Entender a ação de desbloqueio e redirecionamento de URL no Secure Email Gateway

Contents

Introduction

Este documento descreve a diferença entre as ações defang e redirect usadas no filtro de URL e como usar a opção de regravação disponível para o atributo e o texto href.

Prerequisites

Requirements

Para agir com base na reputação da URL ou para aplicar políticas de uso aceitável com a mensagem e filtros de conteúdo, o recurso de filtros de epidemia deve ser habilitado globalmente.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Email Gateway
- Filtros de epidemia
- Filtros de conteúdo e mensagens

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Um dos recursos de filtragem de URL é agir com base na reputação ou categoria do URL com o uso de filtros de mensagem e/ou conteúdo. Com base no resultado da verificação de URL (condição relacionada à URL), uma das três ações disponíveis em uma URL pode ser aplicada:

- Desativar URL
- Redirecionar para o Cisco Security Proxy
- Substituir URL pela mensagem de texto

O foco deste documento é explicar o comportamento entre as opções Defang e Redirect URL. Ele também fornece uma breve descrição e explicação dos recursos de regravação de URL da detecção de ameaças não virais de um filtro de detecção de epidemia.

Exemplo de mensagem

A mensagem de exemplo usada em todos os testes é o tipo de mensagem MIME multipart/alternate e inclui partes text/plain e text/html. Essas partes geralmente são geradas automaticamente por software de e-mail e contêm o mesmo tipo de conteúdo formatado para receptores HTML e não-HTML. Para isso, o conteúdo de text/plain e text/html foi editado manualmente.

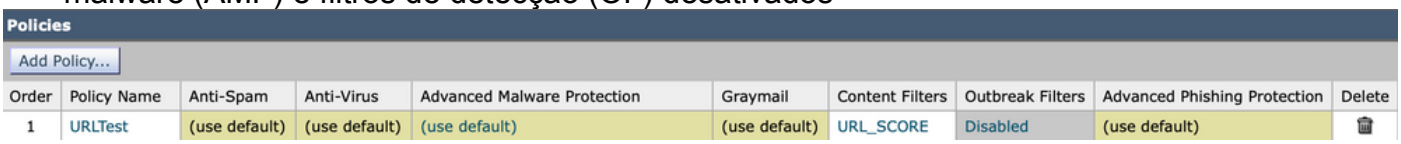
```
Content-Type: multipart/alternative; boundary="===============7781793576330041025==" MIME-
Version: 1.0 From: admin@example.com Date: Mon, 04 Jul 2022 14:38:52 +0200 To: admin@cisco.com
Subject: Test URLs --===============7781793576330041025== Content-Type: text/plain; charset="us-
ascii" MIME-Version: 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

Configurações

Na primeira parte, a configuração usa:

- Política de e-mail com configuração antisspam (AS)/antivírus (AV)/proteção avançada contra malware (AMP) e filtros de detecção (OF) desativados



- Filtro de conteúdo de entrada: Filtro de conteúdo URL_SCORE habilitado

O filtro de conteúdo usa a condição de reputação de URL para corresponder URLs mal-intencionados, aqueles com pontuação entre -6,00 e -10,00. Como ação, o nome do filtro de conteúdo é registrado e a ação de desativação **url-reputation-defang** é tomada.

Ação de defang

Éimportante esclarecer o que é uma ação de descongelamento. O guia do usuário fornece uma explicação; Desative uma URL para que não seja possível clicar nela. Os destinatários da mensagem ainda podem ver e copiar o URL.

Cenário A

Detecção de ameaças não virais do filtro de detecção	No
Ação do filtro de conteúdo	Defang
websecurityadvancedconfig href e a regravação de texto está habilitada	No

Este cenário explica o resultado da ação de desativação configurada com as configurações padrão. Na configuração padrão, o URL é regravado quando apenas as tags HTML são removidas. Observe um parágrafo HTML com alguns URLs:

```
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
```

Nos dois primeiros parágrafos, o URL é representado por uma tag A HTML adequada. O elemento <A> inclui o **href=** atributo que está incluído na própria tag e indica o destino do link. O conteúdo dos elementos de tag também pode indicar o destino do link. Este **text form** do link pode incluir o URL. O primeiro Link1 inclui o mesmo link de URL no atributo href e na parte de texto do elemento. Observe que esses URLs podem ser diferentes. O segundo Link2 inclui o URL apropriado somente dentro do atributo href. O último parágrafo não inclui quaisquer elementos A.

> **Note**: O endereço correto sempre pode ser visto quando você move o cursor sobre o link ou quando você exibe o código-fonte da mensagem. Infelizmente, o código-fonte não pode ser facilmente encontrado com alguns clientes de e-mail populares.

Quando a mensagem é correspondida pelo filtro URL_SCORE, os URLs mal-intencionados são removidos. Quando o log de URL estiver habilitado com o comando **OUTBREAKCONFIG** as pontuações e URLs podem ser encontrados em 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'
```

Isso resulta na mensagem reescrita:

```
--===============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==--
```

O resultado da ação defang tomada na parte text/html da mensagem MIME é uma tag A retirada e o conteúdo da tag é deixado intocado. Nos dois primeiros parágrafos, ambos os links foram desvinculados, onde o código HTML foi removido e a parte de texto do elemento foi deixada. O endereço da URL no primeiro parágrafo é o da parte de texto do elemento HTML. Deve-se notar que o endereço URL do primeiro parágrafo ainda está visível após a ação de descongelamento ter sido tomada, mas sem as tags A HTML, o elemento não deve ser clicável. O terceiro parágrafo não é definido como o endereço da URL aqui não é colocado entre quaisquer marcas A e não é considerado um link. Talvez não seja um comportamento desejável por duas razões. Primeiro, o usuário pode ver e copiar facilmente o link e executá-lo no navegador. A segunda razão é que alguns softwares de e-mail tendem a detectar uma forma válida de URL dentro do texto e torná-lo um link clicável.

Vejamos a parte de texto/sem formatação da mensagem MIME. A parte de texto/sem formatação inclui dois URLs no formulário de texto. O texto/simples é exibido por MUA que não entende o código HTML. Na maioria dos clientes de e-mail modernos, você não vê as partes de texto/sem formatação da mensagem, a menos que tenha configurado intencionalmente seu cliente de e-mail para fazer isso. Geralmente, você precisa verificar o código-fonte da mensagem, um formato EML bruto da mensagem para ver e investigar as partes MIME.

A listagem aqui mostra URLs da parte de texto/sem formatação da mensagem de origem.

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

Um desses dois links teve uma pontuação maliciosa e foi desfigurado. Por padrão, a ação defang realizada na parte de texto/sem formatação do tipo MIME tem um resultado diferente do que na parte de texto/html. Está entre as palavras BLOQUEADAS e todos os pontos entre colchetes.

```
--===============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==
```

Soma:

- Execução de defang na parte TEXT/PLAIN regrava a URL em blocos BLOQUEADOS
- A execução Defang na parte TEXT/HTML regrava o URL a partir de uma tag A HTML quando a tag A é retirada sem o texto entre as tags A tocadas, que também pode ser um endereço URL

Cenário B

Detecção de ameaças não virais do filtro de detecção	No
Ação do filtro de conteúdo	Defang
websecurityadvancedconfig href e a regravação de texto está habilitada	Yes

Este cenário fornece informações sobre como o comportamento da ação de defangs muda após o uso de uma das opções websecurityadvancedconfig. O websecurityadvancedconfig é o comando CLI específico em nível de máquina que permite ajustar configurações específicas para verificação de URL. Uma das configurações aqui permite que você altere o comportamento padrão da ação de desativação.

```
> 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
...
```

Na quarta questão, **Do you want to rewrite both the URL text and the href in the message? ..**, a resposta `Y` indica que, no caso da parte MIME baseada em HTML da mensagem, todas as strings de URL que correspondem independentemente de serem encontradas no atributo href do elemento A-tag, é a parte de texto ou fora de qualquer elemento que seja reescrito. Neste cenário, a mesma mensagem é enviada novamente, mas com um resultado ligeiramente diferente.

Examine novamente o código da peça MIME text/html com os URLs e compare-o com o código HTML processado pelo gateway de e-mail.

```
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
```

Quando a opção de reescrita de texto e href está habilitada, todas as correspondências dos URLs de filtro são desvinculadas, independentemente de o endereço do URL fazer parte do atributo href ou da parte de texto do elemento HTML da tag A, ou de ser encontrado em outra parte do 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==--
```

Os URLs separados agora são reescritos quando o elemento A-tag é removido junto com uma reescrita da parte de texto do link quando ele corresponde ao formato do URL. A parte de texto reescrita é feita da mesma forma que na parte de texto/sem formatação da mensagem MIME. O item é colocado entre palavras BLOQUEADAS e todos os pontos são colocados entre colchetes. Isso impede que o usuário copie e cole o URL, e alguns clientes de software de e-mail tornam o texto clicável.

Soma:

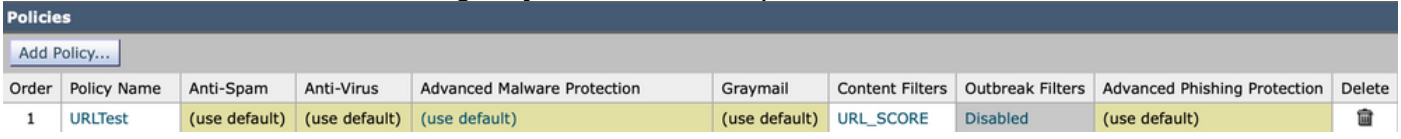
- Execução de defang na parte TEXT/PLAIN regrava a URL em blocos BLOQUEADOS
- A execução defang na parte TEXT/HTML regrava a URL a partir de uma tag A HTML quando uma tag A é retirada
- A execução defang na parte TEXT/HTML regrava todas as strings de URL que correspondem aos blocos BLOQUEADOS

Parte II - Redirecionar

Configurações

Na segunda parte, a configuração usa:

- Política de e-mail com configuração AS/AV/AMP padrão e OF desabilitado



- Filtro de conteúdo de entrada: Filtro de conteúdo URL_SCORE habilitado

O filtro de conteúdo usa a condição de reputação de URL para corresponder URLs mal-intencionados, aqueles com pontuação entre -6,00 e -10,00. Como ação, o nome do filtro de conteúdo é registrado e o **redirect action** é tomada.

Ação de redirecionamento

Redirecionar para o serviço Cisco Security Proxy para avaliação do tempo de clique permite que o destinatário da mensagem clique no link e seja redirecionado para um proxy de segurança da Web da Cisco na nuvem, que bloqueia o acesso se o site for identificado como mal-intencionado.

Cenário C

Detecção de ameaças não virais do filtro de detecção	No
Ação do filtro de conteúdo	Redirecionar
websecurityadvancedconfig href e a regravação de texto está habilitada	No

Esse cenário é muito semelhante em comportamento ao Cenário A a partir da primeira parte com a diferença feita na ação do filtro de conteúdo para redirecionar o URL em vez de desdefini-lo. As configurações de websecurityadvancedconfig são restauradas para as configurações padrão, o que significa que **"Do you want to rewrite both the URL text and the href in the message? ..** está definido como **N.**

O gateway de e-mail detecta e avalia cada um dos URLs. A pontuação mal-intencionada aciona a regra de filtro de conteúdo URL_SCORE e executa a ação **url-reputation-proxy-redirect-action**

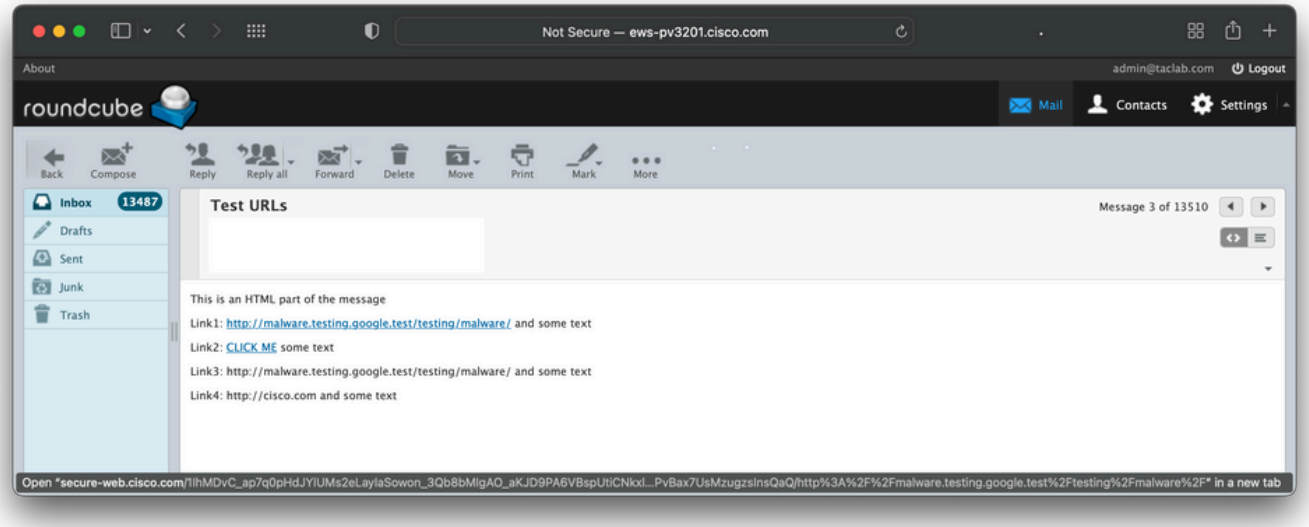
```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/ 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 como os URLs são reescritos na parte HTML da mensagem. O mesmo que no cenário A, somente os URLs encontrados no atributo href de um elemento A-tag são reescritos e os endereços de URL encontrados na parte de texto do elemento A-tag são ignorados. Com uma ação de desativação, um elemento A-tag inteiro é removido, mas com uma ação de redirecionamento a URL no atributo href é reescrita.

```
--===============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, o cliente de e-mail exibe dois links ativos: Link1 e Link2, ambos apontam para o serviço Cisco Web Security Proxy, mas a mensagem exibida no cliente de e-mail exibe a parte de texto da tag A que não é reescrita por padrão. Para ver melhor isso, observe a saída do cliente de webmail que exibe a parte text/html da mensagem.



Na parte de texto/sem formatação da parte MIME, o redirecionamento parece mais fácil de entender, pois cada string de URL que corresponde à pontuação é reescrita.

```
--===============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==
```

Soma:

- A execução de redirecionamento na parte TEXT/PLAIN regrava a string de URL que corresponde ao serviço proxy Cisco Web Secure
- A execução de redirecionamento na parte TEXT/HTML regrava o URL a partir de um atributo HTML A-tag href com o serviço de proxy do Cisco Web Secure, mas deixa todas as outras strings de URL correspondentes sem modificações

Cenário D

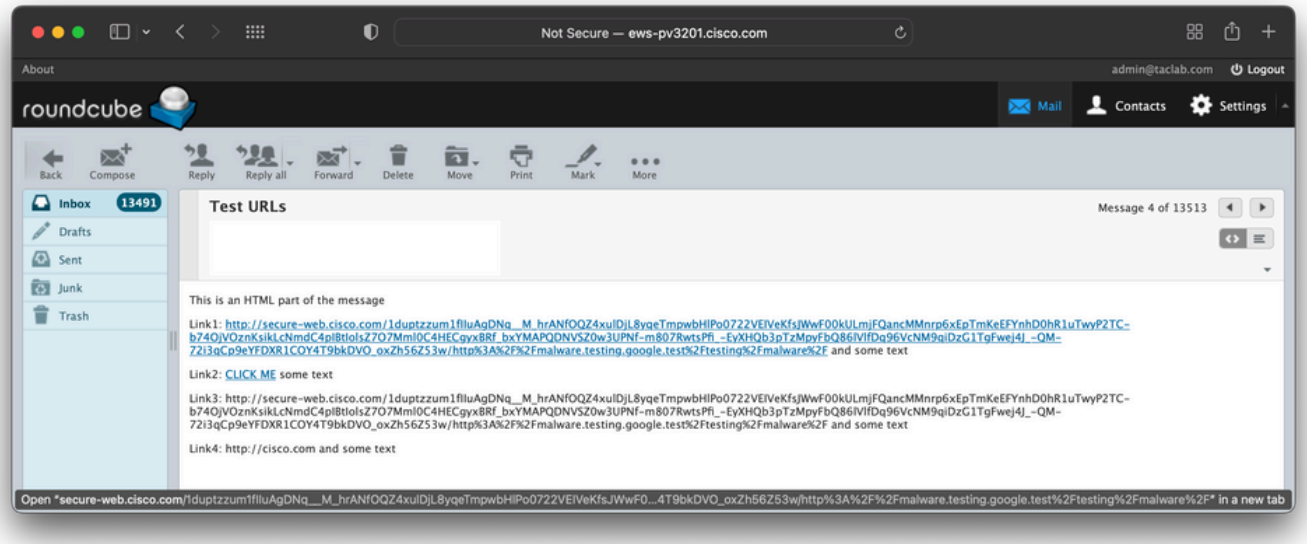
Detecção de ameaças não virais do filtro de detecção	No
Ação do filtro de conteúdo	Redirecionar
websecurityadvancedconfig href e a regravação de texto está habilitada	Yes

Esse cenário é semelhante ao cenário B da parte um. Para regravar todas as strings de URL que correspondem na parte HTML da mensagem está habilitada. Isso é feito com o comando websecurityadvancedconfig quando você responde Y como **"Do you want to rewrite both the URL text and**

the href in the message? .. pergunta.

```
--===============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==--
```

Quando a reescrita de href e texto estiver habilitada, todas as strings de URL que corresponderem às condições do filtro de conteúdo serão redirecionadas. A mensagem no cliente de e-mail agora é apresentada com todo o redirecionamento. Para entender melhor isso, observe a saída do cliente de webmail que exibe a parte de texto/html da mensagem.



A parte de texto/sem formatação da mensagem MIME é a mesma do Cenário C, pois a alteração websecurityadvancedconfig não tem nenhum impacto sobre as partes de texto/sem formatação da mensagem.

```
--===============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==
```

Soma:

- A execução de redirecionamento na parte TEXT/PLAIN regrava as strings de URL que correspondem ao serviço de proxy do Cisco Web Secure
- A execução de redirecionamento na parte TEXT/HTML regrava o URL a partir de um atributo HTML A-tag href junto com a parte de texto, bem como qualquer outra string de URL que corresponda no corpo HTML ao serviço proxy Cisco Web Secure

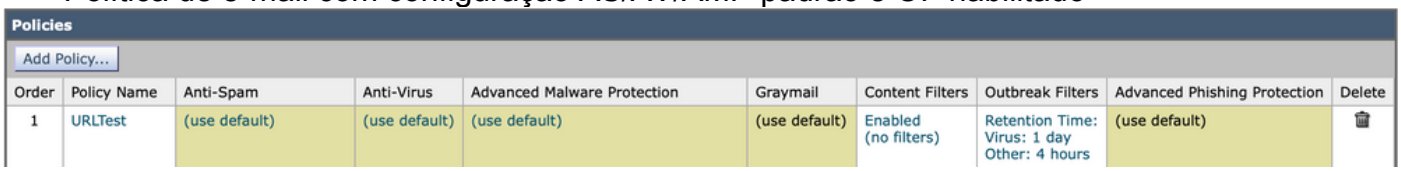
Parte 3 - DE Redirecionamento

Esta parte fornece informações sobre como as configurações de OF para detecção de ameaças não-virais afetam as varreduras de URL.

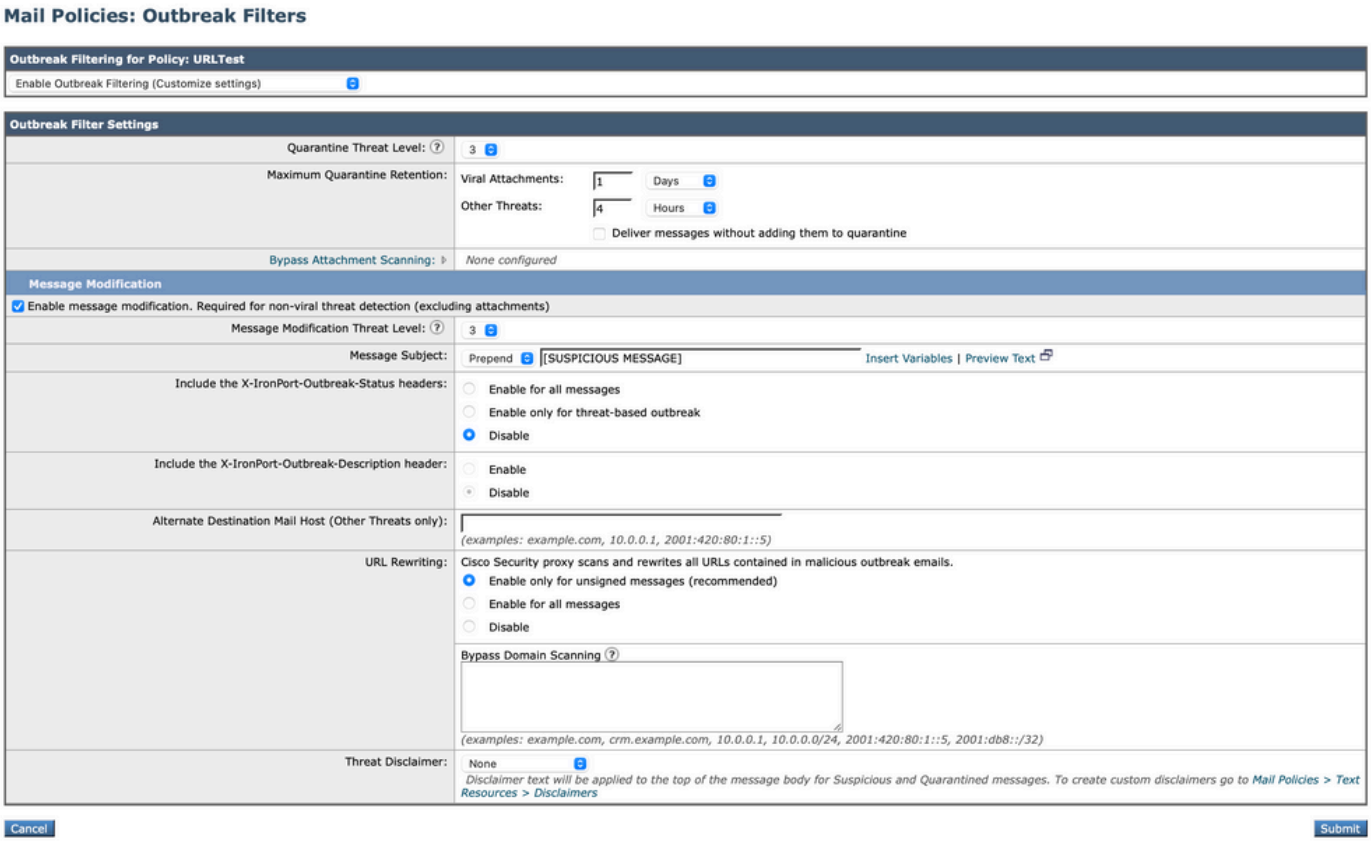
Configuração

Para esse fim, o filtro de conteúdo usado nas duas primeiras partes é desativado.

- Política de e-mail com configuração AS/AV/AMP padrão e OF habilitado



- Os filtros de detecção de ameaças não virais verificam se a detecção de ameaças não é viral e configuram uma reescrita de URL para reescrever todas as URLs contidas em e-mails mal-intencionados



Quando a mensagem é classificada por OF como mal-intencionada, todos os URLs dentro são regravados com o serviço proxy Cisco Web Secure.

Cenário E

Detecção de ameaças não virais do filtro de detecção	Yes
Ação do filtro de conteúdo	No
websecurityadvancedconfig href e a regravação de texto está habilitada	No

Este cenário mostra como a regravação de mensagem funciona com apenas OF habilitado e websecurityadvancedconfig href e a regravação de texto desabilitada.

```
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)
```

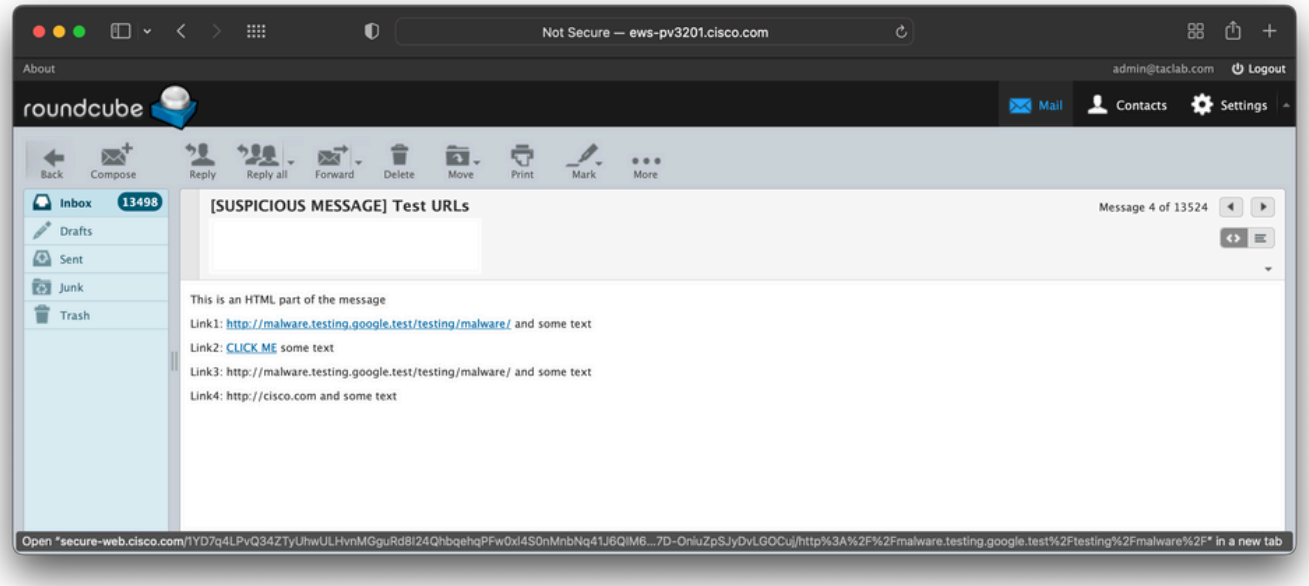
Vamos começar com a parte MIME text/plain. Após uma rápida verificação, pode-se observar que todos os URLs dentro da parte de texto/sem formatação são regravados nos serviços proxy do Cisco Web Secure. Isso acontece porque a regravação de URL está habilitada para todos os URLs dentro da mensagem mal-intencionada de detecção.

```
--===============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 é a parte text/html processada da mensagem 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==--
```



A primeira coisa que pode ser observada aqui é por que Link4 não é reescrito. Se ler o artigo com atenção, já sabe a resposta. A parte text/html do MIME, por padrão, avalia e manipula apenas os atributos href dos elementos de marca A. Se for desejado um comportamento semelhante ao da parte de texto/sem formatação, a href websecurityadvancedconfig e a regravação de texto deverão ser habilitadas. O próximo cenário faz exatamente isso.Soma:

- OF redirect executado na parte TEXT/PLAIN regrava toda a string de URL que corresponde ao serviço proxy Cisco Web Secure
- OF redirect executado na parte TEXT/HTML regrava somente o URL de um atributo HTML A-tag href com o serviço proxy Cisco Web Secure

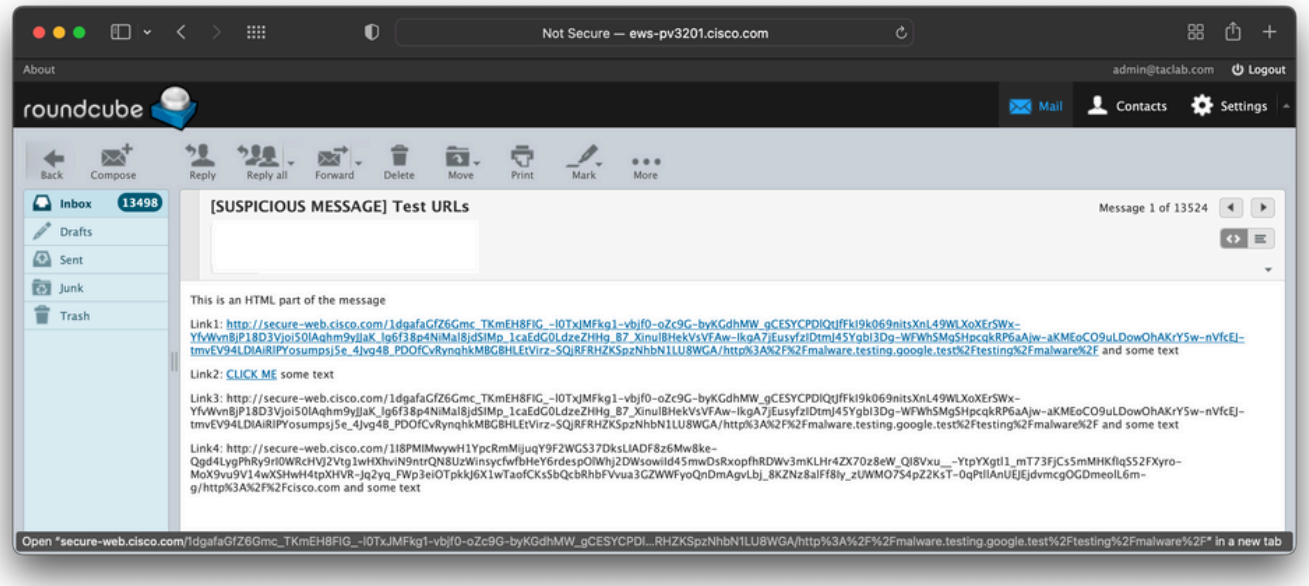
Cenário F

Detecção de ameaças não virais do filtro de detecção	Yes
Ação do filtro de conteúdo	No
websecurityadvancedconfig href e a regravação de texto está habilitada	Yes

Este cenário permite que o websecurityadvancedconfig href e a regravação de texto mostrem como o comportamento na regravação de URL fornecido pelo OF non-viral threat detection muda. Neste momento, deve-se entender que o websecurityadvancedconfig não afeta partes de texto/MIME simples. Vamos avaliar apenas a parte text/html e ver como o comportamento mudou.

```
--===============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==--
```

Pode-se observar que a saída é muito semelhante à do cenário D com a única diferença de que todos os URLs foram regravados, não apenas os mal-intencionados. Todas as strings de URL que correspondem na parte HTML, juntamente com as não-maliciosas, são modificadas aqui.



Soma:

- OF redirect run na parte TEXT/PLAIN regrava todas as strings de URL que correspondem ao serviço proxy Cisco Web Secure
- OF redirect run na parte TEXT/HTML regrava o URL de um atributo HTML A-tag href junto com a parte de texto do elemento e todas as outras strings de URL que correspondem ao serviço de proxy Cisco Web Secure

Cenário G

Detecção de ameaças não virais do filtro de detecção	Yes
Ação do filtro de conteúdo	Defang
websecurityadvancedconfig href e a regravação de texto está habilitada	Yes

Este último cenário valida a configuração.

- Política de e-mail com configuração AS/AV/AMP padrão e OF habilitado

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	URLTest	(use default)	(use default)	(use default)	(use default)	URL_SCORE	Retention Time: Virus: 1 day Other: 4 hours	(use default)	

- A verificação de OF para detecção de ameaças não virais é configurada com Reescrita de URL para reescrever todos os URLs contidos em e-mails mal-intencionados (o mesmo que nos cenários anteriores)
- Filtro de conteúdo de entrada: Filtro de conteúdo URL_SCORE habilitado

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_SCORE	URL_SCORE: if (url-reputation(-10.00, -6.00 , "", 0, 1)) { log-entry("$FilterName"); url-reputation-defang(-10.00, -6.00,"",0); }		

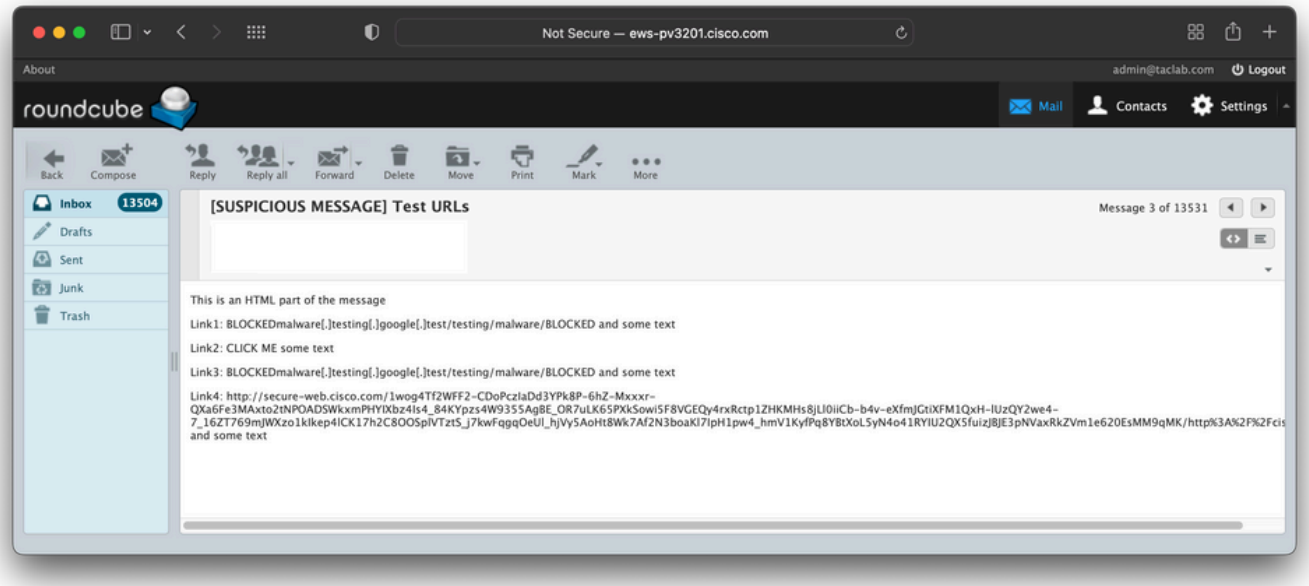
O filtro de conteúdo usa a condição de reputação de URL para corresponder URLs mal-intencionados, aqueles com pontuação entre -6,00 e -10,00. Como ação, o nome do filtro de conteúdo é registrado e a ação de desativação **url-reputation-defang** é tomada.

A mesma cópia da mensagem é enviada e avaliada pelo gateway de e-mail com os 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
```

O pipeline de e-mail explica que a mensagem é avaliada primeiro pelos filtros de conteúdo, onde o filtro URL_SCORE é acionado e a URL-reputation-defang-action é aplicada. Esta ação desativa todos os URLs mal-intencionados nas partes MIME text/plain e text/html. Como o websecurityadvanceconfig href e a regravação de texto estão habilitados, todas as cadeias de caracteres de URL que correspondem dentro do corpo HTML são desvinculadas quando todos os elementos de marca A são retirados e reescrevem partes de texto da URL entre palavras BLOQUEADAS e colocam todos os pontos entre colchetes. O mesmo acontece com outros URLs mal-intencionados não colocados em elementos HTML de marca A. Em seguida, o Filtro de Epidemia processa a mensagem. O OF detecta URLs mal-intencionados e identifica a mensagem como mal-intencionada (Nível de ameaça=5). Como resultado, ele regrava todos os URLs mal-intencionados e não-intencionados encontrados dentro da mensagem. Como a ação de filtro de conteúdo já modificou esses URLs, o OF regrava apenas o restante dos URLs não mal-intencionados, pois foi configurado intencionalmente para fazê-lo. A mensagem exibida no cliente de e-mail como parte das URLs mal-intencionadas removidas e parte da URL não mal-intencionada redirecionada.

```
--===============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==--
```



O mesmo se aplica à parte de texto/sem formatação da mensagem MIME. Todos os URLs não mal-intencionados são redirecionados para o proxy do Cisco Web Secure e os URLs mal-intencionados são desmarcados.

```
--===============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==
```

Soma:

- CF defang executado na parte TEXT/PLAIN regrava a URL em blocos BLOQUEADOS
- CF defang run na parte TEXT/HTML regrava o URL a partir de uma marca A HTML quando uma marca A é retirada
- O CF defang executado na parte TEXT/HTML regrava todas as strings de URL que correspondem aos blocos BLOQUEADOS
- OF redirect executado na parte TEXT/PLAIN regrava todas as strings de URL que correspondem ao serviço de proxy do Cisco Web Secure (não mal-intencionado)
- A execução do redirecionamento de OF na parte TEXT/HTML regrava o URL a partir de um atributo HTML A-tag href junto com a parte de texto do elemento e todas as outras strings de URL que correspondem ao serviço de proxy do Cisco Web Secure (não mal-intencionado)

Troubleshoot

Siga estes pontos quando houver necessidade de investigar o problema com a reescrita de URL.

- Ative o log de URL em seus mail_logs. Executar **OUTBREAKCONFIG** comando e resposta **Y** para **Do you wish to enable logging of URL's?** [N]>"
- Verificar **WEBSECURITYADVANCECONFIG** em cada membro do cluster do gateway de e-mail e certifique-se de que a opção href e a opção de regravação de texto estejam definidas de

acordo e sejam as mesmas em cada máquina. Lembre-se de que esse comando é específico no nível da máquina e as alterações feitas aqui não afetam as configurações de Grupo ou Cluster.
- Verifique as condições e atividades do filtro de conteúdo e certifique-se de que o filtro de conteúdo esteja habilitado e aplicado à política de recebimento de e-mail correta. Verifique se não há outro filtro de conteúdo processado antes com uma ação final que possa pular para processar outros filtros.
- Investigue a cópia bruta da origem e da mensagem final. Tenha em mente para recuperar a mensagem em formato EML, os formatos proprietários como MSG não são confiáveis quando se trata de investigação de mensagem. Alguns clientes de e-mail permitem exibir a mensagem de origem e tentam recuperar a cópia da mensagem com um cliente de e-mail diferente. Por exemplo, o MS Outlook para Mac permite exibir a Origem da mensagem, enquanto a versão do Windows permite que você exiba apenas os cabeçalhos.

Summary

A finalidade deste artigo é ajudar a compreender melhor as opções de configuração disponíveis quando se trata de reescrever URL. É importante lembrar que as mensagens modernas são criadas pela maioria dos softwares de e-mail com o padrão MIME. Isso significa que a mesma cópia da mensagem pode ser exibida de forma diferente, dependendo dos recursos do cliente de e-mail ou/e dos modos ativados (texto versus modo HTML). Por padrão, a maioria dos clientes de e-mail modernos usa HTML para exibir mensagens. Quando se trata de regravação de HTML e URL, tenha em mente que o gateway de e-mail padrão regrava somente URLs encontrados dentro do atributo href do elemento A-tag. Em muitos casos, isso não é suficiente e deve ser considerado para ativar a regravação de href e de texto com o comando WEBSECURITYADVANCECONFIG. Lembre-se de que este é um comando em nível de máquina e, para consistência em todo o cluster, a alteração deve ser aplicada separadamente a cada um dos membros do cluster.