أستكشاف أخطاء أجهزة الويب الآمنة وسجلات الحماية المتقدمة من البرامج الضارة وإصلاحها (إصدار الأحكام)

المحتويات

المقدمة

يصف هذا المستند قسم الأحكام في مستوى سجل **المعلومات وتصحيح الأخطاء** الخاص بمحرك الحماية المتقدمة من البرامج الضارة (AMP) الخاص بجهاز أمان الويب (WSA).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تم تثبيت WSA
- تم تمكين سمعة الملف وتحليل الملفات
- الحماية المتقدمة من البرامج الضارة
- جهاز الويب الآمن من Cisco
- عميل SSH

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

معلومات أساسية

يوفر WSA التكامل مع AMP لنقاط النهاية ومحرك AMP المحلي. توفر AMP الحماية من البرامج الضارة لمدة ال تتجاوز يوما واحدا من خلال مميزات تحليل الملفات والسمعة الجيدة للملفات. يتضمن WSA محرك ما قبل التصنيف مسؤول عن فحص الملفات داخليا قبل

عمليات التحقق من الشبكة العامة. السجلات الموضحة في القسم التالي مرتبطة بمحرك AMP على WSA وليس بسحابة AMP أو شبكة التهديد.

أستكشاف أخطاء سجلات WSA AMP وإصلاحها

الوصول إلى سجلات AMP. قم بتسجيل الدخول عبر واجهة سطر الأوامر (CLI) وتذييل سجلات amp أو تجزئتها:

1. سجل الدخول إلى **واجهة سطر الأوامر** من خلال عميل SSH.

2. اكتب الأمر **grep** واضغط **مفتاح الإدخال**.

3. أدخل رقم **amp_log** عند طلبه.

4. قم بالإجابة على الخيارات التالية (إذا قمت بتشغيل حركة مرور مباشرة، أختر الخيار **لتذييل** السجلات).
5. اضغط على المفتاح **Enter**.

6. يتم عرض السجلات.

توجد سجلات WSA AMP في مستويات مختلفة من المعلومات، يمكنك تحديد مستوى **المعلومات** أو **تصحيح الأخطاء** للنتائج التي تحتوي على إختلافات طفيفة موضحة في القسم التالي.

ملاحظة: يلزم تثبيت ترخيص AMP على WSA لتحديد سجلات AMP.

سجلات مستوى معلومات AMP:

```
Wed Apr 27 12:21:26 2022 Info: Txn 18210 Binary scan on instance[0] Id[1345]: AMP allocated
memory = 0, AMP used memory = 0, Scans in flight = 1, Active faster connections = 1, Active
slower connections = 0
Wed Apr 27 12:21:35 2022 Info: Binary scan on instance[0] id[1345]:
filename[npp.8.4.Installer.x64.exe] filemime[application/x-dosexec] file_extension[exe]
length[4493047b] ampverdict[(1, 1, 'amp', '', 0, 0, True)] scanverdict[0] malwareverdict[0]
spyname[] SHA256[ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1] From[Cloud]
uploadreason[Enqueued in the local queue for submission to upload] verdict_str[FILE UNKNOWN]
is_slow[0] scans_in_flight[0] Active faster connections[0] Active slower connections[0]
Wed Apr 27 12:22:28 2022 Info: File uploaded for analysis. Server:
https://panacea.threatgrid.com, SHA256:
ecdcf497418a1988ebf20c647acadc9eca7bc8569fd980713582acd0de011ba1, Filename:
npp.8.4.Installer.x64.exeTimestamp: 1651044116 sampleid[]
```

سجلات مستوى معلومات AMP (إصدار الأحكام):

```
ampverdict[(1, 1, 'amp', '', 0, 0, True)]
(analysis_Action, scan_verdict, ‘verdict_source', ‘spyname’, malware_verdict, file_reputation,
upload_action)]
```

سجلات مستوى تصحيح أخطاء AMP:

```
Fri Apr 29 01:38:40 2022 Debug: Binary scan: proxid[3951] filename[favicon.ico] len[41566b]
readtime[109.721680ms] scantime[2.205322ms] ampverdict[(1, 1, 'amp', '', 0, 0, False)]
scanverdict[0] malwareverdict[0]
```

```
SHA256[e7a2345c75a03e63202b12301c29bb8b6bae7cef9e191ed58797ec028def7c4f] From[Cloud]
FileName[favicon.ico] FileMime[application/octet-stream]
```

سجلات مستوى تصحيح أخطاء AMP (إصدار الأحكام):

```
ampverdict[(1, 1, 'amp', '', 0, 0, False)]
ampverdict[(analysis_action, scan_verdict,disposition, ‘spyname: policy name if amp registered
with console’, file_reputation, upload_action, ‘sha256', ‘threat_name’)]
```

خيارات حقل تفصيلي مقابل قيمة:

الحقل	القيمة
إجراء_تحليل	يشير "0" إلى أن "الحماية المتقدمة من البرامج الض لم تطلب تحميل الملف للتحليل يشير "1" إلى أن "الحماية المتقدمة من البرامج الض طلبت تحميل الملف للتحليل
Scan_Verdict	0: الملف غير ضار 1: لم يتم مسح الملف ضوئيا بسبب نوع الملف الخاص به 2: انتهت مهلة فحص الملفات 3: خطأ في المسح أكبر من 3: الملف ضار
مصدر الحكم	AMP: تحليل الملفات
قابلية	1: غير معروف 2: نظيف 3: ضار (AMP) 4: غير قابل للمسح (غير قابل للمسح الضوئي)
اسم التجسس	فارغ: إذا لم يتم إستخدام نهج تفشي AMP Simple_Custom_Detection: في حالة إستخدام نهج ت AMP
تحميل_إجراء	صحيح: تم ضبط الملف على وضع الحماية خطأ: لم يتم إرسال الملف إلى المربع الرملي
SHA256	SHA256
اسم_التهديد	اسم التهديد استنادا إلى أنواع تهديدات الحماية المتقدمة (AMP)

معلومات ذات صلة

- دمج الحماية المتقدمة (AMP) لنقاط النهاية وشبكة التهديدات مع WSA
- تصفية سمعة الملف وتحليل الملف
- الدعم التقني والمستندات - Cisco الأنظمة

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).