Häufig gestellte Fragen zur ESA: Häufig gestellte Fragen zu Outbreak-Filtern/Virus-Outbreak-Filtern (VOF)

Inhalt

Einführung
Was sind Outbreak-Filter?
Kann ich Outbreak-Filter auch dann verwenden, wenn ich Sophos oder McAfee Anti-Virus auf meiner ESA nicht verwende?
Wann werden Nachrichten durch Outbreak-Filter unter Quarantäne gestellt?
Wie werden die Outbreak-Filterregeln geschrieben?
Gibt es Best Practices für die Konfiguration von Outbreak-Filtern?
Wie melde ich eine falsche Outbreak-Filterregel?
Was passiert, wenn die Outbreak-Quarantäne abgeschlossen ist?
Was bedeutet die Bedrohungsstufe für eine Outbreak-Regel?
Wie kann ich bei einem Outbreak benachrichtigt werden?
Zugehörige Informationen

Einführung

In diesem Dokument werden einige der häufigsten Fragen zu Outbreak-Filtern oder Virus-Outbreak-Filtern (VOF) der Cisco E-Mail Security Appliance (ESA) beschrieben und beantwortet.

Was sind Outbreak-Filter?

> **Hinweis**: Bitte lesen Sie das Benutzerhandbuch für die derzeit ausgeführte Version von AsyncOS für E-Mail-Sicherheit. Beispiel, Benutzerhandbuch für AsyncOS 13.0 für Cisco Email Security Appliances, Kapitel: Outbreak-Filter

Outbreak-Filter schützen Ihr Netzwerk vor groß angelegten Virenangriffen und kleineren, nicht-viralen Angriffen, wie Phishing-Scams und Malware-Verbreitung, sobald diese auftreten. Im Gegensatz zu den meisten Anti-Malware-Sicherheitssoftware, die neue Outbreaks erst erkennen kann, wenn Daten gesammelt und ein Software-Update veröffentlicht wird, sammelt Cisco Daten über Outbreaks, während diese sich verbreiten, und sendet aktualisierte Informationen in Echtzeit an Ihre ESA, um zu verhindern, dass diese Nachrichten Ihre Benutzer erreichen.

Cisco verwendet globale Datenverkehrsmuster, um Regeln zu entwickeln, die bestimmen, ob eine eingehende Nachricht sicher ist oder Teil eines Outbreaks ist. Nachrichten, die Teil eines Outbreaks sein können, werden unter Quarantäne gestellt, bis sie auf der Grundlage aktualisierter Outbreak-Informationen von Cisco als sicher eingestuft werden oder neue Virendefinitionen von Sophos und McAfee veröffentlicht werden.

Bei Nachrichten, die bei kleinen, nicht-viralen Angriffen verwendet werden, wird ein legitim

aussehendes Design, die Informationen des Empfängers und benutzerdefinierte URLs verwendet, die auf Phishing- und Malware-Websites verweisen, die nur für kurze Zeit online sind und für Websicherheitsdienste unbekannt sind. Outbreak-Filter analysieren den Inhalt einer Nachricht und suchen nach URL-Links, um diese Art von nicht-viralem Angriff zu erkennen. Outbreak-Filter können URLs umschreiben, um den Datenverkehr über einen Websicherheits-Proxy auf potenziell schädliche Websites umzuleiten, der Benutzer warnt, dass die Website, auf die sie zugreifen möchten, möglicherweise schädlich ist, oder die Website vollständig blockiert.

Kann ich Outbreak-Filter auch dann verwenden, wenn ich Sophos oder McAfee Anti-Virus auf meiner ESA nicht verwende?

Cisco empfiehlt, zusätzlich zu Outbreak-Filtern Sophos oder McAfee Anti-Virus zu aktivieren, um Ihre Abwehr gegen virale Anhänge zu verbessern. Outbreak-Filter können jedoch unabhängig arbeiten, ohne dass Sophos oder McAfee Anti-Virus aktiviert werden müssen.

Wann werden Nachrichten durch Outbreak-Filter unter Quarantäne gestellt?

Eine Nachricht wird unter Quarantäne gestellt, wenn sie Dateianhängen enthält, die die aktuellen Outbreak-Regeln und die von Mail-Administratoren festgelegten Schwellenwerte erfüllen oder überschreiten. Cisco veröffentlicht aktuelle Outbreak-Regeln für jede ESA mit einem gültigen Feature-Schlüssel. Nachrichten, die Teil eines Outbreaks sein können, werden unter Quarantäne gestellt, bis sie auf der Grundlage aktualisierter Outbreak-Informationen von Cisco als sicher eingestuft werden oder neue Virendefinitionen von Sophos und McAfee veröffentlicht werden.

Wie werden die Outbreak-Filterregeln geschrieben?

Outbreak-Regeln werden von Cisco Security Intelligence Operations (SIO) veröffentlicht, einem Sicherheitssystem, das globale Bedrohungsinformationen, reputationsbasierte Services und ausgefeilte Analysen von Cisco Security Appliances miteinander verbindet, um einen besseren Schutz bei schnelleren Reaktionszeiten zu gewährleisten. Standardmäßig prüft und lädt Ihre Appliance im Rahmen der Service-Updates alle 5 Minuten neue Outbreak-Regeln.

Die SIO bestehen aus drei Komponenten:

- SenderBase, das weltweit größte Netzwerk zur Bedrohungsüberwachung und Schwachstellendatenbank.
- Talos, das globale Team aus Sicherheitsanalysten und automatisierten Systemen von Cisco.
- Dynamische Updates, Updates in Echtzeit werden bei Ausbrüchen automatisch an Appliances geliefert.

Gibt es Best Practices für die Konfiguration von Outbreak-Filtern?

Ja. Die Empfehlung für den Servicelevel lautet wie folgt:

- *Adaptive Regeln* aktivieren
- Legen Sie *die maximale Nachrichtengröße für den Scan* auf 2 Mio. fest

- Aktivierte *Webinteraktionsverfolgung*

Die Konfiguration auf der Ebene der Richtlinien für eingehende E-Mails muss auf der Basis von Kundenrichtlinien und Richtlinien bestimmt werden.

Wie melde ich eine falsche Outbreak-Filterregel?

Sie können falsch positive oder falsche Negative auf zwei Arten melden:

1. Erstellen Sie ein Support-Ticket von Cisco: https://mycase.cloudapps.cisco.com/case
2. Ticket für Reputation bei Talos eröffnen: https://talosintelligence.com/reputation_center/support

Nachfolgend sind die Bedingungen aufgeführt, unter denen wir die Outbreak-Filterungsregeln verfeinern können:

- Dateierweiterungen
- Dateisignatur (Magic) (Binäre Signatur der Datei, die den 'wahren' Typ angibt)
- URLs
- Dateiname
- Dateigröße

Was passiert, wenn die Outbreak-Quarantäne abgeschlossen ist?

Wenn eine Quarantäne den ihr zugewiesenen Speicherplatz überschreitet oder wenn eine Nachricht die maximale Zeiteinstellung überschreitet, werden die Nachrichten automatisch aus der Quarantäne entfernt, um die Quarantäne einzuschränken. Nachrichten werden auf First-In-First-Out (FIFO)-Basis entfernt. Mit anderen Worten, die ältesten Nachrichten werden zuerst gelöscht. Sie können eine Quarantäne so konfigurieren, dass sie entweder freigegeben (d. h. übermittelt) oder eine Nachricht gelöscht wird, die aus einer Quarantäne entfernt werden muss. Wenn Sie Nachrichten freigeben möchten, können Sie festlegen, dass die Betreffzeile mit dem von Ihnen angegebenen Text gekennzeichnet wird, der den Empfänger darüber informiert, dass die Nachricht aus der Quarantäne erzwungen wurde.

Nach der Veröffentlichung aus dem Outbreak-Quarantänebereich werden die Nachrichten vom Antivirus-Modul erneut gescannt, und die entsprechenden Maßnahmen werden gemäß den Virenschutzrichtlinien ergriffen. Je nach Richtlinie kann eine Nachricht zugestellt, gelöscht oder mit Virenanhängen zugestellt werden. Es wird erwartet, dass Viren häufig während des erneuten Scans nach der Freisetzung aus der Outbreak-Quarantäne gefunden werden. Die ESA-Mail_logs oder die Nachrichtenverfolgung können konsultiert werden, um festzustellen, ob eine einzelne Nachricht, die in der Quarantäne aufgezeichnet wurde, als viral eingestuft wurde und ob und wie sie zugestellt wurde.

Bevor eine Systemquarantäne ausgefüllt wird, wird eine Warnung gesendet, wenn die Quarantäne 75 % voll erreicht, und eine weitere Warnmeldung, wenn sie 95 % voll erreicht. Die Outbreak-Quarantäne verfügt über eine zusätzliche Verwaltungsfunktion, mit der Sie alle Nachrichten löschen oder freigeben können, die einer bestimmten Virenbedrohungsstufe (VTL) entsprechen. Dies ermöglicht eine einfache Säuberung der Quarantäne nach Erhalt einer Antivirus-Aktualisierung, die eine bestimmte Virenbedrohung behebt.

Was bedeutet die Bedrohungsstufe für eine Outbreak-Regel?

Outbreak-Filter reagieren auf Bedrohungsstufen zwischen 0 und 5. Das Bedrohungsniveau erhöht die Wahrscheinlichkeit eines Virusausbruchs. Aufgrund des Risikos eines Virusausbruchs beeinflusst die Bedrohungsstufe die Quarantäne verdächtiger Dateien. Das Bedrohungspotenzial basiert auf einer Reihe von Faktoren, darunter Netzwerkverkehr, verdächtige Dateiaktivitäten, Input von Antivirus-Anbietern und Analysen durch Cisco SIO. Darüber hinaus ermöglichen Outbreak-Filter E-Mail-Administratoren die Steigerung oder Verringerung der Auswirkungen von Bedrohungen für ihre Netzwerke.

Stufe	Risiko	Bedeutung
0	Keine	Es besteht kein Risiko, dass die Nachricht ein Bedrohung.
1	Niedrig	Das Risiko, dass die Nachricht ein Bedrohung ist niedrig.
2	Niedrig/Mittel	Das Risiko, dass die Nachricht ein Bedrohung ist gering bis mittel. Es handelt sich um einen "Verdacht" Bedrohung.
1	Mittel	Entweder ist die Nachricht Teil eines bestätigten Outbreaks, oder es besteht ein mittle bis großes Risiko, dass der Inhalt ein Bedrohung.
4	Hoch	Entweder wird bestätigt, dass die Nachricht Teil eines groß angelegten Outbreaks ist, ihr Inhalt ist sehr gefährlich.
5	Extrem	Der Inhalt der Nachricht wird als Teil eines Outbreaks bestätigt, der entweder extrem oder groß und extrem gefährlich ist.

Wie kann ich bei einem Outbreak benachrichtigt werden?

Wenn Outbreak-Filter neue/aktualisierte Regeln zur Erhöhung der Quarantäne-Bedrohungsstufe für einen bestimmten Meldungsprofil-Typ empfangen, können Sie über eine E-Mail-Nachricht benachrichtigt werden, die an Ihre konfigurierte E-Mail-Adresse für Warnmeldungen gesendet wird. Wenn eine Bedrohungsstufe unter Ihren konfigurierten Grenzwert fällt, wird eine weitere Warnmeldung gesendet. Sie können so den Fortschritt der viralen Anlage(en) überwachen. Diese E-Mails werden als "Info"-E-Mails versendet.

> **Hinweis**: Um sicherzustellen, dass Sie diese E-Mail-Benachrichtigungen erhalten, überprüfen Sie die E-Mail-Adresse, an die Warnmeldungen in der CLI gesendet werden. Verwenden Sie hierzu den Befehl **alertconfig** oder die GUI: **Systemverwaltung > Warnungen**.

So konfigurieren oder überprüfen Sie die Konfiguration

- Benutzeroberfläche: Sicherheitsdienste > Outbreak-Filter und überprüfen Sie die Konfiguration unter **Globale Einstellungen bearbeiten...**
- CLI: **outbreakconfig > Setup**

Beispiel:

```
> 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.
```

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems