ESA FAQ: Uitbraakfilters/virusuitbraken filters (VOF) FAQ

Inhoud

Inleiding

Dit document beschrijft en beantwoord een aantal van de vaakst gestelde vragen over Outbreak Filters, of Virus Outbreak Filters (VOF), op de Cisco e-mail security applicatie (ESA).

Wat zijn Outbreak Filters?

> **Opmerking**: controleer of u de gebruikershandleiding voor de versie van AsyncOS voor e-mailbeveiliging hebt die u momenteel gebruikt. Bijvoorbeeld, gebruikersgids voor AsyncOS 13.0 voor Cisco e-mail security applicaties, hoofdstuk: Outdoorfilters

Uitbraakfilters beschermen uw netwerk tegen grootschalige virusuitbraken en kleinere, niet-virale aanvallen, zoals phishing scams en malware distributie, wanneer ze zich voordoen. Anders dan de meeste anti-malware beveiligingssoftware, die geen nieuwe uitbraken kan detecteren totdat gegevens worden verzameld en een software-update wordt gepubliceerd, verzamelt Cisco gegevens over uitbraken terwijl ze zich verspreiden en stuurt bijgewerkte informatie naar uw ESA in real-time om te voorkomen dat deze berichten uw gebruikers bereiken.

Cisco gebruikt mondiale verkeerspatronen om regels te ontwikkelen die bepalen of een inkomend bericht veilig is of een deel van een uitbraak. Berichten die deel kunnen uitmaken van een uitbraak worden in quarantaine geplaatst totdat is vastgesteld dat ze veilig zijn op basis van bijgewerkte informatie over uitbraken uit Cisco of nieuwe antivirusdefinities worden gepubliceerd door Sofobs en McAfee.

Berichten die gebruikt worden in kleinschalige niet-virale aanvallen gebruiken een legitiem uitziend ontwerp, de informatie van de ontvanger, en aangepaste URL's die op phishing en malware websites wijzen die slechts voor een korte tijd online zijn geweest en onbekend zijn bij web security services. Outdoorfilters analyseren de inhoud van een bericht en zoeken naar URL links

om dit type niet-virale aanval te detecteren. Outbreak Filters kunnen URL's herschrijven om verkeer naar potentieel schadelijke websites te sturen via een web security proxy, die gebruikers waarschuwt dat de website waar ze toegang toe proberen te krijgen, kwaadaardig is of de website volledig blokkeert.

Kan ik Outbreak Filters gebruiken zelfs als ik geen Sofo's of McAfee Anti-Virus op mijn ESA draai?

Cisco raadt u aan Sofos of McAfee Anti-Virus in te schakelen naast Outbreak Filters om uw verdediging tegen virale aanvallen te vergroten. Desondanks kunnen Outbreak Filters onafhankelijk werken zonder dat Sofoos of McAfee Anti-Virus ingeschakeld hoeven te worden.

Wanneer quarantaine-filters een bericht?

Een bericht is in quarantaine geplaatst wanneer het een of meer bestandsbijlage(s) bevat die voldoet aan de huidige regels voor uitsplitsing of de drempels overschrijdt die door mail beheerders zijn ingesteld. Cisco publiceert de huidige regels voor uitbraken aan elke ESA die een geldige functiesleutel heeft. Berichten die deel kunnen uitmaken van een uitbraak worden in quarantaine geplaatst tot ze veilig zijn vastgesteld op basis van bijgewerkte informatie over uitbraken uit Cisco of nieuwe anti-virusdefinities worden gepubliceerd door Sofobs en McAfee.

Hoe worden de regels voor het filter van de breuk geschreven?

Outbreak Regels worden gepubliceerd door Cisco Security Intelligence Operations (SIO), een security ecosysteem dat mondiale bedreigingsinformatie, reputatie-gebaseerde services en geavanceerde analyse van Cisco security apparaten verbindt om betere bescherming te bieden met snellere responsietijden. Uw apparaat controleert standaard op nieuwe uitbarstingsregels en downloads elke 5 minuten als onderdeel van de servicetechniek.

SIO bestaat uit drie componenten:

- SenderBase, 's werelds grootste netwerk voor bedreigingscontrole en kwetsbaarheidsdatabase.
- Talos, het mondiale team van veiligheidsanalisten en geautomatiseerde systemen van Cisco.
- Dynamische updates, real-time updates die automatisch aan apparaten worden geleverd wanneer uitbraken optreden.

Zijn er beste praktijken voor het configureren van omslagfilters?

Ja. De aanbeveling voor het serviceniveau is als volgt:

- *Adaptieve regels* inschakelen
- Stel *maximale berichtgrootte in op Scannen* naar 2M
- Ingeschakelde *Web Interactie Tracking*

De configuratie op het niveau van het inkomende postbeleid zal moeten worden vastgesteld per klant, per beleid.

Hoe kan ik een onjuiste uitbraakfilterregel melden?

U kunt op twee manieren valse positieve of valse negatieve resultaten melden:

1. Open een Cisco-ondersteuningscase: https://mycase.cloudapps.cisco.com/case
2. Open een reputatie-ticket met Talos: https://talosintelligence.com/reputation_center/support

Hieronder staan de voorwaarden die we kunnen verfijnen in Outbreak Filtering-regels:

- Bestandsuitbreidingen
- File Signature (Magic) (Binaire handtekening van het bestand die het "echte" type aangeeft)
- URL's
- Bestandsnaam
- Bestandsgrootte

Wat gebeurt er als de Outbreak quarantaine opvult?

Wanneer een quarantaine de maximumruimte overschrijdt of wanneer een bericht de maximumtijdsinstelling overschrijdt, worden de berichten automatisch uit de quarantaine verwijderd om het binnen de grenzen te houden. Berichten worden verwijderd op basis van een first-in, first-out (FIFO). Met andere woorden, de oudste berichten worden eerst verwijderd. U kunt een quarantaine configureren om een bericht vrij te geven (in de vorm van een levering) of te verwijderen dat uit een quarantaine moet worden gewist. Als u ervoor kiest om berichten vrij te geven, kunt u ervoor kiezen om de onderwerpregel te laten merken aan de tekst die u hebt ingesteld om de ontvanger te waarschuwen dat het bericht uit quarantaine is gedwongen.

Na vrijgave van de Outbreak quarantaine worden de berichten opnieuw gescand door de anti-virusmodule en wordt actie ondernomen volgens het anti-virusbeleid. Afhankelijk van dit beleid kan een bericht worden afgeleverd, verwijderd of geleverd met gestreepte virusbijlagen. Verwacht wordt dat virussen vaak worden aangetroffen tijdens een herscan na vrijgave van de Outbreak quarantaine. De ESA mail_logs of bericht tracking kunnen worden geraadpleegd om vast te stellen of een individueel bericht dat in de quarantaine werd genoteerd viraal bleek te zijn, en of en hoe het werd afgeleverd.

Voordat een systeem-quarantaine wordt ingevuld, wordt een waarschuwing verzonden als de quarantaine 75% vol bereikt, en wordt een andere waarschuwing verstuurd wanneer de quarantaine 95% vol bereikt. De Outbreak Quarantine heeft een extra beheerfunctie die u in staat stelt om alle berichten te verwijderen of vrij te geven die op een bepaald virus bedreigingsniveau (VTL) overeenkomen. Dit maakt het mogelijk de quarantaine gemakkelijk te reinigen nadat een bijwerking tegen het virus is ontvangen die een specifieke virusdreiging aanpakt.

Wat is de betekenis van het dreigingsniveau voor een Outbreak Rule?

Uitbraakfilters werken onder bedreigingsniveaus tussen 0 en 5. Het dreigingsniveau verhoogt de kans op een virale uitbraak. Op basis van het risico van een virale uitbraak beïnvloedt het dreigingsniveau het in quarantaine plaatsen van verdachte bestanden. Het bedreigingsniveau is gebaseerd op een aantal factoren, waaronder maar niet beperkt tot netwerkverkeer, verdachte bestandactiviteit, input van anti-virusverkopers en analyse door Cisco SIO. Daarnaast biedt Outdoorfilter om e-mailbeheerders de impact van bedreigingsniveaus voor hun netwerken te

vergroten of te verminderen.

Niveau risico		Betekenis
0	None	Er bestaat geen risico dat het bericht een bedreiging.
1	Laag	Het risico dat het bericht een bedreiging laag is.
2	Laag/Gemiddeld	Het risico dat het bericht een bedreiging laag tot gemiddeld is. Het is een "vermoeden" bedreiging.
3	Gemiddeld	De boodschap maakt deel uit van een bevestigde uitbraak of de inhoud ervan be uit een gemiddeld tot groot risico bedreiging.
4	Hoog	Ofwel wordt bevestigd dat het bericht deel uitmaakt van een grote uitbraak of da inhoud ervan erg gevaarlijk is.
5	Extreem	De inhoud van de boodschap wordt bevestigd voor een deel van een uitbraak di extreem groot of grootschalig is en extreem gevaarlijk.

Hoe kan ik worden gewaarschuwd als er een uitbraak is?

Wanneer Outbreak Filters nieuwe/updates regels ontvangen om het Quarantine Threat Level voor een bepaald type berichtprofiel te verhogen, kunt u worden gewaarschuwd via een e-mailbericht dat naar uw geconfigureerde alarmadres wordt verstuurd. Als een bedreigingsniveau onder de ingestelde drempel daalt, wordt er een ander alarm verzonden. U kunt dus de voortgang van de virale bijlage(s) bewaken. Deze e-mails worden verzonden als "Info"-e-mails.

> Opmerking: Om te verzekeren u deze e-mailberichten zult ontvangen, verifieer het e-mailadres dat de waarschuwingen in CLI worden verzonden met het **alertfig** bevel, of de GUI: **Systeembeheer > Waarschuwingen**.

De configuratie configureren of bekijken

- GUI: Security Services > Outdoorfilters en bekijk de configuratie onder de **Global Settings...**
- CLI: **uitsterking > instellingen**

Voorbeeld:

```
> 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.
```

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems