إختبار ESA للحماية المتقدمة من البرامج الضارة (AMP)

المحتويات

المقدمة

يوضح هذا المستند كيفية إختبار ميزات الحماية المتقدمة من البرامج الضارة (AMP) والتحقق منها من جهاز أمان البريد الإلكتروني (ESA) من Cisco.

إختبار AMP على ESA

مع إصدار AsyncOS 8.5 ل ESA، تقوم AMP بإجراء مسوحات سمعة الملف وتحليل الملفات لاكتشاف البرامج الضارة في المرفقات.

مفاتيح الميزة

من أجل تنفيذ AMP، يجب أن يكون لديك مفتاح ميزة صالح ونشيط لكل من **سمعة الملف** وتحليل **الملف** على ESA الخاص بك. قم بزيارة **إدارة النظام>**سمة **مفتاح** على ال gui، أو استعملت **سمة** مفتاح على ال CLI، in order to دققت السمة مفتاح.

الخدمات الأمنية

لتمكين الخدمة من واجهة المستخدم الرسومية، انتقل إلى **خدمات الأمان > سمعة الملف وتحليله**. من واجهة سطر

الأوامر (CLI)، يمكنك تشغيل **ampconfig**. إرسال التغييرات التي أجريتها إلى التكوين وتنفيذها.

نهج البريد الوارد

بمجرد تمكين الخدمة، يجب ربط هذه الخدمة بنهج البريد الوارد.

1. انتقل إلى **نهج البريد > نهج البريد الوارد**.

2. حدد **النهج الافتراضي** أو النهج الذي تم تكوينه مسبقا حسب الحاجة. عمود **الحماية المتقدمة من البرامج الضارة** الموجود على طرق عرض صفحة سياسات البريد الوارد.

3. حدد الرابط **معطل** للعمود، و**تمكين سمعة الملف** و**تمكين تحليل الملف** في صفحة الخيارات.

4. يمكنك إجراء أي تحسينات إضافية على التكوين لمسح الرسائل، والإجراءات الخاصة بالمرفقات التي لا يمكن مسحها ضوئيا، والإجراءات الخاصة بالرسائل المحددة بشكل إيجابي، حسب الحاجة.

5. إرسال التغييرات التي أجريتها إلى التكوين وتنفيذها.

إختبار

في هذا الوقت، يتم تمكين نهج البريد الوارد الخاص بك من فحص البرامج الضارة والكشف عنها. يجب أن يكون لديك نموذج برنامج ضار حقيقي للاختبار به. إذا كنت بحاجة إلى أمثلة صالحة، فراجع صفحة التنزيلات الخاصة بالمعهد الأوروبي لأبحاث مكافحة الفيروسات الخاصة بالكمبيوتر (EICAR).

تحذير: لا يمكن أن تتحمل Cisco المسؤولية عندما تتسبب هذه الملفات أو ماسح AV بالاشتراك مع هذه الملفات في أي ضرر على بيئة الكمبيوتر أو الشبكة. يمكنك تنزيل هذه الملفات على مسؤوليتك الخاصة. قم بتنزيل هذه الملفات فقط إذا كنت آمنا بشكل كاف في إستخدام ماسح AV وإعدادات الكمبيوتر وبيئة الشبكة. وتقدم هذه المعلومات على سبيل المجاملة لأغراض الاختبار والاستنساخ.

باستخدام حساب بريد إلكتروني صحيح تم تكوينه مسبقا، قم بإرسال المرفق من خلال ESA الخاص بك والمعالجة العادية. أنت يستطيع استعملت ال CLI من ال in order to **tail mail_log**، ESA راقبت البريد بما أن هو يعالج. سترى معرف الرسالة (MID) المدرج في سجلات البريد. مخرجات مماثلة لهذه الشاشات:

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com (192.168.0.199)
                                                                verified yes
        Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
                                                                SBRS 5.5 [-1.0:10.0]
                                Thu Sep 18 16:17:38 2014 Info: Start MID 1653 ICID 16488
<Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 From: <joe_user@hotmail.com
                                :Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 RID 0 To
                                                                <any.one@mylocal_domain.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 Message-ID '<BLU437-SMTP10E1315A60354F2
                                                                '<906677B9DB70@phx.gbl
                ''Thu Sep 18 16:17:38 2014 Info: MID 1653 Subject 'Your Daily Update
                        Thu Sep 18 16:17:38 2014 Info: MID 1653 ready 2313 bytes from
                                                                <joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 matched all recipients for per-recipient
```

```
policy DEFAULT in the inbound table
Thu Sep 18 16:17:38 2014 Info: ICID 16488 close
:Thu Sep 18 16:17:39 2014 Info: MID 1653 interim verdict using engine
CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 using engine: CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 AMP file reputation verdict : MALWARE
Thu Sep 18 16:17:39 2014 Info: Message aborted MID 1653 Dropped by amp
Thu Sep 18 16:17:39 2014 Info: Message finished MID 1653 done
```

يوضح المثال السابق أن AMP اكتشف مرفق البرامج الضارة **وتم إسقاطه** كإجراء نهائي لكل الإعدادات الافتراضية.

ويمكن الاطلاع على نفس التفاصيل أيضا في ميزة تعقب الرسائل من واجهة المستخدم الرسومية (GUI):

18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 contains attachment 'eicar.com' (SHA256 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f).
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 scanned by Advanced Malware Protection engine. Final verdict: malicious
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 attachment 'eicar.com' scanned by Advanced Malware Protection engine. Verdict: Positive
18 Sep 2014 21:54:30 (GMT -04:00)	Message ID 1655 rewritten to new message ID 1656 by AMP.

إذا أخترت تسليم برامج ضارة محددة بشكل إيجابي أو خيارات متقدمة أخرى في تكوين AMP من نهج البريد الوارد، فقد ترى نتيجة معالجة البريد هذه:

```
Thu Sep 18 21:54:30 2014 Info: MID 1655 AMP file reputation verdict : MALWARE
Thu Sep 18 21:54:30 2014 Info: MID 1655 rewritten to MID 1656 by AMP
```

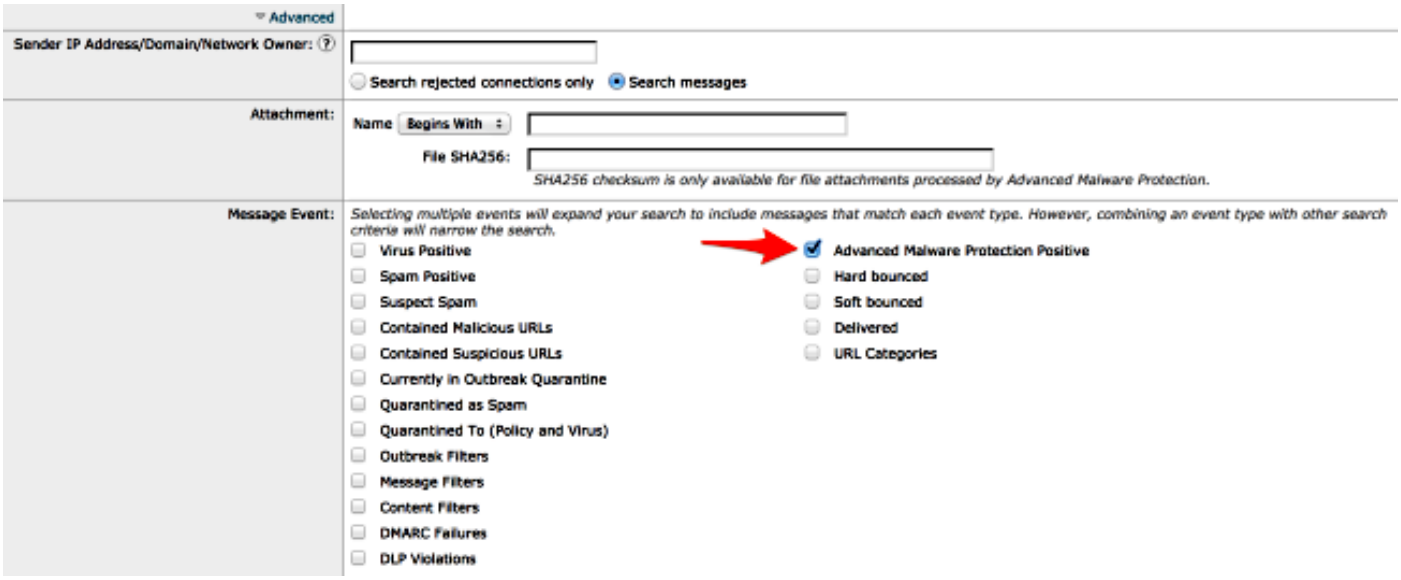
لا يزال الحكم على السمعة إيجابيا بالنسبة للبرامج **الضارة** كما هو موضح. الإجراء المعاد كتابته هو وفقا لإجراءات تعديل الرسالة وبداية سطر الموضوع [**WARNING: البرامج الضارة التي تم الكشف عنها**].

الملف النظيف، أو الملف الذي لم يتم تعريفه في وقت المعالجة على أنه برنامج ضار، يكتب الحكم إلى سجلات البريد:

```
Thu Sep 18 21:58:33 2014 Info: MID 1657 AMP file reputation verdict : CLEAN
```

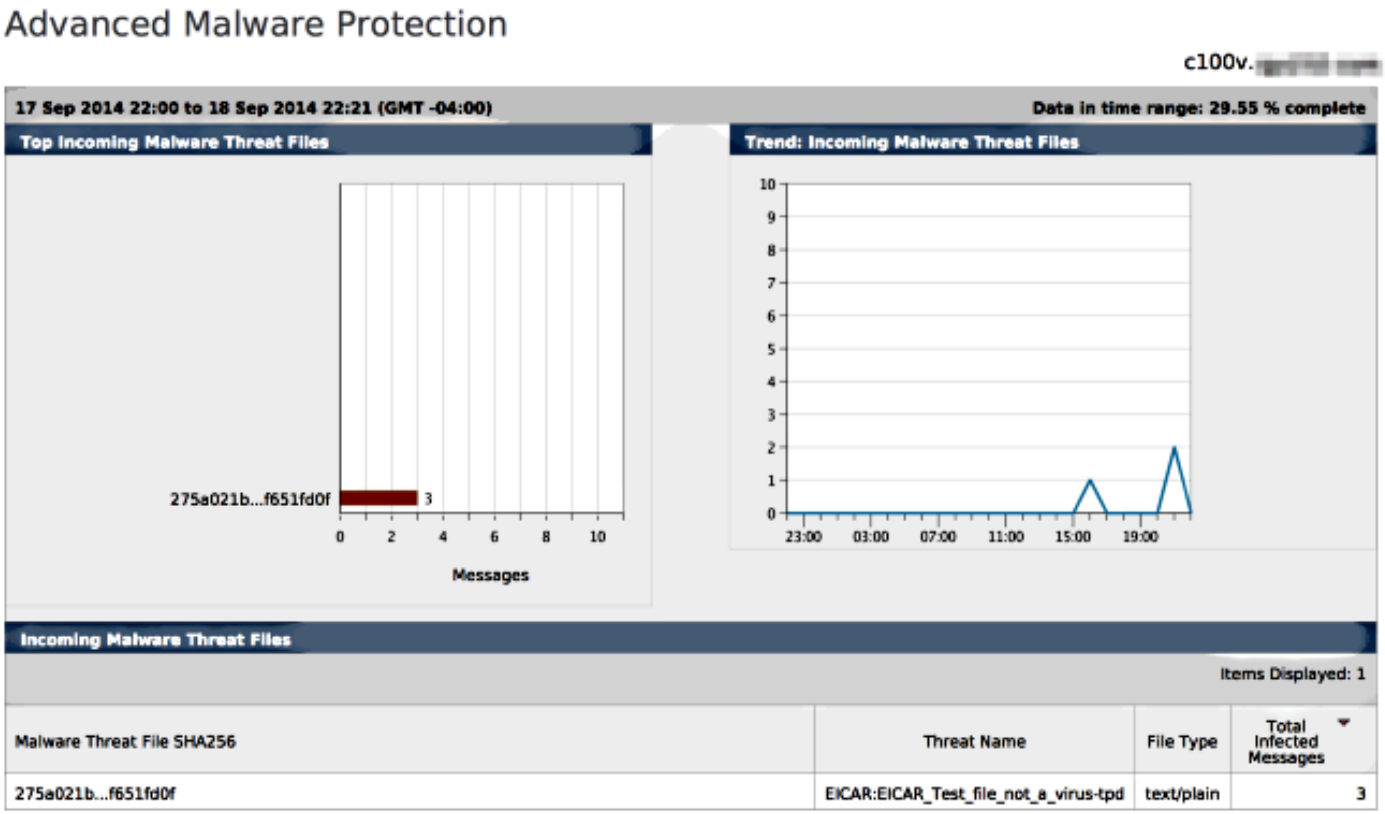
التعقب المتقدم للرسائل لرسائل AMP+

أيضا من واجهة المستخدم الرسومية، عند إستخدام تعقب الرسائل والقائمة المنسدلة المتقدمة، يمكنك إختيار البحث عن رسالة إيجابية متقدمة للحماية من البرامج الضارة مباشرة:



تقارير الحماية المتقدمة من البرامج الضارة

من واجهة المستخدم الرسومية (GUI) لوكالة الفضاء الأوروبية، يمكنك أيضا الاطلاع على تتبع التقارير للرسائل المحددة بشكل إيجابي من خلال AMP. انتقل إلى **الشاشة > الحماية المتقدمة من البرامج الضارة** وقم بتعديل النطاق الزمني حسب الحاجة. يمكنك الآن رؤية أمثلة مماثلة، مع الأمثلة السابقة للإدخال:



استكشاف الأخطاء وإصلاحها

إذا لم يظهر لديك ملف برنامج ضار صحيح معروف يتم مسحه بشكل إيجابي بواسطة AMP، فراجع سجلات البريد للتأكد من أن خدمة أخرى لم تتخذ إجراء على الرسالة و/أو المرفق قبل قيام AMP بمسح الرسالة ضوئيا.

من المثال السابق المستخدم، عند تمكين Sophos Anti-Virus، فإنه يلتقط ويتخذ إجراء على المرفق:

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com (192.168.0.199)
                                                              verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
                                                          SBRS 5.5 [-1.0:10.0]
                                Thu Sep 18 22:15:34 2014 Info: Start MID 1659 ICID 16493
<Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 From: <joe_user@hotmail.com
                                :Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 RID 0 To
                                                          <any.one@mylocal_domain.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 Message-ID '<BLU437-SMTP2399199FA50FB
                                                          '<5E71863489DB40@phx.gbl
'Thu Sep 18 22:15:34 2014 Info: MID 1659 Subject 'Daily Update Final
                                Thu Sep 18 22:15:34 2014 Info: MID 1659 ready 2355 bytes from
                                                          <joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 matched all recipients for per-recipient
                                                          policy DEFAULT in the inbound table
```

```
Thu Sep 18 22:15:35 2014 Info: ICID 16493 close
:Thu Sep 18 22:15:35 2014 Info: MID 1659 interim verdict using engine
CASE spam negative
Thu Sep 18 22:15:35 2014 Info: MID 1659 using engine: CASE spam negative
Thu Sep 18 22:15:37 2014 Info: MID 1659 interim AV verdict using Sophos VIRAL
'Thu Sep 18 22:15:37 2014 Info: MID 1659 antivirus positive 'EICAR-AV-Test
Thu Sep 18 22:15:37 2014 Info: Message aborted MID 1659 Dropped by antivirus
Thu Sep 18 22:15:37 2014 Info: Message finished MID 1659 done
```

تم تعيين إعدادات تكوين Sophos Anti-virus على نهج البريد الوارد إلى **إسقاط** للرسائل المصابة بالفيروس. في هذه الحالة، لا يتم الوصول إلى AMP أبدا لإجراء الفحص أو الإجراء على المرفق.

وهذه ليست الحال دائما. قد تكون هناك حاجة إلى مراجعة سجلات البريد ومعرفات الرسائل (MIDs) لضمان عدم إتخاذ خدمة أخرى أو عامل تصفية محتوى/رسالة إجراء مقابل MID قبل معالجة AMP والوصول إلى إجراء.

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).