Comprendere l'azione di disinnesto e reindirizzamento dell'URL su Secure Email Gateway

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Esempio di messaggio
Parte I - Disinnesto
Configurazioni
Azione di disinnesto
Scenario A
Scenario B
Parte II - Reindirizzamento
Configurazioni
Azione reindirizzamento
Scenario C
Scenario D
Parte 3 - del reindirizzamento
Configurazione
Scenario E
Scenario F
Scenario G
Risoluzione dei problemi
Riepilogo

Introduzione

In questo documento viene descritta la differenza tra le azioni di disinnesto e reindirizzamento utilizzate nel filtro URL e viene spiegato come utilizzare l'opzione di riscrittura disponibile per l'attributo href e il testo.

Prerequisiti

Requisiti

Per prendere decisioni in base alla reputazione dell'URL o per applicare le policy sull'utilizzo accettabile usando i filtri messaggi e contenuti, abilitare i filtri epidemie a livello globale.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Email Gateway
- Filtri epidemie
- Filtri contenuti e messaggi

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Una delle funzionalità del filtro URL è quella di basarsi sulla reputazione o la categoria dell'URL e usare i filtri messaggi e/o contenuti. In base al risultato dell'analisi dell'URL (condizione correlata all'URL), è possibile applicare una delle tre azioni disponibili a un URL:

- Disinnesca URL
- Reindirizza a Cisco Security Proxy
- Sostituisci URL con l'SMS

In questo documento viene illustrato il comportamento tra le opzioni Disinnesca e Reindirizza URL. Fornisce anche una breve descrizione e spiegazione delle funzionalità di riscrittura degli URL per il rilevamento non virale della minaccia di un filtro epidemie.

Esempio di messaggio

Il messaggio di esempio utilizzato in tutti i test è il tipo di messaggio MIME multipart/alternativo e include sia le parti text/plain che text/html. Tali parti vengono in genere generate automaticamente dal software di posta elettronica e contengono lo stesso tipo di contenuto formattato per i ricevitori HTML e non HTML. Per questo, il contenuto di text/plain e text/html è stato modificato 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
```

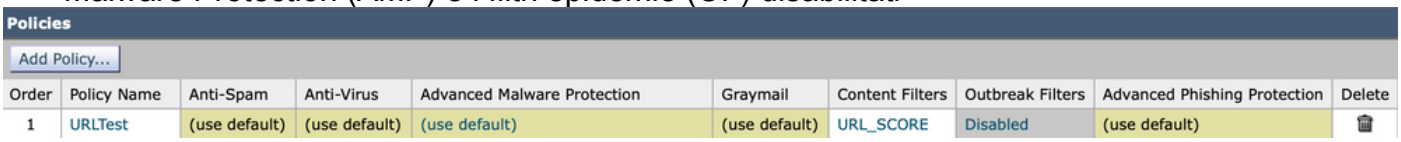
--==========778179357633004102 5==--

Parte I - Disinnesto

Configurazioni

Nella prima parte la configurazione utilizza:

- Criterio di posta con la configurazione predefinita Anti-Spam (AS)/ Anti-Virus (AV)/ Advanced Malware Protection (AMP) e i filtri epidemie (OF) disabilitati



- Filtro contenuti in arrivo: Filtro contenuto URL_SCORE abilitato

Il filtro dei contenuti utilizza la condizione di reputazione dell'URL per trovare la corrispondenza con URL dannosi, ovvero URL con punteggio compreso tra -6,00 e -10,00. Come azione, viene registrato il nome del filtro dei contenuti e l'azione di disinnesco **url-reputation-defang** viene eseguita.

Azione di disinnesto

Èimportante chiarire che cos'è un'azione di disinnesco. Il manuale per l'utente fornisce una spiegazione; Disattivare un URL in modo che non sia possibile selezionarlo. I destinatari del messaggio possono comunque visualizzare e copiare l'URL.

Scenario A

Rilevamento di minacce non virali tramite filtro epidemie	No
Operazione filtro contenuto	Disinnescare
websecurityadvancedconfig href e la riscrittura del testo è abilitata	No

In questo scenario viene illustrato il risultato dell'azione di disinnesco configurata con le impostazioni predefinite. Per impostazione predefinita, l'URL viene riscritto quando vengono eliminati solo i tag HTML. Osservare un paragrafo HTML contenente alcuni URL:

```
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
```

Nei primi due paragrafi l'URL è rappresentato da un tag HTML A appropriato. L'elemento <A> include **href=** che è racchiuso nel tag stesso e indica la destinazione del collegamento. Il contenuto

all'interno degli elementi tag può inoltre indicare la destinazione del collegamento. Questo **text form** del link può includere l'URL. Il primo Link1 include lo stesso collegamento URL sia nell'attributo href che nella parte di testo dell'elemento. Si noti che questi URL possono essere diversi. Il secondo Link2 include l'URL corretto solo all'interno dell'attributo href. L'ultimo paragrafo non include alcun elemento A.

> **Nota:** L'indirizzo corretto può sempre essere visualizzato quando si sposta il cursore sul collegamento o quando si visualizza il codice sorgente del messaggio. Purtroppo, il codice sorgente non può essere facilmente trovato con alcuni client di posta elettronica popolari.

Dopo aver individuato la corrispondenza tra il messaggio e il filtro URL_SCORE, gli URL dannosi vengono disinnescati. Quando la registrazione degli URL è abilitata con **OUTBREAKCONFIG** I punteggi e gli URL sono disponibili in 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'
```

Il risultato è il messaggio riscritto:

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

Il risultato dell'azione di disinnesto eseguita sulla parte di testo/html del messaggio MIME è un tag A rimosso e il contenuto del tag non viene modificato. Nei primi due paragrafi, entrambi i collegamenti sono stati disinnescati nel punto in cui il codice HTML è stato rimosso e la parte di testo dell'elemento è stata lasciata. L'indirizzo URL del primo paragrafo corrisponde a quello della parte di testo dell'elemento HTML. È necessario notare che l'indirizzo URL del primo paragrafo è ancora visibile dopo l'azione di disinnesco, ma senza i tag HTML A, l'elemento non deve essere selezionabile. Il terzo paragrafo non viene disinnescato in quanto l'indirizzo URL qui non viene posizionato tra i tag A e non viene considerato un collegamento. Forse non è un comportamento auspicabile per due motivi. In primo luogo, l'utente può facilmente vedere e copiare il collegamento ed eseguirlo nel browser. Il secondo motivo è che alcuni software di posta elettronica tendono a rilevare una forma valida di URL all'interno del testo e a renderlo un collegamento selezionabile.

Esaminiamo la parte di testo del messaggio MIME. La parte di testo normale include due URL nel

modulo di testo. Il testo normale viene visualizzato da MUA che non riconosce il codice HTML. Nella maggior parte dei client di posta elettronica moderni non è possibile visualizzare il testo o le parti normali del messaggio a meno che non sia stato intenzionalmente configurato il client di posta elettronica per farlo. In genere, è necessario controllare il codice sorgente del messaggio, un formato EML non elaborato del messaggio per vedere e analizzare le parti MIME.

Nell'elenco che segue sono riportati gli URL della parte di testo normale del messaggio di origine.

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

Uno di questi due link ha ricevuto un punteggio dannoso ed è stato disinnescato. Per impostazione predefinita, l'azione di disinnesto eseguita sulla parte di testo normale del tipo MIME ha un risultato diverso rispetto alla parte di testo o html. Si trova tra parole BLOCCATE e tutti i punti tra parentesi quadre.

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

Somma:

- L'esecuzione della deframmentazione sulla parte TEXT/PLAIN riscrive l'URL in blocchi BLOCCATI
- L'opzione Defang eseguita sulla parte TEXT/HTML riscrive l'URL da un tag A HTML quando il tag A viene rimosso senza che il testo tra i tag A venga toccato, che può anche essere un indirizzo URL

Scenario B

Rilevamento di minacce non virali tramite filtro epidemie	No
Operazione filtro contenuto	Disinnescare
websecurityadvancedconfig href e la riscrittura del testo è abilitata	Sì

In questo scenario vengono fornite informazioni sulle modifiche del comportamento dell'azione di disinnesco dopo l'utilizzo di una delle opzioni websecurityadvancedconfig. websecurityadvancedconfig è il comando CLI specifico del computer che consente di regolare le impostazioni specifiche per la scansione degli URL. Una delle impostazioni qui riportate consente di modificare il comportamento predefinito dell'azione di disinnesto.

```
> 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
...
```

Alla quarta questione, **Do you want to rewrite both the URL text and the href in the message? ..**, la risposta **Y** indica che, nel caso della parte MIME basata su HTML del messaggio, tutte le stringhe URL che

corrispondono indipendentemente dal fatto che vengano trovate nell'attributo href dell'elemento A-tag sono parti di testo o elementi esterni a quelli riscritti. In questo scenario lo stesso messaggio è presente, ma con un risultato leggermente diverso.

Osservare di nuovo il codice MIME text/html con gli URL e confrontarlo con il codice HTML elaborato dal gateway di posta elettronica.

```
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 l'opzione href e la riscrittura del testo sono abilitate, tutte le corrispondenze con gli URL del filtro vengono disinnescate, indipendentemente dal fatto che l'indirizzo URL faccia parte dell'attributo href o della parte di testo dell'elemento HTML A-tag, o che venga trovato in un'altra 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==--
```

Gli URL disinnescati vengono ora riscritti quando l'elemento A-tag viene rimosso insieme a una riscrittura della parte di testo del link quando corrisponde al formato dell'URL. La parte di testo riscritta viene eseguita nello stesso modo della parte di testo normale del messaggio MIME. L'elemento viene inserito tra le parole BLOCCATO e tutti i punti vengono inseriti tra parentesi quadre. In questo modo si impedisce all'utente di copiare e incollare l'URL e alcuni client di posta elettronica consentono di fare clic sul testo.

Somma:

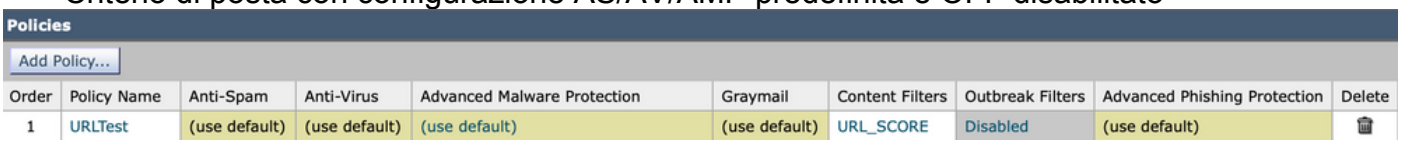
- L'esecuzione della deframmentazione sulla parte TEXT/PLAIN riscrive l'URL in blocchi BLOCCATI
- L'opzione Defang eseguita sulla parte TEXT/HTML riscrive l'URL da un tag A HTML quando un tag A viene eliminato
- L'esecuzione del comando Defang sulla parte TEXT/HTML riscrive tutte le stringhe URL che corrispondono ai blocchi BLOCCATI

Parte II - Reindirizzamento

Configurazioni

Nella seconda parte la configurazione utilizza:

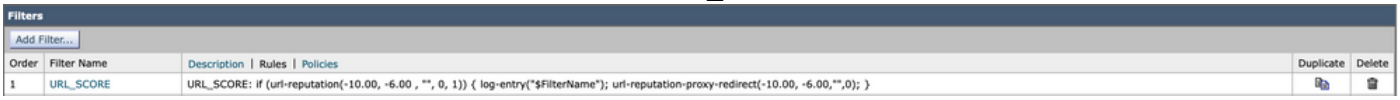
- Criterio di posta con configurazione AS/AV/AMP predefinita e OFF disabilitato


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	Disabled	(use default)	

- Filtro contenuti in arrivo: Filtro contenuto URL_SCORE abilitato


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-proxy-redirect(-10.00, -6.00,"",0); }		

Il filtro dei contenuti utilizza la condizione di reputazione dell'URL per trovare la corrispondenza con URL dannosi, ovvero URL con punteggio compreso tra -6,00 e -10,00. Come azione, viene registrato il nome del filtro dei contenuti e **redirect action** viene eseguita.

Azione reindirizzamento

Il reindirizzamento al servizio proxy di sicurezza Cisco per una valutazione in tempo reale consente al destinatario del messaggio di fare clic sul collegamento e di essere reindirizzato a un proxy di sicurezza Web Cisco nel cloud, che blocca l'accesso se il sito è identificato come dannoso.

Scenario C

Rilevamento di minacce non virali tramite filtro epidemie	No
Operazione filtro contenuto	Reindirizzamento
websecurityadvancedconfig href e la riscrittura del testo è abilitata	No

Questo scenario ha un comportamento molto simile a quello dello scenario A a partire dalla prima parte, con la differenza nell'operazione filtro dei contenuti che consiste nel reindirizzare l'URL anziché disinnescarlo. Le impostazioni di websecurityadvancedconfig vengono ripristinate ai valori predefiniti, ovvero **"Do you want to rewrite both the URL text and the href in the message? ..** è impostato su **N**.

Il gateway di posta elettronica rileva e valuta ogni URL. Il punteggio dannoso attiva la regola di filtro del contenuto URL_SCORE e interviene **url-reputation-proxy-redirect-action**

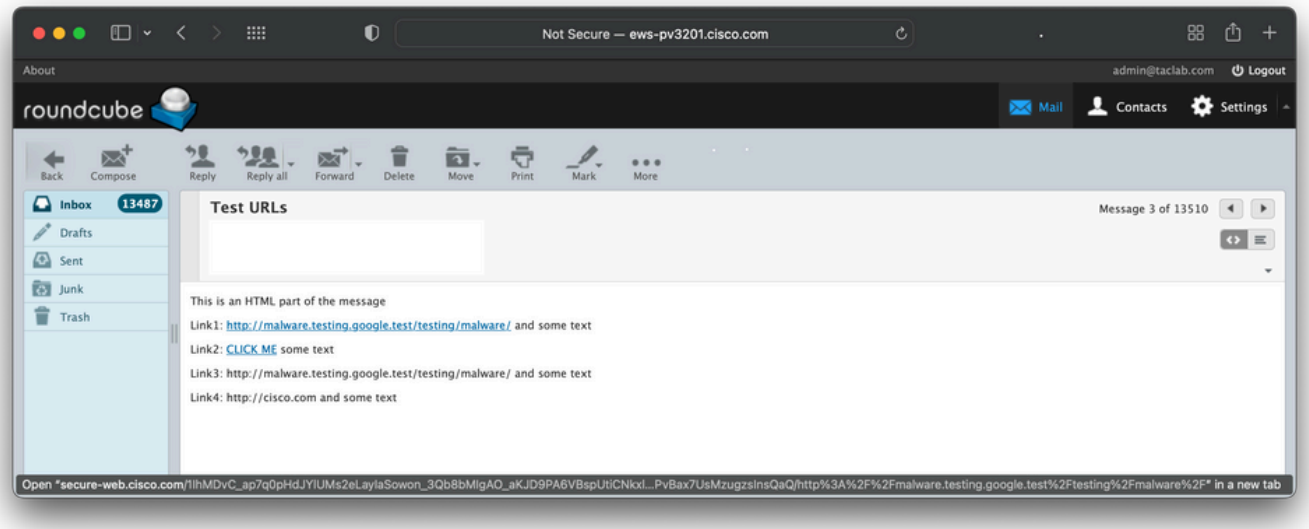
```
Tue Jul 5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/
has reputation -9.4 matched Condition: URL Reputation Rule Tue Jul 5 12:42:19 2022 Info: MID
139508 Custom Log Entry: URL_SCORE Tue Jul 5 12:42:19 2022 Info: MID 139508 URL
http://malware.testing.google.test/testing/malware/ 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'
```

Osservare come gli URL vengono riscritti nella parte HTML del messaggio. Come nello scenario A, vengono riscritti solo gli URL trovati nell'attributo href di un elemento A-tag e gli indirizzi URL trovati nella parte testo dell'elemento A-tag vengono ignorati. Con un'azione di disinnesco un

intero elemento A-tag viene eliminato, ma con un'azione di reindirizzamento l'URL nell'attributo href viene riscritto.

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

Di conseguenza, il client di posta elettronica visualizza due collegamenti attivi: Link1 e Link2, entrambi puntano al servizio proxy Cisco Web Security, ma il messaggio visualizzato nel client e-mail mostra la parte di testo del tag A che non viene riscritta per impostazione predefinita. Per una migliore comprensione di questo, dare un'occhiata all'output dal client webmail che visualizza la parte testo / html del messaggio.



Nella parte di testo normale della parte MIME, il reindirizzamento risulta più comprensibile in quanto ogni stringa URL che corrisponde al punteggio viene riscritta.

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

Somma:

- L'esecuzione del reindirizzamento sulla parte TEXT/PLAIN riscrive la stringa dell'URL che corrisponde al servizio proxy Cisco Web Secure

- Il reindirizzamento viene eseguito sulla parte TEXT/HTML e riscrive l'URL da un attributo HTML A-tag href con il servizio proxy Cisco Web Secure, ma lascia invariate tutte le altre stringhe URL corrispondenti

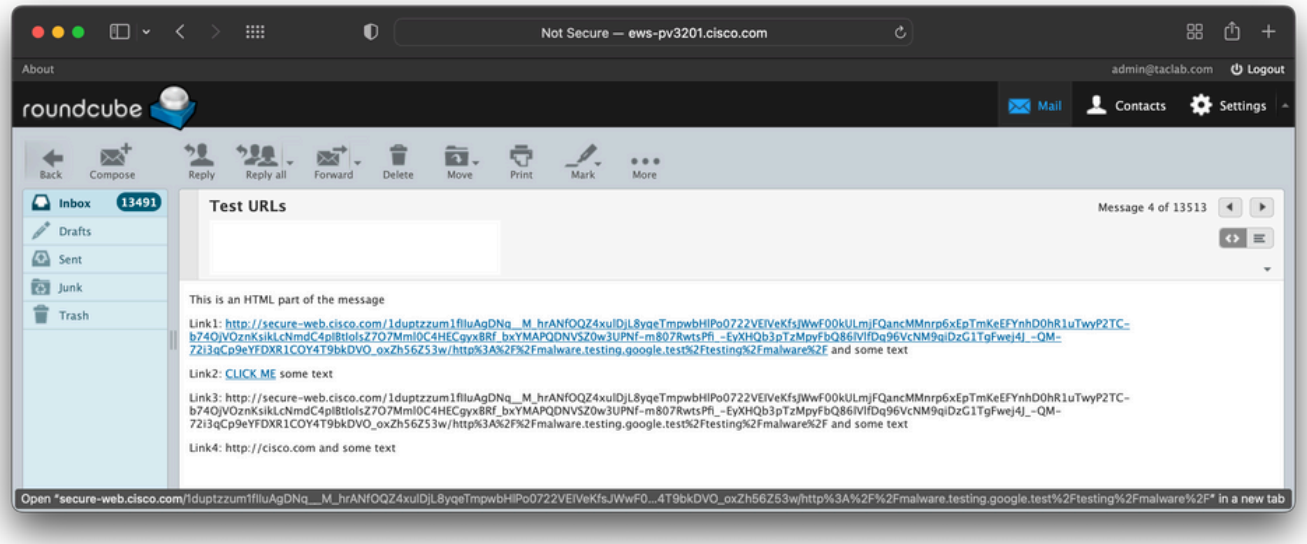
Scenario D

Rilevamento di minacce non virali tramite filtro epidemie	No
Operazione filtro contenuto	Reindirizzamento
websecurityadvancedconfig href e la riscrittura del testo è abilitata	Sì

Questo scenario è simile allo scenario B della prima parte. Per riscrivere tutte le stringhe URL corrispondenti nella parte HTML del messaggio è abilitato. Questa operazione viene eseguita con il comando websecurityadvancedconfig quando si risponde Y per **"Do you want to rewrite both the URL text and the href in the message? ..** domanda.

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

Dopo aver abilitato la riscrittura del testo e della href, tutte le stringhe URL che soddisfano le condizioni del filtro dei contenuti vengono reindirizzate. Il messaggio nel client di posta elettronica viene ora presentato con tutto il reindirizzamento. Per comprendere meglio questa funzionalità, esaminare l'output del client webmail che visualizza la parte text/html del messaggio.



La parte di testo normale del messaggio MIME è la stessa dello scenario C in cui la modifica websecurityadvancedconfig non ha alcun impatto sulle parti di testo normale del messaggio.

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

Somma:

- L'esecuzione del reindirizzamento sulla parte TEXT/PLAIN riscrive le stringhe dell'URL che corrispondono al servizio proxy Cisco Web Secure
- Il reindirizzamento eseguito sulla parte TEXT/HTML riscrive l'URL da un attributo HTML A-tag href insieme alla parte text e a qualsiasi altra stringa URL che corrisponde nel corpo HTML al servizio proxy Cisco Web Secure

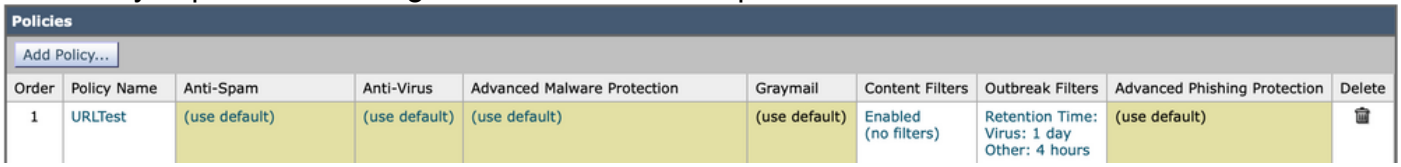
Parte 3 - del reindirizzamento

Questa parte fornisce informazioni su come le impostazioni di sicurezza per le scansioni URL non virali di rilevamento minacce.

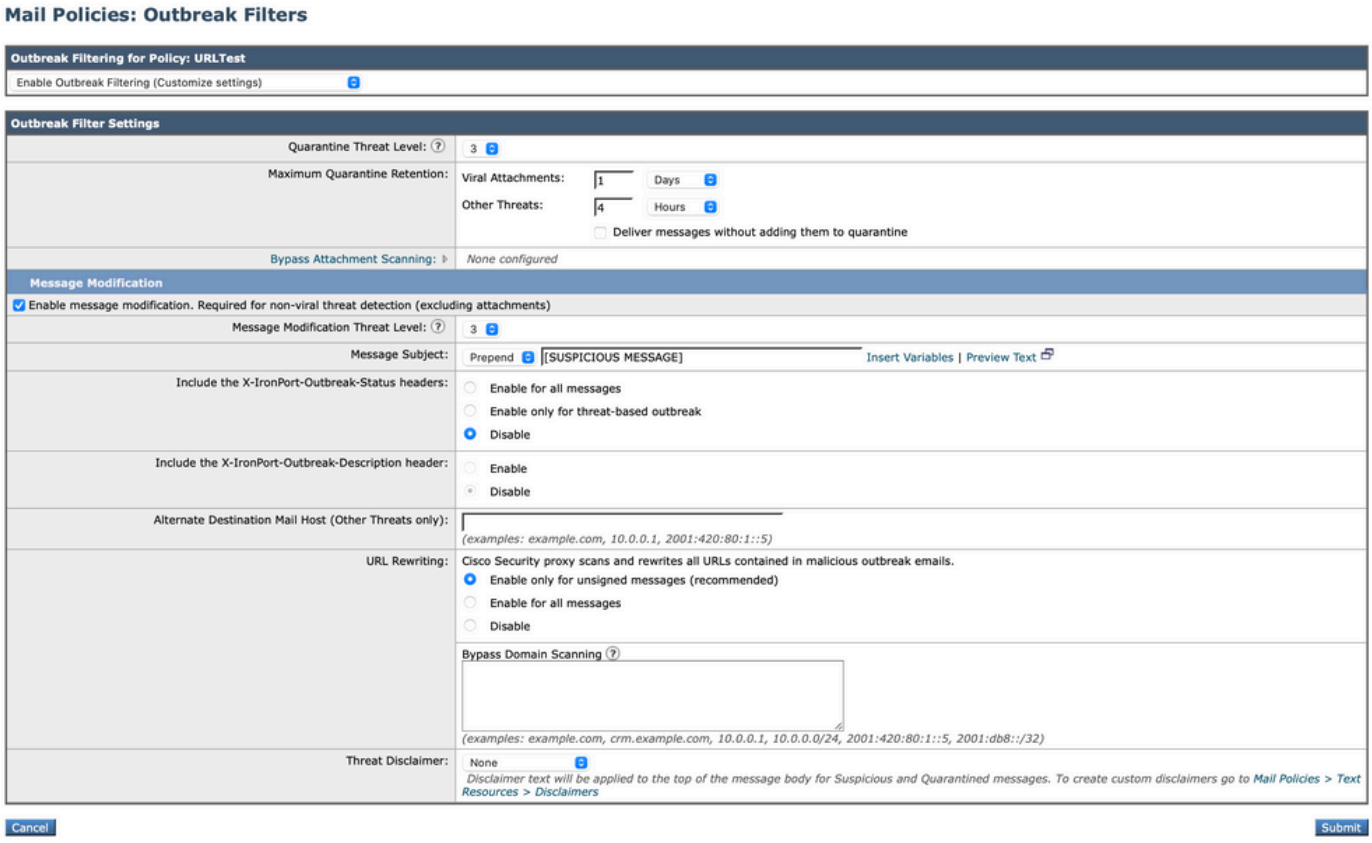
Configurazione

A questo scopo, il filtro contenuti utilizzato nelle prime due parti è disattivato.

- Policy di posta con configurazione AS/AV/AMP predefinita e OFF abilitata



- L'analisi dei filtri epidemie per il rilevamento di minacce non virali è configurata con un set di riscrittura degli URL per riscrivere tutti gli URL contenuti in messaggi di posta elettronica dannosi



Quando il messaggio viene classificato da OF come Dannoso, tutti gli URL in esso contenuti vengono riscritti con il servizio proxy Cisco Web Secure.

Scenario E

Rilevamento di minacce non virali tramite filtro epidemie	Sì
Operazione filtro contenuto	No
websecurityadvancedconfig href e la riscrittura del testo è abilitata	No

In questo scenario viene mostrato come la riscrittura del messaggio funziona solo con OF abilitato e websecurityadvancedconfig href e la riscrittura del testo disabilitata.

```
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)
```

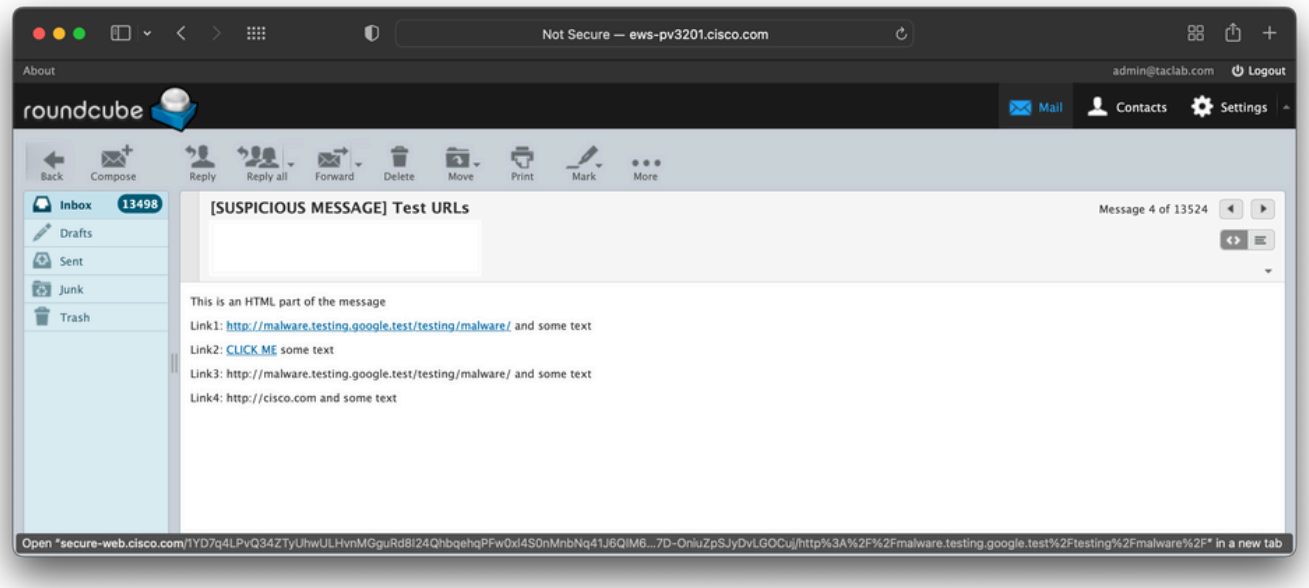
Iniziamo con la parte MIME di testo. Dopo un rapido controllo, si può notare che tutti gli URL all'interno della parte di testo o normale vengono riscritti sui servizi proxy Cisco Web Secure. Il

problema si verifica perché la riscrittura degli URL è abilitata per tutti gli URL inclusi nel messaggio dannoso dell'epidemia.

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

Parte text/html elaborata del messaggio 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==--
```



Il primo che si può notare qui è perché Link4 non viene riscritto. Se leggete l'articolo con attenzione sapete già la risposta. Per impostazione predefinita, la parte text/html di MIME valuta e modifica solo gli attributi href degli elementi tag A. Se si desidera un comportamento simile a quello di una parte di testo normale, è necessario attivare websecurityadvancedconfig href e la riscrittura del testo. Lo scenario successivo fa esattamente questo.Somma:

- Il reindirizzamento OF viene eseguito sulla parte TEXT/PLAIN e riscrive tutte le stringhe

dell'URL che corrispondono al servizio proxy Cisco Web Secure
- del reindirizzamento eseguito sulla parte TEXT/HTML riscrive solo l'URL da un attributo HTML A-tag href con il servizio proxy Cisco Web Secure

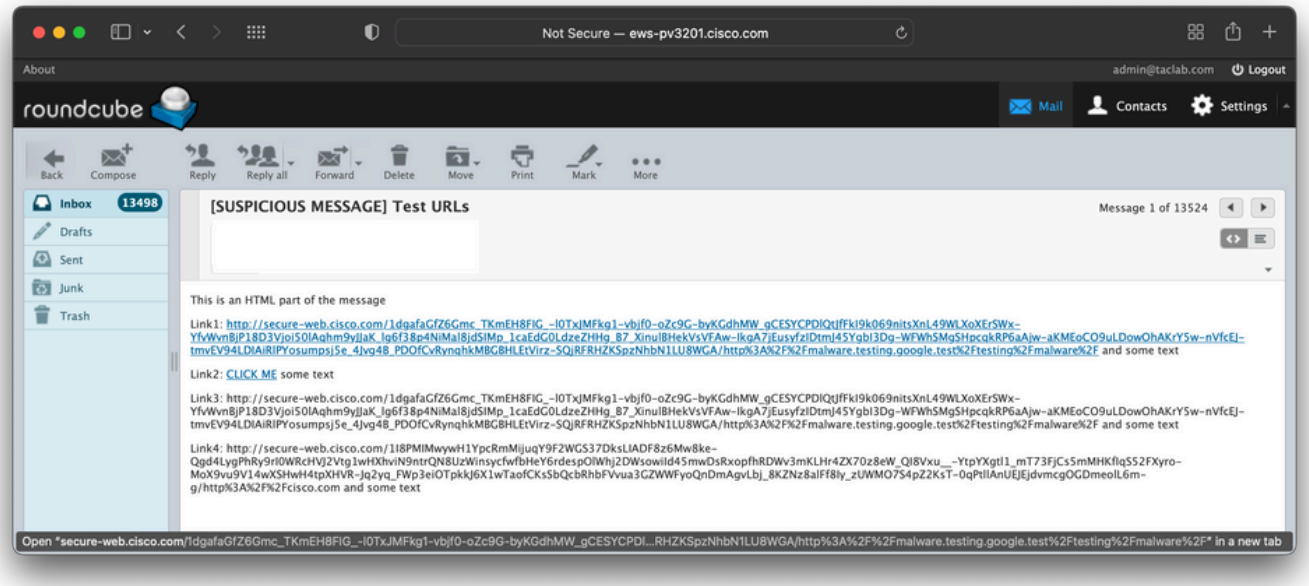
Scenario F

Rilevamento di minacce non virali tramite filtro epidemie	Sì
Operazione filtro contenuto	No
websecurityadvancedconfig href e la riscrittura del testo è abilitata	Sì

In questo scenario vengono abilitati la funzione websecurityadvancedconfig href e la funzione di riscrittura del testo per mostrare come cambia il comportamento della funzione di riscrittura dell'URL fornita dal rilevamento di minacce non virali. In questo momento è necessario tenere presente che websecurityadvancedconfig non influisce sulle parti MIME di testo o semplici. Valutiamo solo la parte text/html e vediamo come il comportamento è cambiato.

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

Si noti che l'output è molto simile a quello dello scenario D, con l'unica differenza che tutti gli URL sono stati riscritti, non solo quelli dannosi. In questa sezione vengono modificate tutte le stringhe URL corrispondenti nella parte HTML e quelle non dannose.



Somma:

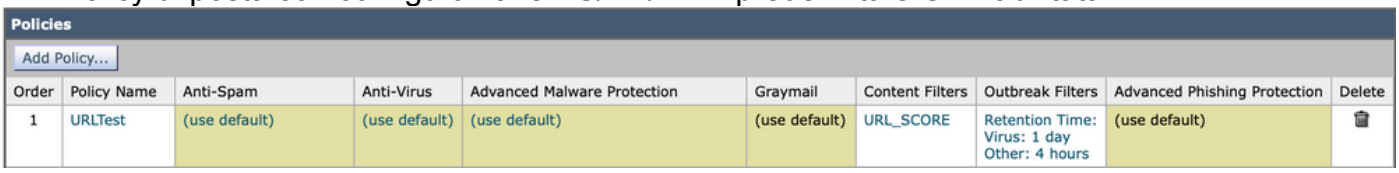
- Il reindirizzamento OF viene eseguito sulla parte TEXT/PLAIN e riscrive tutte le stringhe URL che corrispondono al servizio proxy Cisco Web Secure
- Il reindirizzamento OF viene eseguito sulla parte TEXT/HTML e riscrive l'URL da un attributo HTML A-tag href insieme alla parte text dell'elemento e a tutte le altre stringhe URL corrispondenti al servizio proxy Cisco Web Secure

Scenario G

Rilevamento di minacce non virali tramite filtro epidemie	Sì
Operazione filtro contenuto	Disinnescare
websecurityadvancedconfig href e la riscrittura del testo è abilitata	Sì

Questo ultimo scenario convalida la configurazione.

- Policy di posta con configurazione AS/AV/AMP predefinita e OFF abilitata



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)	

- L'analisi OF per il rilevamento di minacce non virali è configurata con l'opzione URL Rewrite (Riscrittura URL) impostata su rewrite (Riscrittura URL) per riscrivere tutti gli URL contenuti in messaggi di posta elettronica dannosi (come negli scenari precedenti)
- Filtro contenuti in arrivo: Filtro contenuto URL_SCORE abilitato

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); }		

Il filtro dei contenuti utilizza la condizione di reputazione dell'URL per trovare la corrispondenza con URL dannosi, ovvero URL con punteggio compreso tra -6,00 e -10,00. Come azione, viene

registrato il nome del filtro dei contenuti e l'azione di disinnesco **url-reputation-defang** viene eseguita.

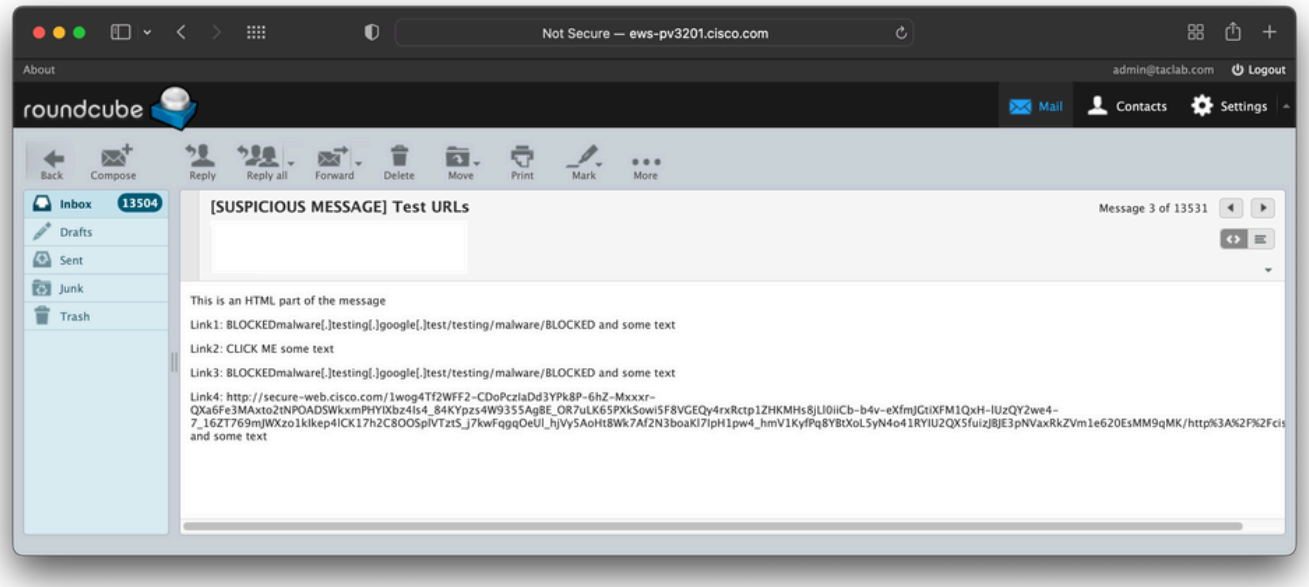
La stessa copia del messaggio viene inviata e valutata dal gateway di posta elettronica con i risultati seguenti:

```
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 pipeline di posta elettronica spiega che il messaggio viene valutato prima dai filtri contenuti, dove viene attivato il filtro URL_SCORE e applicato l'URL-reputation-defang-action. Questa azione disinnesca tutti gli URL dannosi nelle parti MIME text/plain e text/html. Poiché la funzione websecurityadvanceconfig href e la riscrittura del testo sono attivate, tutte le stringhe URL che corrispondono al corpo HTML vengono disinnescate quando tutti gli elementi del tag A vengono eliminati e le parti di testo dell'URL vengono riscritte tra parole BLOCCATE e tutti i punti vengono posizionati tra parentesi quadre. Lo stesso accade con altri URL dannosi non inseriti negli elementi HTML A-tag. Il filtro epidemie elabora quindi il messaggio. La funzione OF rileva gli URL dannosi e identifica il messaggio come dannoso (livello di minaccia=5). Di conseguenza, vengono riscritti tutti gli URL dannosi e non dannosi trovati all'interno del messaggio. Poiché l'operazione filtro contenuti ha già modificato questi URL, il modulo OF riscrive solo gli URL non dannosi rimanendo intenzionalmente configurati per farlo. Il messaggio visualizzato nel client di posta elettronica come parte degli URL dannosi disinnescati e parte dell'URL non dannoso reindirizzato.

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



La stessa regola viene applicata alla parte di testo normale del messaggio MIME. Tutti gli URL non dannosi vengono reindirizzati al proxy Cisco Web Secure e gli URL dannosi vengono disinnescati.

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

Somma:

- L'esecuzione della disattivazione della CF sulla parte TEXT/PLAIN riscrive l'URL in blocchi BLOCCATI
- La disinnesto CF viene eseguito sulla parte TEXT/HTML e riscrive l'URL da un tag A HTML quando un tag A viene eliminato
- La disinnesto CF viene eseguito sulla parte TEXT/HTML e riscrive tutte le stringhe URL corrispondenti in blocchi BLOCCATI
- Esecuzione del reindirizzamento OF sulla parte TEXT/PLAIN che riscrive tutte le stringhe URL che corrispondono al servizio proxy Cisco Web Secure (non dannoso)
- Il reindirizzamento OF viene eseguito sulla parte TEXT/HTML e riscrive l'URL da un attributo HTML A-tag href insieme alla parte text dell'elemento e a tutte le altre stringhe URL corrispondenti al servizio proxy Cisco Web Secure (non dannoso)

Risoluzione dei problemi

Attenersi a questa procedura quando è necessario esaminare il problema con la riscrittura degli URL.

- Abilitare la registrazione degli URL nei log di posta. Lanciare **OUTBREAKCONFIG** comando e

risposta **Y** a **Do you wish to enable logging of URL's?** [N]**>"**

- Verifica **WEBSECURITYADVANCECONFIG** in ogni membro del cluster gateway di posta elettronica e assicurarsi che l'opzione di riscrittura href e text sia impostata di conseguenza e che sia la stessa in ogni computer. Tenere presente che questo comando è specifico del computer e che le modifiche apportate non influiscono sulle impostazioni del gruppo o del cluster.
- Verificare le condizioni e le attività del filtro contenuti e assicurarsi che il filtro contenuti sia abilitato e applicato al criterio di posta in arrivo corretto. Verificare se non vi sono altri filtri dei contenuti elaborati in precedenza con un'azione finale che può saltare per elaborare altri filtri.
- Esaminare la copia non elaborata del messaggio di origine e finale. Ricordarsi di recuperare il messaggio in formato EML, i formati proprietari come MSG non sono affidabili quando si tratta di indagine del messaggio. Alcuni client di posta elettronica consentono di visualizzare il messaggio di origine e tentare di recuperare la copia del messaggio con un client di posta elettronica diverso. Ad esempio, MS Outlook per Mac consente di visualizzare l'origine del messaggio mentre la versione di Windows consente solo di visualizzare le intestazioni.

Riepilogo

Lo scopo di questo articolo è quello di aiutare a comprendere meglio le opzioni di configurazione disponibili quando si tratta di riscrittura degli URL. È importante ricordare che i messaggi moderni sono costruiti dalla maggior parte dei software di posta elettronica con lo standard MIME. Significa che la stessa copia del messaggio può essere visualizzata in modo diverso, a seconda delle capacità del client di posta elettronica o/e modalità abilitate (modalità testo o HTML). Per impostazione predefinita, la maggior parte dei client di posta elettronica moderni utilizza il codice HTML per visualizzare i messaggi. Quando si tratta di riscrittura HTML e URL, tenere presente che per impostazione predefinita il gateway e-mail riscrive solo gli URL trovati nell'attributo href dell'elemento A-tag. In molti casi questo non è sufficiente e deve essere considerato per abilitare sia href che text rewrite con il comando WEBSECURITYADVANCECONFIG. Tenere presente che si tratta di un comando a livello di computer e per garantire la coerenza all'interno del cluster, è necessario applicare la modifica separatamente a ogni membro del cluster.