Prueba avanzada de la protección ESA Malware (AMP)

Contenido

Introducción

Este documento describe cómo probar y verificar las características avanzadas de la protección de Malware (AMP) de Cisco envíe por correo electrónico el dispositivo de seguridad (ESA).

Pruebe el AMP en el ESA

Con la versión de AsyncOS 8.5 para el ESA, el AMP realiza las exploraciones de la reputación del archivo y el análisis del archivo para detectar el malware en las conexiones.

Teclas de función

Para implementar el AMP, usted debe tener las teclas de función válidas y activas para la **reputación del archivo** y **clasifiar el análisis** en su ESA. Visite las **teclas de función del sistema Administration>** en el GUI, o utilice los **featurekeys** en el CLI, para verificar las teclas de función.

Servicios de seguridad

Para habilitar el servicio del GUI, navegue a los **Servicios de seguridad > a la reputación y al**

análisis del archivo. Del CLI, usted puede ejecutar el **ampconfig**. Someta y confíe sus cambios a la configuración.

Directivas del correo entrante

Una vez que usted ha habilitado el servicio, usted debe tener este servicio atado a una directiva del correo entrante.

1. Navegue **para enviar las directivas > las directivas del correo entrante**.
2. Seleccione su **política predeterminada** o directiva preconfigurada según las necesidades. **La Columna de protección avanzada de Malware** en el correo entrante limpia las páginas muestra.
3. Seleccione el link de los **minusválidos** para la columna, y **habilite la reputación del archivo** y **habilite el análisis del archivo** en la página opciones.
4. Usted puede hacer cualquier mejoras más otra de la configuración a la exploración del mensaje, a las acciones para las conexiones O.N.U-scannable, y a las acciones para los mensajes positivamente identificados, según las necesidades.
5. Someta y confíe sus cambios a la configuración.

Prueba

Ahora, su directiva del correo entrante se habilita para analizar y para detectar el malware. Usted debe tener una muestra verdadera del malware con la cual probar. Si usted necesita los ejemplos válidos, visite al instituto europeo para la página (eicar) de las descargas de la investigación del antivirus de la Computadora.

> **Caution**: Cisco no puede ser sostenido responsable cuando estos archivos o su escáner AV conjuntamente con estos archivos causan cualquier daño a su ordenador o entorno de red. USTED DESCARGA ESTOS ARCHIVOS BAJO SU PROPIO RIESGO. Descargue estos archivos solamente si usted es suficientemente seguro en el uso de su escáner AV, configuraciones del ordenador, y entorno de red. Esta información se proporciona como cortesía para los propósitos de la prueba y de la reproducción.

Con el uso de un válido una cuenta de correo electrónico preconfigurada, envía la conexión con su ESA y proceso normal. Usted puede utilizar el CLI del ESA, y los **mail_logs de la cola** para monitorear el correo como él procesan. Usted verá el ID del mensaje (MEDIADOS DE) enumerado en los registros del correo. La salida similar a esto visualiza:

```
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 el AMP detectó la conexión del malware y **cayó** como la última acción por las configuraciones predeterminadas.

Los mismos detalles también se consideran adentro Seguimiento de mensajes del 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.

Si usted elige entregar el malware positivamente identificado, u otras opciones avanzadas en la configuración AMP de las directivas del correo entrante, usted puede ser que vea este correo el procesar del resultado:

```
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
```

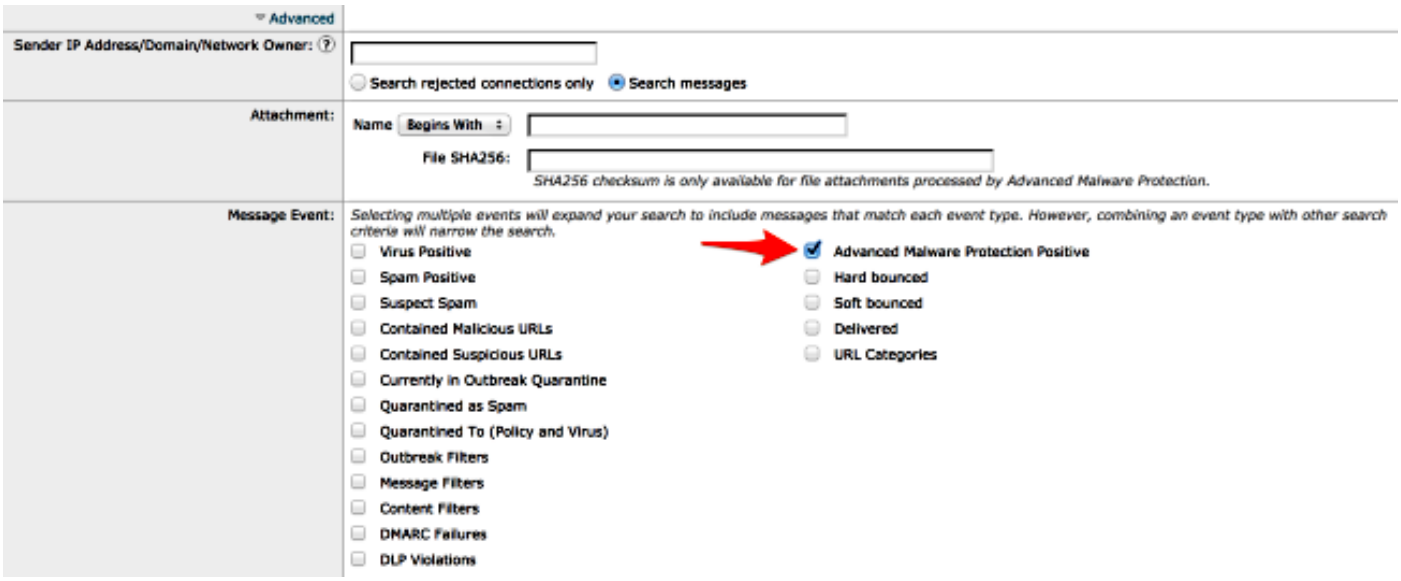
El veredicto de la reputación es todavía positivo para **MALWARE** como se muestra. La acción reescrita está por las acciones de la modificación del mensaje y prepending del asunto de **[ADVIRTIENDO: MALWARE DETECTADO]**.

Un archivo limpio, o un archivo que no se ha identificado en el tiempo de procesamiento como malware, tiene este veredicto escrito a los registros del correo:

```
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
```

Avanzado Seguimiento de mensajes para los mensajes AMP+

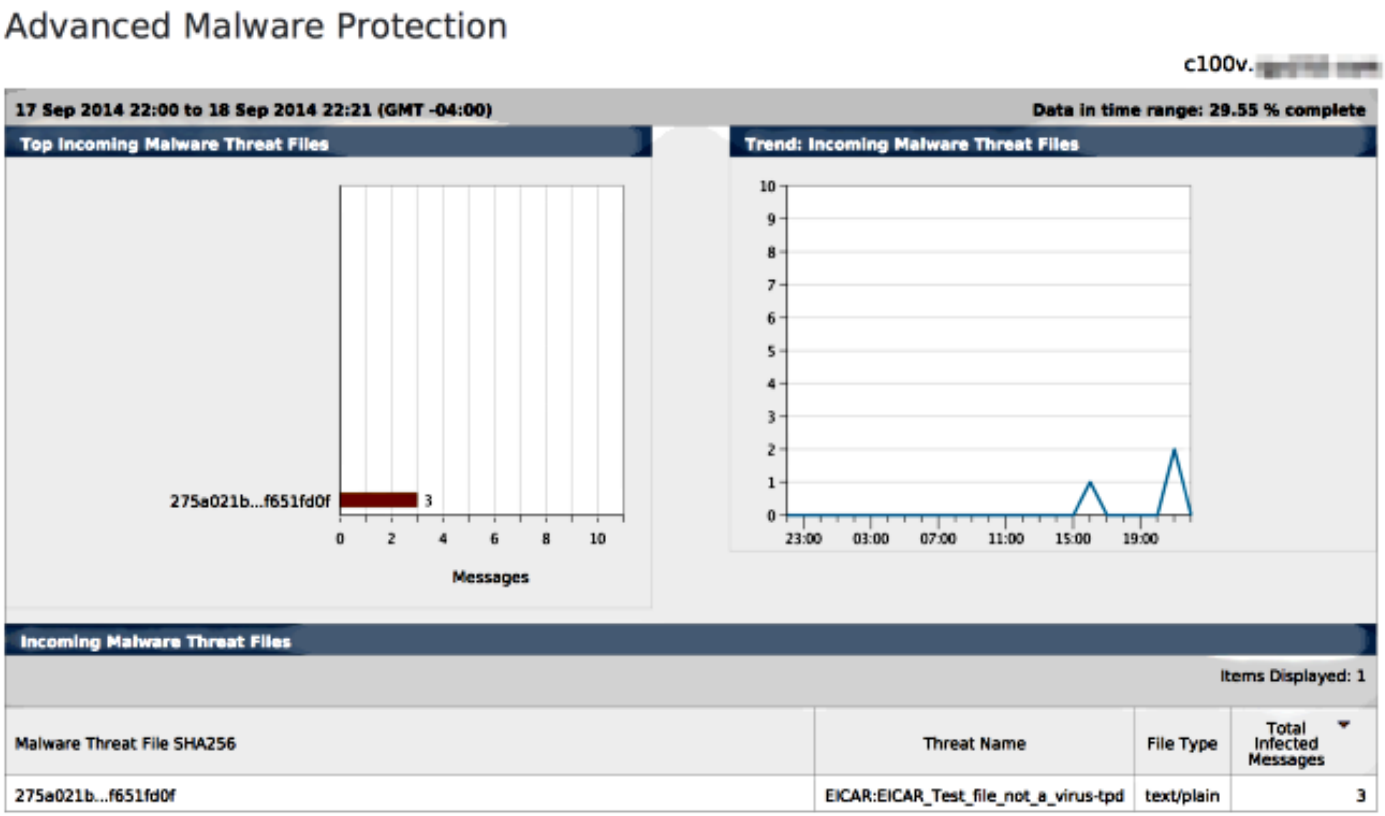
También del GUI, cuando usted utiliza Seguimiento de mensajes y el menú desplegable avanzado, usted puede elegir buscar para un mensaje positivo de la protección avanzada de Malware directamente:



Informes avanzados de la protección de Malware

Del ESA GUI, usted también ve que el informe que seguía para los mensajes positivamente

identificados a través de AMP. Navigate **para monitorear > avanzó la protección de Malware** y modifica el rango de tiempo según las necesidades. Usted ahora ve similar, con los ejemplos anteriores para la entrada:



Troubleshooting

Si usted no ve haber sabido, el archivo verdadero del malware que es analizado positivamente por el AMP, revisa el correo abre una sesión la orden para asegurar que otro servicio no tomó medidas en el mensaje y/o la conexión antes de que el AMP analizara el mensaje.

Del ejemplo anterior usado, cuando se habilita el contra virus de Sophos, coge y toma realmente medidas en la conexión:

```
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 ajustes de la configuración del contra virus de Sophos en la directiva del correo entrante se fijan **para caer** para los mensajes infectados virus. El en este caso, AMP nunca se alcanza para analizar o para tomar medidas en la conexión.

Éste no es siempre el caso. Un estudio de los registros y de los ID del mensaje (MIDs) del correo pudo ser necesario para asegurar que otro servicio O un filtro contento/del mensaje no tomó medidas contra el MEDIADOS DE antes del AMP que procesaba y una acción fue alcanzado.

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems