Domande frequenti ESA: Filtri epidemie/Filtri epidemie di virus (VOF) - Domande frequenti

Sommario

Introduzione

Questo documento descrive e risponde ad alcune delle domande più frequenti sui filtri epidemie, o filtri epidemie di virus (VOF), su Cisco Email Security Appliance (ESA).

Cosa sono i filtri epidemie?

> **Nota**: consultare la Guida dell'utente per la versione di AsyncOS for Email Security attualmente in esecuzione. Esempio, Guida per l'utente di AsyncOS 13.0 for Cisco Email Security Appliance, capitolo: Filtri epidemie

I filtri epidemie proteggono la rete da epidemie di virus su larga scala e da attacchi non virali di piccole dimensioni, ad esempio truffe di phishing e distribuzione di malware. A differenza della maggior parte dei software di sicurezza antimalware, che non possono rilevare nuovi focolai finché non vengono raccolti dati e pubblicato un aggiornamento software, Cisco raccoglie dati sui focolai mentre si diffondono e invia informazioni aggiornate all'ESA in tempo reale per impedire che questi messaggi raggiungano gli utenti.

Cisco utilizza i modelli di traffico globali per sviluppare regole che determinano se un messaggio in arrivo è sicuro o fa parte di un'epidemia. I messaggi che possono far parte di un'epidemia vengono messi in quarantena finché non vengono accertati che sono sicuri in base alle informazioni aggiornate sull'epidemia fornite da Cisco o finché non vengono pubblicate nuove definizioni antivirus da Sophos e McAfee.

I messaggi utilizzati in attacchi non virali su piccola scala sono strutturati in modo da apparire legittimi, le informazioni sul destinatario e gli URL personalizzati che puntano a siti di phishing e malware online solo per un breve periodo di tempo e sconosciuti ai servizi di sicurezza Web. I filtri epidemie analizzano il contenuto di un messaggio e cercano i link URL per rilevare questo tipo di

attacco non virale. I filtri epidemie possono riscrivere gli URL per reindirizzare il traffico a siti Web potenzialmente dannosi tramite un proxy di sicurezza Web, che avvisa gli utenti che il sito Web a cui stanno tentando di accedere potrebbe essere dannoso o blocca completamente il sito Web.

Posso utilizzare i filtri epidemie anche se non eseguo Sophos o McAfee Anti-Virus sulla mia ESA?

Cisco consiglia di abilitare, oltre ai filtri epidemie, l'antivirus Sophos o McAfee per aumentare la capacità di difesa dagli allegati virali. Tuttavia, i filtri epidemie possono funzionare in modo indipendente senza che sia necessario abilitare Sophos o McAfee Anti-Virus.

Quando i filtri epidemie mettono in quarantena un messaggio?

Un messaggio viene messo in quarantena quando contiene allegati che soddisfano o superano le regole epidemie correnti e le soglie impostate dagli amministratori della posta. Cisco pubblica le attuali regole epidemie per ciascuna ESA che ha una chiave di funzionalità valida. I messaggi che possono far parte di un'epidemia vengono messi in quarantena finché non vengono determinati come sicuri in base alle informazioni aggiornate sull'epidemia fornite da Cisco o finché non vengono pubblicate nuove definizioni antivirus da Sophos e McAfee.

Come vengono scritte le regole del filtro epidemie?

Le regole epidemie sono pubblicate da Cisco Security Intelligence Operations (SIO), un ecosistema di sicurezza che collega le informazioni sulle minacce globali, i servizi basati sulla reputazione e le analisi sofisticate delle appliance di sicurezza Cisco per fornire una protezione più efficace con tempi di risposta più rapidi. Per impostazione predefinita, l'accessorio controlla e scarica nuove regole epidemie ogni 5 minuti come parte degli aggiornamenti del servizio.

Il SIO è costituito da tre componenti:

- SenderBase, la più grande rete mondiale di monitoraggio delle minacce e database sulle vulnerabilità.
- Talos, il team globale di analisti della sicurezza e sistemi automatizzati di Cisco.
- Aggiornamenti dinamici e aggiornamenti in tempo reale distribuiti automaticamente agli accessori in caso di epidemie.

Esistono best practice per la configurazione dei filtri epidemie?

Sì. Il livello di servizio consigliato è il seguente:

- Abilita *regole adattive*
- Imposta *dimensione massima messaggio su* 2 MB
- *Registrazione interazione Web* abilitata

La configurazione a livello di criteri di posta in arrivo dovrà essere determinata in base al cliente e alle regole.

Come posso segnalare una regola del filtro epidemie non

corretta?

Puoi segnalare falsi positivi o falsi negativi in uno dei due modi seguenti:

1. Apri una richiesta di assistenza Cisco: https://mycase.cloudapps.cisco.com/case
2. Apri un ticket di reputazione con Talos: https://talosintelligence.com/reputation_center/support

Di seguito sono elencate le condizioni in cui possiamo perfezionare le regole del filtro epidemie:

- Estensioni di file
- Firma file (Magic) (firma binaria del file che indica il tipo 'true')
- URL
- Nome file
- Dimensioni file

Cosa succede quando si riempie la quarantena?

Quando una quarantena supera lo spazio massimo allocato o se un messaggio supera il valore impostato, i messaggi vengono eliminati automaticamente dalla quarantena per mantenerli entro i limiti. I messaggi vengono rimossi in base al FIFO (First-In, First-Out). In altre parole, i messaggi meno recenti vengono eliminati per primi. È possibile configurare una quarantena in modo che rilasci, ovvero recapiti, o elimini un messaggio che deve essere eliminato da una quarantena. Se si sceglie di rilasciare i messaggi, è possibile scegliere di contrassegnare la riga dell'oggetto con il testo specificato per avvisare il destinatario che il messaggio è stato escluso dalla quarantena.

Dopo il rilascio dalla quarantena di un focolaio, i messaggi vengono nuovamente analizzati dal modulo antivirus e l'azione viene intrapresa in base alla policy antivirus. A seconda di questa regola, è possibile che un messaggio venga recapitato, eliminato o consegnato con allegati virali rimossi. Si prevede che i virus saranno spesso trovati durante la nuova scansione dopo il rilascio dalla quarantena epidemica. È possibile consultare i log di posta dell'ESA o la verifica dei messaggi per determinare se un singolo messaggio registrato durante la quarantena è risultato virale e se e come è stato recapitato.

Prima che la quarantena di un sistema si esaurisca, viene inviato un avviso quando la quarantena raggiunge il 75% di spazio pieno e un altro avviso quando raggiunge il 95% di spazio pieno. La quarantena di epidemie dispone di una funzionalità di gestione aggiuntiva che consente di eliminare o rilasciare tutti i messaggi che corrispondono a un particolare livello di rischio di virus (VTL). In questo modo è possibile pulire facilmente la quarantena dopo aver ricevuto un aggiornamento antivirus che risolve una particolare minaccia di virus.

Qual è il significato del livello di minaccia per una regola per i focolai epidemici?

I filtri epidemie operano con livelli di minaccia compresi tra 0 e 5. Il livello di minaccia determina la probabilità di un'epidemia virale. In base al rischio di un'epidemia virale, il livello di minaccia influenza la quarantena dei file sospetti. Il livello di minaccia si basa su una serie di fattori, tra cui, a titolo esemplificativo ma non esaustivo, traffico di rete, attività sospetta dei file, input da parte dei fornitori di antivirus e analisi da parte di Cisco IOS. I filtri epidemie consentono inoltre agli amministratori della posta di aumentare o diminuire l'impatto dei livelli di minaccia sulle loro reti.

Livello	Rischio	Significato
0	Nessuna	Non vi è alcun rischio che il messaggio minaccia.
1	Bassa	Il rischio che il messaggio sia minaccia è bassa.
2	Bassa/media	Il rischio che il messaggio sia minaccia è da bassa a media. È un "sospetto" minacci
3	Media	Il messaggio fa parte di un focolaio confermato oppure esiste un rischio medio-grand il suo contenuto minaccia.
4	Alta	Il messaggio è confermato come parte di un'epidemia su larga scala oppure il suo contenuto è molto pericoloso.
5	Estremo	Il contenuto del messaggio è confermato in una parte di un focolaio che è estremam su larga scala o su larga scala ed estremamente pericoloso.

Come posso essere avvisato quando si verifica un'epidemia?

Quando Filtri epidemie riceve regole nuove o aggiornate per elevare il livello di minaccia di quarantena per un particolare tipo di profilo di messaggio, è possibile ricevere un avviso tramite un messaggio e-mail inviato all'indirizzo e-mail di avviso configurato. Quando un livello di minaccia scende al di sotto della soglia configurata, viene inviato un altro avviso. È quindi possibile monitorare lo stato degli allegati virali. Queste email sono inviate come email informative.

> **Nota:** Per essere certi di ricevere queste notifiche e-mail, verificare l'indirizzo e-mail a cui vengono inviati gli avvisi nella CLI usando il comando **alertconfig** o la GUI: **Amministrazione sistema > Avvisi**.

Per configurare o rivedere la configurazione

- GUI: Security Services > Outbreak Filters e rivedere la configurazione in **Edit Global Settings...**
- CLI: **outbreakconfig > imposta**

Esempio:

```
> outbreakconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine esa2.hc3033-47.iphmx.com).

What would you like to do?
1. Switch modes to edit at mode "Cluster Hosted_Cluster".
2. Start a new, empty configuration at the current mode (Machine esa2.hc3033-47.iphmx.com).
3. Copy settings from another cluster mode to the current mode (Machine esa2.hc3033-
47.iphmx.com).
[1]>

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? [Y]> y

What is the largest size message Outbreak Filters should scan?
[2097152]>

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

Logging of URLs is currently enabled.

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

Web Interaction Tracking is currently enabled.

Do you wish to disable Web Interaction Tracking? [N]>

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.
```

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems