Reescritura de prueba del filtro URL del brote

Contenido

Introducción

Este documento describe cómo probar la opción de la modificación del mensaje de los filtros del brote (DE) para la reescritura URL.

Antecedentes

Si el nivel de la amenaza del mensaje excede el umbral de la modificación del mensaje, la característica de los filtros del brote reescribe todos los URL en el mensaje para reorientar al usuario a la página del chapoteo del proxy de la Seguridad de la red de Cisco si hacen clic en ningunos de ellos. AsyncOS reescribe todos los URL dentro de un mensaje a excepción de los que señala a los dominios desviados.

Las opciones siguientes están disponibles para la reescritura URL:

- Permiso solamente para los mensajes sin signo. Esta opción permite que AsyncOS reescriba los URL en los mensajes sin signo que resuelven o exceden el umbral de la modificación del mensaje, pero los mensajes no firmados. Cisco recomienda el usar de esta configuración para la reescritura URL. **Note**: El dispositivo de seguridad del correo electrónico puede reescribir los URL en un mensaje DomainKeys/DKIM-signed e invalidar la firma del mensaje si un servidor o un dispositivo en su red con excepción del dispositivo de seguridad del correo electrónico es responsable de verificar la firma DomainKeys/DKIM. El dispositivo considera un mensaje firmado si se cifra usando S/MIME o contiene una firma S/MIME. El dispositivo de seguridad del correo electrónico puede reescribir los URL en un mensaje DomainKeys/DKIM-signed e invalidar la firma del mensaje si un servidor o un dispositivo en su red con excepción del dispositivo de seguridad del correo electrónico es responsable de verificar la firma DomainKeys/DKIM.El dispositivo considera un mensaje firmado si se cifra usando S/MIME o contiene una firma S/MIME.
- Permiso para todos los mensajes. Esta opción permite que AsyncOS reescriba los URL en todos los mensajes que resuelvan o excedan el umbral de la modificación del mensaje, incluyendo firmados. Si AsyncOS modifica un mensaje firmado, la firma llega a ser inválida.
- Neutralización. Esta opción inhabilita la reescritura URL para los filtros del brote.

Usted puede modificar una directiva para excluir los URL a ciertos dominios de la modificación. Para desviar los dominios, ingrese el direccionamiento IPv4, el direccionamiento del IPv6, el rango CIDR, el hostname, el hostname parcial o el dominio en el campo de la exploración del dominio de puente. Separe las entradas múltiples usando las comas.

La característica de la exploración del dominio de puente es similar a, pero independiente de, la lista blanca global usada por el Filtrado de URL. Para más información sobre esa lista blanca, vea “crear las listas blancas para el Filtrado de URL” en la guía de usuario ESA.

Reescritura de prueba del filtro URL del brote

Hay dos opciones a la prueba en DEL ESA.

Prueba de la parte una

Incluya un URL malévolo en el cuerpo del correo electrónico. Prueba segura URL que puede ser utilizada:

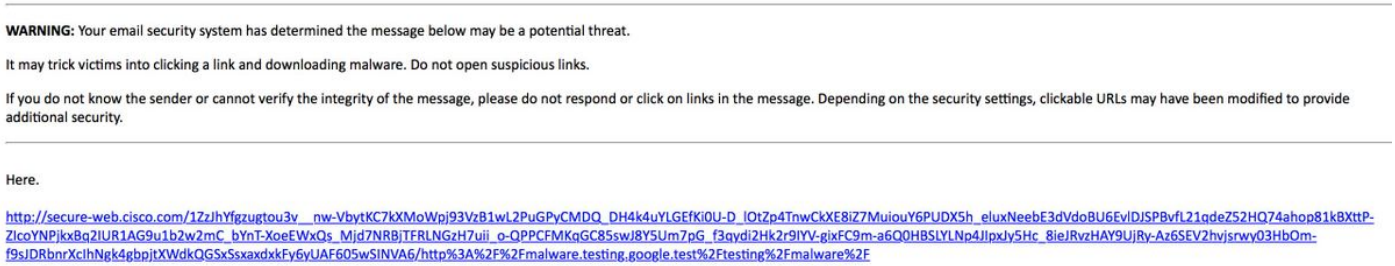
http://malware.testing.google.test/testing/malware/

Cuando está enviado, el ejemplo de los registros del correo debe contener similar al siguiente:

```
Tue Jul  3 09:31:38 2018 Info: MID 185843 Outbreak Filters: verdict positive
Tue Jul  3 09:31:38 2018 Info: MID 185843 Threat Level=5 Category=Malware Type=Malware
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten URL
u'http://malware.testing.google.test/testing/malware/'
Tue Jul  3 09:31:38 2018 Info: MID 185843 rewritten to MID 185844 by url-threat-protection
filter 'Threat Protection'
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185843 done
Tue Jul  3 09:31:38 2018 Info: MID 185844 Virus Threat Level=5
Tue Jul  3 09:31:38 2018 Warning: MID 185844 Failed to add disclaimer as header. Disclaimer has
been added as attachment.
Tue Jul  3 09:31:38 2018 Info: MID 185844 rewritten to MID 185845 by add-heading filter 'Heading
Stamping'
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185844 done
Tue Jul  3 09:31:38 2018 Info: Message finished MID 185846 done
Tue Jul  3 09:31:38 2018 Info: MID 185845 enqueued for transfer to centralized quarantine
"Outbreak" (Outbreak rule Malware: Malware)
Tue Jul  3 09:31:38 2018 Info: MID 185845 queued for delivery
```

Tome la nota que los registros del correo muestran nos a “URL reescrito”, indicación DE ha reescrito este URL con el proxy de la Seguridad de la red de Cisco. También, sea consciente que el mensaje puede estar en la cuarentena del brote, como se muestra aquí en nuestro ejemplo.

El resultado final tendrá el cuerpo del correo electrónico entregado que muestra el siguiente:



WARNING: Your email security system has determined the message below may be a potential threat.

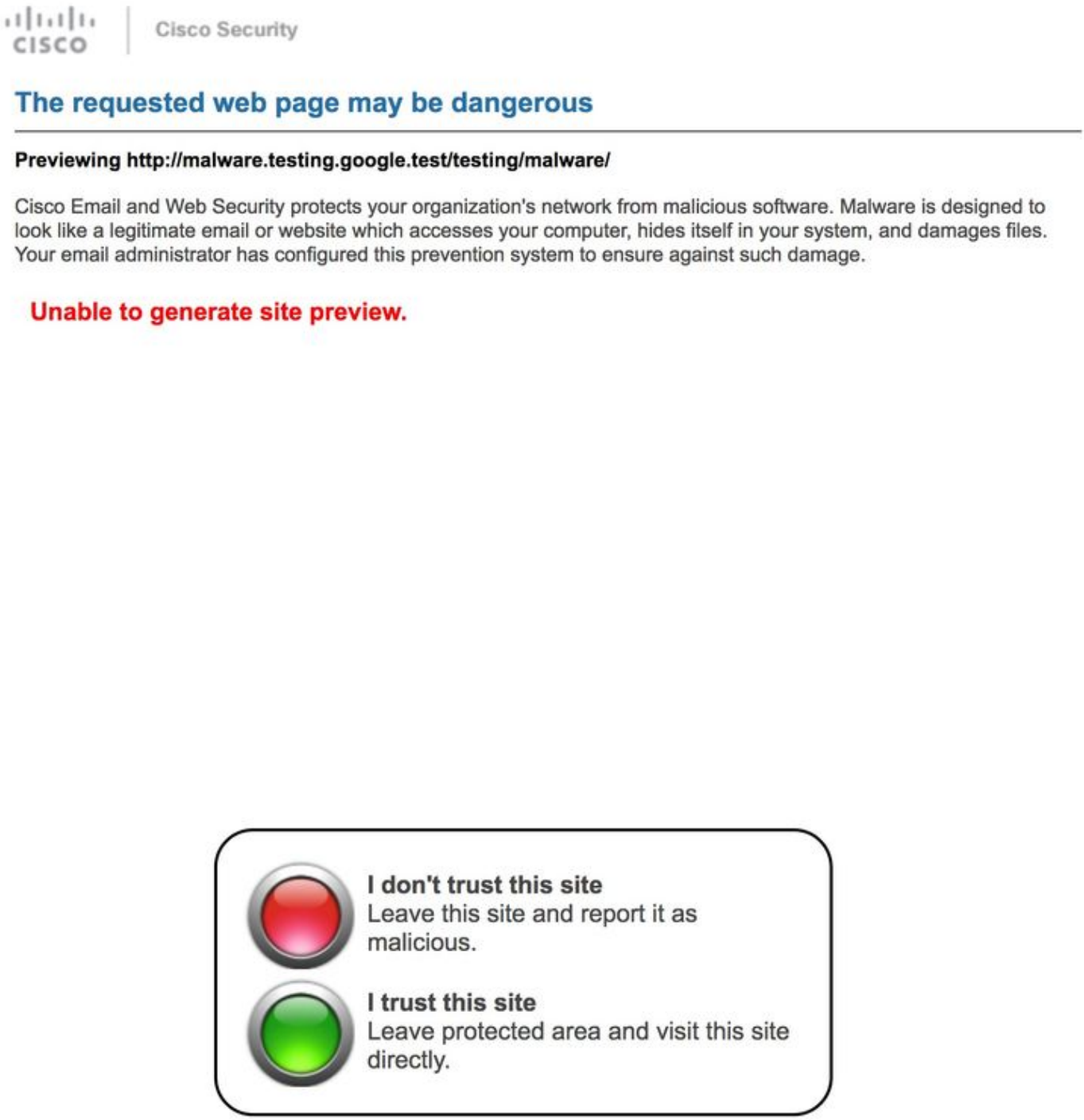
It may trick victims into clicking a link and downloading malware. Do not open suspicious links.

If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.

Here.

http://secure-web.cisco.com/1ZzJhYfgzugtou3v__nw-VbytKC7kXMoWpj93VzB1wL2PuGPyCMDQ_DH4k4uYLGEfKi0U-D_lOtZp4TnwCkXE8iZ7MuiouY6PUDX5h_eluxNeebE3dVdoBU6EvlDJSPBvfL21qdeZ52HQ74ahop81kBXttP-ZlcoYNPjkxBq2lUR1AG9u1b2w2mC_bYnT-XoeEWxQs_Mjd7NRBjTFRLNGzH7uii_o-QPPCFMKqGC85swJ8Y5Um7pG_f3qydi2Hk2r9IYV-gixFC9m-a6Q0HBSLYLNp4JIpxJy5Hc_8ieJRvzHAY9UjRy-Az6SEV2hvjsrwy03HbOm-f9sJDRbnrXclhNgk4gbpjtXWdkQGSxSsxaxdxkFy6yUAF605wSINVA6/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F

Cuando el usuario final ahora recibe el correo electrónico, hace clic el URL reescrito, se reorientan al proxy de la Seguridad de la red de Cisco y ven:



Note: “Incapaz de generar el avance del sitio” será visualizada basó en el HTML/encoding del URL o del sitio web original. Un sitio web con los cristales CSS, HTML, o la representación compleja no podrá generar un avance del sitio.

Prueba de la parte dos

La segunda opción es incluir los datos dentro del cuerpo del correo electrónico o de la conexión para tener del activador.

Hay dos opciones para tener éxito:

1. Cree un fichero (el fichero de texto simple hará) con el nombre “hello.voftest” entre el tamaño de 25000 y 30000 bytes, y asocíelo que fichero a su correo electrónico de la prueba. Esto accionará las reglas de la conexión del virus.
2. Ponga el stringtext siguiente de la prueba 72-byte GTUBE (“prueba genérica para el correo electrónico a granel no solicitado”) en el cuerpo de un correo electrónico:

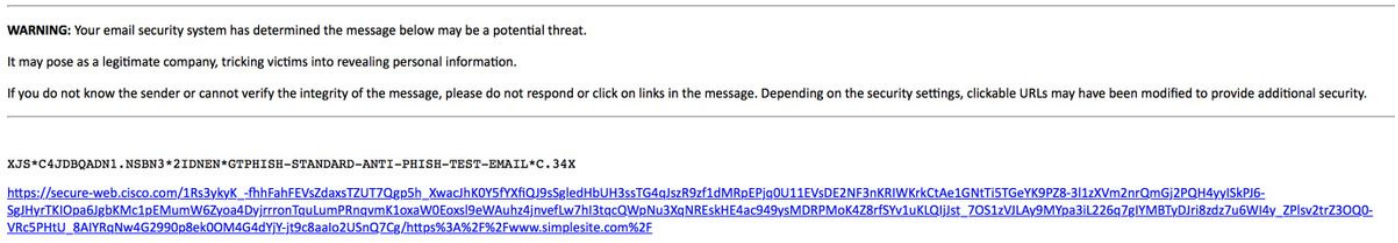
```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTPHISH-STANDARD-ANTI-PHISH-TEST-EMAIL*C.34X
```

Esto accionará DE y las reglas phish. El ejemplo de los registros del correo debe contener similar al siguiente:

```
Tue Jul  3 09:44:12 2018 Info: MID 185880 Outbreak Filters: verdict positive
Tue Jul  3 09:44:12 2018 Info: MID 185880 Threat Level=5 Category=Phish Type=Phish
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten URL u'https://www.simplesite.com/'
Tue Jul  3 09:44:12 2018 Info: MID 185880 rewritten to MID 185881 by url-threat-protection
filter 'Threat Protection'
Tue Jul  3 09:44:12 2018 Info: Message finished MID 185880 done
Tue Jul  3 09:44:12 2018 Info: MID 185881 Virus Threat Level=5
Tue Jul  3 09:44:12 2018 Warning: MID 185881 Failed to add disclaimer as header. Disclaimer has
been added as attachment.
Tue Jul  3 09:44:12 2018 Info: MID 185881 rewritten to MID 185882 by add-heading filter 'Heading
Stamping'
Tue Jul  3 09:44:12 2018 Info: Message finished MID 185881 done
Tue Jul  3 09:44:13 2018 Info: MID 185882 enqueued for transfer to centralized quarantine
"Outbreak" (Outbreak rule Phish: Phish)
Tue Jul  3 09:44:13 2018 Info: MID 185882 queued for delivery
```

Tome la nota que los registros del correo muestran nos a “URL reescrito”, indicación DE ha reescrito este URL con el proxy de la Seguridad de la red de Cisco. También, sea consciente que el mensaje puede estar en la cuarentena del brote, como se muestra aquí en nuestro ejemplo.

El resultado final tendrá el cuerpo del correo electrónico entregado que muestra el siguiente:



WARNING: Your email security system has determined the message below may be a potential threat.

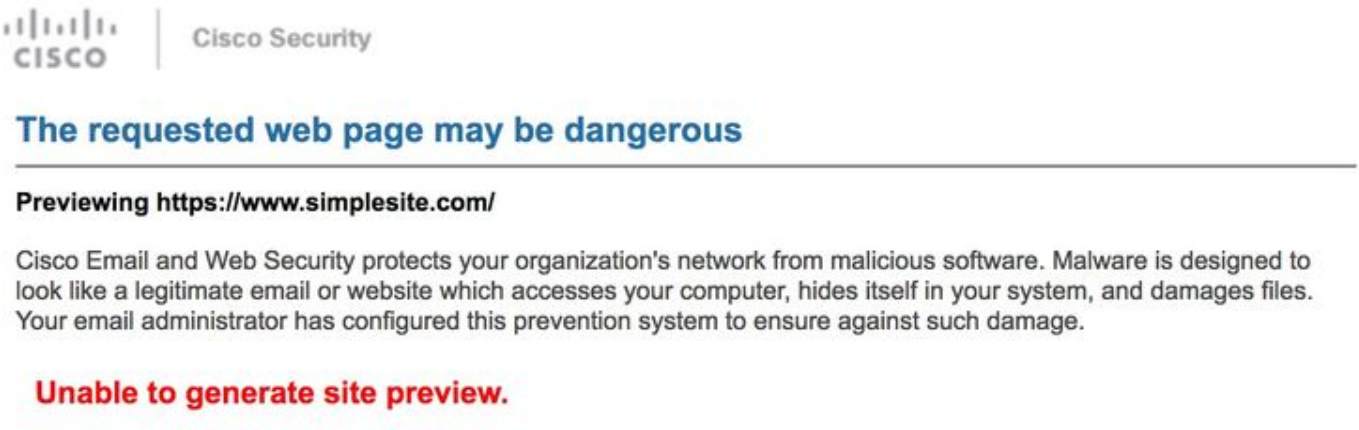
It may pose as a legitimate company, tricking victims into revealing personal information.

If you do not know the sender or cannot verify the integrity of the message, please do not respond or click on links in the message. Depending on the security settings, clickable URLs may have been modified to provide additional security.

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTPHISH-STANDARD-ANTI-PHISH-TEST-EMAIL*C.34X

https://secure-web.cisco.com/1Rs3ykyK_-fhhFahFEVsZdaxsTZUT7Qgp5h_XwacJhK0Y5fYXfiQJ9sSgledHbUH3ssTG4qJszR9zf1dMRpEPjq0U11EVsDE2NF3nKRlWKrkCtAe1GNtTi5TGeYK9PZ8-3l1zXVm2nrQmGj2PQH4yylSkPJ6-SgJHyrTKlOpa6JgbKMc1pEMumW6Zyoa4DyjrrronTquLumPRnqvmK1oxaW0Eoxsl9eWAuhz4jnvefLw7hl3tqcQWpNu3XqNREskHE4ac949ysMDRPMoK4Z8rfSYv1uKLQIjJst_7OS1zVJLAy9MYpa3iL226q7gIYMBTyDJri8zdz7u6WI4y_ZPlsv2trZ3OQ0-VRc5PHtU_8AlYRqNw4G2990p8ek0OM4G4dYjY-jt9c8aaIo2U5nQ7Cg/https%3A%2F%2Fwww.simplesite.com%2F

Cuando el usuario final ahora recibe el correo electrónico, hace clic el URL reescrito, se reorientan al proxy de la Seguridad de la red de Cisco y ven:



Note: “Incapaz de generar el avance del sitio” será visualizada basó en el HTML/encoding del URL o del sitio web original. Un sitio web con los cristales CSS, HTML, o la representación compleja no podrá generar un avance del sitio.

Información Relacionada

- Guías del usuario final del dispositivo de seguridad del correo electrónico de Cisco
- Soporte técnico y documentación - Cisco Systems