FOIRE AUX QUESTIONS ESA : Les filtres d'épidémie/attaque de virus filtre la Foire aux questions (VOF)

Contenu

Introduction

Ce document décrit et répond à certains de plus de forums aux questions concernant des filtres d'épidémie, ou l'attaque de virus filtre, sur l'appliance de sécurité du courrier électronique (ESA).

Quels sont des filtres d'épidémie, ou l'attaque de virus filtre-t-elle (VOF) ?

Les filtres d'épidémie protègent votre réseau contre des attaques de virus de grande puissance et plus petits, non viral attaque, comme des escroqueries de phishing et la distribution de malware, car ils se produisent. À la différence de la plupart de logiciel de sécurité d'anti-malware, qui ne peut pas détecter de nouvelles épidémies jusqu'à ce que des données soient collectées et une mise à jour logicielle est éditée, données de rassemblements de Cisco sur des épidémies comme ils se propagent et envoient les informations mises à jour à votre ESA en temps réel d'empêcher ces messages d'atteindre vos utilisateurs.

Cisco emploie les structures de trafic globales pour développer les règles qui déterminent si un message entrant est sûr ou une partie d'une épidémie. Des messages qui peuvent faire partie d'une épidémie sont mis en quarantaine jusqu'à ce qu'ils soient déterminés pour être coffre-fort basé sur les informations mises à jour d'épidémie à partir de Cisco ou nouvelles définitions d'antivirus sont édités par Sophos et McAfee.

Les messages utilisés dans les attaques à petite échelle et non virales utilisent une conception à

l'air légitime, les informations du destinataire, et la coutume URLs qui indiquent les sites Web de phishing et de malware qui ont été en ligne seulement pendant une courte période et sont inconnus aux services de sécurité Web. Les filtres d'épidémie analysent un contenu de message et recherchent des liens URL pour détecter ce type d'attaque non virale. Les filtres d'épidémie peuvent réécrire l'URLs pour réorienter le trafic aux sites Web potentiellement néfastes par un proxy de sécurité Web, que l'un ou l'autre avertit les utilisateurs qui le site Web qu'ils tentent d'accéder à peut être malveillant ou bloque le site Web complètement.

Est-ce que je peux utiliser des filtres d'épidémie même si je n'exécute pas Sophos ou l'antivirus de McAfee sur mon ESA ?

Cisco recommande que vous permettiez à Sophos ou à l'antivirus de McAfee en plus des filtres d'attaque de virus d'augmenter votre défense contre des virus. Cependant, VOF peut fonctionner indépendamment sans exiger Sophos ou l'antivirus de McAfee à activer.

Quand les filtres d'épidémie mettent en quarantaine-ils des messages ?

Un message est mis en quarantaine quand il contient les connexions de fichier qui rencontrent ou dépassent les règles en cours d'épidémie et par la poste les administrateurs réglés par seuils. Cisco édite des règles en cours d'épidémie à chaque ESA qui a une touche de fonction valide, et sur notre portail de support. Des messages qui peuvent faire partie d'une épidémie sont mis en quarantaine jusqu'à ce qu'ils soient déterminés pour être coffre-fort basé sur les informations mises à jour d'épidémie à partir de Cisco ou nouvelles définitions d'antivirus sont édités par Sophos et McAfee.

Des informations sur des attaques de virus en cours peuvent être trouvées sur SenderBase

Le site Web des opérations secrètes de sécurité Cisco (SIO) fournit une liste de menaces non virales en cours, y compris le Spam, le phishing, et les tentatives de distribution de malware.

Que se produit quand la quarantaine d'épidémie se remplit ?

Quand une quarantaine dépasse l'espace maximum alloué à elle, ou si un message dépasse le paramètre horaire maximum, des messages sont automatiquement taillés de la quarantaine pour la garder dans les limites. Des messages sont retirés sur une base du first-in, first-out (FIFO). En d'autres termes, les messages les plus anciens sont supprimés d'abord. Vous pouvez configurer une quarantaine à la release (c'est-à-dire, livrez) ou supprimer un message qui doit être taillé d'une quarantaine. Si vous choisissez de relâcher des messages, vous pouvez choisir d'avoir le champ objet étiqueté avec le texte que vous spécifiez qui alertera le destinataire que le message a été forcé hors d'une quarantaine.

La release suivante de la quarantaine d'épidémie, des messages sont rebalayées par le module d'antivirus, et une mesure est prise selon la stratégie d'antivirus. Selon cette stratégie, un

message peut être fourni, supprimé, ou fourni avec les connexions virales éliminées. On s'attend à ce que des virus souvent soient trouvés pendant le retour après que release de la quarantaine d'épidémie. Les mail_logs ESA ou le cheminement de message peuvent être consultés pour déterminer si un message individuel qui a été noté dans la quarantaine s'avéraient viral, et si et comment il a été livré.

Avant qu'une quarantaine de système se remplisse, une alerte est envoyée quand la quarantaine atteint 75% plein, et une autre alerte est envoyée quand elle atteint 95% plein. La quarantaine d'épidémie a une fonctionnalité de gestion supplémentaire qui te permet pour supprimer ou libérer tous les messages qui apparient un niveau particulier de menace de virus (VTL). Ceci tient compte de l'effacement facile de la quarantaine après qu'on reçoive une mise à jour d'antivirus qui adresse une menace particulière de virus.

Quelle est la signification du niveau de menace pour une règle d'épidémie ?

Les filtres d'épidémie agissent sous des niveaux de menace entre 0 et 5. Le niveau de menace évalue la probabilité d'une épidémie virale. Basé sur le risque d'une épidémie virale, le niveau de menace influence mettre en quarantaine des fichiers méfiants. Le niveau de menace est basé sur un certain nombre de facteurs, y compris notamment le trafic réseau, le taux de mouvements du fichier méfiant, l'entrée des constructeurs d'antivirus, et l'analyse par le centre d'opérations de la menace de Cisco. En outre, les filtres d'épidémie permet à des administrateurs de messagerie pour augmenter ou diminuer l'incidence des niveaux de menace pour leurs réseaux.

Niveau	Risque	Signification
0	Aucun	Il n'y a aucun risque que le message est une menace.
1	Bas	Le risque que le message est une menace est bas.
2	Bas/support	Le risque que le message est une menace est bas au support. C'est a ? suspecté ? menace.
3	Support	Ou le message fait partie d'une épidémie confirmée ou il y a un support au grand risc son contenu étant une menace.
4	Haute	Ou le message est confirmé pour faire partie d'une épidémie de large échelle ou son contenu est très dangereux.
5	Extrême	Le message ? le contenu s est confirmé à une partie d'une épidémie qui est extrême large échelle ou large échelle et extrêmement dangereuse.

Comment est-ce que je peux être alerté quand une attaque de virus se produit ?

Quand le réseau de SenderBase élève un VTL pour un type particulier de profil de message, vous pouvez être alerté par l'intermédiaire d'un message électronique envoyé à votre adresse e-mail vigilante configurée. Quand un VTL tombe au-dessous de votre seuil configuré, une autre alerte est envoyée. Vous pouvez surveiller ainsi la progression du virus. Pour vous assurer recevra ces alertes, vérifient l'adresse e-mail que des alertes sont envoyées à dans le CLI utilisant la commande d'**alertconfig**.

Pour configurer, ou confirugation de reivew

- GUI : Les Services de sécurité > les filtres d'épidémie et passent en revue la configuration sous les **paramètres généraux d'éditer…**

- CLI : **outbreakconfig > installé**

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.
```

Une nouvelle attaque de virus sera d'abord détectée par SenderBase et VTL sera élevé. Vous recevrez une alerte si le VTL rencontre ou dépasse votre seuil configuré VTL. Les alertes de Sophos suivront comme le virus est identifié et capturé, et quand le nouveau virus identifiant des signatures deviennent disponible.

Informations connexes

- Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur
- Support et documentation techniques - Cisco Systems