أمر عزل ESA/CES عند تمييز مواضيع متعددة باستخدام خدمات متعددة

المحتويات

المقدمة

يصف هذا المستند سلوك أجهزة جهاز أمان البريد الإلكتروني (ESA) وأمان البريد الإلكتروني السحابي (CES) من Cisco عندما يتم وضع علامة على البريد الإلكتروني بواسطة خدمات متعددة لعزل البريد الإلكتروني وتدفق البريد الإلكتروني عبر باقي تدفقات البريد الإلكتروني.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco ESA باستخدام الإصدار AsyncOS 12.1.0.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تتبع رسائل البريد الإلكتروني التي تتدفق من خلال أجهزة Cisco ESA و CES للتصفية تدفقات قائمة انتظار عمل البريد الإلكتروني. يكون خط الأنابيب ساكنا وإذا كانت هناك إجراءات متعددة من خدمات متعددة معرفة لوضع علامة على بريد إلكتروني للحجر الصحي، فإنه لا يتبع الأمر كما هو الحال في خط الأنابيب، وبدلا من ذلك، يقوم ESA/CES بحجره بطلبه الخاص.

ملاحظة: سيكون لرسائل البريد الإلكتروني التي تم وضع علامة عليها (الإجراء النهائي) الأسبقية الفورية وستخرج من معالجة قائمة انتظار العمل.

ماذا يحدث للبريد الإلكتروني عند وضع علامة عليه بواسطة خدمات متعددة لإجراء العزل؟

يتم ترتيب البريد الإلكتروني حسب الأولوية في الحجر الصحي الخاص بتفشي الفيروسات (PVO) الخاص بالسياسة أولا. لا يوجد أي أمر محدد يفرض الحجر الصحي على النهج الذي يتم وضعه فيه حيث تقوم PVO بسرد كل حجر صحي آخر يتم الاحتفاظ به في البريد الإلكتروني أيضا. بعد تفريغ البريد الإلكتروني من أحد المحاجر الموجودة في مخفر PVO، يتم وضعه في أي محجر خاص ليتم وضع علامة عليه فيه.

بعد إصدار البريد الإلكتروني (إما يدويا أو من خلال المؤقت حيث تم تعيين الإجراء الافتراضي على إصدار)، تدخل رسائل البريد الإلكتروني الإلكتروني الإلكتروني غير الهام حجر العزل. عند إصدار البريد الإلكتروني من العزل العشوائي، فإنه يتحول إلى قائمة انتظار التسليم التسليم التسليم النهائي بعد ذلك.

ملاحظة: سيقوم البريد الإلكتروني الذي تم حذفه من عملية عزل PVO بإزالة البريد الإلكتروني من جميع عمليات الحجر الصحي التالية التي يتم الاحتفاظ بها كذلك.

- تتم إعادة صياغة الرسائل التي يتم إصدارها من الحجر الصحي الخاص بالسياسة والفيروسات بواسطة برامج مكافحة الفيروسات والحماية المتقدمة من البرامج الضارة ومحركات بريد الرسومات.
- يتم إعادة صياغة الرسائل التي يتم إصدارها من الحجر الصحي على "التفشي" بواسطة محركات مكافحة البريد العشوائي والفيروسات و AMP.
- يتم إعادة تعيين الرسائل التي تم إصدارها من الفحص الخاص ب "تحليل الملفات" للتهديدات.
- يتم إعادة صياغة الرسائل التي تحتوي على مرفقات بواسطة خدمة سمعة الملفات عند إصدارها من الحجر الصحي "النهج" و"الفيروسات" و"التفشي".

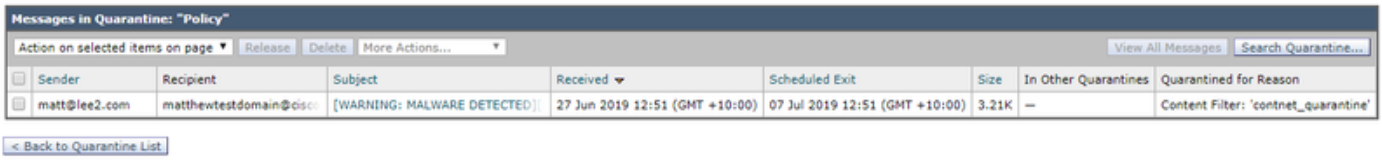
حقن البريد الإلكتروني الأولي مع التصفية التي يتم إجراؤها بواسطة ESA. في هذا الإخراج، ترى أنه تم وضع علامة عليه بواسطة العزل العشوائي والحجر الصحي للفيروسات والحجر الصحي للنهج:

```
Thu Jun 27 12:51:03 2019 Info: Start MID 378951 ICID 391696
<Thu Jun 27 12:51:03 2019 Info: MID 378951 ICID 391696 From: <matt@lee2.com
<Thu Jun 27 12:51:10 2019 Info: MID 378951 ICID 391696 RID 0 To: <matthewtestdomain@cisco.com
'Thu Jun 27 12:51:14 2019 Info: MID 378951 Subject 'Test email with AV EICAR and other triggers
<Thu Jun 27 12:51:15 2019 Info: MID 378951 ready 3292 bytes from <matt@lee2.com
Thu Jun 27 12:51:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
                                                                in the inbound table
    Thu Jun 27 12:51:15 2019 Info: MID 378951 interim verdict using engine: CASE spam positive
                Thu Jun 27 12:51:15 2019 Info: MID 378951 using engine: CASE spam positive
                    Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine
            Thu Jun 27 12:51:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
               'Thu Jun 27 12:51:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test
            Thu Jun 27 12:51:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
                                'Thu Jun 27 12:51:15 2019 Info: MID 378951 attachment 'testAV.txt
Thu Jun 27 12:51:15 2019 Info: MID 378951 URL https://ihaveabadreputation.com has reputation -
                                                                9.3 matched Condition: URL Reputation Rule
        Thu Jun 27 12:51:15 2019 Info: MID 378951 Custom Log Entry:  - Match whole word filter
(Thu Jun 27 12:51:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine
                Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Policy" (content
                                                                (filter:contnet_quarantine
            (Thu Jun 27 12:51:15 2019 Info: MID 378951 quarantined to "Virus" (a/v verdict:VIRAL
                Thu Jun 27 12:51:15 2019 Info: Message finished MID 378951 done
                Thu Jun 27 12:51:15 2019 Info: ICID 391696 close
```

بمجرد التحقيق داخل الحجر الصحي، تتم مشاهدة البريد الإلكتروني الموجود في حجر PVO الذي قمت بوضع علامة عليه، بالإضافة إلى أي حجر صحي آخر يعلموا الدخول إليه.

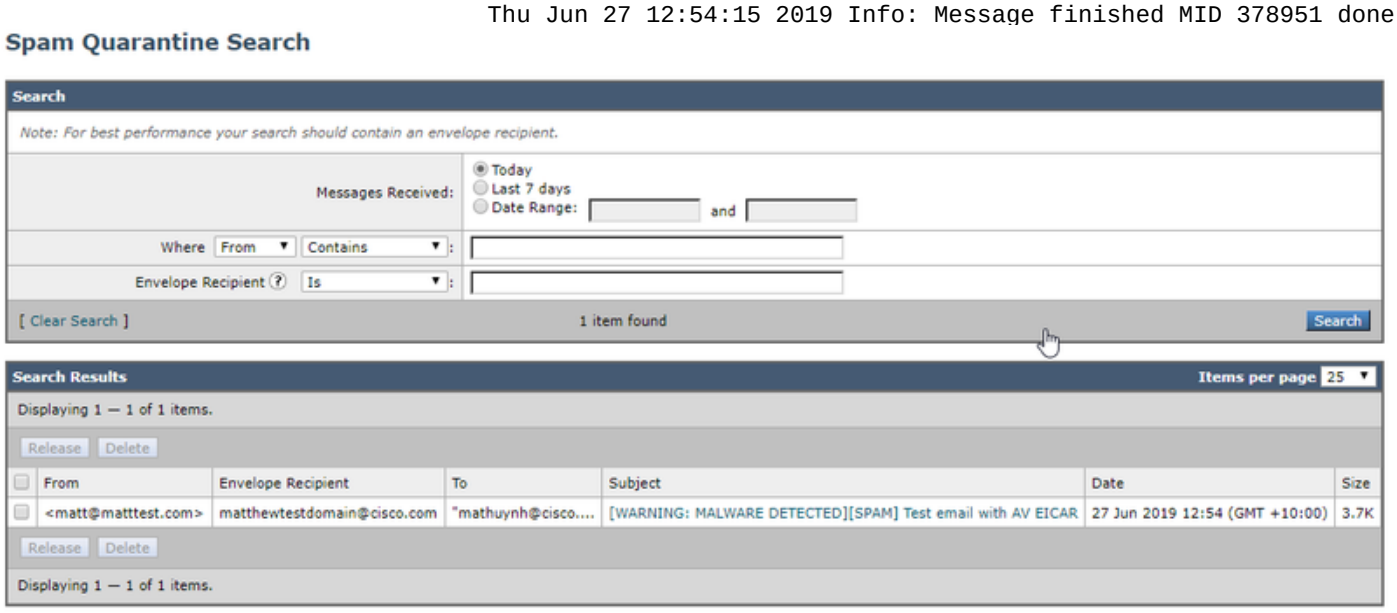
بعد أن يتم إصداره من هذا الفحص، يقوم بتسجيل هذا الحدث في **mail_log** الخاص بك وينعكس على عمليات الحجر الأخرى أيضا أنه لم يعد متوفرا في العزل الآخر.

```
Thu Jun 27 12:52:59 2019 Info: MID 378951 released from quarantine "Virus" (manual) t=104
```



قم بإخراجه من حجر PVO الذي يبقى يسمح لرسائل البريد الإلكتروني بالسفر إلى الحجر الصحي للبريد العشوائي الذي تم وضع علامة عليه بعد ذلك.

```
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from quarantine "Policy" (manual) t=180
Thu Jun 27 12:54:15 2019 Info: MID 378951 released from all quarantines
Thu Jun 27 12:54:15 2019 Info: MID 378951 matched all recipients for per-recipient policy matt
in the inbound table
Thu Jun 27 12:54:15 2019 Info: MID 378951 interim AV verdict using Sophos VIRAL
'Thu Jun 27 12:54:15 2019 Info: MID 378951 antivirus positive 'EICAR-AV-Test
Thu Jun 27 12:54:15 2019 Info: MID 378951 AMP file reputation verdict : MALWARE
(Thu Jun 27 12:54:15 2019 Info: ISQ: Tagging MID 378951 for quarantine (X-Ironport-Quarantine
Thu Jun 27 12:54:15 2019 Info: MID 378951 queued for delivery
Thu Jun 27 12:54:15 2019 Info: RPC Delivery start RCID 13914 MID 378951 to local IronPort Spam
Quarantine
Thu Jun 27 12:54:15 2019 Info: ISQ: Quarantined MID 378951
Thu Jun 27 12:54:15 2019 Info: RPC Message done RCID 13914 MID 378951
Thu Jun 27 12:54:15 2019 Info: Message finished MID 378951 done
```



هناك في الإصدار النهائي من العزل العشوائي، يتم توجيه البريد الإلكتروني لقائمة انتظار التسليم.

(Thu Jun 27 12:55:33 2019 Info: **Start MID 378952 ICID 0 (ISQ Released Message**
Thu Jun 27 12:55:33 2019 Info: ISQ: Reinjected MID 378951 as MID 378952
<Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 From: <matt@lee2.com
<Thu Jun 27 12:55:33 2019 Info: MID 378952 ICID 0 RID 0 To: <matthewtestdomain@cisco.com
Thu Jun 27 12:55:33 2019 Info: MID 378952 Subject '[WARNING: MALWARE DETECTED][SPAM] Test email
'with AV EICAR
<Thu Jun 27 12:55:33 2019 Info: MID 378952 ready 9661 bytes from <matt@lee2.com
Thu Jun 27 12:55:33 2019 Info: **MID 378952 queued for delivery**

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).