أستكشاف أخطاء حماية البرامج النصية وإصلاحها في AMP لنقاط النهاية

المحتويات

المقدمة

يصف هذا المستند تكوين محرك حماية البرنامج النصي في الحماية المتقدمة من البرامج الضارة (AMP) لنقاط النهاية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وصول المسؤول إلى وحدة تحكم AMP

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الموصل الإصدار 7.2.1 أو إصدار أحدث
- Windows 10 الإصدار 1709 والإصدارات الأحدث أو Windows Server 2016 الإصدار 1709 والإصدارات الأحدث

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

معلومات أساسية

يوفر محرك حماية البرامج النصية القدرة على اكتشاف البرامج النصية التي يتم

تنفيذها على نقاط النهاية الخاصة بك وحظرها، كما يساعد على الحماية من الهجمات القائمة على البرامج النصية التي تستخدمها البرامج الضارة بشكل عام. ويوفر برنامج "مسار الجهاز" إمكانية رؤية فائقة أثناء تنفيذ السلسلة، وبهذا يمكنك مراقبة التطبيقات التي تقوم بتنفيذ البرامج النصية على أجهزتك.

يسمح المحرك للموصل بمسح أنواع ملفات البرنامج النصي التالية:

التطبيق	ملحق الملف
تطبيق HTML	hta
البرامج النصية	BAT و CMD و VB و VBS و JS
برنامج نصي مشفر	cjs إس إي، cjs إس إي
Windows Script	WS و WASF و SWC و WSH
واو شل	PS1، PS1XML، PSC1، PSC2، MSH، MSH1، MSH2، MSHXML، MSH1XML، MSH2X
الاختصار	SCF
رابط	LNK
إعداد	INF و INX
السجل	reg
كلمة	DOCX و dotx و DOCM و DOTM
Excel	XLS و XLSX و XLTX و XLSM و XLTM و XLAM
واو بوينت	PPT و PPTX و POTX و POTM و PPTM و PPAM و PPSM و SLDM

تعمل حماية البرنامج النصي مع مترجمي البرنامج النصي التاليين:

- PowerShell (الإصدار الثالث والإصدارات الأحدث)
- Windows Script Host (wscript.exe و cscript.exe)
- JavaScript (غير متصفح)
- VBScript
- وحدات ماكرو Office VBA

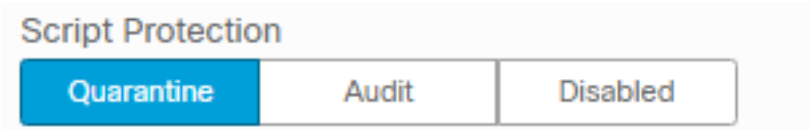
تحذير: لا توفر حماية البرامج النصية إمكانية الرؤية أو الحماية من البرامج النصية المفسرة غير التابعة لـ Microsoft مثل Python أو Perl أو PHP أو Ruby.

تحذير: من المحتمل أن يؤثر وضع إدانة الحجر الصحي على تطبيقات المستخدم مثل Word و Excel و PowerPoint. إذا حاولت هذه التطبيقات تنفيذ برنامج VBA نصي ضار، سيتم إيقاف التطبيق.

تعمل حماية البرنامج النصي **على** إحترام **وضع التشغيل عند التنفيذ**، وتعمل على وضعين مختلفين: **Active** و**Passive**. في الوضع النشط، يتم منع البرامج النصية من التنفيذ حتى يستلم الموصل معلومات عما إذا كان خبيثا أو تم الوصول إلى مهلة. في الوضع الخامل، يتم السماح بتنفيذ البرامج النصية أثناء البحث عن البرنامج النصي لتحديد ما إذا كان خبيثا أم لا.

التكوين

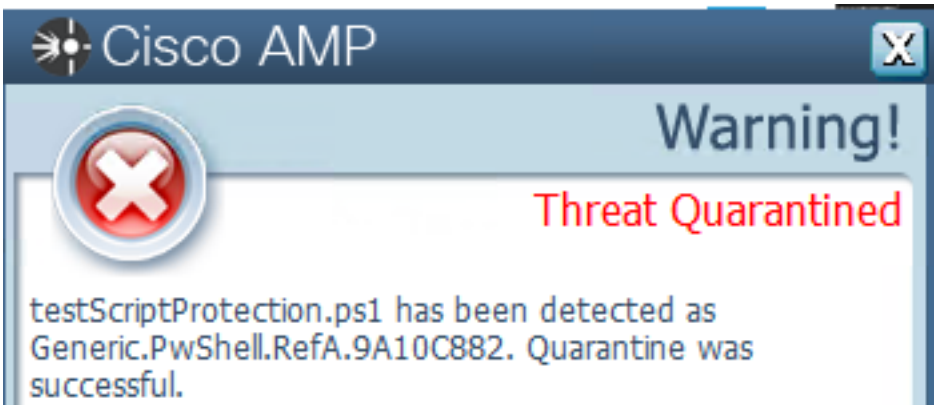
لتمكين حماية البرامج النصية، انتقل إلى إعدادات النهج، ثم تحت "الأوضاع والمحركات" حدد وضع الإدانة للتدقيق أو العزل أو التعطيل، كما هو موضح في الصورة.



ملاحظة: ال تعتمد حماية البرامج النصية على TETRA ولكن إذا تم تمكين TETRA فإنها تستخدم لتوفير حماية إضافية.

اكتشاف

بمجرد تشغيل الكشف، يتم عرض إعلام منبثق على نقطة النهاية، كما هو موضح في الصورة.



تعرض وحدة التحكم حدث "تم الكشف عن تهديد"، كما هو موضح في الصورة.

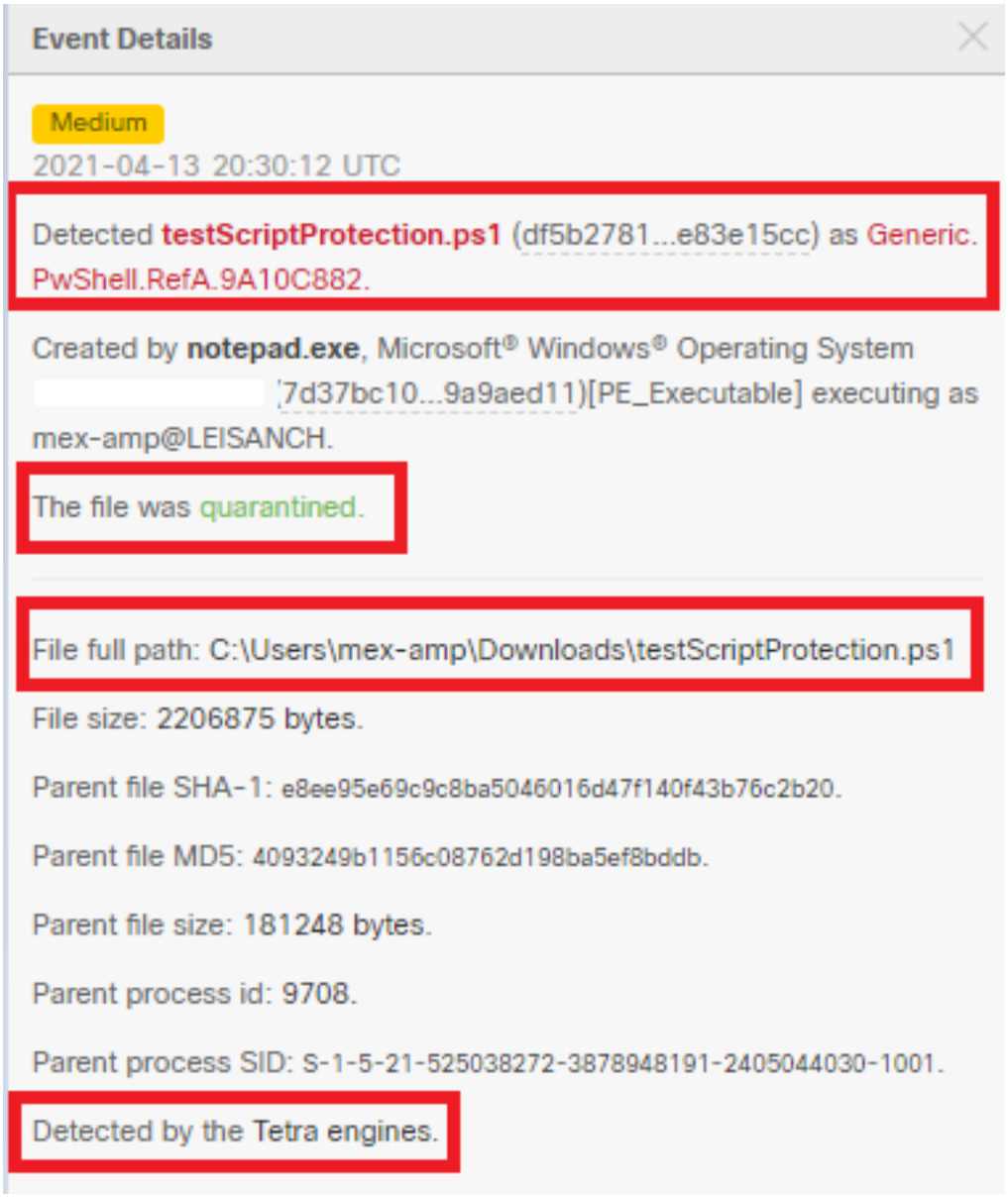
ملاحظة: يخلق وضع التدقيق حدثا عند تنفيذ برنامج نصي ضار، ومع ذلك، فإنه ال يتم عزله.

استكشاف الأخطاء وإصلاحها

ال تحتوي حماية البرامج النصية على نوع حدث محدد عند تشغيل الكشف في وحدة التحكم، وهي طريقة للتعرف على من يكتشف الملف الضار استنادا إلى نوع الملف وأين يتم تشغيله.

1. وقفا لما هو موضح مع البرامج النصية المدعومة، قم بتعريف ملحق الملف، على سبيل المثال، هو برنامج نصي ل .ps1.

2. انتقل إلى **مسار الجهاز > تفاصيل الحدث**، في هذا القسم يتم عرض المزيد من التفاصيل المتعلقة بالملف الذي تم الكشف عنه، مثل SHA256، وهو مسار تم فيه تحديد موقع الملف، واسم التهديد، والإجراء الذي تم إتخاذه بواسطة موصل AMP، والمحرك الذي يكتشفه. في حالة عدم تمكين TETRA، يكون المحرك المعروض SHA Engine، على سبيل المثال، يتم عرض TETRA حيث أنه عند تمكين TETRA، يعمل مع حماية البرنامج النصي لتوفير حماية إضافية، كما هو موضح في الصورة.

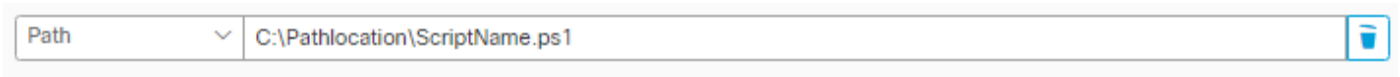


التحقيق في الكشف

لتحديد ما إذا كان الكشف صادرا بالفعل أم لا، يمكنك إستخدام "مسار الجهاز" لتوفير إمكانية رؤية للأحداث التي حدثت أثناء تشغيل البرنامج النصي مثل العمليات الأصلية، والاتصالات بالمضيفين عن بعد، والملفات غير المعروفة التي يمكن تنزيلها من قبل البرامج الضارة.

الكشف الإيجابي الكاذب

بمجرد التعرف على الكشف وإذا كان البرنامج النصي موثوقا به ومعروفا من قبل البيئة الخاصة بك، يمكن تسميته موجب كاذب. لمنع الموصل من مسحه، يمكنك إنشاء إستثناء لذلك البرنامج النصي، كما هو موضح في الصورة.



ملاحظة: تأكد من إضافة مجموعة الاستبعاد إلى السياسة المطبقة على الموصل المتأثر.

معلومات ذات صلة

- دليل مستخدم AMP
- 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).