الأسئلة المتداولة حول وكالة الفضاء الأوروبية: عوامل تصفية التفشي/عوامل تصفية تفشي الفيروسات (VOF)

المحتويات

المقدمة

يصف هذا المستند بعض الأسئلة الأكثر شيوعا المتعلقة بعوامل تصفية تفشي الفيروسات أو عوامل تصفية تفشي الفيروسات (VOF)، في جهاز أمان البريد الإلكتروني من Cisco (ESA) ويجيب عليها.

ما هي عوامل تصفية التفشي؟

ملاحظة: الرجاء التأكد من مراجعة دليل المستخدم لإصدار AsyncOS لأمان البريد الإلكتروني الذي تقوم بتشغيله حاليا. على سبيل المثال، دليل المستخدم ل AsyncOS 13.0 لأجهزة أمان البريد الإلكتروني من Cisco، الفصل: عوامل تصفية التفشي

تحمي عوامل تصفية الفاشية شبكتك من تفشي الفيروسات على نطاق واسع ومن الهجمات الأصغر غير الفيروسية، مثل رسائل التصيد الاحتيالي وتوزيع البرامج الضارة، عند حدوثها. على عكس معظم برامج الحماية من البرامج الضارة، التي لا يمكنها اكتشاف حالات تفشي جديدة حتى يتم تجميع البيانات ونشر تحديث للبرامج، تقوم Cisco بجمع البيانات عن حالات التفشي أثناء نشرها وإرسال معلومات محدثة إلى ESA في الوقت الفعلي لمنع هذه الرسائل من الوصول إلى المستخدمين لديك.

تستخدم Cisco أنماط حركة المرور العالمية لتطوير القواعد التي تحدد ما إذا كانت الرسالة الواردة آمنة أو جزءا من التفشي. يتم وضع الرسائل التي قد تكون جزءا من تفشي المرض في الحجر الصحي إلى أن يتم تحديد كونها آمنة استنادا إلى المعلومات المحدثة الخاصة بتفشي المرض من Cisco أو التعريفات الجديدة لمكافحة الفيروسات التي يتم نشرها بواسطة Sophos و McAfee.

تستخدم الرسائل المستخدمة في الهجمات غير الفيروسية صغيرة الحجم تصميما ذا مظهر شرعي ومعلومات المستلم وعناوين URL المخصصة التي تشير إلى مواقع ويب التصيد الاحتيالي والبرامج الضارة التي كانت متصلة فقط لفترة قصيرة من الوقت وغير معروفة لخدمات أمان الويب. تقوم "عوامل تصفية التفشي" بتحليل محتوى رسالة والبحث عن

إرتباطات URL لاكتشاف هذا النوع من الهجمات غير الفيروسية. يمكن لعوامل تصفية التفشي إعادة كتابة عناوين URL لإعادة توجيه حركة مرور البيانات إلى مواقع ويب التي قد تكون ضارة من خلال وكيل أمان الويب، والذي يقوم إما بتحذير المستخدمين من أن موقع الويب الذي يحاولون الوصول إليه قد يكون ضار أو يقوم بحظر موقع الويب بالكامل.

هل يمكنني إستخدام "فلاتر التفشي" حتى لو لم أقم بتشغيل برنامج Sophos أو McAfee Anti-Virus في وكالة الفضاء الأوروبية؟

توصي Cisco بتمكين Sophos أو McAfee Anti-Virus بالإضافة إلى عوامل تصفية التفشي لزيادة دفاعك ضد الملحقات الفيروسية. ومع ذلك، يمكن تشغيل عوامل تصفية التفشي بشكل مستقل دون الحاجة إلى تمكين برامج Sophos أو برامج McAfee لمكافحة الفيروسات.

متى تقوم "عوامل تصفية التفشي" بعزل رسالة؟

يتم عزل الرسالة عندما تحتوي على مرفق (مرفقات) ملف تفي أو تتجاوز قواعد التفشي الحالية والحدود التي تم تعيينها بواسطة مسؤولي البريد. تنشر Cisco قواعد التفشي الحالية لكل ESA يحتوي على مفتاح ميزة صالح. يتم وضع الرسائل التي قد تكون جزءا من تفشي المرض في الحجر الصحي إلى أن يتم تحديد كونها آمنة استنادا إلى المعلومات المحدثة الخاصة بتفشي المرض من Cisco أو التعريفات الجديدة لمكافحة الفيروسات التي يتم نشرها بواسطة Sophos و McAfee.

كيف تتم كتابة قواعد "عامل تصفية التفشي"؟

يتم نشر قواعد التفشي بواسطة Cisco Security Intelligence Operations (SIO)، وهو نظام إيكولوجي أمني يربط معلومات التهديد العالمي، والخدمات القائمة على السمعة، والتحليل المتطور لأجهزة أمان Cisco لتوفير حماية أقوى مع أوقات إستجابة أسرع. بشكل افتراضي، يقوم الجهاز بفحص قواعد التفشي الجديدة وتنزيلها كل 5 دقائق كجزء من تحديثات الخدمة.

يتكون SIO من ثلاثة مكونات:

- SenderBase، أكبر شبكة لمراقبة التهديدات في العالم وقاعدة بيانات الثغرات.
- Talos، فريق Cisco العالمي من محللي الأمان والأنظمة المؤتمتة.
- تحديثات ديناميكية وتحديثات في الوقت الفعلي يتم تسليمها تلقائيا إلى الأجهزة عند حدوث حالات تفشي.

هل هناك أفضل الممارسات لتكوين عوامل تصفية التفشي؟

نعم. وفيما يلي التوصية المتعلقة بمستوى الخدمة:

- تمكين *القواعد المتكيفة*
- تعيين *الحد الأقصى لحجم الرسالة للمسح الضوئي* إلى 2 م
- تمكين *تعقب تفاعل الويب*

يلزم تحديد التكوين على مستوى سياسة البريد الوارد على أساس كل عميل على حدة.

كيف يمكنني الإبلاغ عن قاعدة "عامل تصفية التفشي" غير الصحيحة؟

يمكنك الإبلاغ عن السلبيات الخاطئة أو الإيجابية بإحدى طريقتين:

1. فتح حالة دعم Cisco: https://mycase.cloudapps.cisco.com/case
2. افتح تذكرة سمعة مع Talos: https://talosintelligence.com/reputation_center/support

فيما يلي الشروط التي يمكننا من خلالها تحسين قواعد تصفية الفاشية:

- امتدادات الملف
- توقيع ملف (Magic) (توقيع ثنائي للملف يشير إلى النوع 'true' الخاص به)
- URLs
- اسم الملف
- حجم الملف

ما الذي يحدث عندما يملأ الحجر الصحي بسبب تفشي المرض؟

عندما يتجاوز الفحص الحد الأقصى للمساحة المخصصة له، أو إذا تجاوزت الرسالة الحد الأقصى لإعدادات الوقت، يتم تلقائيا تنقيح الرسائل من العزل لإبقائها ضمن الحدود. تتم إزالة الرسائل على أساس الإدخال الأول والإخراج الأول (FIFO). بمعنى آخر، يتم حذف الرسائل الأقدم أولا. يمكنك تكوين عزل إما لإصدار (أي تسليم) أو حذف رسالة يجب تنقيحها من حجر صحي. إذا أخترت إصدار رسائل، يمكنك إختيار وضع علامة على سطر الموضوع بالنص الذي تقوم بتحديده والذي سينبه المستلم إلى أنه تم إجباره على الخروج من الحجر الصحي.

بعد الإفراج من الحجر الصحي على "تفشي الأمراض"، تتم إعادة فحص الرسائل بواسطة وحدة مكافحة الفيروسات، ويتم إتخاذ إجراء وفقا لسياسة مكافحة الفيروسات. وفقا لهذا النهج، يمكن تسليم رسالة أو حذفها أو تسليمها مع المرفقات الفيروسية التي تم تجريدها. ومن المتوقع ان يتم العثور على فيروسات عادة خلال اعادة المسح بعد اطلاق المرض من الحجر الصحي. يمكن الرجوع إلى ESA mail_log أو تعقب الرسائل لتحديد ما إذا كان قد تم اكتشاف أن رسالة فردية تمت الإشارة إليها في الحجر الصحي فيروسية، وما إذا كان يتم تسليمها وكيف يتم ذلك.

قبل أن يتم ملء العزل الخاص بالنظام، يتم إرسال تنبيه عندما يصل الحجر الصحي إلى 75٪ ممتلئ، ويتم إرسال تنبيه آخر عندما يصل إلى 95٪ ممتلئ. يحتوي "العزل ضد التفشي" على ميزة إدارة إضافية تسمح لك بحذف جميع الرسائل التي تطابق مستوى تهديد فيروس معين (VTL) أو إصدارها. وهذا يسمح بتنظيف الحجر الصحي بسهولة بعد تلقي تحديث لمكافحة الفيروسات يعالج تهديدا معينا للفيروسات.

ما معنى مستوى التهديد لقاعدة انتشار الوباء؟

تعمل عوامل تصفية التفشي تحت مستويات التهديد بين صفر و 5. وينسب مستوى التهديد احتمال حدوث فاشية فيروسية. واستنادا إلى خطر تفشي الفيروس، يؤثر مستوى التهديد في عزل الملفات المشبوهة. يعتمد مستوى التهديد على عدد من العوامل، بما في ذلك على سبيل المثال لا الحصر حركة مرور الشبكة ونشاط الملفات المريب والمدخلات من بائعي مكافحة الفيروسات والتحليل من قبل Cisco SIO. وبالإضافة إلى ذلك، تسمح "عوامل تصفية التفشي" لمسؤولي البريد بزيادة أو تقليل تأثير مستويات التهديدات على شبكاتهم.

مستوى	خطر
0	None
1	منخفض
2	منخفض/متوسط

3	الوسيطة
4	عالي
5	درجة قصوى

كيف يمكنني ان أنبه عندما يحدث تفش؟

عندما تتلقى "عوامل تصفية التفشي" قواعد جديدة/تحديثات لرفع مستوى تهديد الحجر الصحي لنوع معين من ملف تعريف الرسائل، يمكن تنبيهك عبر رسالة بريد إلكتروني مرسلة إلى عنوان البريد الإلكتروني الخاص بالتنبيه الذي تم تكوينه. عندما ينخفض مستوى التهديد عن الحد الذي تم تكوينه، يتم إرسال تنبيه آخر. وبذلك يمكنك مراقبة تقدم المرفق (الملحقات) الفيروسية. يتم إرسال رسائل البريد الإلكتروني هذه كرسائل بريد إلكتروني "معلومات".

ملاحظة: لضمان تلقي إعلامات البريد الإلكتروني هذه، تحقق من عنوان البريد الإلكتروني الذي يتم إرسال التنبيهات إليه في واجهة سطر الأوامر باستخدام الأمر **notifyConfig**، أو واجهة المستخدم الرسومية (GUI): **إدارة النظام > التنبيهات**.

لتكوين التكوين أو مراجعته

- واجهة المستخدم الرسومية: خدمات الأمان > عوامل تصفية التفشي ومراجعة التكوين ضمن **تحرير الإعدادات العامة...**
- CLI: **Outbreakconfig** > **إعداد**

مثال:

```
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
."Switch modes to edit at mode "Cluster Hosted_Cluster .1
.(Start a new, empty configuration at the current mode (Machine esa2.hc3033-47.iphmx.com .2
Copy settings from another cluster mode to the current mode (Machine esa2.hc3033- .3
.(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
```

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).