ESA Advanced Malware Protection (AMP)-Test

Inhalt

[Einführung](#)
[AMP auf der ESA testen](#)
[Feature-Schlüssel](#)
[Security-Services](#)
[Richtlinien für eingehende E-Mails](#)
[Test](#)
[Erweiterte Nachrichtenverfolgung für AMP+-Nachrichten](#)
[Advanced Malware Protection-Berichte](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt, wie die AMP-Funktionen (Advanced Malware Protection) der Cisco E-Mail Security Appliance (ESA) getestet und verifiziert werden.

AMP auf der ESA testen

Mit der Veröffentlichung von AsyncOS 8.5 für die ESA führt AMP Dateireputations-Scans und Dateianalysen durch, um Malware in Anhängen zu erkennen.

Feature-Schlüssel

Um AMP zu implementieren, benötigen Sie einen gültigen und aktiven Feature-Schlüssel für **Dateireputation** und **Dateianalyse** auf Ihrer ESA. Besuchen Sie **Systemverwaltung > Feature Keys** in der GUI, oder verwenden Sie **Feature Keys** in der CLI, um die Feature-Schlüssel zu überprüfen.

Security-Services

Um den Dienst über die Benutzeroberfläche zu aktivieren, wählen Sie **Sicherheitsdienste > Dateireputation und Analyse aus**. Über die CLI können Sie **Ampconfig** ausführen. Senden Sie Ihre Änderungen und bestätigen Sie sie.

Richtlinien für eingehende E-Mails

Sobald Sie den Dienst aktiviert haben, muss dieser Dienst an eine Richtlinie für eingehende E-Mails gebunden sein.

1. Navigieren Sie zu **Mail-Policys > Mail-Policys für eingehende E-Mails**.
2. Wählen Sie Ihre **Standardrichtlinie** oder vorkonfigurierte Richtlinie aus. Die Spalte **"Advanced Malware Protection"** auf der Seite "Incoming Mail Polices" (Mail-Polices für eingehende E-Mails) wird angezeigt.
3. Wählen Sie den Link **Deaktiviert** für die Spalte aus, und **aktivieren Sie auf** der Optionsseite Dateireputation und **Dateianalyse aktivieren**.
4. Sie können bei Bedarf weitere Konfigurationsverbesserungen beim Scannen von Nachrichten, Aktionen für nicht scannbare Anhänge und Aktionen für positiv identifizierte Nachrichten vornehmen.
5. Senden Sie Ihre Änderungen und bestätigen Sie sie.

Test

Zu diesem Zeitpunkt ist Ihre Richtlinie für eingehende E-Mails aktiviert, um Malware zu prüfen und zu erkennen. Sie benötigen ein echtes Malware-Beispiel, mit dem Sie testen können. Wenn Sie gültige Beispiele benötigen, besuchen Sie die Download-Seite des European Institute for Computer Antivirus Research (eicar).

> **Vorsicht**: Cisco kann nicht haftbar gemacht werden, wenn diese Dateien oder Ihr AV-Scanner in Verbindung mit diesen Dateien Schäden an Ihrem Computer oder Ihrer Netzwerkumgebung verursachen. SIE LADEN DIESE DATEIEN AUF EIGENES RISIKO HERUNTER. Laden Sie diese Dateien nur herunter, wenn Sie über ausreichende Sicherheit bei der Verwendung Ihres AV-Scanners, der Computereinstellungen und der Netzwerkumgebung verfügen. Diese Informationen werden zu Test- und Reproduktionszwecken zur Verfügung gestellt.

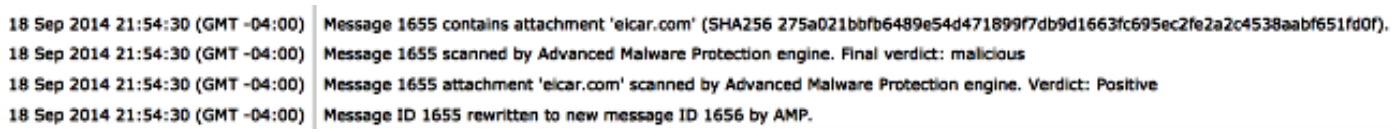
Wenn Sie ein gültiges vorkonfiguriertes E-Mail-Konto verwenden, senden Sie den Anhang über Ihre ESA und normale Verarbeitung. Sie können die CLI der ESA und **tail mail_logs** verwenden, um die E-Mail bei der Verarbeitung zu überwachen. Die Nachrichten-ID (MID) wird in den Mail-Protokollen angezeigt. Eine ähnliche Ausgabe wird angezeigt:

```
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
```

Das vorherige Beispiel zeigt, dass AMP den Malware-Anhang erkannt und gemäß den Standardeinstellungen als endgültige Aktion **verworfen hat**.

Die gleichen Details werden auch in der Nachrichtenverfolgung über die GUI angezeigt:



Wenn Sie eine positiv identifizierte Malware oder andere erweiterte Optionen in der AMP-Konfiguration aus den Richtlinien für eingehende E-Mails bereitstellen möchten, sehen Sie möglicherweise das folgende Ergebnis für die E-Mail-Verarbeitung:

```
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
```

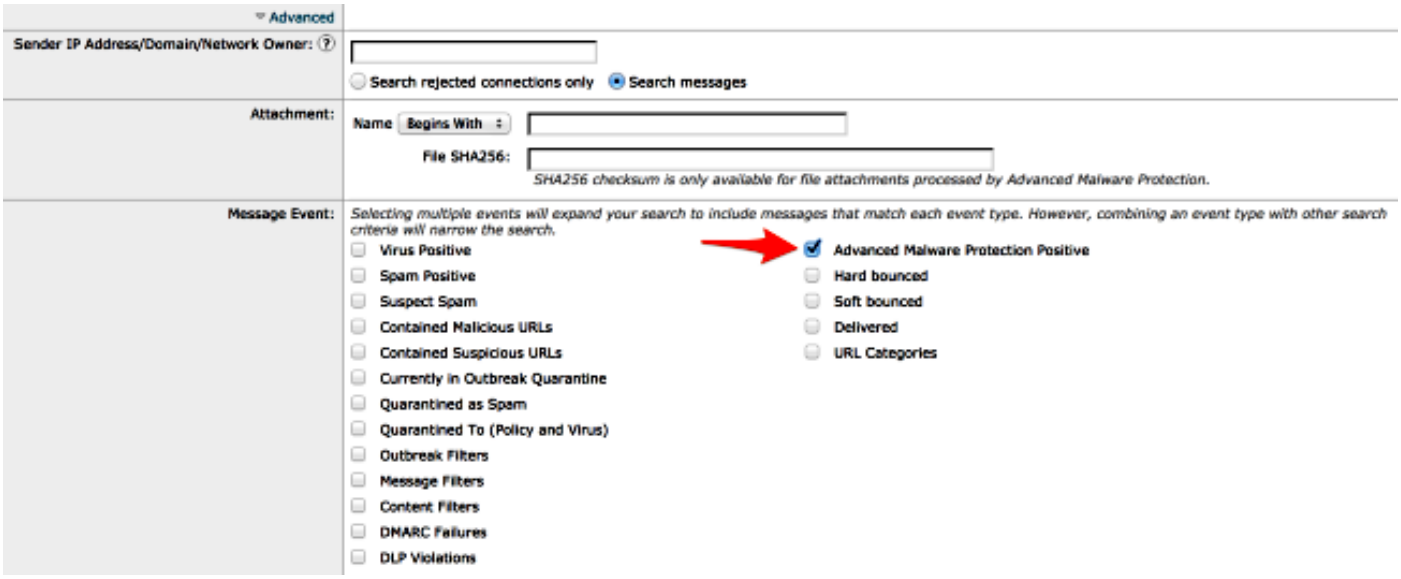
Das Reputationsergebnis für **MALWARE** ist wie gezeigt noch positiv. Die umgeschriebene Aktion gilt für die Aktionen zum Ändern von Nachrichten und für die Betreffzeile vor **[WARNUNG: MALWARE ERKANNT]**.

Bei einer sauberen Datei oder einer Datei, die zur Verarbeitungszeit nicht als Malware identifiziert wurde, wurde dieses Urteil in die E-Mail-Protokolle geschrieben:

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

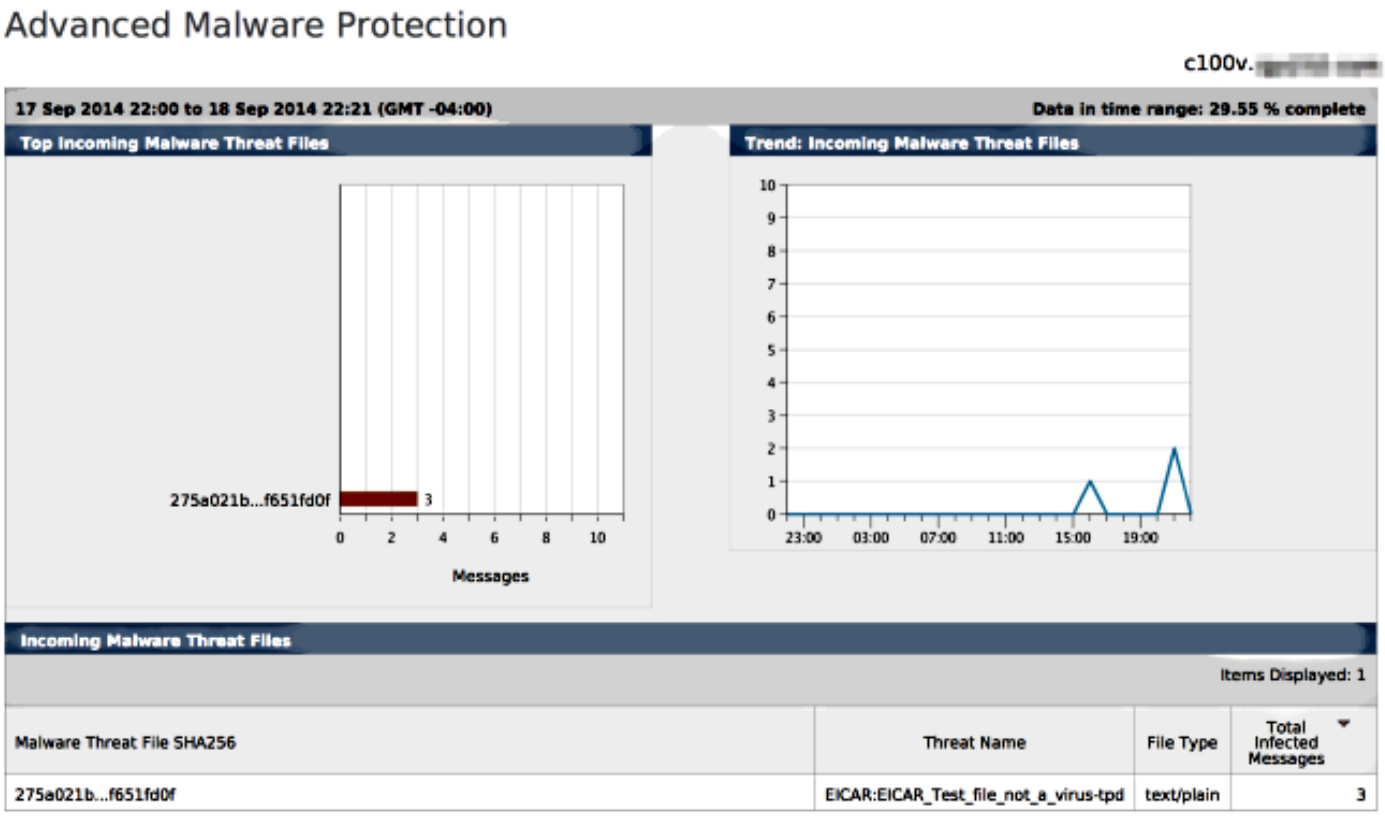
Erweiterte Nachrichtenverfolgung für AMP+-Nachrichten

Wenn Sie die Nachrichtenverfolgung über die Benutzeroberfläche und das Dropdown-Menü Advanced (Erweitert) verwenden, können Sie auch direkt nach einer Nachricht mit dem Status Advanced Malware Protection Positive suchen:



Advanced Malware Protection-Berichte

In der ESA-GUI wird zudem die Berichtsverfolgung für positiv identifizierte Nachrichten über AMP angezeigt. Navigieren Sie zu **Monitor > Advanced Malware Protection**, und ändern Sie den Zeitraum nach Bedarf. Ähnlich sehen Sie nun mit den vorherigen Beispielen für die Eingabe:



Fehlerbehebung

Wenn Sie keine bekannte, echte Malware-Datei sehen, die von AMP positiv gescannt wird, überprüfen Sie die Mail-Protokolle, um sicherzustellen, dass ein anderer Dienst keine Maßnahmen

bezüglich der Nachricht und/oder des Anhangs ergriffen hat, bevor AMP die Nachricht gescannt hat.

Wenn Sophos Anti-Virus aktiviert ist, fängt das zuvor verwendete Beispiel die Anlage an und unternimmt entsprechende Maßnahmen:

```
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
```

Die Sophos Anti-Virus-Konfigurationseinstellungen in der Richtlinie für eingehende E-Mails sind auf **Drop** für mit Viren infizierte Nachrichten eingestellt. In diesem Fall wird AMP nie erreicht, um den Anhang zu scannen oder zu bearbeiten.

Das ist nicht immer der Fall. Möglicherweise ist eine Überprüfung der Mail-Protokolle und Nachrichten-IDs (MIDs) erforderlich, um sicherzustellen, dass ein anderer Dienst ODER ein Content-/Nachrichtenfilter vor der AMP-Verarbeitung keine Maßnahmen gegen die MID ergriffen und eine Aktion erreicht hat.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems