Тест Усовершенствованной вредоносной защиты (AMP) ESA

Содержание

Введение

Этот документ описывает, как протестировать и проверить функции Усовершенствованной вредоносной защиты (AMP) Cisco Email Security Appliance (ESA).

Тестовый AMP на ESA

С выпуском AsyncOS 8.5 для ESA AMP выполняет просмотры репутации файла и анализ файла для обнаружения вредоносного ПО в прикреплениях.

Характерные черты

Для реализации AMP у вас должна быть допустимая и активная характерная черта и для **Анализа Репутации** и для **Файла Файла** вашего ESA. **Администрирование системы** посещения**> Характерные черты** на GUI или использование **featurekeys** на CLI, для проверки характерных черт.

Сервисы безопасности

Для включения сервиса от GUI перейдите к **Сервисам безопасности> Репутация Файла и Анализ**. От CLI можно выполнить **ampconfig**. Отправьте и передайте свои изменения конфигурации.

Политика входящей почты

Как только вы включили сервис, необходимо было связать этот сервис с политикой входящей почты.

1. Перейдите для **Отправки по почте Политики> Политика Входящей почты**.
2. Выберите свою **Политику по умолчанию** или предварительно сконфигурированную политику по мере необходимости. **Усовершенствованный Вредоносный Столбец Защита** на отображениях страницы Полицейских Входящей почты.
3. Выберите **Отключенную** ссылку для столбца, и **Включите Репутацию Файла** и **Включите Анализ Файла** страницы параметров.
4. Можно сделать дальнейшие усовершенствования конфигурации для обмена сообщениями сканирования, действий для неподдающихся сканированию прикреплений и действий для положительно определенных сообщений, по мере необходимости.
5. Отправьте и передайте свои изменения конфигурации.

Тест

В это время вашей политике входящей почты позволяют просмотреть и обнаружить вредоносное ПО. У вас должна быть истинная вредоносная выборка, с которой можно протестировать. Если вы нуждаетесь в достоверных примерах, посещаете европейский Институт Компьютерного Исследования Антивируса (eicar) страница загрузок.

> **Внимание. :** Когда эти файлы или ваш сканер AV в сочетании с этими файлами наносят любой ущерб вашему компьютеру или сетевой среде, Cisco не может считаться ответственной. ЗАГРУЗКА YOU AT ФАЙЛОВ THESE YOUR OWN RISK. Загрузите эти файлы, только если вы достаточно безопасны в использовании вашего сканера AV, компьютерных параметрах настройки и сетевой среде. Эта информация предоставлена как любезность в целях воспроизведения и тесте.

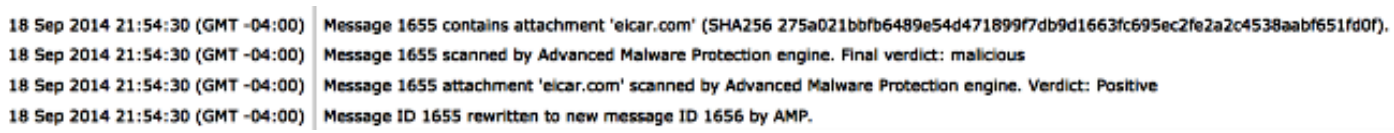
С использованием допустимого предварительно сконфигурированный почтовый ящик передайте прикрепление через свой ESA и обычную обработку. Можно использовать CLI ESA и **хвост mail_logs** для мониторинга почты, поскольку это обрабатывает. Вы будете видеть Идентификатор сообщения (MID), перечисленный в почтовых журналах. Выходные данные, подобные этому, отображаются:

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
```

```
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
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
```

Предыдущий пример показывает, что AMP обнаружил вредоносное прикрепление и **понизился** как заключительное действие на настройки по умолчанию.

Те же подробные данные также замечены в Отслеживании сообщений по 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.

Если вы принимаете решение отправить положительно определенное вредоносное ПО или другие расширенные настройки в конфигурации AMP от Политики Входящей почты, вы могли бы видеть, что эта почта обработала результат:

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
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
```

Вердикт репутации все еще положителен для **ВРЕДОНОСНОГО ПО** как показано. Переписанное действие на действия модификации сообщения и предварительное

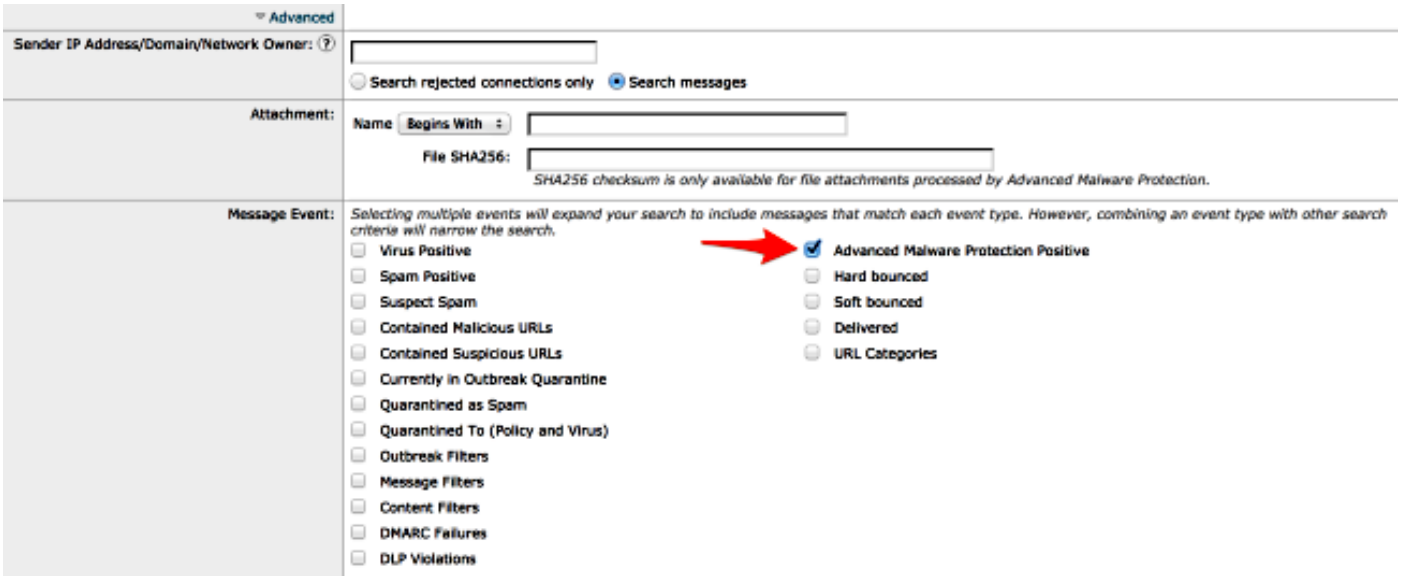
ожидание строки темы **[ПРЕДУПРЕЖДАТЬ: ВРЕДОНОСНОЕ ПО, ОБНАРУЖЕННОЕ]**.

Чистому файлу или файлу, который не был определен во время обработки как вредоносное ПО, записали этот вердикт в почтовые журналы:

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
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
```

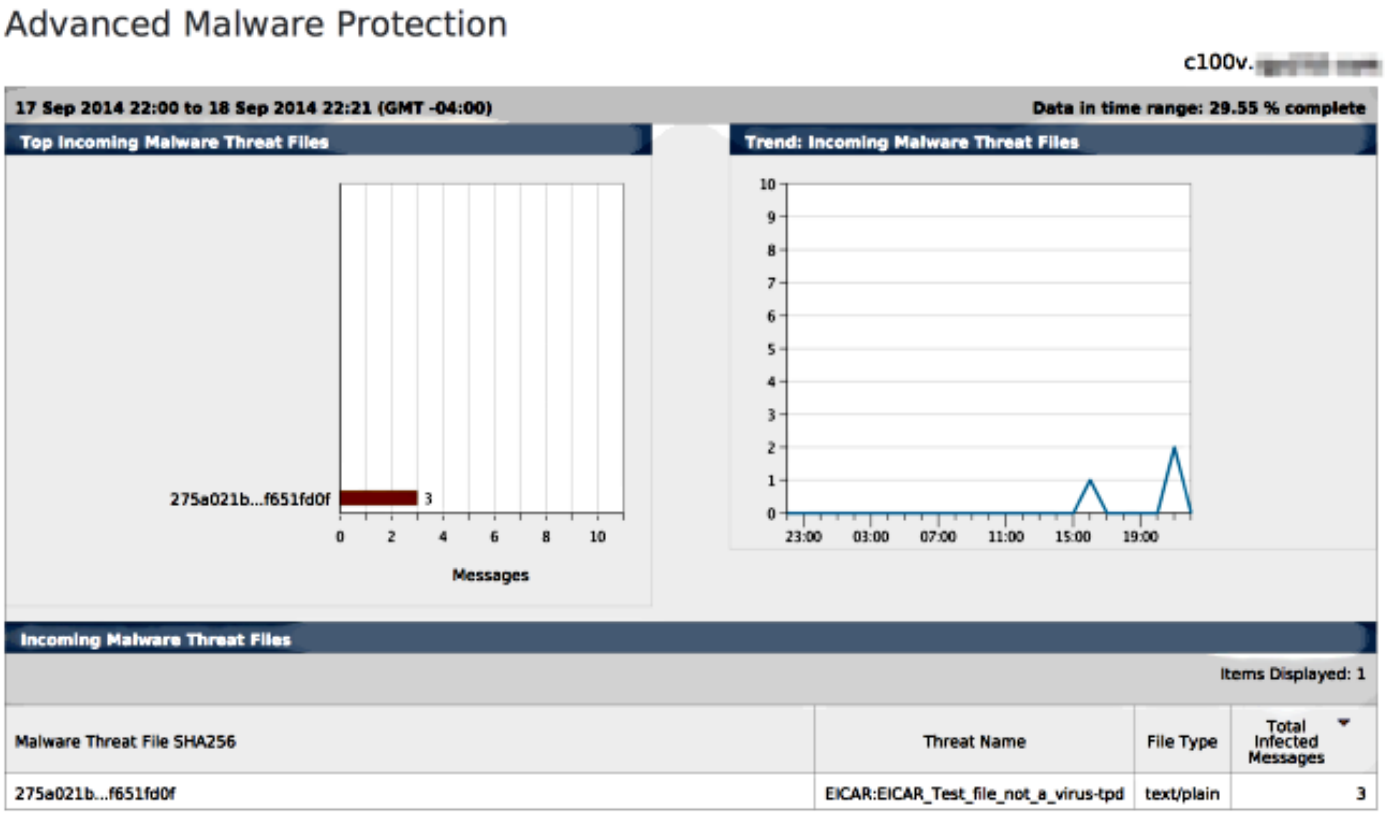
Усовершенствованное отслеживание сообщений для AMP + сообщения

Также от GUI при использовании Отслеживания сообщений и Усовершенствованного раскрывающегося меню можно принять решение искать Усовершенствованный Вредоносный Позитивный сигнал Защиты непосредственно:



Усовершенствованные вредоносные отчёты о защите

От GUI ESA вы также видите отчёт отследить для положительно определенных сообщений через AMP. Перейдите, чтобы **Контролировать> Усовершенствованная Вредоносная Защита** и модифицировать временной диапазон по мере необходимости. Вы теперь видите подобный с предыдущими примерами для ввода:



Устранение неполадок

Если вы не видите известный, истинный вредоносный файл, который положительно просмотрен AMP, рассмотрите почтовые журналы, чтобы гарантировать, что другой сервис не принял меры на сообщении и/или прикреплении, прежде чем AMP просмотрел сообщение.

От более раннего используемого примера, когда Антивирус Sophos включен, он фактически ловит и принимает меры на прикреплении:

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
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
```

Антивирусные параметры конфигурации Sophos на политике входящей почты собираются **понизиться** для зараженных сообщений вируса. В этом случае AMP никогда не достигается, чтобы просмотреть или принять меры на прикреплении.

Это не всегда имеет место. Анализ почтовых журналов и Идентификаторов сообщения (СЕРЕДИНЫ) мог бы быть необходим, чтобы гарантировать, что был достигнут другой сервисный OR, фильтр содержания/сообщения не принял меры против MID перед обработкой AMP и действием.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация