Test ESA Advanced Malware Protection

Sommario

Introduzione

In questo documento viene descritto come testare e verificare le funzionalità Advanced Malware Protection (AMP) di Cisco Email Security Appliance (ESA).

AMP di prova sull'UEE

Con il rilascio di AsyncOS 8.5 per ESA, AMP esegue scansioni della reputazione dei file e analisi dei file per rilevare malware negli allegati.

Chiavi funzionalità

Per implementare AMP, è necessario disporre di una chiave di funzionalità valida e attiva sia per la **reputazione dei file** che per l'**analisi dei file** sull'ESA. Visitare il sito **System Administration> Feature Keys** (Amministrazione del sistema) sulla GUI o usare **feature keys** sulla CLI per verificare le feature key.

Servizi di sicurezza

Per abilitare il servizio dalla GUI, selezionare **Security Services > File Reputation and Analysis** (Servizi di sicurezza > Reputazione e analisi file). Dalla CLI, è possibile eseguire **ampconfig**.

Inviare e confermare le modifiche alla configurazione.

Criteri posta in arrivo

Dopo aver abilitato il servizio, è necessario che il servizio sia collegato a un criterio di posta in arrivo.

1. Selezionare **Mail Policies > Incoming Mail Policies** (Policy di posta > Criteri posta in arrivo).
2. Selezionare il **criterio predefinito** o il criterio preconfigurato in base alle esigenze. Verrà visualizzata la colonna **Protezione avanzata da malware** nella pagina Criteri posta in arrivo.
3. Selezionare il collegamento **Disabilitato** per la colonna e **Abilita reputazione file** e **Abilita analisi file** nella pagina delle opzioni.
4. Se necessario, è possibile apportare ulteriori miglioramenti alla configurazione dell'analisi dei messaggi, delle azioni per gli allegati non analizzabili e delle azioni per i messaggi identificati in modo positivo.
5. Inviare e confermare le modifiche alla configurazione.

Test

Al momento, i criteri di posta in arrivo sono abilitati per l'analisi e il rilevamento di malware. È necessario disporre di un vero campione di malware da testare. Per ottenere esempi validi, visitare la pagina dedicata ai download dell'Istituto europeo per la ricerca antivirus sui computer (EICAR).

> **Attenzione**: Cisco non può essere ritenuta responsabile quando questi file o lo scanner AV in combinazione con questi file causano danni al computer o all'ambiente di rete. I FILE VENGONO SCARICATI A PROPRIO RISCHIO. Scaricare i file solo se si dispone di sufficiente protezione nell'utilizzo dello scanner AV, delle impostazioni del computer e dell'ambiente di rete. Queste informazioni sono fornite a scopo di prova e riproduzione.

Utilizzando un account e-mail preconfigurato valido, inviare l'allegato attraverso l'ESA e la normale elaborazione. È possibile usare la CLI dell'ESA e **tagliare mail_logs** per monitorare la posta mentre viene elaborata. L'ID messaggio (MID) verrà visualizzato nei log di posta. Uscita simile a questa:

```
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
```

Nell'esempio precedente viene mostrato che AMP ha rilevato l'allegato malware ed è **stato eliminato** come azione finale in base alle impostazioni predefinite.

Gli stessi dettagli si trovano anche nel Message Tracking dalla 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.

Se si sceglie di recapitare malware identificato in modo positivo o altre opzioni avanzate nella configurazione AMP da Criteri posta in arrivo, è possibile che venga visualizzato questo risultato dell'elaborazione della posta:

```
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
```

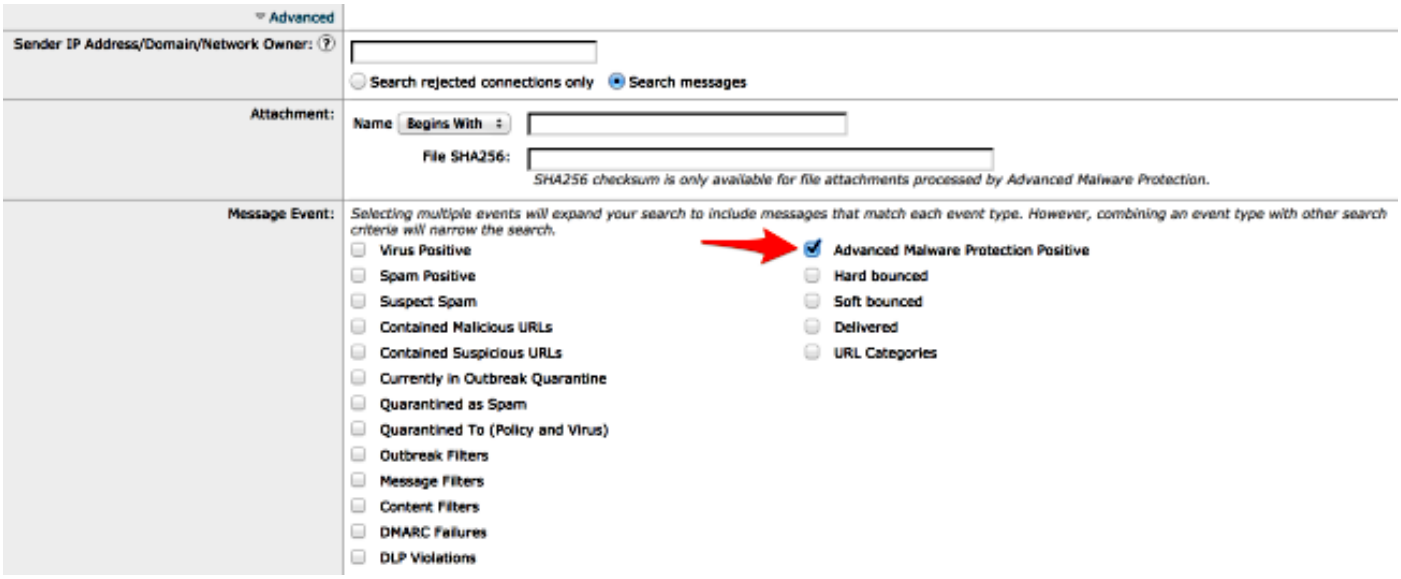
Il verdetto sulla reputazione è ancora positivo per il **MALWARE** come mostrato. L'azione riscritta è basata sulle azioni di modifica del messaggio e sulla riga dell'oggetto che precedono **[AVVISO: MALWARE RILEVATO]**.

Un file pulito o un file che non è stato identificato al momento dell'elaborazione come malware, ha questo verdetto scritto nei log di posta:

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

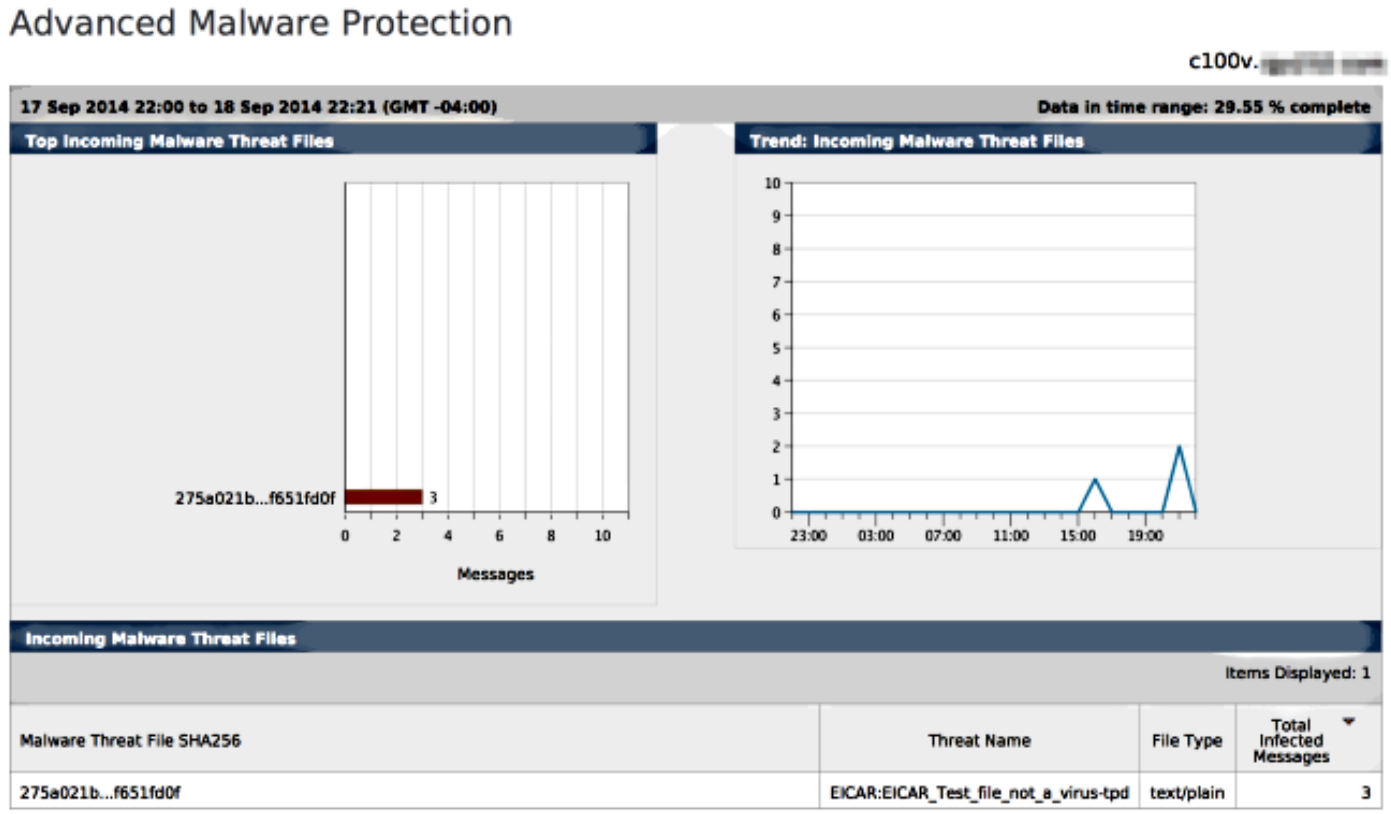
Verifica avanzata messaggi per messaggi AMP+

Inoltre, dalla GUI, quando si usa il Message Tracking e il menu a discesa Advanced, è possibile scegliere di cercare direttamente un messaggio positivo di Advanced Malware Protection:



Rapporti di Advanced Malware Protection

Dalla GUI ESA è inoltre possibile visualizzare i report di rilevamento dei messaggi identificati positivamente tramite AMP. Passare a **Monitor > Advanced Malware Protection** e modificare l'intervallo di tempo in base alle esigenze. Si noterà ora una situazione simile, con gli esempi precedenti relativi all'input:



Risoluzione dei problemi

Se non viene visualizzato un vero e proprio file malware noto analizzato da AMP, esaminare i log

di posta per assicurarsi che un altro servizio non abbia eseguito alcuna operazione sul messaggio e/o sull'allegato prima che AMP analizzasse il messaggio.

Dall'esempio utilizzato in precedenza, quando è abilitato l'antivirus Sophos, questo intercetta e interviene sull'allegato:

```
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
```

Le impostazioni di configurazione antivirus Sophos nel criterio posta in arrivo sono impostate su **drop** per i messaggi con virus infetti. In questo caso, AMP non viene mai raggiunto per eseguire la scansione o l'azione sull'allegato.

Non è sempre così. Potrebbe essere necessario rivedere i log di posta e gli ID dei messaggi (MID, Message ID) per assicurarsi che un altro servizio O un filtro contenuti/messaggi non abbia eseguito alcuna azione sul MID prima dell'elaborazione dell'AMP e che sia stata raggiunta un'azione.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems