaça influencia quarantining de arquivos suspeitos. O nível da ameaça é baseado em um número de fatores, incluindo mas não limitado ao tráfego de rede, à atividade de arquivo suspeito, à entrada dos vendedores anti-vírus, e à análise pelo centro de operações da ameaça de Cisco. Além, os filtros da manifestação permitem que os administradores do correio aumentem ou diminuam o impacto de níveis da ameaça para suas redes.

Nível	Risco	Significado
0	Nenhum	Não há nenhum risco que a mensagem é uma ameaça.
1	Baixa	O risco que a mensagem é uma ameaça é baixo.
2	Baixo/media	O risco que a mensagem é uma ameaça é baixo ao media. É a? suspeitado? ameaça
3	Médio	Ou a mensagem é parte de uma manifestação confirmada ou há um media ao grande de seu índice que está uma ameaça.
4	Alto	Ou a mensagem é confirmada para ser parte de uma manifestação da larga escala ou índice é muito perigoso.
5	Extremo	A mensagem? o índice s é confirmado parte da uma manifestação que seja extremam larga escala ou larga escala e extremamente perigosa.

Como posso eu ser alertado quando uma manifestação do vírus ocorre?

Quando a rede de SenderBase eleva um VTL para um tipo particular de perfil da mensagem, você pode ser alertado através de um mensagem de Email enviado a seu endereço email alerta configurado. Quando um VTL cai abaixo de seu limiar configurado, um outro alerta está enviado. Você pode assim monitorar o progresso do vírus. Para assegurá-lo receberá estes alertas, verifica o endereço email que os alertas estão enviados no CLI usando o comando do **alertconfig**.

Para configurar, ou confirugation do reivew

- GUI: Os Serviços de segurança > os filtros da manifestação e reveem a configuração sob as **configurações globais da edição…**

- CLI: **outbreakconfig > setup**

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.
```

Uma manifestação nova do vírus será detectada primeiramente por SenderBase e VTL será elevado. Você receberá um alerta se o VTL encontra ou excede seu ponto inicial configurado VTL. Os alertas de Sophos seguirão como o vírus está identificado e capturado, e quando o vírus novo que identifica assinaturas se torna disponível.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems