فهم إجراء إلغاء توجيه URL وإعادة توجيهه على بوابة البريد الإلكتروني الآمنة

المحتويات

المقدمة

يصف هذا وثيقة الفرق بين إلغاء الربط وعمليات إعادة التوجيه المستخدمة في مرشح عنوان الربط، وكيفية إستخدام خيار إعادة الكتابة المتاح للسمة href والنص.

المتطلبات الأساسية

المتطلبات

لاتخاذ إجراء استنادا إلى سمعة عنوان URL، أو لفرض سياسات إستخدام مقبولة باستخدام

عوامل تصفية الرسائل والمحتوى، يجب تمكين ميزة "عوامل تصفية التفشي" بشكل عام.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- بوابة البريد الإلكتروني الآمنة من Cisco
- عوامل تصفية التفشي
- عوامل تصفية المحتوى والرسائل

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

إحدى قدرات ميزة تصفية URL هي إتخاذ إجراء بناء على سمعة أو فئة URL باستخدام عوامل تصفية الرسائل و/أو المحتوى. استنادا إلى نتيجة فحص عنوان URL (الشرط المرتبط بعنوان URL)، يمكن تطبيق أحد الإجراءات الثلاثة المتاحة على عنوان URL:

- إزالة الخطر من عنوان URL
- إعادة التوجيه إلى Cisco Security Proxy
- إستبدال URL برسالة نصية

التركيز في هذا المستند هو شرح السلوك بين خيارات عنوان URL إعادة التوجيه و Defang. كما يقدم وصفا موجزا وتوضيحا لقدرات إعادة كتابة عنوان URL لاكتشاف التهديد غير الفيروسي لعامل تصفية التفشي.

نموذج الرسالة

الرسالة النموذجية المستخدمة في جميع الاختبارات هي نوع الرسالة MIME متعدد الأجزاء/البديل وتتضمن كل من أجزاء النص/السهل والنص/html. عادة ما يتم إنشاء هذه الأجزاء تلقائيا بواسطة برنامج البريد الإلكتروني وتحتوي على نفس نوع المحتوى المنسق لمستقبلات HTML وغير HTML. ولهذا الغرض، تم تحرير محتوى النص/السهل والنص/html يدويا.

```
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==--
```

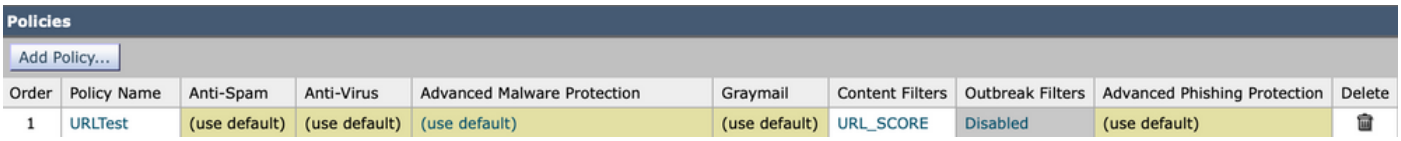
الجزء الأول - ديفانغ

التكوينات

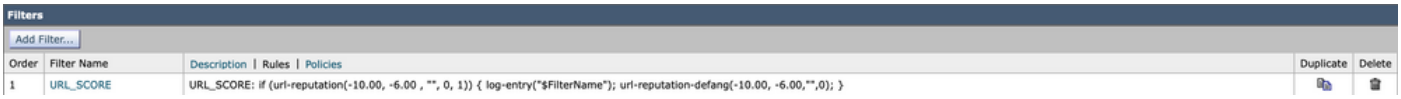
في الجزء الأول، يستخدم التكوين:

- نهج البريد مع تعطيل إعداد برامج مكافحة البريد العشوائي الافتراضية (AS)/ مكافحة الفيروسات (AV)/ الحماية المتقدمة من البرامج الضارة (AMP) وعوامل تصفية

التفشي (OF)



- عامل تصفية المحتوى الوارد: تم تمكين عامل تصفية محتوى URL_SCORE



يستخدم عامل تصفية المحتوى حالة سمعة عنوان URL لمطابقة عناوين URL الضارة، تلك التي تشير إلى ما بين -10.00 و -6.00. كإجراء، يتم تسجيل اسم عامل تصفية المحتوى ويتم إتخاذ إجراء إلغاء url-reputation-defang الارتباط.

عملية الدفاع

ومن الأهمية بمكان أن نوضح ما هو العمل الدفاعي. يقدم دليل المستخدم تفسيرا؛ قم بإلغاء تحديد عنوان URL بحيث لا يمكن النقر فوقه. لا يزال بإمكان مستلمي الرسائل رؤية عنوان URL ونسخه.

السيناريو أ

الكشف عن التهديد غير الفيروسي بمرشح التفشي	لا
إجراء مرشح المحتوى	دي فانغ
أمان الويب تم تمكين AdvancedConfig href وإعادة كتابة النص	لا

يشرح هذا السيناريو نتيجة إجراء إلغاء الارتباط الذي تم تكوينه بالإعدادات الافتراضية. في الإعداد الافتراضي، تتم إعادة كتابة عنوان URL عندما يتم جرد علامات HTML فقط. ألق نظرة على فقرة HTML تحتوي على بعض عناوين URL بداخلها:

```
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
```

في الفقرتين الأوليين، يتم تمثيل عنوان URL بعلامة تمييز HTML A مناسبة.
يتضمن العنصر <a> السمة **href=** المرفقة في العلامة نفسها ويشير إلى وجهة الارتباط.
اذه نتضمن أن يشير المحتوى ضمن عناصر علامة التمييز إلى وجهة الارتباط. يمكن أن
text form الارتباط عنوان URL. يتضمن الارتباط الأول 1 لإرتباط عنوان URL في كل من
سمة href وجزء النص من العنصر. يمكن ملاحظة أن عنوانين URL تلك يمكن أن تكون
مختلفة. يتضمن الارتباط الثاني عنوان URL المناسب فقط داخل سمة href. الفقرة
الأخيرة ال تتضمن أي عناصر A.

ملاحظة: ويمكن دائما ملاحظة العنوان الصحيح عندما تقوم بتحريك المؤشر فوق الارتباط أو عندما تقوم بعرض التعليمات البرمجية للمصدر الخاصة بالرسالة. لسوء الحظ، ال يمكن العثور على التعليمات البرمجية المصدر بسهولة مع بعض عملاء البريد الإلكتروني المشهورين.

بمجرد مطابقة الرسالة بعامل تصفية URL_SCORE، يتم إلغاء تحديد عناوين URL الضارة.
رمز **OUTBREAKCONFIG** باستخدام الأمر عند تمكين تسجيل عنوان URL يمكن العثور على العلامات
وعناوين URL في mail_log.

```
Mon Jul  4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has
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
Mon Jul  4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has
Mon Jul  4 14:46:43 2022 Info: MID 139502 URL http://malware.testing.google.test/testing/malware/ has
Mon Jul  4 14:46:43 2022 Info: MID 139502 rewritten to MID 139503 by url-reputation-defang-action filt
```

وينتج عن ذلك رسالة تمت إعادة كتابتها:

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

ةدرجم زييمت ةمالع يه MIME ةلاسر نم html/صنلا ءزج ىلع مت يذلا طبرلا ءاغلإ ءارجإ ةجيتن الك طبر ءاغلإ مت ،نييلوألا نيترقفلا يف .سمل نودب كرت زييمتلا ةمالع ىوتحمو ةرقفلا يف URL ناونع .رصنعلا نم صنلا ءزج كرتو HTML ةرفش درج مت ثيح نيطبرلا ةرقفلا نم URL ناونع نأ ةظحالم بجي .HTML رصنعب صاخلا صنلا ءزج نم ناونع وه ىلوألا نوكي الأ بجي ،HTML A تامالع نودب نكلو طابترالا ءاغلإ ءارجإ ذاختإ دعب ايئرم لازي ال ىلوألا متي ال انه URL ناونع نأ ثيح ةثلاثلا ةرقفلا ةئزجت ءاغلإ متي ال .رقنلل لباق رصنعلا هيف ابوغرم الكولس نوكي ال دق .طابترإ هرابتعا متي الو ،A زييمت تامالع يأ نيب هعضو يف هذيفنتو هخسنو طابترالا ةيؤر ةلوهسب مدختسملل نكمي ،الوأ .نيببسل فاشتكا ىلإ ليمت ينورتكلإلا ديربلا جمارب ضعب نأ وه يناثلا ببسلاو .ضرعتسملا لكش نم حيحص نيوانع URL لخاد صنلا هلعجو اطبار لباقلا رقنلل.

فلنلق ةرظن ىلع صنلا/ءزجلا طيسبلا نم ةلاسر MIME. يداعلا ءزجلا/صنلا نمضتي ينوانع URL يف جذومن صنلا .صنلا ضرع متي صنلا/لهسلا ةطساوب MUA يذلا ال مهفي تاميلعت HTML ةيجمربلا .يف مظعم ءالمع ديربلا ينورتكلإلا نيثيدحلا، ىرت ال ادمع كب صاخلا ينورتكلإلا ديربلا ليمع نيوكتب مقت مل ام ةلاسرلل ةيداعلا ءازجألا/صنلا يلوأ EML قيسنت وهو ،ةلاسرلل ردصملا زمرلا نم ققحتلا ىلإ جاتحت ،ةداع .كلذب مايقلل ةلاسرلل ةيؤرل ءازجأ MIME ققحتلاو اهنم.

رهظي جاردإلا انه URLs نم صنلا/ءزج يداع نم ةلاسرلا ردصملا.

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

ىدحاو هذه طباورلا حصلت ىلع ةجيتن ةثيبخ متو عزن اهليعفت .لكشب يضارتفا ،نوكي نع ةفلتخم ةجيتن MIME عون نم يداعلا ءزجلا/صنلا ىلع هذاختإ مت يذلا طبرلا ءاغلإ ءارجإل كلت يتلا يف ءزج صنلا/HTML. يقب عقي نيب تاملكلا ةروظحملا لكو طاقنلا نيب ساوقأ ةعبرم.

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

التلخيص:

- إلغاء التشغيل على "النص"/"الجزء العادي" يعيد كتابة URL إلى كتل محظورة
- إلغاء التشغيل على جزء TEXT/HTML يعيد كتابة عنوان URL من علامة تمييز HTML A إلى علامة تمييز A بدون النص الموجود بين علامات تمييز متالمس، والذي عندما تكون علامة تمييز A يمكن أن يكون عنوان URL أيضا

السيناريو ب

الكشف عن التهديد غير الفيروسي بمرشح التفشي	ال
إجراء مرشح المحتوى	ديفانغ
أمان الويب تم تمكين AdvancedConfig href وإعادة كتابة النص	نعم

يوفر هذه السيناريو معلومات حول كيفية تغيير سلوك إجراء إلغاء التجزئة بعد إستخدام أحد خيارات webSecurityAdvancedConfig. WebSecurityAdvancedConfig هو أمر CLI الخاص بمستوى الجهاز الذي يسمح بضبط الإعدادات الخاصة بمسح URL. يسمح لك أحد الإعدادات هنا بتغيير السلوك الافتراضي لإجراء التعطيل.

```
> 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 rewritt

...
```

في السؤال الرابع، **Do you want to rewrite both the URL text and the href in the message?** ..تشير الإجابة Y إلى أنه في حالة جزء MIME المستند إلى HTML من الرسالة، فإن كل سلاسل عنوان URL التي تطابق أيا كانت الحالة التي تم العثور عليها في سمة href لعنصر A-tag، تكون جزء نص أو خارج أي عناصر تمت إعادة كتابتها. وفي هذا السيناريو تكون الرسالة ذاتها مستاءة، ولكن بنتائج مختلفة قليلا.

ألق نظرة على كود جزء MIME/text HTML باستخدام عناوين URL مرة أخرى وقارنه برمز HTML الذي تمت معالجته بواسطة بوابة البريد الإلكتروني.

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

عندما يتم تمكين خيار href و إعادة كتابة النص، فإن كل ما يطابقه هو عناوين URL للتصفية يتم إلغائها سواء كان عنوان URL جزءا من سمة href أو جزء نص عنصر HTML لعلامة تمييز A، أو تم العثور عليه في جزء آخر من وثيقة 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==--
```

يتم الآن إعادة كتابة عناوين URL التي تم تفكيكها عندما يتم تجريد عنصر علامة التمييز A مع إعادة كتابة جزء النص الخاص بالارتباط عندما يطابق تنسيق عنوان URL. يتم عمل جزء النص المعاد كتابته بنفس الطريقة الموجودة في النص/الجزء العادي من رسالة MIME. يتم وضع العنصر بين الكلمات المحظورة وكل النقاط يتم وضعها بين أقواس مربعة. يمنع ذلك المستخدم من نسخ عنوان URL ولصقه، ويجعل بعض عملاء برامج البريد الإلكتروني النص قابلا للنقر.

التلخيص:

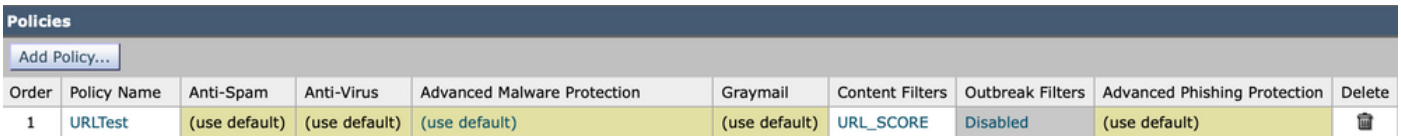
- إلغاء التشغيل على "النص"/"الجزء العادي" يعيد كتابة URL إلى كتل محظورة
- إلغاء التشغيل على جزء TEXT/HTML يعيد كتابة عنوان URL من علامة تمييز HTML A عندما يتم تجريد علامة تمييز A
- يؤدي تشغيل إلغاء التثبيت على جزء TEXT/HTML إلى إعادة كتابة كافة سلاسل URL التي تتطابق مع كتل محظورة

الجزء الثاني - إعادة التوجيه

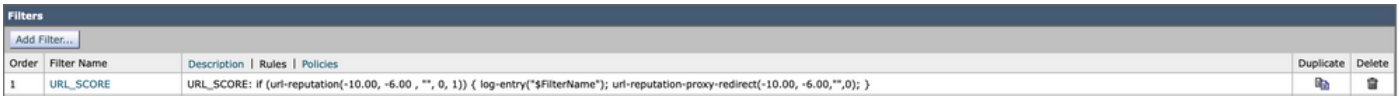
التكوينات

في الجزء الثاني يستخدم التكوين:

- نهج البريد مع تكوين AS/AV/AMP الافتراضي ومن معطل



- عامل تصفية المحتوى الوارد: تم تمكين عامل تصفية محتوى URL_SCORE



يستخدم عامل تصفية المحتوى حالة السمعة لعنوان URL لمطابقة عناوين URL الضارة، التي تشير إلى ما بين -10.00 و -6.00. كإجراء، يتم تسجيل اسم عامل تصفية المحتوى ويتم **redirect action** إتخاذ الإجراء.

فعل إعادة التوجيه

تتيح إعادة التوجيه إلى خدمة وكيل أمان Cisco لتقييم وقت النقر لمستلم الرسالة النقر فوق الارتباط وإعادة توجيهه إلى وكيل أمان الويب من Cisco في السحابة، والذي يمنع الوصول إذا تم تعريف الموقع على أنه ضار.

السيناريو جيم

الكشف عن التهديد غير الفيروسي بمرشح التفشي	ال
إجراء مرشح المحتوى	إعادة توجيه
أمان الويب تم تمكين AdvancedConfig href وإعادة كتابة النص	ال

هذا السيناريو مشابه جدا في السلوك للسيناريو (أ) من الجزء الأول مع الفرق الذي تم إجراؤه في إجراء تصفية المحتوى لإعادة توجيه عناوين URL بدلا من إلغاء تثبيته. يتم إستعادة إعدادات WebSecurityAdvancedConfig إلى الإعدادات الافتراضية، مما يعني **"Do you want to rewrite both the URL text and the href in the message? ..** تعيين هذه الإعدادات على **N.**

تقوم بعرض البريد الإلكتروني باكتشاف كل عناوين URLs وتقييمه. تقوم نطاق الضارة بتشغيل قاعدة مرشح محتوى URL_SCORE وتأخذ الإجراء **url-reputation-proxy-redirect-action**

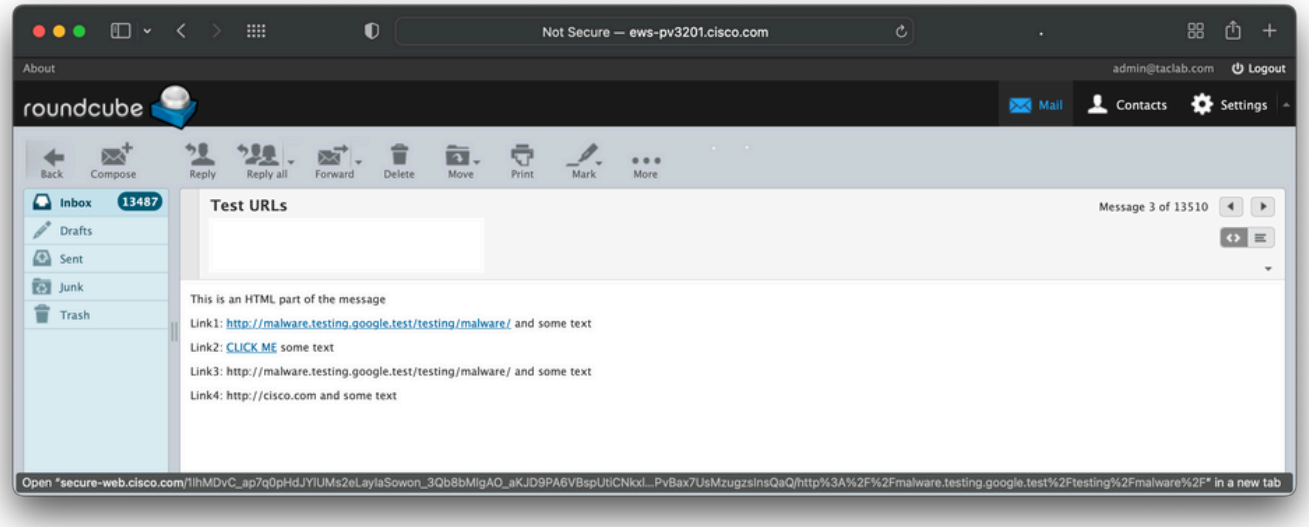
```
Tue Jul  5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/ has re
 Tue Jul  5 12:42:19 2022 Info: MID 139508 Custom Log Entry: URL_SCORE
Tue Jul  5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/ has re
Tue Jul  5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/ has re
Tue Jul  5 12:42:19 2022 Info: MID 139508 URL http://malware.testing.google.test/testing/malware/ has re
Tue Jul  5 12:42:19 2022 Info: MID 139508 rewritten to MID 139509 by url-reputation-proxy-redirect-acti
```

ألق نظرة على كيفية إعادة كتابة عناوين URL في جزء HTML من الرسالة. نفس الموجود في السيناريو أ، يتم إعادة كتابة عناوين URL الموجودة في سمة href لعنصر علامة تمييز فقط ويتم تخطي عناوين URL الموجودة في جزء النص من عنصر a-tag. مع إجراء إلغاء الربط يتم تجريد عنصر علامة تمييز A بأكمله لكن مع إجراء إعادة توجيه، تتم إعادة كتابة عنوان URL في سمة 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==--
```

ونتيجة لذلك، يعرض عميل البريد الإلكتروني ارتباطين نشطين: يشير كل من Link1 و Link2 إلى خدمة وكيل أمان الويب من Cisco ولكن الرسالة المعروضة في عميل البريد الإلكتروني تعرض جزء النص من عالمة a والتي ال يتم إعادة كتابتها بشكل افتراضي. إلى مستوى أفضل تحت هذا، الرجاء إلقاء نظرة على الإخراج من عميل بريد الويب الذي يعرض جزء النص/html من الرسالة.



في النص/الجزء العادي من جزء MIME، تبدو إعادة التوجيه أسهل للفهم لأن كل سلسلة عنوان URL التي تطابق النتيجة يتم إعادة كتابتها.

```
--===============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_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfs
     Link2: http://cisco.com and some text

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

التلخيص:

- إعادة توجيه التشغيل على النص/الجزء العادي يعيد كتابة سلسلة عنوان URL التي تتطابق مع خدمة وكيل Cisco Web Secure
- إعادة التشغيل على جزء TEXT/HTML يعيد كتابة URL من سمة HTML A-Tag href التي تتطابق مع خدمة وكيل Cisco Web Secure باستخدام سلاسل URL الأخرى ولكنه يترك جميع غير معدلة

السيناريو دال

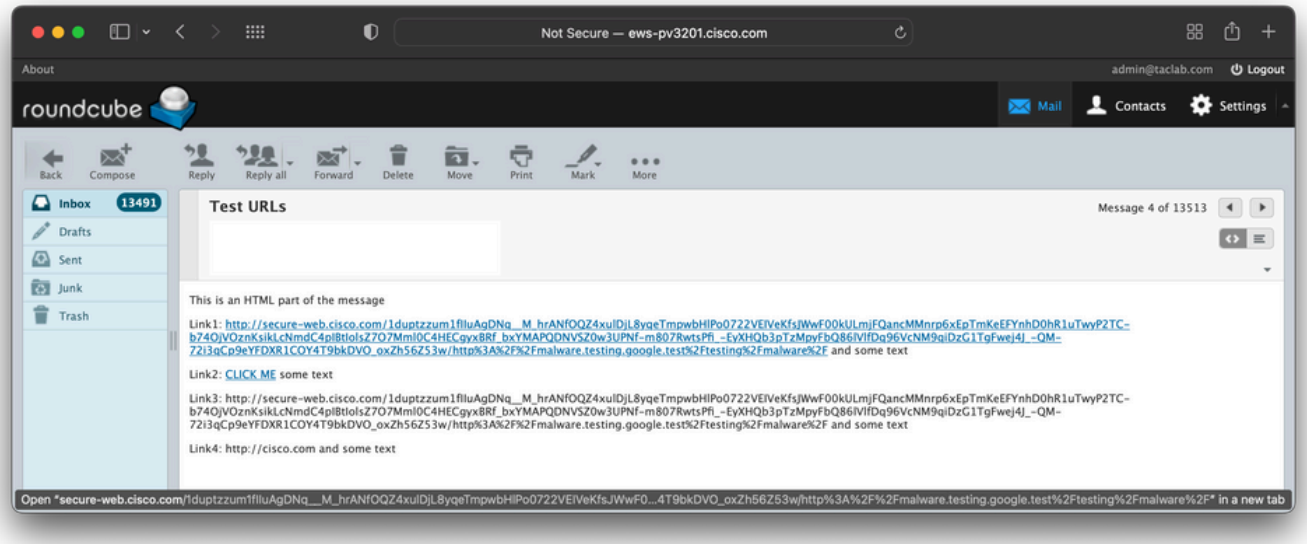
ال	الكشف عن التهديد غير الفيروسي بمرشح التفشي
إعادة توجيه	إجراء مرشح المحتوى
نعم	أمان الويب تم تمكين AdvancedConfig href وإعادة كتابة النص

وهذا السيناريو مشابه للسيناريو (ب) الوارد في الجزء الأول. لإعادة كتابة كافة سلاسل (ب) عنوان URL التي تتطابق في جزء HTML من الرسالة تم تمكينها. يتم القيام بذلك باستخدام أمر webSecurityAdvancedConfig عندما توقوم بالإجابة على Y **"Do you want to rewrite both the URL text and the href in the message? ..** على السؤال.

```
--===============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_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF0

Link2: CLICK ME some text

Link3: http://secure-web.cisco.com/1duptzzum1fIIuAgDNq__M_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfsJWwF0

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


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

بمجرد تمكين href وإعادة كتابة النص، تتم إعادة توجيه جميع سلاسل عنوان URL التي تطابق شروط مرشح المحتوى. تقدم الرسالة الموجودة في عميل البريد الإلكتروني الآن مع كل إعادة التوجيه. لفهم هذا بشكل أفضل، راجع إخراج عميل بريد الويب الذي يعرض جزء النص/html من الرسالة.



النص/الجزء العادي من رسالة MIME وه نفسه كما في السيناريو C حيث أن تغيير

WebSecurityAdvancedConfig ال يؤثر على النص/الأجزاء العادية من الرسالة.

```
--================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_hrANfOQZ4xulDjL8yqeTmpwbHlPo0722VEIVeKfs
     Link2: http://cisco.com and some text

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

التلخيص:

- إعادة توجيه التشغيل على النص/الجزء العادي يعيد كتابة سلاسل عنوان URL التي تتطابق مع خدمة وكيل Cisco Web Secure
- يعيد تشغيل Redirect على الجزء TEXT/HTML كتابة URL من سمة HTML A-Tag href مع جزء النص بالإضافة إلى أي سلسلة URL أخرى تتطابق في نص HTML مع خدمة وكيل Cisco Web Secure

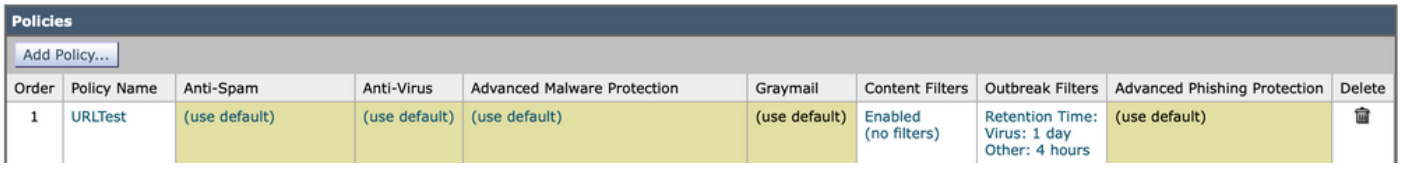
الجزء 3 - إعادة التوجيه

يوفر هذا الجزء معلومات حول كيفية قيام إعدادات الكشف عن تأثير التهديدات غير الفيروسية بمسح URL.

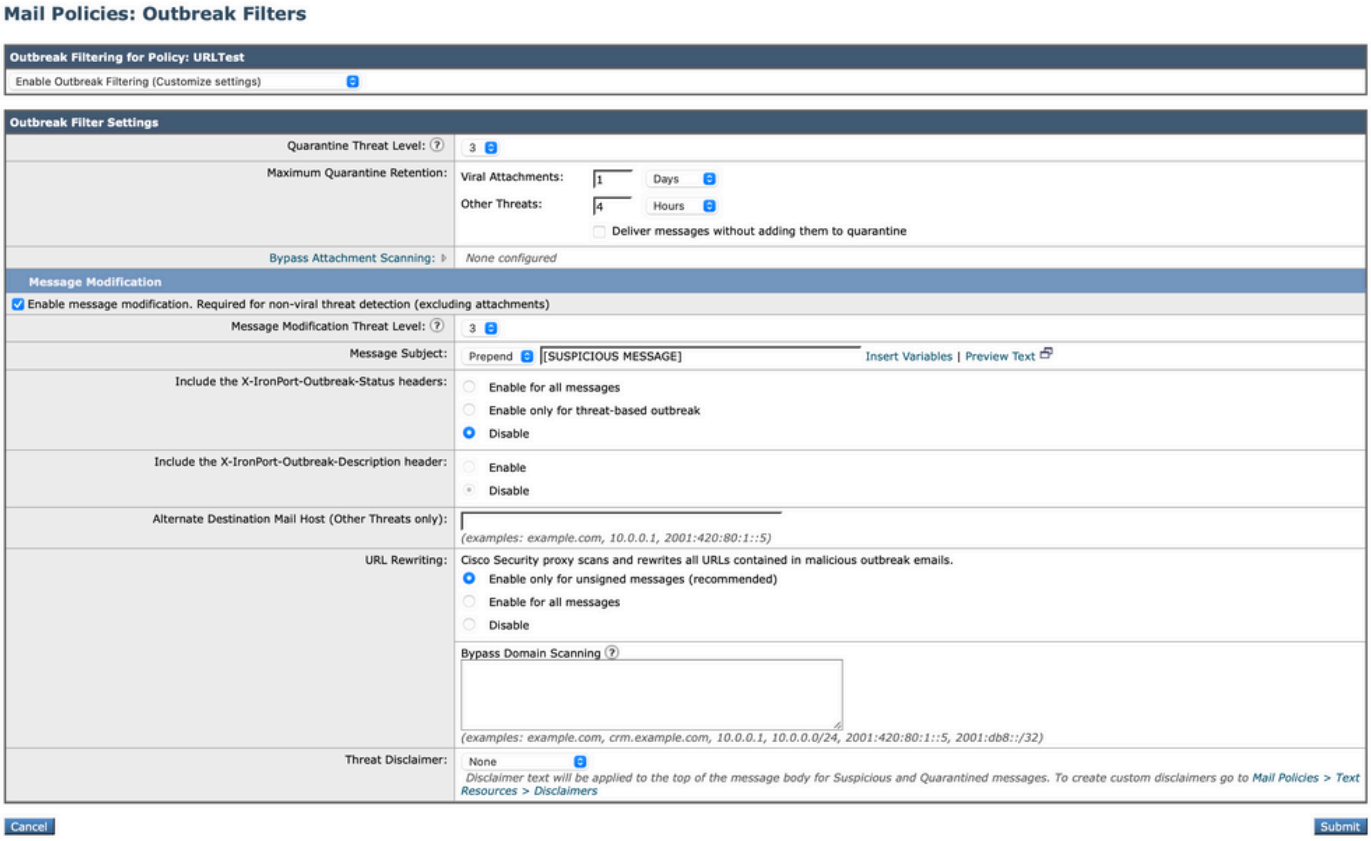
التكوين

لهذا الغرض، يتم تعطيل عامل تصفية المحتوى المستخدم في الجزأين الأولين.

- نهج البريد مع تكوين AS/AV/AMP الافتراضي ومع تمكين



- تم تكوين "فحص عوامل تصفية التفشي" للكشف عن التهديدات غير الفيروسية باستخدام مجموعة إعادة كتابة URL لإعادة كتابة كافة URLs الموجودة في رسائل البريد الإلكتروني الضارة



عندما يتم تصنيف الرسالة بواسطة OF كرسالة ضارة، تتم إعادة كتابة جميع عناوين URL الموجودة داخل الرسالة باستخدام خدمة وكيل Cisco Web Secure.

السيناريو E

الكشف عن التهديد غير الفيروسي بمرشح التصفية	نعم
إجراء مرشح المحتوى	لا
أمان الويب تم تمكين AdvancedConfig href وإعادة كتابة النص	لا

يوضح هذا السيناريو كيفية عمل إعادة كتابة الرسالة مع تعطيل إعادة كتابة النص و OF Enabled و WebSecurityAdvancedConfig href فقط.

```
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/ma
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/ma
```

```
Wed Jul  6 14:09:19 2022 Info: MID 139514 rewritten URL u'http://malware.testing.google.test/testing/ma
Wed Jul  6 14:09:19 2022 Info: MID 139514 rewritten to MID 139515 by url-threat-protection filter 'Thre
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)
```

فلنبدأ بجزء النص/MIME العادي. بعد التحقق السريع، يمكن ملاحظة إعادة كتابة جميع عناوين URL الموجودة داخل النص/الجزء العادي إلى خدمات وكيل Cisco Web Secure. يحدث ذلك لأن إعادة كتابة عنوان URL ممكنة لكافة عناوين URL الموجودة داخل الرسالة الضارة لتفشي الوباء.

```
--================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-zC86MO2dm_fOXCqKT0tDET3RD_KAeUWTWhWZvN9i8lLPcwBBBi9TLjMAMnRKPmeg=
En_YQvDnCzTB4qYkG8aUQlFsecXB-V_HU1vL8IRFRP-uGINjhHp9kWCnntJBJEm0MheA1T6mBJJ=
ZhBZmfymfOddXs-xIGiYXn3juN1TvuOlCceo3YeaiVrbOXc0lZs3FO8xvNjOnwVKN181yGKPQ9Y=
cn5aSWvg/http%3A%2F%2Fcisco.com and some text

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

هذا هو جزء النص/html الذي تمت معالجته من رسالة MIME.

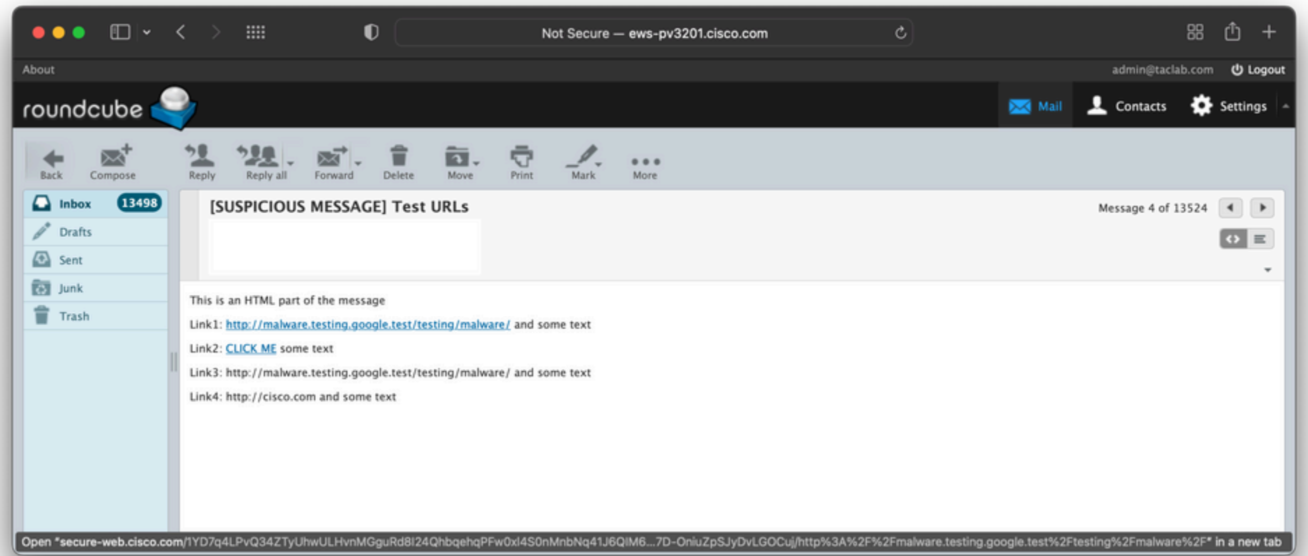
```
--================7781793576330041025==
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable




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=
 text]

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

[=20
--===============7781793576330041025==--]



[وعلى النقطة الأولى التي يمكن ملاحظتها هي انه اذا لم تتم إعادة كتابة الارتباط 4. إذا قرأت المقالة بعناية فأنت تعرف الجواب. يقوم جزء النص/html من MIME بشكل افتراضي بتقييم ومعالجة سمات href لعناصر a-tag فقط. إذا كان هناك سلوك لمثال كما هو الحال مع النص/الجزء العادي مرغوب، فيجب تمكين WebSecurityAdvancedConfig href وإعادة كتابة النص. السيناريو التالي يقوم بذلك بالضبط.]

التلخيص:

- إعادة توجيه التشغيل على النص/الجزء العادي يعيد كتابة جميع سلسلة عنوان URL التي تتطابق مع خدمة وكيل Cisco Web Secure
- لإعادة التشغيل على الجزء TEXT/HTML، تتم إعادة كتابة عنوان URL فقط من سمة html A-Tag href باستخدام خدمة الوكيل الآمن للويب من Cisco

السيناريو واو

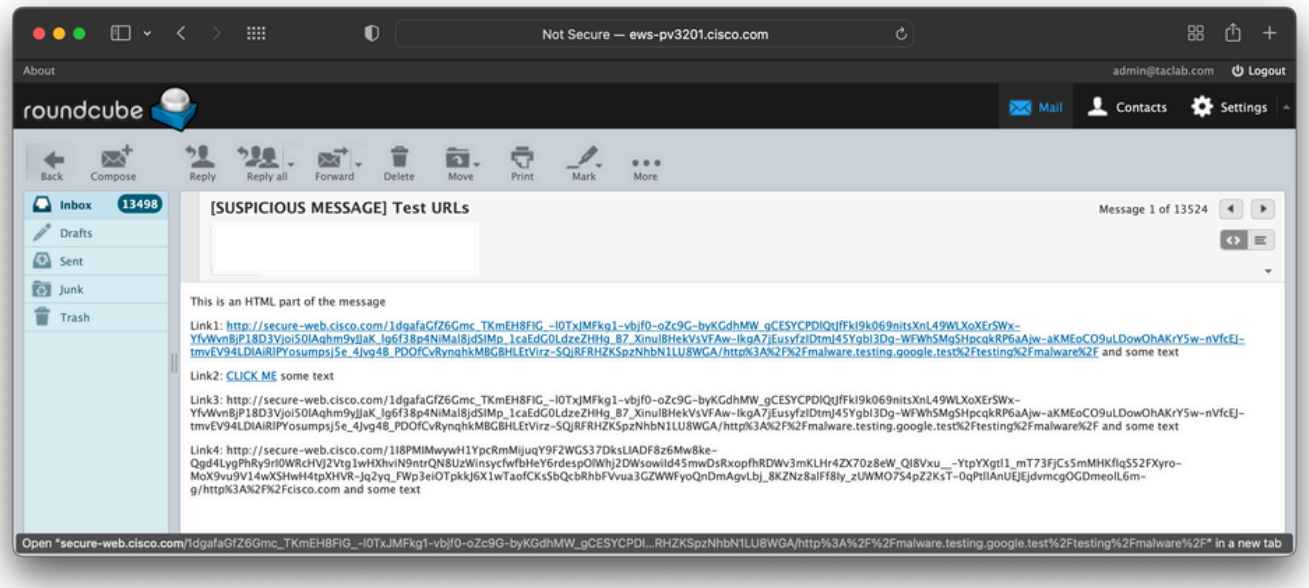
الكشف عن التهديد غير الفيروسي بمرشح التفشي	نعم
إجراء مرشح المحتوى	ال
أمان الويب تم تمكين AdvancedConfig href وإعادة كتابة النص	نعم

يتيح هذا السيناريو تمكين webSecurityAdvancedConfig href وإعادة كتابة النص لإظهار تغييرات اكتشاف التهديدات غير الفيروسية. في هذه اللحظة، يجب أن WebSecurityAdvancedConfig ال يؤثر على أجزاء النص/MIME العادية. عند تقييم طلب جزء النص/html ونرى كيف تتغير السلوك.

```
--================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=
D3Vjoi5OlAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdGOLdzeZHHg_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=
18D3Vjoi5OlAqhm9yJJaK_lg6f38p4NiMal8jdSIMp_1caEdGOLdzeZHHg_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==--
```

يمكن ملاحظة أن المخرجات مشابهة جدا للتي كانت في السيناريو D مع الفرق الوحيد أن كل عناوين URL تمت إعادة كتابتها، وليس فقط تلك الخبيثة. يتم تعديل جميع سلاسل عنوان URL التي تتطابق في جزء HTML مع السلاسل غير الضارة هنا.



التلخيص:

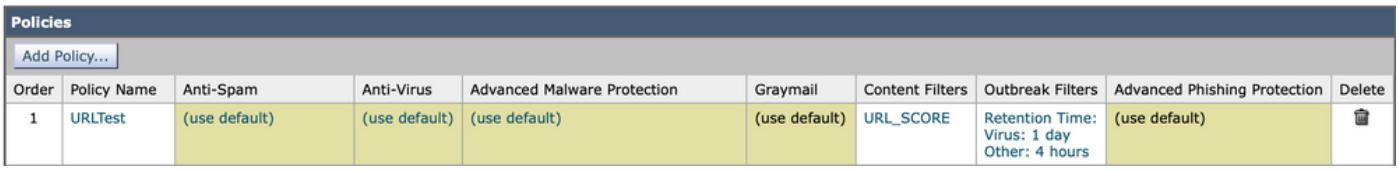
- إعادة توجيه التشغيل على النص/الجزء العادي يعيد كتابة جميع سلاسل عنوان URL التي تتطابق مع خدمة وكيل Cisco Web Secure
- للإعادة التشغيل على جزء TEXT/HTML، يعيد كتابة URL من سمة html A-Tag href مع جزء النص من العنصر وجميع سلاسل URL الأخرى التي تتطابق مع خدمة الوكيل الآمن ل Cisco Web

السيناريو الي

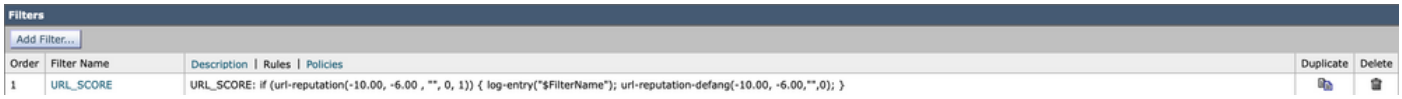
الكشف عن التهديد غير الفيروسي بمرشح التفشي	نعم
إجراء مرشح المحتوى	ديفانغ
أمان الويب تم تمكين AdvancedConfig href وإعادة كتابة النص	نعم

يتحقق هذا السيناريو الأخير من التكوين.

- نهج البريد مع تكوين AS/AV/AMP الافتراضي ومع تمكين



- يتم تكوين الفحص للكشف عن التهديدات غير الفيروسية باستخدام مجموعة إعادة كتابة عنوان URL لإعادة كتابة جميع عناوين URL الموجودة في رسائل البريد الإلكتروني الضارة (مثل السيناريوهات السابقة)
- عامل تصفية المحتوى الوارد: تم تمكين عامل تصفية محتوى URL_SCORE



يستخدم عامل تصفية المحتوى حالة سمعة عنوان URL لمطابقة عناوين URL الضارة، تلك التي تشير إلى ما بين -10.00 و -6.00. كإجراء، يتم تسجيل اسم عامل تصفية المحتوى ويتم إتخاذ إجراء إلغاء **url-reputation-defang** الارتباط.

يتم إرسال نفس نسخة الرسالة وتقييمها بواسطة بوابة البريد الإلكتروني مع النتائج:

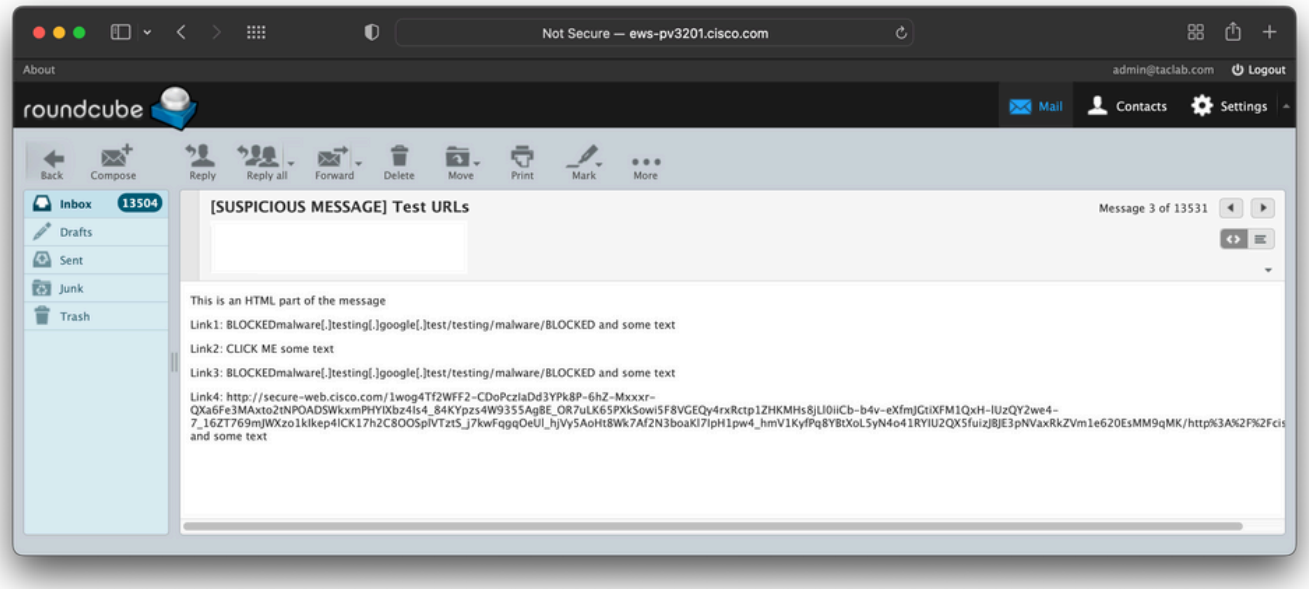
```
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 Custom Log Entry: URL_SCORE
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 URL http://malware.testing.google.test/testing/malware/ has r
Wed Jul  6 15:13:10 2022 Info: MID 139518 rewritten to MID 139519 by url-reputation-defang-action filte
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 'Threa
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
```

ثيح ،ىوتحملا ةيفصت لماوع ةطساوب الوأ ةلاسرلا ينورتكلإلا ديربلا تاقفدت حرشي URL-REPUTATION-DEFANG- قيبطت متيو URL_SCORE ةيفصت لماع ليغشت متي ACTION. ءازجأ نم لك يف ةراضلا URL نيوانع عيمج ليطعت ىلإ ءارجإلا اذه يدؤي صنلا ةباتك ةداعإو WebSecurityAdvancedConfig href نأل .html MIME/صنلاو لهسلا/صنلا لك حسم متي امدنع HTML صن لخاد قباطت يتلا URL ناونع لسالس لك نيكمت متي لك عضوو ةروظحملا تاملكلا نيب URL ناونع صن ءازجأ ةباتك ةداعإو زييمت ةمالع رصانع زييمت ةمالع يف عضوي ال راض رخآ URLs عم ثدحي ءيشلا سفن .ةعبرم ساوقأ نيب طاقنلا رصانع HTML. جلاعي "ماع لماع ةيفصت يشفتلا" يلاتلا ةلاسرلا. موقي OF فاشتكاب نيوانع URL ةراضلا ويرعف ةلاسرلا نأب اهنإ ةراض (ىوتسم ديدهتلا=5). وتنيجة ذلكل، هنإف ديعي ةباتك عيمج نيوانع URL ةراضلا ريغو ةراضلا يتلا مت روثعلا اهيلع لخاد ةلاسرلا. نأل ارظن ءارجإ لماع ةيفصت ىوتحملا دق ماق بالفعل ليدعتب نيوانع URLs هذه، نإف OF موقي ةداعإب ةباتك يقاب نيوانع URL ريغ ةراضلا طقف ثيح مت كوتنيهاو لكشب دمعتم .كلذب مايقلل مت ءاغلإ هيجوت ةلاسرلا ةعورعملا يف ءزج يف ليمع ديربلا ينورتكلإلا نم ءزج نيوانع URL ةراضلا وءزج نم ناونع URL ريغ راضلا يذلا تمت ةداعإ هيجوتها.

```
--===============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=
wi5F8VGEQy4rxRctp1ZHKMHs8jLlOiiCb-b4v-eXfmJGtiXFM1QxH-lUzQY2we4-7_16ZT769mJ=
```

```
WXzo1kIkep4lCK17h2C8OOSplVTztS_j7kwFqgqOeUl_hjVy5AoHt8Wk7Af2N3boaKl7IpH1pw4=
_hmV1KyfPq8YBtXoL5yN4o41RYIU2QX5fuizJBJE3pNVaxRkZVm1e620EsMM9qMK/http%3A%2F=
%2Fcisco.com and some text



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



يتم تطبيق نفس الإجراء على النص/الجزء العادي من رسالة MIME. تتم إعادة توجيه جميع عناوين URL غير الضارة إلى وكيل Cisco Web Secure ويتم إلغاء توجيه عناوين URL الضارة.

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

التلخيص:

- إعادة تشغيل CF على "النص/الجزء العادي" يعيد كتابة URL إلى كتل محظورة

- إعادة تشغيل CF على جزء TEXT/HTML يعيد كتابة URL من علامة تمييز HTML A عندما يتم تجريد علامة تمييز A
- إعادة تشغيل CF على جزء TEXT/HTML كتابة كافة سلاسل URL التي تتطابق مع تلك محظورة
- إعادة توجيه التشغيل على النص/الجزء العادي يعيد كتابة جميع سلاسل عناوين URL التي تتطابق مع خدمة وكيل Cisco Web Secure (غير راض)
- لإعادة التشغيل على جزء TEXT/HTML، يعيد كتابة URL من سمة html A-Tag href مع جزء النص الخاص بالعنصر وجميع سلاسل URL الأخرى التي تتطابق مع خدمة الوكيل الآمن ل Cisco على الويب (غير راض)

استكشاف الأخطاء وإصلاحها

اتبع تلك النقاط عندما تكون هناك حاجة للتحقيق في المسألة بإعادة كتابة عنوان الربط.

- قم بتمكين تسجيل URL في mail_log. قم بتشغيل **OUTBREAKCONFIG** الأمر والإجابة **Y** على **Do you wish to enable logging of URL's?** [N]>
- تحقق من **WEBSECURITYADVANCECONFIG** الإعدادات الموجودة تحت كل وضع من أعضاء نظام المجموعة بوابة البريد الإلكتروني وتأكد من تعيين خيار إعادة كتابة النص و href جهاز. تذكر أن هذا الأمر خاص على مستوى الجهاز على كل على الخيار نفسه أن ومن كذلك وفقا المجموعة أو أعضاء نظام المجموعة. الإعدادات على انه أدرجها تم التي الإعدادات لا تؤثر على التغيير
- تحقق من شروط وأنشطة عامل تصفية المحتوى، وتأكد من تمكين عامل تصفية المحتوى وتطبيقه على عنه البريد الوارد الصحيح. تحقق من عدم وجود عامل تصفية محتوى آخر تمت معالجته من قبل استخدام الإجراء النهائي الذي يمكنه التخطي لمعالجة عوامل التصفية الأخرى.
- تحقق من النسخة الأولية للمصدر والرسالة النهائية. تذكر تذكر إسترجاع الرسالة بتنسيق EML، أن التنسيقات الخاصة مثل MSG ال يمكن الاعتماد عليها عندما يتعلق الأمر بالتحقيق في الرسائل. يسمح كل عميل البريد الإلكتروني بعرض الرسالة المصدر، ومحاولة إسترداد نسخة الرسالة مع عميل بريد إلكتروني مختلف. على سبيل المثال، يسمح كل MS Outlook for Mac بعرض مصدر الرسالة بينما يسمح إصدار Windows بعرض الرؤوس فقط.

ملخص

الغرض من هذه المقالة هو المساعدة في فهم خيارات التكوين المتوفرة بشكل أفضل عندما يتعلق الأمر بإعادة كتابة عناوين URL. ومن المهم أن تتذكر أن الرسائل الحديثة يتم بناؤها باستخدام معايير MIME. وهذا يعني أنه يمكن عرض برامج البريد الإلكتروني بلغة وسيطة. يقرأ البريد الإلكتروني أو يختار عميل البريد الإلكتروني على إمكانيات عرض الرسالة بشكل صحيح. ملفات عرض بأنواع مختلفة (النص والأوضاع المختلفة وعرض HTML). بشكل افتراضي، يستخدم معظم عملاء البريد الإلكتروني الحديثة HTML لعرض الرسائل. عندما يتعلق الأمر بإعادة كتابة HTML و URL، الرجاء مراعاة أن بوابة البريد الإلكتروني الافتراضية موقتة بإعادة كتابة عناوين URL الموجودة فقط داخل سمة href لعنصر a-tag. في كثير من الحالات التي لا تكون كافية ويجب أخذ الأمر باستخدام النص وإعادة كتابة href من كل التمكين لاعتبارها webSecurityAdvancedConfig. تذكر أن هذا الأمر على مستوى الجهاز، وللتنسيق عبر نظام المجموعة، يجب تطبيق التغيير بشكل منفصل على كل وضع من أعضاء نظام المجموعة.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).