Prueba de protección frente a malware avanzado (AMP) de ESA

Contenido

Introducción

Este documento describe cómo probar y verificar las funciones de protección frente a malware avanzado (AMP) de Cisco Email Security Appliance (ESA).

Probar AMP en ESA

Con la versión de AsyncOS 8.5 para el ESA, AMP realiza análisis de reputación de archivos y análisis de archivos para detectar malware en archivos adjuntos.

Claves de característica

Para implementar AMP, debe tener una clave de característica válida y activa para **Reputación de archivos** y **Análisis de archivos** en su ESA. Visite **Administración del sistema> Claves de funciones** en la GUI, o utilice **claves de funciones** en la CLI, para verificar las claves de característica.

Servicios de seguridad

Para habilitar el servicio desde la GUI, navegue hasta **Servicios de seguridad > Reputación y análisis de archivos**. Desde la CLI, puede ejecutar **ampconfig**. Envíe y confirme los cambios en la configuración.

Políticas de correo entrante

Una vez habilitado el servicio, debe tener este servicio vinculado a una política de correo entrante.

1. Navegue hasta **Políticas de correo > Políticas de correo entrante**.
2. Seleccione su **Política predeterminada** o la política preconfigurada según sea necesario. Se muestra la columna **Protección frente a malware avanzado** de la página Políticas de correo entrante.
3. Seleccione el enlace **Disabled** para la columna, **Enable File Reputation** y **Enable File Analysis** en la página de opciones.
4. Puede realizar cualquier otra mejora de la configuración para el escaneo de mensajes, acciones para adjuntos no escaneables y acciones para mensajes identificados positivamente, según sea necesario.
5. Envíe y confirme los cambios en la configuración.

Prueba

En este momento, la política de correo entrante está habilitada para analizar y detectar el malware. Debe tener una muestra de malware real con la que probar. Si necesita ejemplos válidos, visite la página de descargas del Instituto Europeo para la Investigación del Antivirus Informático (eicar).

> **Precaución**: Cisco no puede ser considerado responsable cuando estos archivos o su escáner antivirus en combinación con estos archivos causen daños en su ordenador o entorno de red. DESCARGUE ESTOS ARCHIVOS A SU PROPIO RIESGO. Descargue estos archivos sólo si está lo suficientemente seguro en el uso del escáner AV, la configuración del equipo y el entorno de red. Esta información se proporciona como cortesía a efectos de prueba y reproducción.

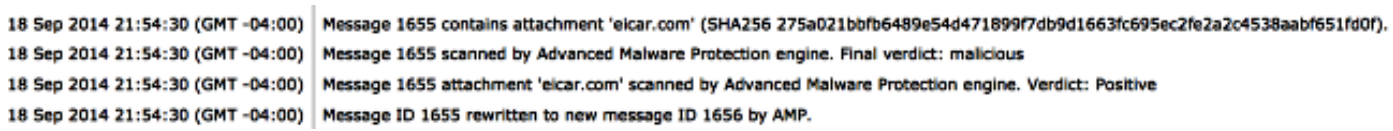
Con el uso de una cuenta de correo electrónico preconfigurada válida, envíe el archivo adjunto a través de su ESA y el procesamiento normal. Puede utilizar la CLI del ESA, y **tail mail_logs** para monitorear el correo mientras se procesa. Verá la ID de mensaje (MID) que se muestra en los registros de correo. Se muestra una salida similar a esta:

```
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
```

El ejemplo anterior muestra que AMP detectó el archivo adjunto de malware y **se descartó** como la acción final según la configuración predeterminada.

Los mismos detalles también se ven en Rastreo de mensajes desde la GUI:



Si decide ofrecer malware identificado positivamente u otras opciones avanzadas en la configuración de AMP de las políticas de correo entrante, es posible que vea este resultado de procesamiento de correo:

```
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
```

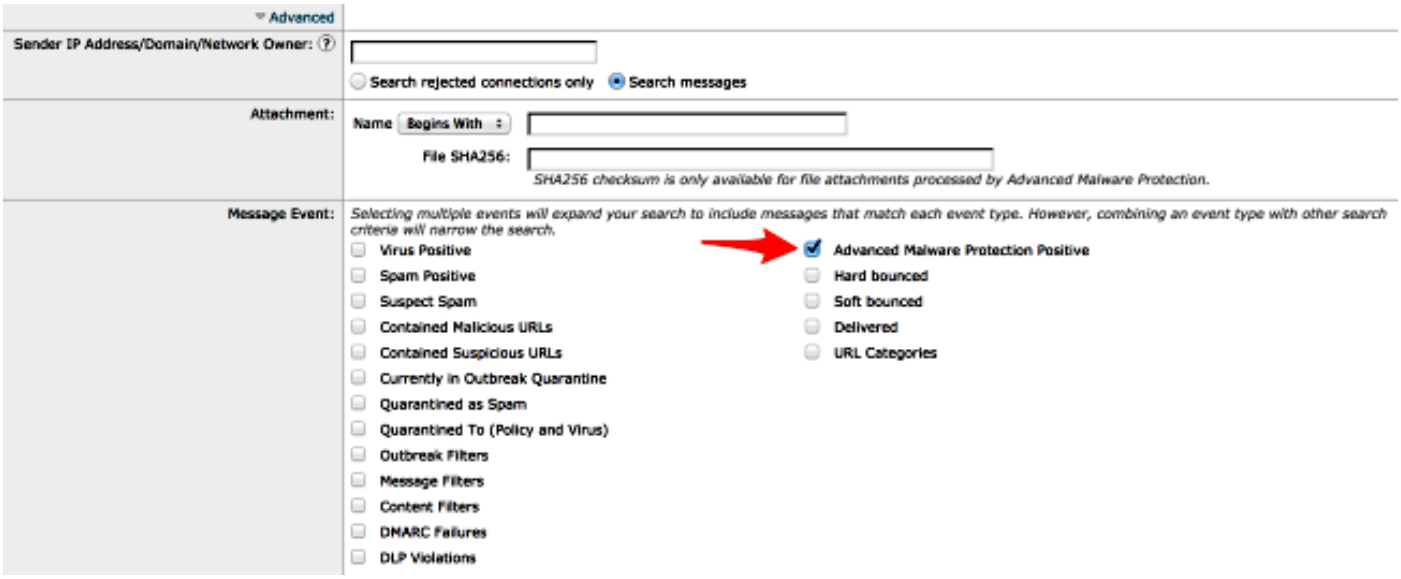
El veredicto de reputación sigue siendo positivo para **MALWARE** como se muestra. La acción reescrita se basa en las acciones de modificación del mensaje y en la línea del asunto que precede a **[ADVERTENCIA: MALWARE DETECTADO]**.

Este veredicto se ha escrito en los registros de correo en un archivo limpio o en un archivo que no se ha identificado en tiempo de procesamiento como malware:

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

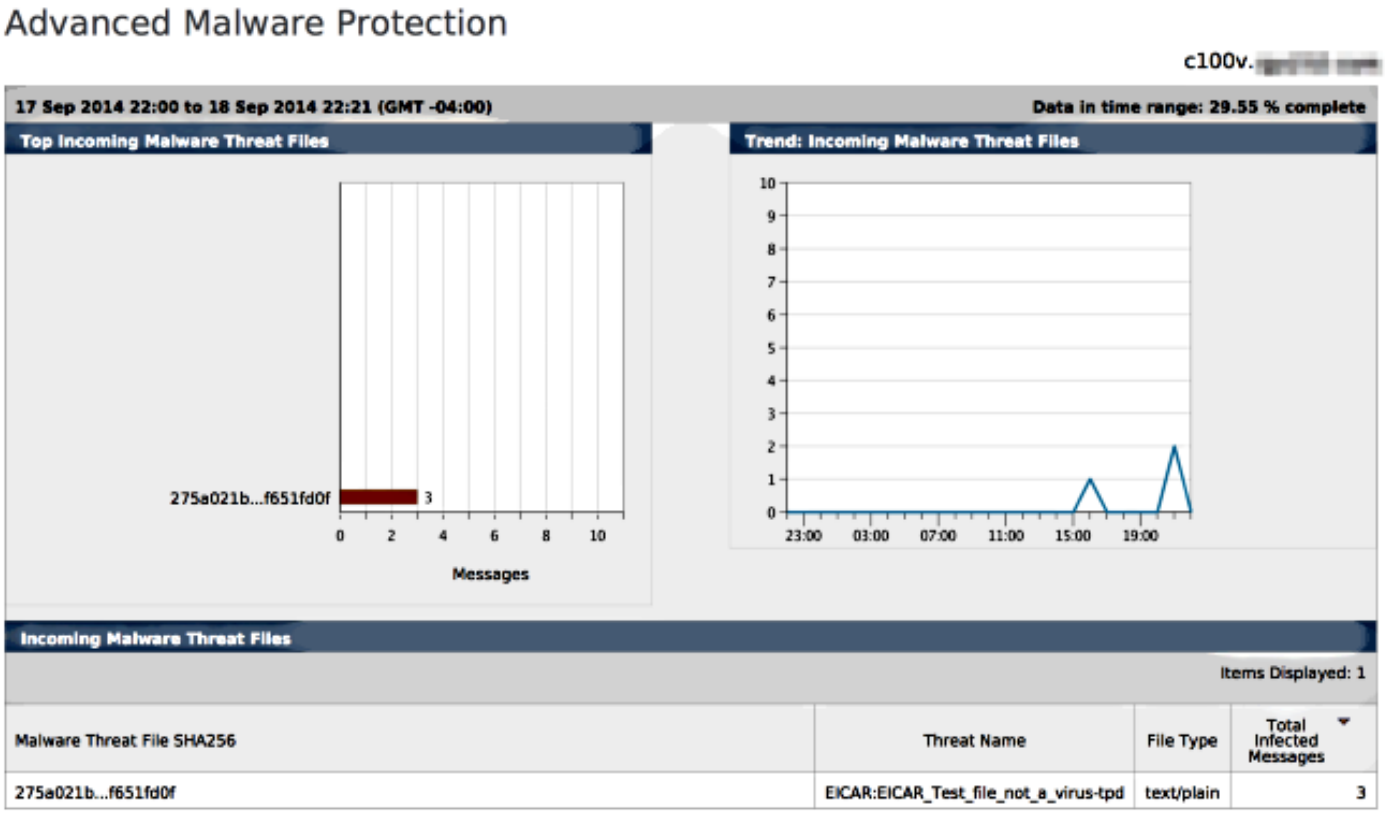
Rastreo de mensajes avanzado para mensajes AMP+

También desde la GUI, cuando utiliza Rastreo de mensajes y el menú desplegable Avanzado, puede optar por buscar un mensaje Positivo de protección frente a malware avanzado directamente:



Informes de protección frente a malware avanzado

Desde la interfaz gráfica de usuario de ESA, también puede ver el seguimiento de informes para detectar mensajes identificados positivamente a través de AMP. Vaya a **Monitor > Advanced Malware Protection** y modifique el rango de tiempo según sea necesario. Ahora puede ver ejemplos similares, con los ejemplos anteriores para la entrada:



Troubleshoot

Si no ve un archivo de malware conocido y verdadero que AMP escanee de forma positiva, revise

los registros de correo para asegurarse de que otro servicio no haya tomado medidas sobre el mensaje o el archivo adjunto antes de que AMP escanee el mensaje.

Desde el ejemplo anterior utilizado, cuando Sophos Anti-virus está habilitado, realmente detecta y realiza acciones en el archivo adjunto:

```
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
```

Los valores de configuración de Sophos Anti-virus en la política de correo entrante se establecen como **descartar** para los mensajes infectados por virus. En este caso, nunca se llega a AMP para analizar o tomar medidas sobre el archivo adjunto.

No siempre es así. Es posible que sea necesaria una revisión de los registros de correo y los ID de mensaje (MID) para asegurarse de que otro servicio O un filtro de contenido/mensaje no haya tomado medidas contra el MID antes del procesamiento de AMP y se haya alcanzado una acción.

Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance - Guías de usuario final
- Soporte Técnico y Documentación - Cisco Systems