ESA Advanced Malware Protection (AMP) Test

Inhoud

[Inleiding](#)
[Test AMP op de ESE](#)
[Functiesets](#)
[Security services](#)
[Inkomensbeleid per e-mail](#)
[Test](#)
[Geavanceerde berichttracering voor AMP+ berichten](#)
[Geavanceerde Malware-beschermingsrapporten](#)
[Problemen oplossen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe de Advanced Malware Protection (AMP)-functies van de Cisco e-mail security applicatie (ESA) moeten worden getest en geverifieerd.

Test AMP op de ESE

Met de release van AsyncOS 8.5 voor het ESA, voert AMP scans van de bestands reputatie en bestandsanalyse uit om malware in bijlagen te detecteren.

Functiesets

Om een Advanced Malware Protection te kunnen implementeren, moet u een geldige en actieve functiesets hebben voor zowel **File Reputation** als **File Analysis** op uw ESA. Bezoek **System Administration> Functiesets** op de GUI, of gebruik **functies** op de CLI om de functietoetsen te controleren.

Security services

Om de service vanuit de GUI te activeren, navigeer naar **Security Services > File Reputation and Analysis**. Van de CLI, kun je **ampfig** uitvoeren. Geef uw wijzigingen in de configuratie voor.

Inkomensbeleid per e-mail

Nadat u de service hebt ingeschakeld, dient u deze service aan een inkomend postbeleid te gekoppeld.

1. Navigeer naar **postbeleid > Inkomend postbeleid**.
2. Selecteer uw standaardbeleid of **vooringesteld** beleid indien nodig. De kolom **Advanced Malware Protection** in de pagina met inkomende e-mail politiek toont.
3. Selecteer de koppeling **Uitgeschakeld** voor de kolom en **Bestand uploaden** en **Bestandsanalyse** op de optiepagina **inschakelen**.
4. U kunt indien nodig verdere configuratieverbeteringen aanbrengen in het scannen van berichten, in acties voor niet-gescande bijlagen en in acties voor positief geïdentificeerde berichten.
5. Geef uw wijzigingen in de configuratie voor.

Test

Op dit moment is uw inkomende e-mailbeleid in staat om malware te scannen en te detecteren. U moet een echt malware monster hebben waarmee u kunt testen. Indien u goede voorbeelden nodig hebt, bezoek dan de downloads van de downloads van het Europese Instituut voor Computer Antivirus Research (ECAR).

> **Waarschuwing**: Cisco kan niet verantwoordelijk worden gehouden wanneer deze bestanden of uw AV-scanner in combinatie met deze bestanden uw computer of netwerkomgeving beschadigen. U DOWNLOAD DEZE BESTANDEN OP UW EIGEN RISICO. Download deze bestanden alleen als u voldoende veilig bent in het gebruik van uw AV-scanner, computerinstellingen en een netwerkomgeving. Deze informatie wordt verstrekt met het oog op test- en reproductiedoeleinden.

Verstuur de bijlage met behulp van een geldig vooraf ingesteld e-mailaccount en normale verwerking. U kunt de CLI van de ESA gebruiken, en **tail mail_logs** om de mail te controleren zoals het verwerkt. U ziet de Bericht-ID (MID) in de maillogs. Uitvoer vergelijkbaar met deze displays:

```
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
```

Het vorige voorbeeld toont aan dat AMP de malware bijlage heeft gedetecteerd en als de definitieve actie per de standaardinstellingen **is gevallen**.

Dezelfde details worden ook gezien in Message Tracking van de 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.

Als u er voor kiest om positief geïdentificeerd malware of andere geavanceerde opties in de configuratie van het KAMP van het Inkomende beleid van de Post te leveren, kunt u deze uitkomst van de postverwerking zien:

```
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
```

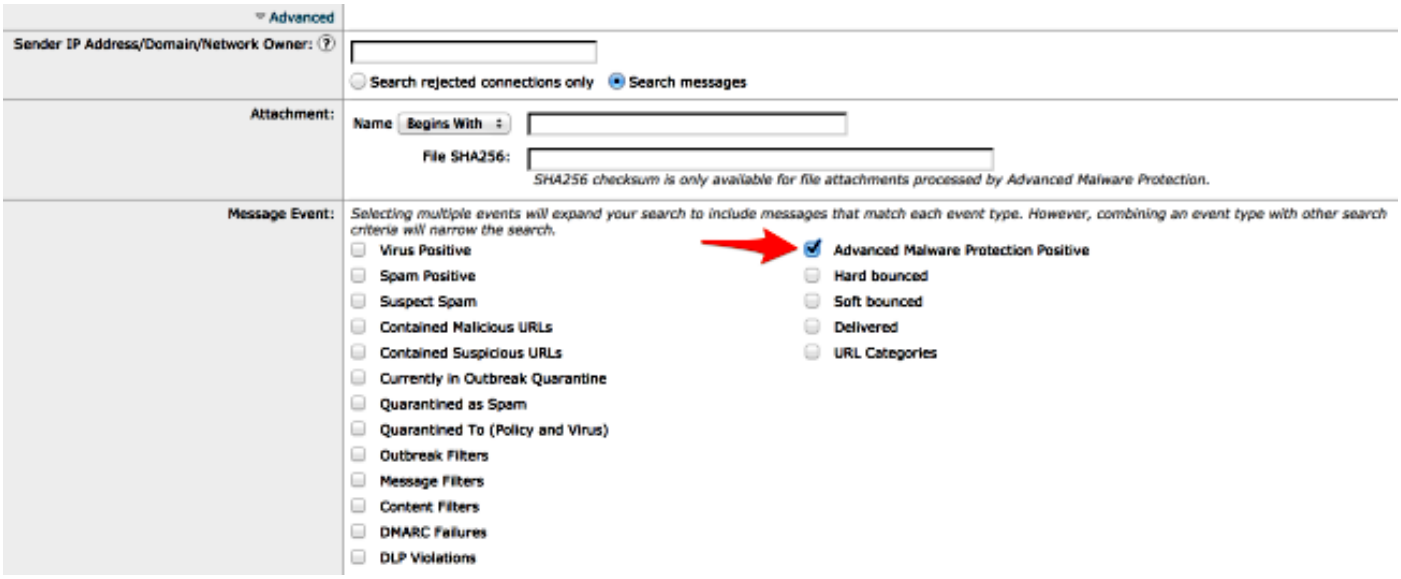
Het reputatievonnis is nog steeds positief voor **MALWARE**, zoals wordt getoond. De herschreven actie is gebaseerd op de acties voor de wijziging van het bericht en het onderwerp vooraf van **[WAARSCHUWING: MALWARE DETECTEERD]**.

In een reinigingsbestand of in een bestand dat tijdens het verwerken van het bestand niet als malware is geïdentificeerd, wordt dit vonnis aan de postbestanden geschreven:

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

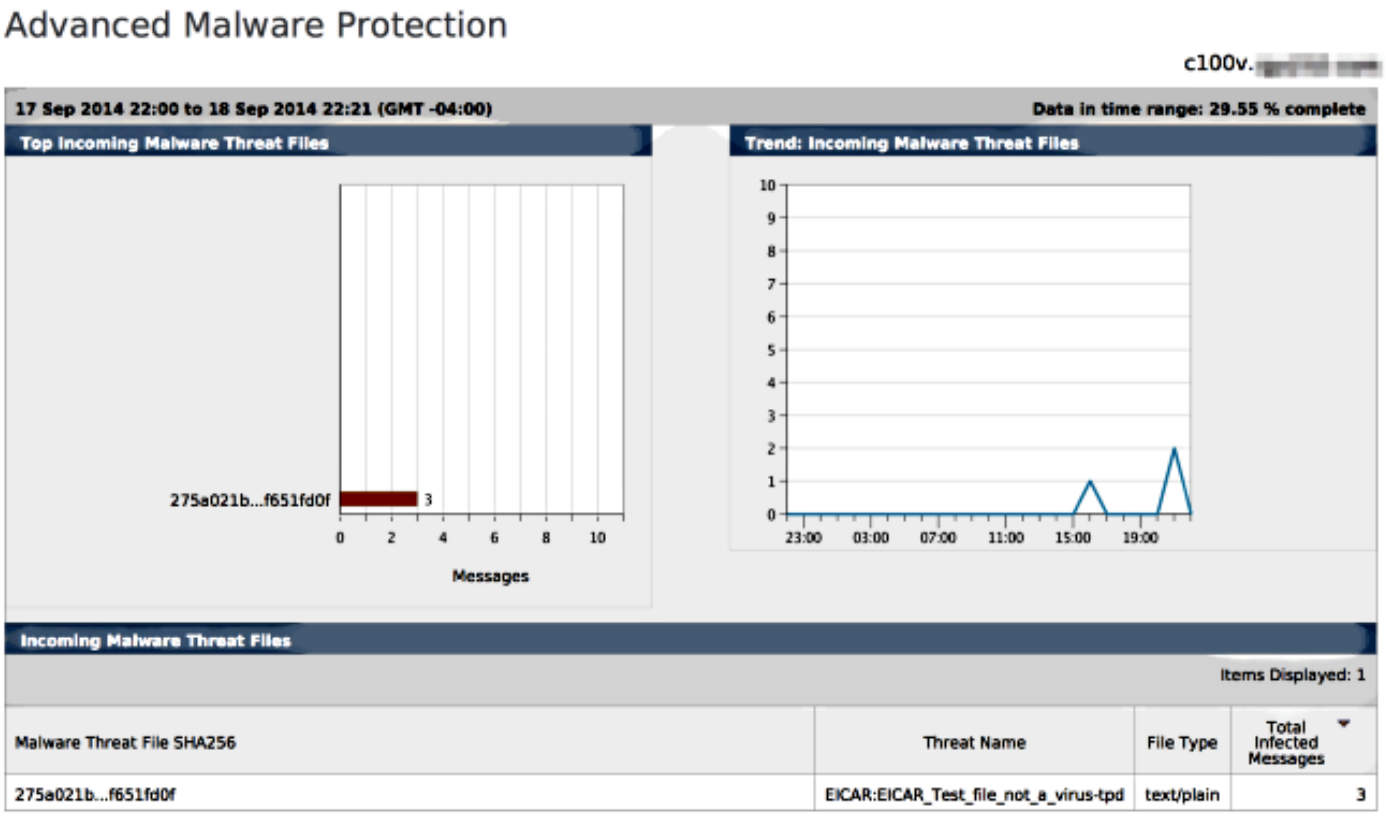
Geavanceerde berichttracering voor AMP+ berichten

Tevens kunt u in de GUI, wanneer u Message Tracking en het geavanceerde vervolgkeuzemenu gebruikt, ervoor kiezen om rechtstreeks naar een Advanced Malware Protection Positive-bericht te zoeken:



Geavanceerde Malware-beschermingsrapporten

Vanuit de ESA GUI, zie je ook het volgen van rapporten voor positief geïdentificeerde berichten door middel van AMP. Navigeer naar **monitor > Advanced Malware Protection** en wijzig het tijdbereik indien nodig. U ziet nu hetzelfde, met de vorige voorbeelden voor invoer:



Problemen oplossen

Als u geen bekend, waar malware-bestand ziet dat positief door AMP is gescand, bekijkt u de e-mailbestanden om er zeker van te zijn dat een andere dienst geen actie tegen het bericht en/of de

bijlage heeft ondernomen voordat AMP het bericht heeft gescand.

In het eerder gebruikte voorbeeld, als Sofas Anti-virus is ingeschakeld, vangt het feitelijk en treedt het op tegen de bijlage:

```
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
```

De anti-virusconfiguratie-instellingen van Sofo's op het inkomende e-mailbeleid worden voor virusgeïnfecteerde berichten afgebroken. In dit geval wordt AMP nooit bereikt om te scannen of actie te ondernemen tegen de bijlage.

Dit is niet altijd het geval. Het kan nodig zijn de maillogs en de Berichten-ID's (MID's) te herzien om te garanderen dat een andere dienst of een inhoud/berichtfilter geen actie tegen de MID heeft ondernomen voordat de WMA-verwerking werd verwerkt en een actie werd ondernomen.

Gerelateerde informatie

- Cisco e-mail security applicatie – eindgebruikershandleiding
- Technische ondersteuning en documentatie – Cisco Systems