Comprensión de la acción de redirección y desinfección de URL en el gateway de correo electrónico seguro

Contenido

Introducción

Este documento describe la diferencia entre las acciones de defang y redirect utilizadas en el filtro de URL, y cómo utilizar la opción de reescritura disponible para el atributo href y el texto.

Prerequisites

Requirements

Para tomar medidas basadas en la reputación de URL o para aplicar políticas de uso aceptable con los filtros de mensaje y contenido, la función de filtros de brote de virus debe estar habilitada globalmente.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Email Gateway
- Filtros de brote
- Filtros de contenido y mensajes

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Una de las funciones de filtrado de URL es tomar medidas basadas en la reputación o categoría de URL mediante el uso de filtros de mensajes o contenido. Según el resultado del análisis de URL (condición relacionada con URL), se puede aplicar una de las tres acciones disponibles en una URL:

- Depurar URL
- Redirigir al proxy de seguridad de Cisco
- Reemplazar URL por el mensaje de texto

El objetivo de este documento es explicar el comportamiento entre las opciones Defang y Redirect URL. También proporciona una breve descripción y explicación de las capacidades de reescritura de URL de la detección de amenazas no virales de un filtro de brotes de virus.

Ejemplo Message

El mensaje de ejemplo utilizado en todas las pruebas es el tipo de mensaje MIME multipart/alternate e incluye partes text/plain y text/html. Esas partes son generadas automáticamente por el software de correo electrónico y contienen el mismo tipo de contenido formateado para receptores HTML y no HTML. Para esto, el contenido de text/plain y text/html fue editado manualmente.

```
Content-Type: multipart/alternative; boundary="===============7781793576330041025==" MIME-
Version: 1.0 From: admin@example.com Date: Mon, 04 Jul 2022 14:38:52 +0200 To: admin@cisco.com
Subject: Test URLs --===============7781793576330041025== Content-Type: text/plain; charset="us-
ascii" MIME-Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
http://malware.testing.google.test/testing/malware/ and some text Link2: http://cisco.com and
some text --===============7781793576330041025== Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text
```

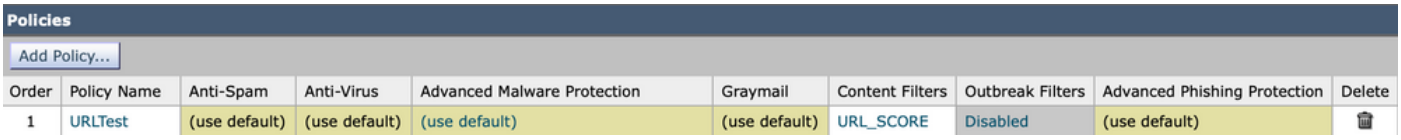
--===============7781793576330041025==--

Parte I - Defang

Configuraciones

En la primera parte la configuración utiliza:

- Política de correo electrónico con la configuración predeterminada Anti-Spam (AS)/Anti-Virus (AV)/Protección frente a malware avanzado (AMP) y filtros de brote de virus (OF) desactivados



- Filtro de contenido entrante: Filtro de contenido URL_SCORE habilitado

El filtro de contenido utiliza la condición de reputación de URL para hacer coincidir las URL malintencionadas, aquellas que tienen una puntuación entre -6.00 y -10.00. Como acción, se registra el nombre del filtro de contenido y se realiza la acción defang **url-reputation-defang** está ocupado.

Acción Defang

Es importante aclarar qué es una acción de descolgar. La guía del usuario proporciona una explicación; Defienda una URL para que no se pueda hacer clic en ella. Los destinatarios del mensaje aún pueden ver y copiar la URL.

Escenario A

Detección de amenazas no virales con filtro de brotes	No
Acción de filtro de contenido	Descolgar
websecurityadvancedconfig href y la reescritura de texto está habilitada	No

Este escenario explica el resultado de la acción defang configurada con las configuraciones predeterminadas. En la configuración predeterminada, la URL se reescribe cuando sólo se eliminan las etiquetas HTML. Eche un vistazo a un párrafo HTML con algunas URL en su interior:

```
Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text
```

En los dos primeros párrafos, la URL está representada por una etiqueta HTML A adecuada. El

elemento <A> incluye el elemento **href=** que se incluye en la propia etiqueta e indica el destino del vínculo. El contenido de los elementos de etiqueta también puede indicar el destino del vínculo. Esto **text form** del enlace puede incluir la URL. El primer Link1 incluye el mismo vínculo URL en el atributo href y en la parte de texto del elemento. Se puede observar que esas URL pueden ser diferentes. El segundo Link2 incluye la dirección URL correcta sólo dentro del atributo href. El último párrafo no incluye ningún elemento A.

> **Nota:** La dirección correcta siempre se puede ver cuando se mueve el cursor sobre el vínculo o cuando se ve el código fuente del mensaje. Desafortunadamente, el código fuente no se puede encontrar fácilmente con algunos clientes de correo electrónico populares.

Una vez que el filtro URL_SCORE hace coincidir el mensaje, las URL malintencionadas se desactivan. Cuando el registro de URL está habilitado con el **OUTBREAKCONFIG** comando las puntuaciones y URL se pueden encontrar en mail_logs.

```
Mon Jul 4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Cond tion: URL Reputation Rule Mon Jul 4 14:46:43 2022 Info: MID
139502 Custom Log Entry: URL_SCORE Mon Jul 4 14:46:43 2022 Info: MID 139502 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Acti n: URL
defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Acti n: URL
defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Acti n: URL
defanged Mon Jul 4 14:46:43 2022 Info: MID 139502 rewritten to MID 139503 by url-reputation-
defang-action filter 'URL_SCORE'
```

Esto da como resultado el mensaje reescrito:

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text

--===============7781793576330041025==--
```

El resultado de la acción defang tomada en la parte text/html del mensaje MIME es una etiqueta A despojada y el contenido de la etiqueta se deja intacto. En los dos primeros párrafos, ambos vínculos se desactivaron en el lugar donde se quitó el código HTML y se dejó la parte de texto del elemento. La dirección URL del primer párrafo es la de la parte de texto del elemento HTML. Debe tenerse en cuenta que la dirección URL del primer párrafo sigue siendo visible después de realizar la acción de descolgar, pero sin las etiquetas A HTML, no se puede hacer clic en el elemento. El tercer párrafo no está descolgado ya que la dirección URL aquí no se coloca entre ninguna etiqueta A y no se considera un enlace. Tal vez no es un comportamiento deseable debido a dos razones. En primer lugar, el usuario puede ver y copiar fácilmente el enlace y ejecutarlo en el navegador. La segunda razón es que algún software de correo electrónico tiende a detectar una forma válida de URL dentro del texto y convertirlo en un enlace en el que se pueda hacer clic.

Echemos un vistazo a la parte de texto/plano del mensaje MIME. La parte de texto/sin formato incluye dos URL en el formulario de texto. El texto/plano es mostrado por MUA que no entiende el código HTML. En la mayoría de los clientes de correo electrónico modernos no se ven las partes de texto/sin formato del mensaje a menos que haya configurado intencionadamente el cliente de correo electrónico para hacerlo. Por lo general, debe verificar el código fuente del mensaje, un formato EML sin procesar del mensaje para ver e investigar las partes MIME.

El listado aquí muestra las URLs de la parte sin formato del mensaje de origen.

```
Link1: http://malware.testing.google.test/testing/malware/ and some text Link2: http://cisco.com
and some text
```

Uno de esos dos enlaces obtuvo una puntuación maliciosa y fue descolgado. De forma predeterminada, la acción defang realizada en la parte text/plain del tipo MIME tiene un resultado diferente que en la parte text/html. Se encuentra entre las palabras BLOQUEADAS y todos los puntos entre corchetes.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text Link2:
http://cisco.com and some text --===============7781793576330041025==
```

Suma:

- La ejecución de Defang en la parte TEXT/PLAIN reescribe la URL en bloques BLOQUEADOS
- Depurar la ejecución en la parte TEXT/HTML vuelve a escribir la URL de una etiqueta A HTML cuando la etiqueta A se quita sin el texto entre las etiquetas A tocadas, que también puede ser una dirección URL

Situación B

Detección de amenazas no virales con filtro de brotes	No
Acción de filtro de contenido	Descolgar
websecurityadvancedconfig href y la reescritura de texto está habilitada	Yes

Este escenario proporciona información sobre cómo cambia el comportamiento de la acción defangs después del uso de una de las opciones websecurityadvancedconfig. El websecurityadvancedconfig es el comando CLI específico de nivel de equipo que permite ajustar la configuración específica para el análisis de URL. Una de las configuraciones permite cambiar el comportamiento predeterminado de la acción defang.

```
> websecurityadvancedconfig Enter URL lookup timeout in seconds: [15]> Enter the maximum number
of URLs that can be scanned in a message body: [100]> Enter the maximum number of URLs that can
be scanned in the attachments in a message: [25]> Do you want to rewrite both the URL text and
the href in the message? Y indicates that the full rewritten URL will appear in the email body.
N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]> Y
...
```

En la cuarta cuestión prejudicial, **Do you want to rewrite both the URL text and the href in the message? ..**, la respuesta `Y` indica que, en el caso de la parte MIME basada en HTML del mensaje, todas las cadenas URL que coincidan, independientemente de si se encuentran en el atributo href del

elemento A-tag, son parte de texto o están fuera de los elementos que se reescriben. En esta situación, se presenta el mismo mensaje, pero con un resultado ligeramente diferente.

Eche un vistazo al código de parte MIME text/html con las URL una vez más y compárelo con el código HTML procesado por el gateway de correo electrónico.

```
Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text
```

Cuando está habilitada la opción de reescritura de href y texto, todas las direcciones URL coincidentes con el filtro se eliminan sin importar si la dirección URL forma parte del atributo href o del texto del elemento HTML de la etiqueta A, o si se encuentra en otra parte del documento HTML.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text

Link2: CLICK ME some text

Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKED and some text

Link4: http://cisco.com and some text

--===============7781793576330041025==--
```

Las URL descolgadas ahora se reescriben cuando el elemento A-tag se quita junto con una reescritura de la parte de texto del vínculo cuando coincide con el formato de URL. La parte de texto reescrita se realiza de la misma manera que en la parte de texto/sin formato del mensaje MIME. El elemento se coloca entre palabras BLOQUEADAS y todos los puntos se colocan entre corchetes. Esto evita que el usuario copie y pegue la URL, y algunos clientes de software de correo electrónico hacen que el texto sea clicable.

Suma:

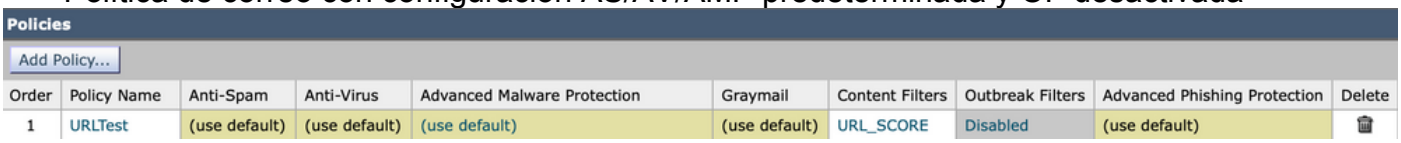
- La ejecución de Defang en la parte TEXT/PLAIN reescribe la URL en bloques BLOQUEADOS
- Depurar la ejecución en la parte TEXT/HTML vuelve a escribir la dirección URL desde una etiqueta A HTML cuando se quita una etiqueta A
- La ejecución de Defang en la parte TEXT/HTML reescribe todas las cadenas URL que coincidan en bloques BLOCKED

Parte II - Redirección

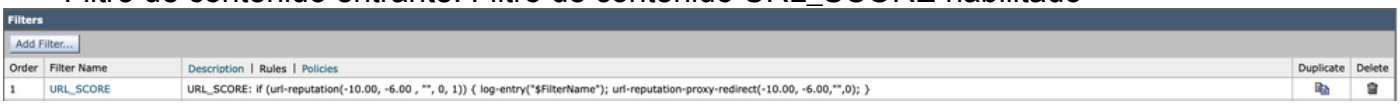
Configuraciones

En la segunda parte, la configuración utiliza:

- Política de correo con configuración AS/AV/AMP predeterminada y OF desactivada



- Filtro de contenido entrante: Filtro de contenido URL_SCORE habilitado



El filtro de contenido utiliza la condición de reputación de URL para hacer coincidir las URL malintencionadas, aquellas que tienen una puntuación entre -6.00 y -10.00. Como acción, se registra el nombre del filtro de contenido y se **redirect action** está ocupado.

Acción de redireccionamiento

La redirección al servicio Cisco Security Proxy para la evaluación en el momento del clic permite al destinatario del mensaje hacer clic en el enlace y ser redirigido a un proxy de Cisco Web Security en la nube, que bloquea el acceso si el sitio se identifica como malicioso.

Situación C

Detección de amenazas no virales con filtro de brotes	No
Acción de filtro de contenido	Redireccionar
websecurityadvancedconfig href y la reescritura de texto está habilitada	No

Este escenario es muy similar en comportamiento al Escenario A desde la primera parte con la diferencia realizada en la acción de filtrado de contenido para redirigir la URL en lugar de descolgarla. La configuración de websecurityadvancedConfig se restaura a la configuración predeterminada, lo que significa que **"Do you want to rewrite both the URL text and the href in the message? ..** se establece en **N**.

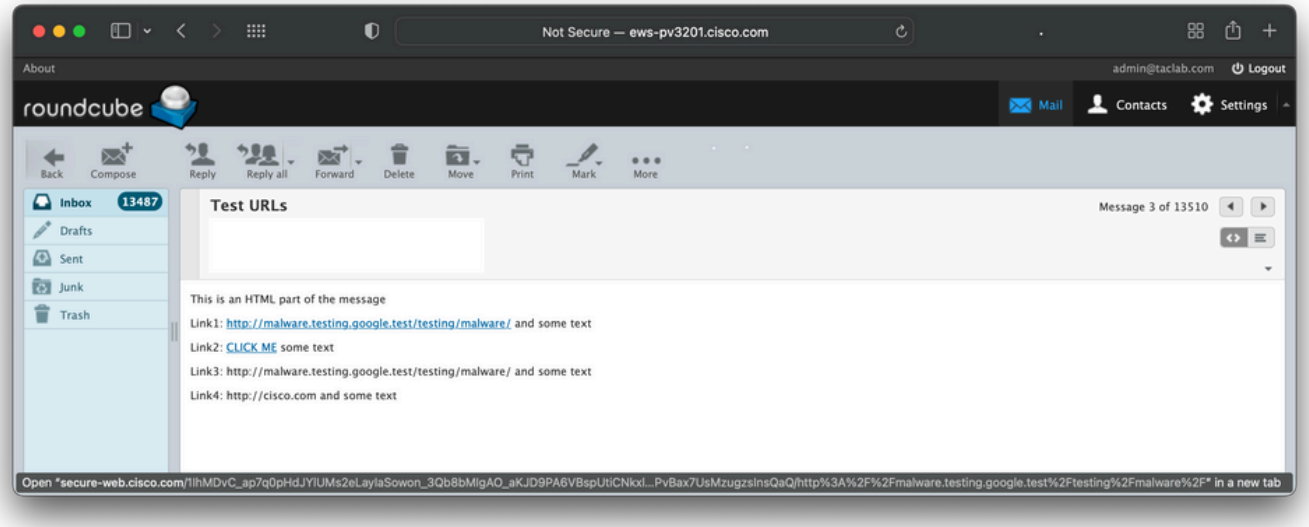
El gateway de correo electrónico detecta y evalúa cada una de las URL. La puntuación maliciosa activa la regla de filtro de contenido URL_SCORE y realiza la acción **url-reputation-proxy-redirect-action**

```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL
redirected to Cisco Security proxy Tue Jul 5 12:42:19 2022 Info: MID 139508 rewritten to MID
139509 by url-reputation-proxy-redirect-action filter 'URL SCORE'
```

Observe cómo se reescriben las direcciones URL en la parte HTML del mensaje. Igual que en el escenario A, sólo se reescriben las direcciones URL que se encuentran en el atributo href de un elemento A-tag y se omiten las direcciones URL que se encuentran en la parte de texto del elemento A-tag. Con una acción defang, se quita un elemento A-tag completo, pero con una acción de redirección se reescribe la dirección URL del atributo href.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

Link1: http://malware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME some text

Link3: http://malware.testing.google.test/testing/malware/ and some text

Link4: http://cisco.com and some text

--===============7781793576330041025==--
```

Como resultado, el cliente de correo electrónico muestra dos enlaces activos: Link1 y Link2, ambos apuntan al servicio Cisco Web Security Proxy pero el mensaje que se muestra en el cliente de correo electrónico muestra la parte de texto de la etiqueta A que no se reescribe de forma predeterminada. Para mejorar esta opción, eche un vistazo a la salida del cliente de correo web que muestra la parte text/html del mensaje.



En la parte de texto/plano de la parte MIME, la redirección parece más fácil de entender porque cada cadena de URL que coincide con la puntuación se reescribe.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F and some text Link2: http://cisco.com and some text --===============7781793576330041025==
```

Suma:

- La ejecución de redirección en la parte TEXT/PLAIN vuelve a escribir la cadena URL que coincide con el servicio de proxy de Cisco Web Secure
- La ejecución de redirección en la parte TEXT/HTML vuelve a escribir la dirección URL desde un atributo A-tag href de HTML con el servicio de proxy de Cisco Web Secure, pero deja todas las demás cadenas de URL que coincidan sin modificar

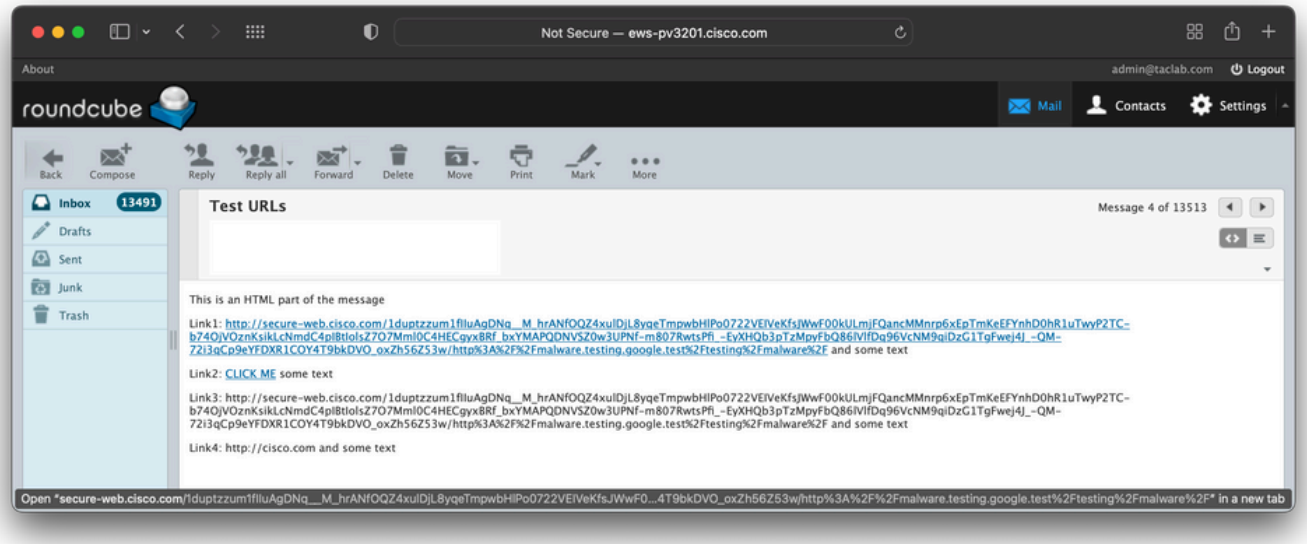
Situación D

Detección de amenazas no virales con filtro de brotes	No
Acción de filtro de contenido	Redireccionar
websecurityadvancedconfig href y la reescritura de texto está habilitada	Yes

Este escenario es similar al Escenario B de la primera parte. Para reescribir todas las cadenas de URL que coincidan en la parte HTML del mensaje está habilitado. Esto se realiza con el comando websecurityadvancedconfig al responder Y para el **"Do you want to rewrite both the URL text and the href in the message? ..** pregunta.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: 7bit

This is an HTML part of the message

Link1: http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F and some text

Link2: CLICK ME some text

Link3: http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F and some text

Link4: http://cisco.com and some text

--===============7781793576330041025==--
```

Una vez habilitadas la href y la reescritura de texto, se redirigen todas las cadenas URL que coincidan con las condiciones del filtro de contenido. El mensaje en el cliente de correo electrónico ahora se presenta con toda la redirección. Para entender mejor esto, mire la salida del cliente de correo web que muestra la parte text/html del mensaje.



La parte de texto/sin formato del mensaje MIME es la misma que en el escenario C, ya que el cambio websecurityadvancedconfig no tiene ningún impacto en las partes de texto/sin formato del mensaje.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: 7bit This is text part of the message Link1:
http://secure-
web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF00kULmjFQancMMn
rp6xEpTmKeEFYnhD0hR1uTwyP2TC-
b74OjVOznKsikLcNmdC4pIBtIolsZ7O7Mml0C4HECgyxBRf_bxYMAPQDNVSZ0w3UPNf-m807RwtsPfi_-
EyXHQb3pTzMpyFbQ86lVlfDq96VcNM9qiDzG1TgFwej4J_-QM-
72i3qCp9eYFDXR1COY4T9bkDVO_oxZh56Z53w/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalwa
re%2F and some text Link2: http://cisco.com and some text --===============7781793576330041025==
```

Suma:

- La ejecución de redirección en la parte TEXT/PLAIN vuelve a escribir las cadenas de URL que coinciden con el servicio de proxy de Cisco Web Secure
- La ejecución de redirección en el elemento TEXT/HTML vuelve a escribir la dirección URL desde un atributo A-tag href de HTML junto con el elemento de texto, así como cualquier otra cadena de URL que coincida en el cuerpo de HTML con el servicio de proxy de Cisco Web Secure

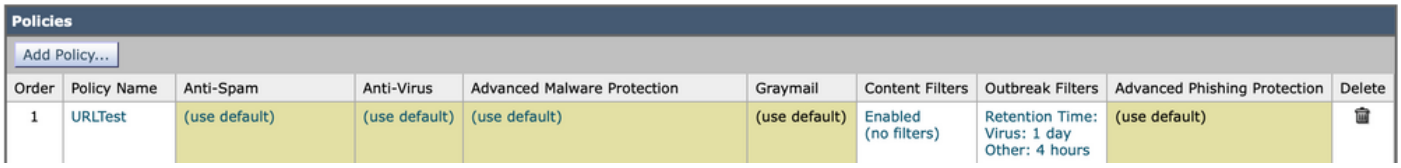
Parte 3 - OF Redirect

Esta parte proporciona información sobre cómo la configuración OF para la detección de amenazas no virales afecta a los análisis de URL.

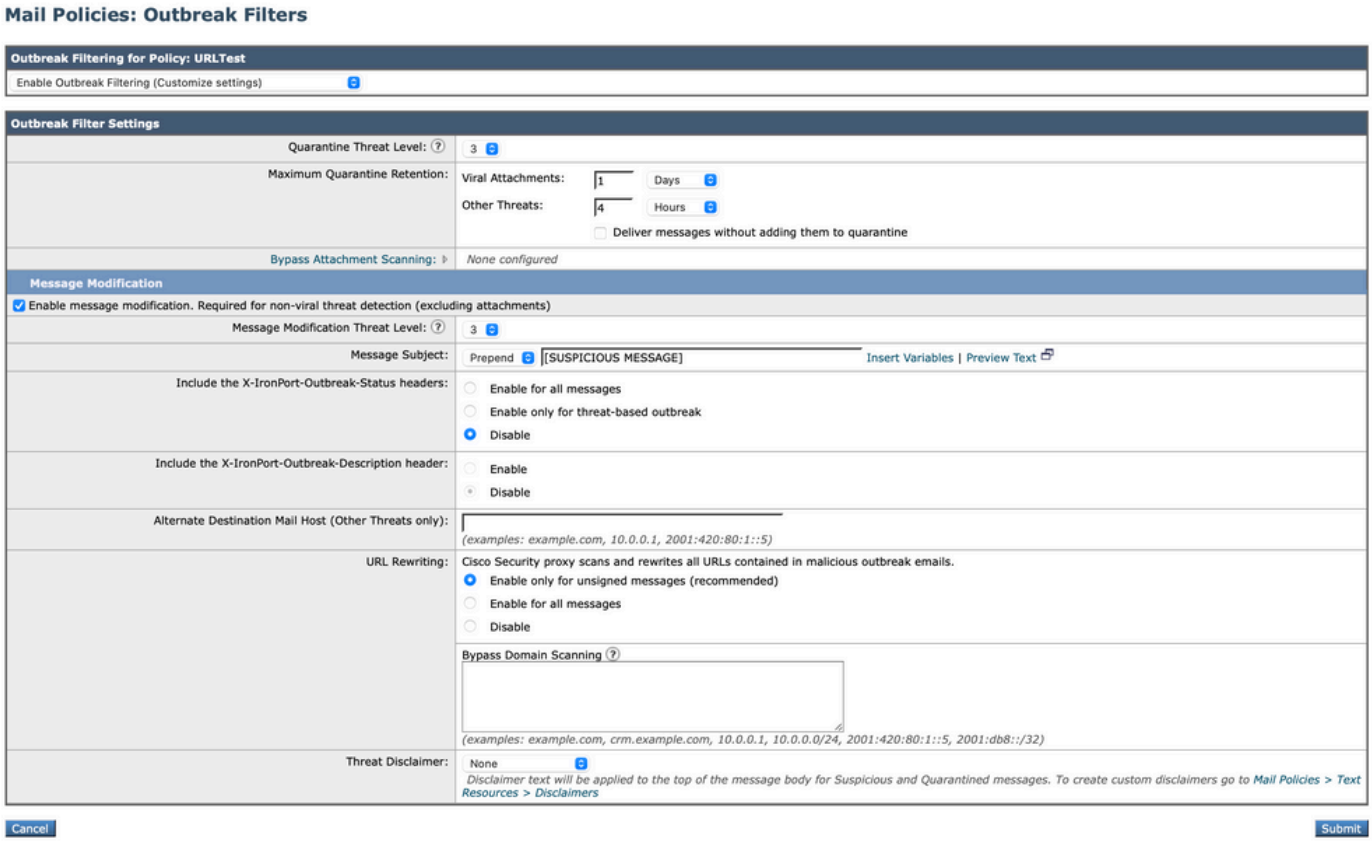
Configuración

Para ello, se desactiva el filtro de contenido utilizado en las dos primeras partes.

- Política de correo con configuración predeterminada de AS/AV/AMP y OFF activada



- El análisis de filtros de brote de virus para la detección de amenazas no virales se configura con un conjunto de reescritura de URL para reescribir todas las URL contenidas en correos electrónicos maliciosos



Cuando OF clasifica el mensaje como malicioso, todas las URL incluidas se reescriben con el servicio de proxy de Cisco Web Secure.

Situación E

Detección de amenazas no virales con filtro de brotes	Yes
Acción de filtro de contenido	No
websecurityadvancedconfig href y la reescritura de texto está habilitada	No

Este escenario muestra cómo funciona la reescritura de mensajes sólo con OF habilitado y websecurityadvanced config href y la reescritura de texto deshabilitada.

```
Wed Jul 6 14:09:19 2022 Info: MID 139514 Outbreak Filters: verdict positive Wed Jul 6 14:09:19
2022 Info: MID 139514 Threat Level=5 Category=Phish Type=Phish Wed Jul 6 14:09:19 2022 Info: MID
139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19
2022 Info: MID 139514 rewritten URL u'http://cisco.com' Wed Jul 6 14:09:19 2022 Info: MID 139514
rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6 14:09:19 2022
Info: MID 139514 rewritten URL u'http://malware.testing.google.test/testing/malware/' Wed Jul 6
14:09:19 2022 Info: MID 139514 rewritten to MID 139515 by url-threat-protection filter 'Threat
Protection' Wed Jul 6 14:09:19 2022 Info: Message finished MID 139514 done Wed Jul 6 14:09:19
```

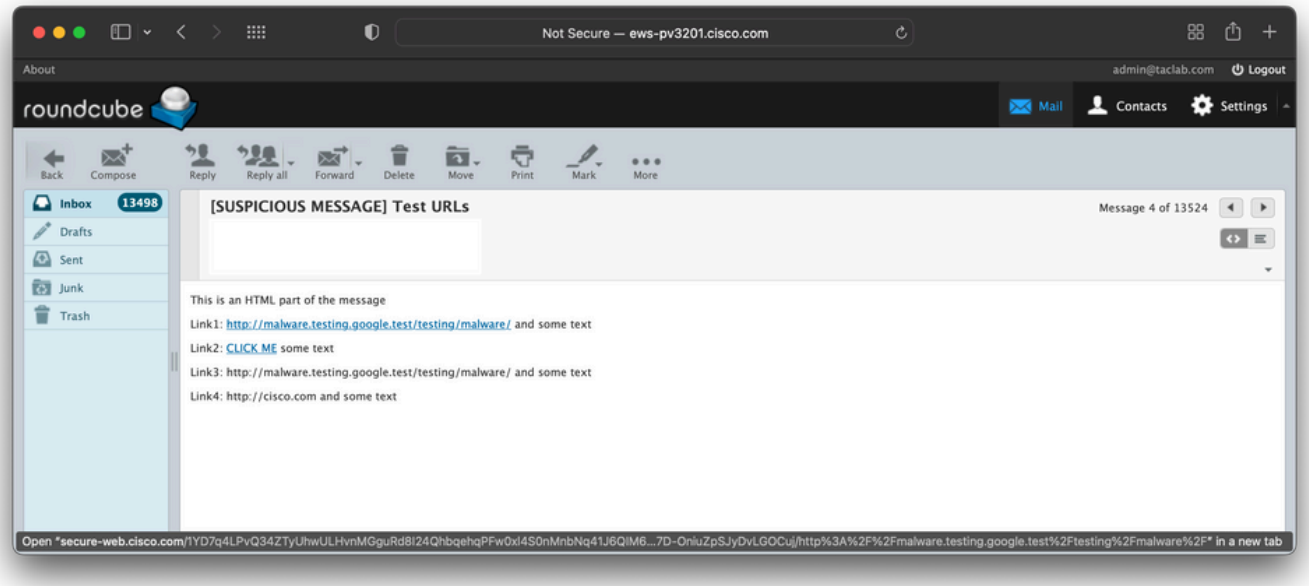
```
2022 Info: MID 139515 Virus Threat Level=5 Wed Jul 6 14:09:19 2022 Info: MID 139515 quarantined
to "Outbreak" (Outbreak rule:Phish: Phish)
```

Comencemos con la parte MIME text/plain. Después de realizar una comprobación rápida, se puede observar que todas las URL que se encuentran dentro de la parte sin formato o de texto se reescriben en los servicios proxy de Cisco Web Secure. Esto sucede porque la reescritura de URL está habilitada para todas las URL dentro del mensaje malicioso de Outbreak.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: quoted-printable This is text part of the message Link1:
http://secure-web.cisco.com/11ZWFnZYM5Rp_tvvnco4I3GtnExIEFqpirK= f5WBmD_7X-
8wSvnm0QxYNYhb4aplEtOXp_-0CMTnyw6WX63xZIFnj5S_n0vY18F9GOJWCSoVJpK= 3OEq8lB-jcbjx9BWlZaNbl-t-
uTOLj107Z3j8XCAdOwHe1t7GGF8LFt1GNFRCVLEM_wQZyo-uxh= UfkhZVETXPZAdddg6-
uCeoeimiRZUOAzqvgw2axm903AUpieDdfeMHYXpmzeMwu574FRGbbr7uV=
tB65hfy29t2r_VyWA24b6nyaKyJ_hmRf2A4PBWOTe37cRLveONF9cI3P51GxU/http%3A%2F%2F=
malware.testing.google.test%2Ftesting%2Fmalware%2F and some text Link2: http://secure-
web.cisco.com/1o7068d-d0bG3Sqwcifil89X-tY7S4csHT6=
LsLToTUYJqWzfLfODch91yXWfJ8aOxPq1PQBSACgJlDt4hCZipXXmC1XI3-XdNLGBMd0bLfj1cB= hY_OWlBfLD-
zC86M02dm_fOXCqKT0tDET3RD_KAeUWTWhWZvN9i8lLPcwBBBi9TLjMAMnRKPmeg= En_YQvDnCzTB4qYkG8aUQlFsecXB-
V_HU1vL8IRFRP-uGINjhHp9kWCnntJBJEm0MheA1T6mBJJ= ZhBZmfymfOddXs-
xIGiYXn3juN1TvuOlCceo3YeaiVrbOXc0lZs3FO8xvNjOnwVKN181yGKPQ9Y= cn5aSWvg/http%3A%2F%2Fcisco.com
and some text --===============7781793576330041025==
```

Esta es la parte text/html procesada del mensaje MIME.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

=20
Link1: http://ma= lware.testing.google.test/testing/malware/ and some text

Link2: CLICK ME<= /a> some text

Link3: http://malware.testing.google.test/testing/malware/ and some= textLink4: http://cisco.com
and some text=20 --===============7781793576330041025==--
```



La primera razón que se puede observar aquí es por qué Link4 no se reescribe. Si lees el artículo con cuidado ya sabes la respuesta. De forma predeterminada, la parte text/html de MIME evalúa y

manipula sólo los atributos href de los elementos A-tag. Si se desea un comportamiento similar al de la parte de texto/sin formato, se deben habilitar websecurityadvancedconfig href y la reescritura de texto. El siguiente escenario hace exactamente esto.Suma:

- La ejecución de redirección de OF en la parte TEXT/PLAIN vuelve a escribir toda la cadena de URL que coincida con el servicio de proxy de Cisco Web Secure
- La ejecución de redirección de OF en la parte TEXT/HTML reescribe sólo la URL de un atributo A-tag href de HTML con el servicio de proxy de Cisco Web Secure

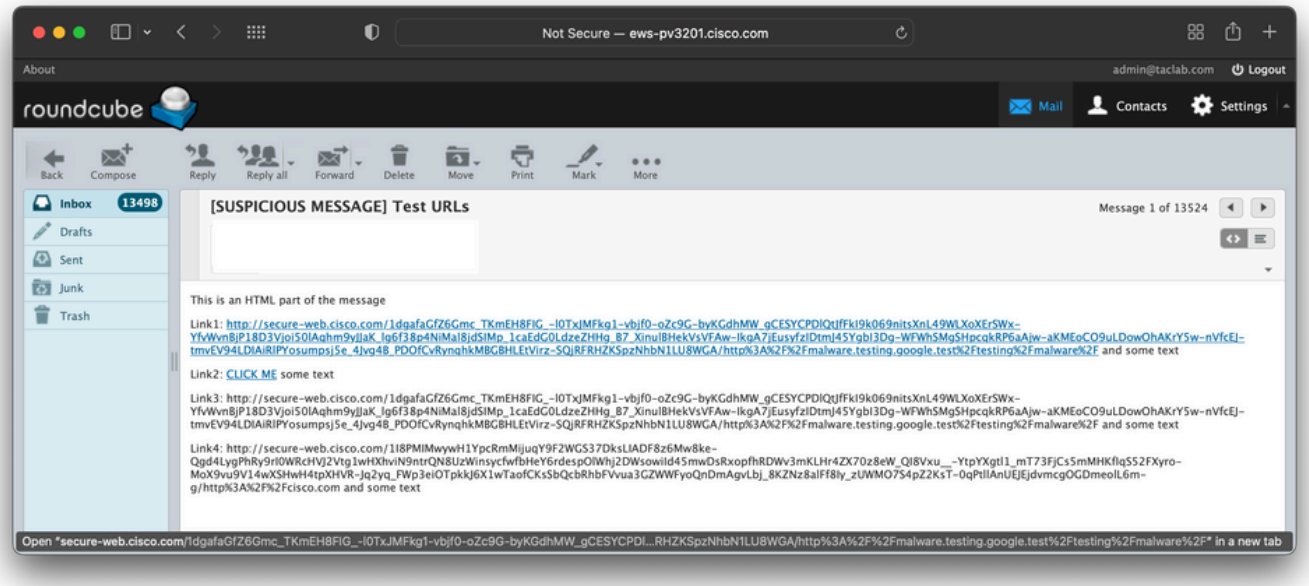
Situación F

Detección de amenazas no virales con filtro de brotes	Yes
Acción de filtro de contenido	No
websecurityadvancedconfig href y la reescritura de texto está habilitada	Yes

Este escenario permite que websecurityadvancedconfig href y la reescritura de texto muestren cómo cambia el comportamiento en la reescritura de URL proporcionada por la detección de amenazas no virales. En este momento debe entenderse que websecurityadvancedconfig no afecta a las partes MIME text/plain. Evaluemos solamente la parte text/html y veamos cómo ha cambiado el comportamiento.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version:
1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

=20
Link1: http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-l0TxJMFkg=_1-vbjf0-oZc9G-
byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP18=
D3Vjoi50lAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_XinulBHekVsVFAw=_-
IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDowOhAKrY5w-nVfc=_EJ-
tmvEV94LDIAiRlPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-SQjRFRHZKSpzNh=
bN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F_and_some_text

Link2: CLICK ME some text

Link3: http://secure-web.cisco.com/1dgafaGfZ6Gmc_TKmEH8FIG_-l0TxJMF= kg1-vbjf0-oZc9G-
byKGdhMW_gCESYCPDlQtJfFkI9k069nitsXnL49WLXoXErSWx-YfvWvnBjP=
18D3Vjoi50lAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdG0LdzeZHHg_B7_XinulBHekVsVF= Aw-
IkgA7jEusyfzIDtmJ45YgbI3Dg-WFWhSMgSHpcqkRP6aAjw-aKMEoCO9uLDowOhAKrY5w-nV= fcEJ-
tmvEV94LDIAiRlPYosumpsj5e_4Jvg4B_PDOfCvRynqhkMBGBHLEtVirz-SQjRFRHZKSpz=
NhbN1LU8WGA/http%3A%2F%2Fmalware.testing.google.test%2Ftesting%2Fmalware%2F= and some text

Link4: http://secure-web.cisco.com/1I8PMIMwywH1YpcRmMijuqY9F2WGS37D= ksLIADF8z6Mw8ke-
Qgd4LygPhRy9rI0WRcHVJ2Vtg1wHXhviN9ntrQN8UzWinsycfwfbHeY6rde=
spOlWhj2DWsowiId45mwDsRxopfhRDWv3mKLHr4ZX70z8eW_QI8Vxu__-YtpYXgtl1_mT73FjCs= 5mMHKfIqS52FXyro-
MoX9vu9V14wXSHwH4tpXHVR-Jq2yq_FWp3eiOTpkkJ6X1wTaofCKsSbQcb=
RhbFVvua3GZWWFyoQnDmAgvLbj_8KZNz8alFf8Iy_zUWMO7S4pZ2KsT-0qPtllAnUEJEjdvmcgO= GDmeolL6m-
g/http%3A%2F%2Fcisco.com and some text

=20 --===============7781793576330041025==--
```

Se puede observar que el resultado es muy similar al del Escenario D con la única diferencia de que todas las URLs han sido reescritas, no solo las maliciosas. Aquí se modifican todas las cadenas de URL que coinciden en la parte HTML junto con las no malintencionadas.



Suma:

- La ejecución de redirección de OF en la parte TEXT/PLAIN vuelve a escribir todas las cadenas de URL que coincidan con el servicio de proxy de Cisco Web Secure
- La ejecución de redirección de OF en el elemento TEXT/HTML vuelve a escribir la dirección URL desde un atributo A-tag href de HTML junto con el elemento de texto del elemento y todas las demás cadenas de URL que coincidan con el servicio de proxy de Cisco Web Secure

Situación G

Detección de amenazas no virales con filtro de brotes	Yes
Acción de filtro de contenido	Descolgar
websecurityadvancedconfig href y la reescritura de texto está habilitada	Yes

Este último escenario valida la configuración.

- Política de correo con configuración predeterminada de AS/AV/AMP y OFF activada

- El análisis de OF para la detección de amenazas no víricas se configura con la función de reescritura de URL configurada para reescribir todas las URL incluidas en los correos electrónicos maliciosos (igual que en escenarios anteriores)
- Filtro de contenido entrante: Filtro de contenido URL_SCORE habilitado

El filtro de contenido utiliza la condición de reputación de URL para hacer coincidir las URL malintencionadas, aquellas que tienen una puntuación entre -6.00 y -10.00. Como acción, se

registra el nombre del filtro de contenido y se realiza la acción defang **url-reputation-defang** está ocupado.

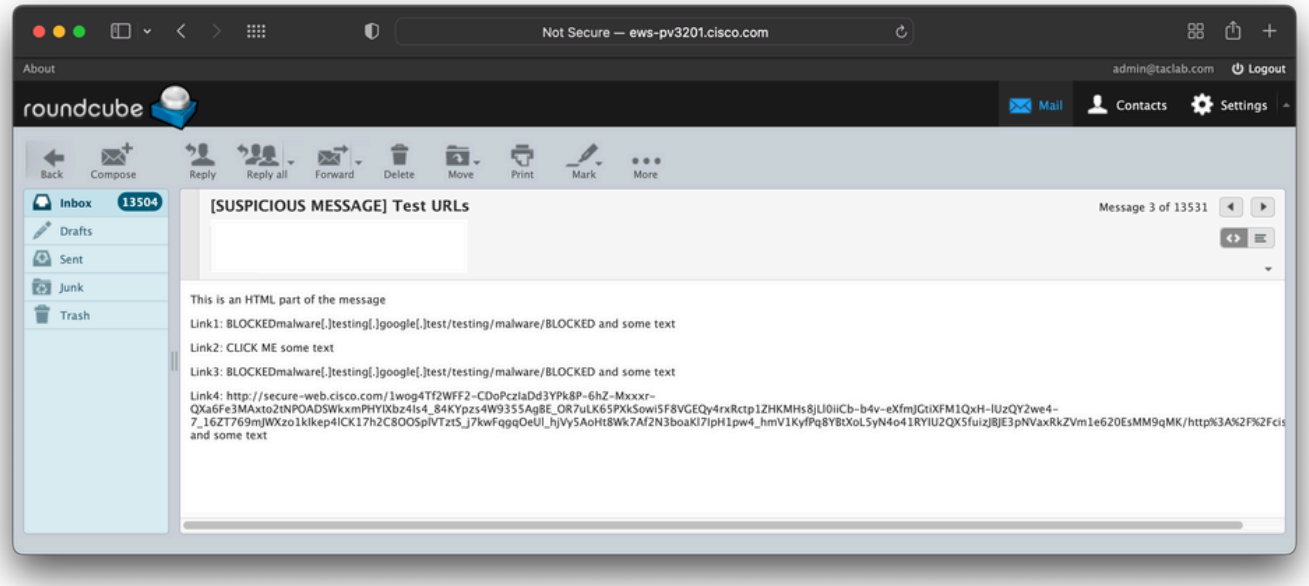
El gateway de correo electrónico envía y evalúa la misma copia del mensaje con los resultados:

```
Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Condition: URL Reputation Rule Wed Jul 6 15:13:10 2022 Info: MID 139518 Custom Log Entry: URL_SCORE Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has reputation -9.4 matched Action: URL defanged Wed Jul 6 15:13:10 2022 Info: MID 139518 rewritten to MID 139519 by url-reputation-defang-action filter 'URL_SCORE' Wed Jul 6 15:13:10 2022 Info: Message finished MID 139518 done Wed Jul 6 15:13:10 2022 Info: MID 139519 Outbreak Filters: verdict positive Wed Jul 6 15:13:10 2022 Info: MID 139519 Threat Level=5 Category=Phish Type=Phish Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten URL u'http://cisco.com' Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten URL u'http://cisco.com' Wed Jul 6 15:13:10 2022 Info: MID 139519 rewritten to MID 139520 by url-threat-protection filter 'Threat Protection' Wed Jul 6 15:13:10 2022 Info: Message finished MID 139519 done Wed Jul 6 15:13:10 2022 Info: MID 139520 Virus Threat Level=5
```

La canalización de correo electrónico explica que el mensaje es evaluado primero por los filtros de contenido, donde se activa el filtro URL_SCORE y se aplica URL-reputación-defang-action. Esta acción desactiva todas las URL maliciosas en las partes MIME text/plain y text/html. Debido a que websecurityadvanceconfig href y la reescritura de texto están habilitadas, todas las cadenas de URL que coincidan dentro del cuerpo HTML se desactivan cuando se eliminan todos los elementos de la etiqueta A y se reescriben partes de texto de la URL entre palabras BLOQUEADAS y se colocan todos los puntos entre corchetes. Lo mismo ocurre con otras URL malintencionadas que no se colocan en elementos HTML de etiqueta A. A continuación, el filtro de brotes de virus procesa el mensaje. El OF detecta las URL maliciosas e identifica el mensaje como malicioso (Nivel de amenaza=5). Como resultado, vuelve a escribir todas las URL malintencionadas y no malintencionadas que se encuentran dentro del mensaje. Debido a que la acción de filtrado de contenido ya ha modificado esas URL, el OF solo reescribe el resto de las URL no malintencionadas, ya que se configuró de forma intencionada para hacerlo. El mensaje que se muestra en el cliente de correo electrónico como parte de las URL maliciosas desactivadas y parte de la URL no maliciosa redirigida.

```
--===============7781793576330041025== Content-Type: text/html; charset="us-ascii" MIME-Version: 1.0 Content-Transfer-Encoding: quoted-printable

This is an HTML part of the message

=20
Link1: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO= CKED and some text

Link2: CLICK ME some text

Link3: BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLO= CKED and some text

Link4: http://secure-web.cisco.com/1wog4Tf2WFF2-CDoPczIaDd3YPk8P-6h= Z-Mxxxr-
QXa6Fe3MAxto2tNPOADSWkxmPHYIXbz4Is4_84KYpzs4W9355AgBE_OR7uLK65PXkSo=
wi5F8VGEQy4rxRctp1ZHKMHs8jLl0iiCb-b4v-eXfmJGtiXFM1QxH-lUzQY2we4-7_16ZT769mJ=
WXzo1kIkep4lCK17h2C8OOSplVTztS_j7kwFqgqOeUl_hjVy5AoHt8Wk7Af2N3boaKl7IpH1pw4=
```

```
_hmV1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F= %2Fcisco.com and
some text

=20 --===============7781793576330041025==--
```



Lo mismo se aplica a la parte de texto/sin formato del mensaje MIME. Todas las URL no malintencionadas se redirigen al proxy de Cisco Web Secure y las URL malintencionadas se desactivan.

```
--===============7781793576330041025== Content-Type: text/plain; charset="us-ascii" MIME-
Version: 1.0 Content-Transfer-Encoding: quoted-printable This is text part of the message Link1:
BLOCKEDmalware[.]testing[.]google[.]test/testing/malware/BLOCKE= D and some text Link2:
http://secure-web.cisco.com/1wog4Tf2WFF2-CDoPczIaDd3YPk8P-6hZ-M= xxxr-
QXa6Fe3MAxto2tNPOADSWkxmPHYIXbz4Is4_84KYpzs4W9355AgBE_OR7uLK65PXkSowi5=
F8VGEQy4rxRctp1ZHKMHs8jLl0iiCb-b4v-eXfmJGtiXFM1QxH-lUzQY2we4-7_16ZT769mJWXz=
o1kIkep4lCK17h2C8OOSplVTztS_j7kwFqgqOeUl_hjVy5AoHt8Wk7Af2N3boaKl7IpH1pw4_hm=
V1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F%2F= cisco.com and some
text --===============7781793576330041025==
```

Suma:

- CF defang run en la parte TEXT/PLAIN reescribe la URL en bloques BLOQUEADOS
- CF defang run en la parte TEXT/HTML reescribe la URL de una etiqueta A HTML cuando se quita una etiqueta A
- CF defang run en la parte TEXT/HTML reescribe todas las cadenas URL que coinciden en bloques BLOCKED
- La ejecución de redirección de OF en la parte TEXT/PLAIN vuelve a escribir todas las cadenas de URL que coincidan con el servicio de proxy de Cisco Web Secure (no malintencionado)
- La ejecución de redirección de OF en el elemento TEXT/HTML vuelve a escribir la dirección URL desde un atributo A-tag href de HTML junto con el elemento de texto del elemento y todas las demás cadenas de URL que coincidan con el servicio proxy de Cisco Web Secure (no malintencionado)

Troubleshoot

Siga estos puntos cuando haya que investigar el problema con la reescritura de URL.

- Active el registro de URL en mail_logs. Ejecute **OUTBREAKCONFIG** comando y respuesta **Y** a **Do you wish to enable logging of URL's?** [N]**>"**
- Verificación **WEBSECURITYADVANCECONFIG** en cada miembro del clúster de puerta de enlace de correo electrónico y asegúrese de que la opción href y text rewrite está establecida en consecuencia y es la misma en cada equipo. Tenga en cuenta que este comando es específico de cada equipo y que los cambios realizados aquí no afectan a la configuración del grupo o clúster.
- Verifique las condiciones y actividades de su filtro de contenido y asegúrese de que el filtro de contenido esté habilitado y aplicado a la política de correo entrante correcta. Verifique si no hay ningún otro filtro de contenido procesado antes con una acción final que pueda saltar para procesar otros filtros.
- Investigue la copia sin procesar del mensaje de origen y final. Tenga en cuenta para recuperar el mensaje en formato EML, los formatos patentados como MSG no son fiables cuando se trata de la investigación de mensajes. Algunos clientes de correo electrónico permiten ver el mensaje de origen e intentar recuperar la copia del mensaje con un cliente de correo electrónico diferente. Por ejemplo, MS Outlook para Mac le permite ver el Origen del mensaje, mientras que la versión de Windows sólo le permite ver los encabezados.

Summary

El propósito de este artículo es ayudar a entender mejor las opciones de configuración disponibles cuando se trata de reescritura de URL. Es importante recordar que los mensajes modernos son construidos por la mayoría del software de correo electrónico con el estándar MIME. Significa que la misma copia del mensaje puede mostrarse de forma diferente, lo que depende de las capacidades del cliente de correo electrónico y/o de los modos habilitados (modo texto vs HTML). De forma predeterminada, la mayoría de los clientes de correo electrónico modernos utilizan HTML para mostrar mensajes. Cuando se trata de reescritura de URL y HTML, tenga en cuenta que, de forma predeterminada, la puerta de enlace de correo electrónico solo reescribe las URL que se encuentran dentro del atributo href del elemento A-tag. En muchos casos, esto no es suficiente y se debe considerar habilitar tanto href como la reescritura de texto con el comando WEBSECURITYADVANCECONFIG. Recuerde que se trata de un comando de nivel de máquina y, para mantener la coherencia en el clúster, el cambio debe aplicarse por separado a cada uno de los miembros del clúster.