كيفية حظر مجموعات الأحرف المستندة إلى نوع المحتوى

المحتويات

المقدمة

يصف هذا المستند كيفية كتابة عامل تصفية وتكوينه لاكتشاف مجموعات الأحرف المستندة إلى نوع المحتوى واتخاذ إجراء بشأنها على جهاز أمان البريد الإلكتروني (ESA) من Cisco. يمكن إستخدام المستند التالي لاكتشاف الأحرف المستندة إلى اللغات الأجنبية التي يتم رؤيتها في رسائل البريد العشوائي.

معلومات أساسية

قد يتلقى مسؤولو وكالة الفضاء الأوروبية تدفقا من رسائل البريد التي تحتوي على لغات أجنبية تستند إلى الأحرف ولا تعتبر بريدا شرعيا لشركتهم أو مجالاتهم. هناك طريقة واحدة لتناول هذا الموضوع من وكالة الفضاء الأوروبية، وهي ثلاثة خيارات:

3. اكتب عامل تصفية باستخدام لغة رسالة الشرط. (هذا الخيار هو ميزة جديدة لأمان البريد الإلكتروني في AsyncOS 10.0.0-203 والأحدث.)

كيفية حظر مجموعات الأحرف المستندة إلى نوع المحتوى

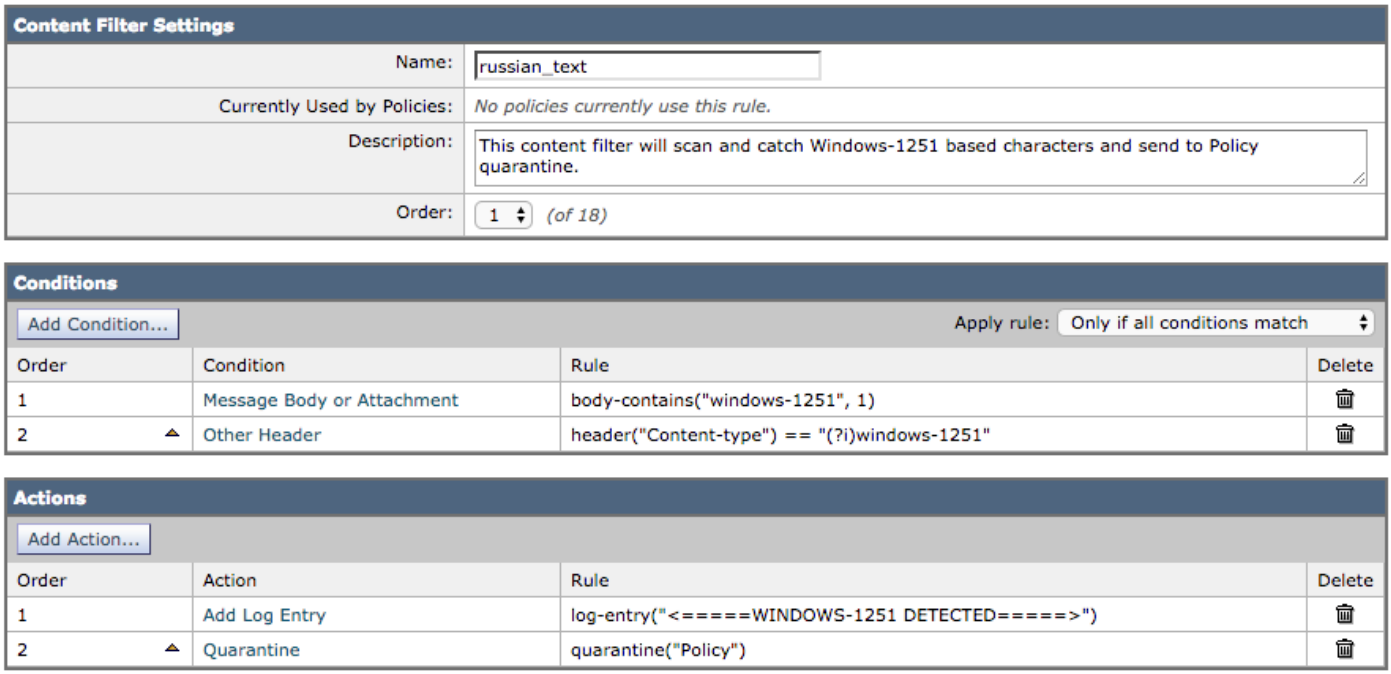
كتابة عامل تصفية لاكتشاف نوع المحتوى

الخيار الأول هو أن يقوم المسؤول بكتابة عامل تصفية وتكوينه، وإقرانه بنهج بريد، حسب الحاجة.

ملاحظة: قد تكون كتابة عامل التصفية هذا وتكوينه كعامل تصفية رسائل أمرا باهظ التكلفة من حيث الموارد من أجل مسح مجموعة رسائل البريد الإلكتروني الخاصة بمجموعات الأحرف.

ملاحظة: يتم اقتراح تكوين هذا كعامل تصفية محتوى بشدة، حيث تحدث عوامل تصفية المحتوى بعد المسح الضوئي لمكافحة البريد العشوائي. ومع ذلك، يمكن كتابة هذا العنصر وتكوينه كعامل تصفية للرسائل، إذا لزم الأمر.

سيأخذ المثال التالي بعين الاعتبار رسالة بريد تحتوي على أحرف روسية (سيريلية) مستندة إلى مجموعة الأحرف المستندة إلى Windows-1251. تمت كتابته كعامل تصفية محتوى:



Content Filter Settings

Name:	russian_text
Currently Used by Policies:	*No policies currently use this rule.*
Description:	This content filter will scan and catch Windows-1251 based characters and send to Policy quarantine.
Order:	1 *(of 18)*

Conditions

Add Condition... Apply rule: Only if all conditions match

Order	Condition	Rule	Delete
1	Message Body or Attachment	body-contains("windows-1251", 1)	
2	Other Header	header("Content-type") == "(?i)windows-1251"	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<=====WINDOWS-1251 DETECTED=====>")	
2	Quarantine	quarantine("Policy")	

يحتوي البريد الإلكتروني للاختبار المستخدم على ما يلي في نص البريد الإلكتروني:

```
Russian uses , , , , o, , , , ,  as vowels. You could create a message filter set to "Matches
any of the following" that test whether "Body" "contains" "", "Body" "contains" "" and so forth
until you covered all of the vowels. Ssince English also uses "a" , "e" , "o", and "y" letters
don't test for them. The reason for "Matches any of the following" is to logically OR them - you
.want the action to take place if any of those letters are found
```

مع تكوين عامل تصفية المحتوى كما هو موضح أعلاه، يتم تسجيل سجلات البريد كما يلي:

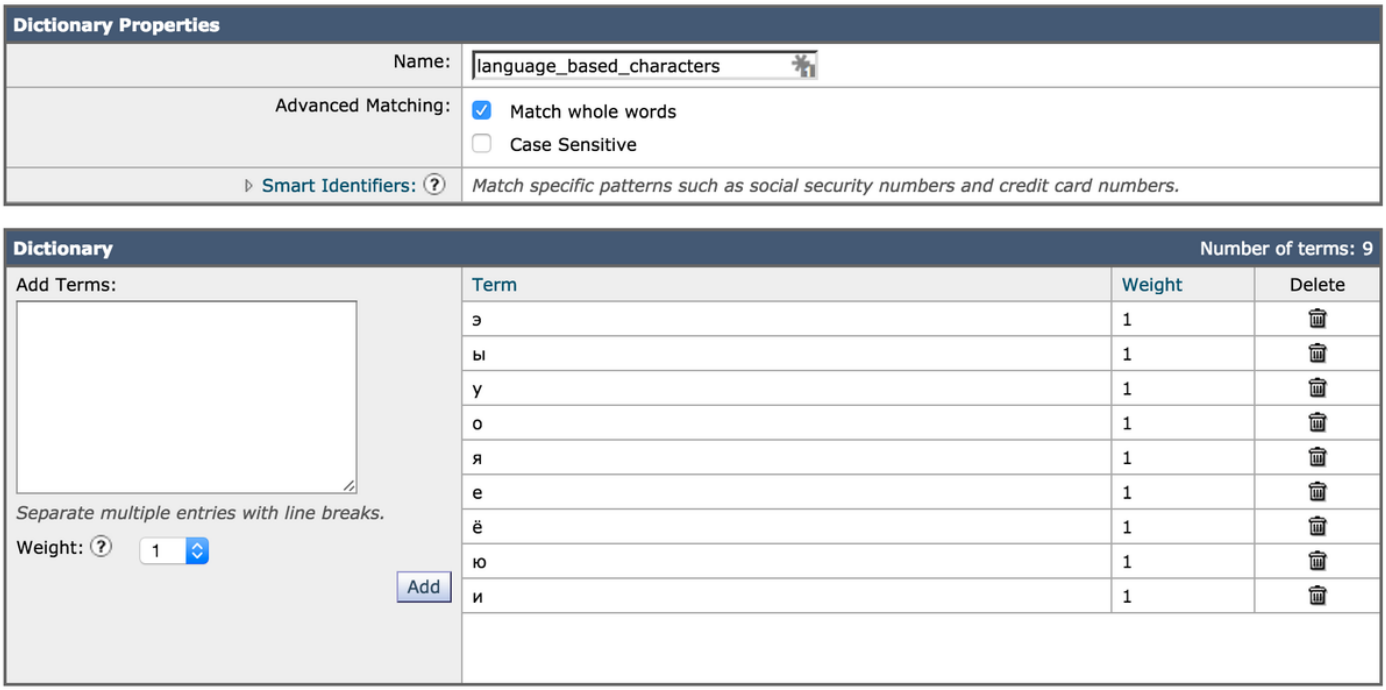
```
                                Thu Sep 10 14:50:09 2015 Info: Start MID 164993 ICID 266729
            <Thu Sep 10 14:50:09 2015 Info: MID 164993 ICID 266729 From: <end_user@test.com
        <Thu Sep 10 14:50:09 2015 Info: MID 164993 ICID 266729 RID 0 To: <recpient@my_co.com
Thu Sep 10 14:50:09 2015 Info: MID 164993 using engine: SPF Verdict Cache using cached verdict
            Thu Sep 10 14:50:09 2015 Info: MID 164993 Message-ID '<7A961F85-A5F1-413F-87CB-
                                                                  '<C31D2E5605EC@my_co.com
                          'Thu Sep 10 14:50:09 2015 Info: MID 164993 Subject 'russian test
       <Thu Sep 10 14:50:09 2015 Info: MID 164993 ready 2302 bytes from <end_user@test.com
    Thu Sep 10 14:50:09 2015 Info: MID 164993 matched all recipients for per-recipient policy
                                                        DEFAULT in the inbound table
          Thu Sep 10 14:50:09 2015 Info: MID 164993 AMP file reputation verdict : CLEAN
              Thu Sep 10 14:50:09 2015 Info: MID 164993 using engine: GRAYMAIL negative
    Thu Sep 10 14:50:09 2015 Info: MID 164993 Custom Log Entry: <====== WINDOWS-1251 DETECTED
                                                                                  <======
(Thu Sep 10 14:50:09 2015 Info: MID 164993 quarantined to "Policy" (content filter:russian_text
                          Thu Sep 10 14:50:09 2015 Info: Message finished MID 164993 done
```

يمكن إستخدام لغات أخرى ومجموعات أحرف أخرى. الرجاء مراجعة قسم المراجع للحصول على معلومات إضافية.

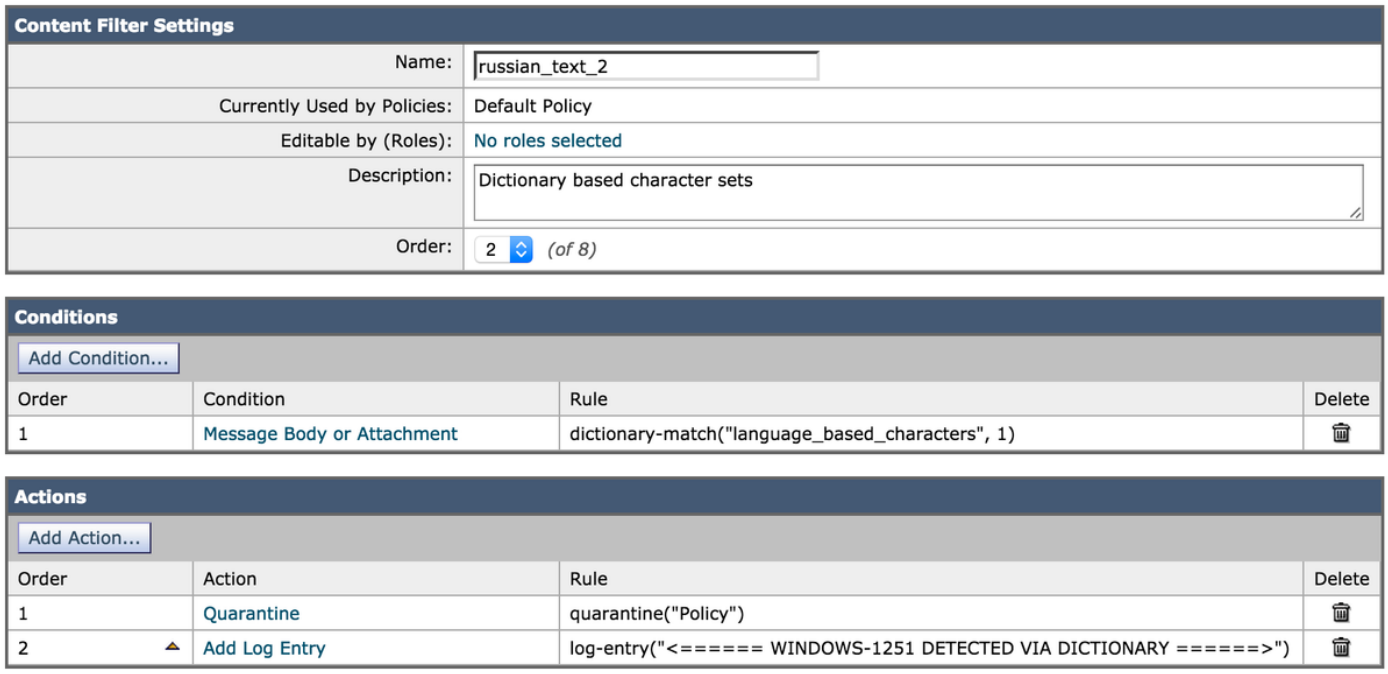
كتابة مرشح للإشارة إلى قاموس مستند إلى حرف

الخيار الثاني هو إضافة قائمة مجموعات الحروف إلى ملف نص القاموس وإحالة ذلك في المرشح.

مثال لإضافة الحروف إلى القاموس:



يتم تعيين الحروف الآن للقاموس ويتم الإشارة إلى القاموس نفسه في عناصر الشرط للمرشح:



باستخدام نفس رسالة الاختبار الإلكترونية أعلاه، تحتوي على ما يلي في متن البريد الإلكتروني:

```
Russian uses , , , , o, , , , ,  as vowels. You could create a message filter set to "Matches
any of the following" that test whether "Body" "contains" "", "Body" "contains" "" and so forth
until you covered all of the vowels. Ssince English also uses "a" , "e" , "o", and "y" letters
don't test for them. The reason for "Matches any of the following" is to logically OR them - you
.want the action to take place if any of those letters are found
```

مع تكوين عامل تصفية المحتوى كما هو أعلاه باستخدام حالة مطابقة القاموس، يتم تسجيل سجلات البريد كما يلي:

```
Thu Sep 10 15:26:08 2015 Info: Start MID 164995 ICID 266737
<Thu Sep 10 15:26:08 2015 Info: MID 164995 ICID 266737 From: <end_user@test.com
<Thu Sep 10 15:26:08 2015 Info: MID 164995 ICID 266737 RID 0 To: <recpient@my_co.com
Thu Sep 10 15:26:08 2015 Info: MID 164995 using engine: SPF Verdict Cache using cached verdict
```

```
Thu Sep 10 15:26:08 2015 Info: SPF Verdict Cache cache status: hits = 6, misses = 4, expires =
                                    1, adds = 4, seconds saved = 0.50, total seconds = 0.85
          Thu Sep 10 15:26:08 2015 Info: MID 164995 Message-ID '<BCC88307-EB91-476E-8732-
                                                                '<334E9EE84EC8@my_co.com
                       'Thu Sep 10 15:26:08 2015 Info: MID 164995 Subject 'russian test 3
     <Thu Sep 10 15:26:08 2015 Info: MID 164995 ready 2316 bytes from <end_user@test.com
  Thu Sep 10 15:26:08 2015 Info: MID 164995 matched all recipients for per-recipient policy
                                                          DEFAULT in the inbound table
        Thu Sep 10 15:26:08 2015 Info: MID 164995 AMP file reputation verdict : CLEAN
            Thu Sep 10 15:26:08 2015 Info: MID 164995 using engine: GRAYMAIL negative
Thu Sep 10 15:26:08 2015 Info: MID 164995 Custom Log Entry: <====== WINDOWS-1251 DETECTED VIA
                                                                <====== DICTIONARY
      Thu Sep 10 15:26:08 2015 Info: MID 164995 quarantined to "Policy" (content
                                                                (filter:russian_text_2
          Thu Sep 10 15:26:08 2015 Info: Message finished MID 164995 done
```

كتابة عامل تصفية محتوى باستخدام شرط "لغة الرسالة"

الخيار الثالث هو إستخدام شرط "لغة الرسالة". وتستخدم الإيسا محرك اكتشاف اللغة المدمج لاكتشاف اللغة في رسالة ما. يستخرج الجهاز الموضوع والنص الأساسي للرسالة ويمرره إلى محرك اكتشاف اللغة.

يحدد محرك اكتشاف اللغة أحتمالية كل لغة في النص المستخرج ويمررها مرة أخرى إلى الجهاز. يعتبر الجهاز اللغة ذات الاحتمال الأكبر لغة الرسالة. يعتبر الجهاز لغة الرسالة "غير محددة" في أحد السيناريوهات التالية:

- إذا كانت اللغة التي تم اكتشافها غير معتمدة من قبل ESA
- إذا كان الجهاز غير قادر على اكتشاف لغة الرسالة
- إذا كان الحجم الإجمالي للنص المستخرج الذي تم إرساله إلى محرك اكتشاف اللغة أقل من 50 بايت.

ملاحظة: هذا الخيار هو ميزة جديدة لأمان البريد الإلكتروني في AsyncOS 10.0.0-203 والأحدث.

سيأخذ المثال التالي بعين الاعتبار رسالة بريد تحتوي على مجموعة أحرف صينية/تايوانية. تمت كتابته كعامل تصفية محتوى:

Content Filter Settings

Name:	Chinese_text
Currently Used by Policies:	Default Policy
Description:	
Order:	1 ▼ *(of 21)*

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	Message Language	message-language == "zh-tw"	🗑

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	quarantine("Policy")	🗑
2 ▲	Add Log Entry	log-entry("<==========Chinese/Taiwan Language Detected==========>")	🗑

مع تكوين عامل تصفية المحتوى كما هو موضح أعلاه، يتم تسجيل سجلات البريد كما يلي:

```
                                  Tue Feb 28 06:53:18 2017 Info: Start MID 481 ICID 27
<Tue Feb 28 06:53:18 2017 Info: MID 481 ICID 27 From: <end_user@test.com
```

```
<Tue Feb 28 06:53:18 2017 Info: MID 481 ICID 27 RID 0 To: <recipient@my_co.com
'Tue Feb 28 06:53:18 2017 Info: MID 481 Subject 'Chinese text test
<Tue Feb 28 06:53:18 2017 Info: MID 481 ready 1047 bytes from <end_user@test.com
Tue Feb 28 06:53:18 2017 Info: MID 481 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Tue Feb 28 06:53:18 2017 Info: MID 481 interim verdict using engine: CASE spam negative
Tue Feb 28 06:53:18 2017 Info: MID 481 using engine: CASE spam negative
Tue Feb 28 06:53:18 2017 Info: MID 481 interim AV verdict using Sophos CLEAN
Tue Feb 28 06:53:18 2017 Info: MID 481 antivirus negative
Tue Feb 28 06:53:18 2017 Info: MID 481 using engine: GRAYMAIL negative
'Tue Feb 28 06:53:18 2017 Info: MID 481 Message language: 'Chinese/Taiwan
Tue Feb 28 06:53:18 2017 Info: MID 481 Custom Log Entry: <=========Chinese/Taiwan Language
<=========Detected
Tue Feb 28 06:53:18 2017 Info: MID 481 Outbreak Filters: verdict negative
(Tue Feb 28 06:53:18 2017 Info: MID 481 quarantined to "Policy" (content filter:Chinese_text
Tue Feb 28 06:53:18 2017 Info: Message finished MID 481 done
```

المراجع

- توفر Microsoft أسماء مجموعات الأحرف (*اسم .NET*) في معرفات صفحات التعليمات البرمجية يمكن الإشارة إليه عند كتابة عوامل التصفية وتكوينها.

ملاحظة: يمكن أن تكون صفحات رموز ANSI مختلفة على أجهزة كمبيوتر مختلفة، أو يمكن تغييرها لكمبيوتر واحد، مما يؤدي إلى تلف البيانات. للحصول على أكثر النتائج تناسقا، يجب أن تستخدم التطبيقات Unicode، مثل UTF-8 أو UTF-16، بدلا من صفحة ترميز محددة.

- موزيلازين يقدم تفاصيل متعمقة لنوع المحتوى: الرأس، الحروف الأجنبية، الكلمات الأجنبية، والمزيد، في مقالهم ل بريد إلكتروني عشوائي بلغة أجنبية

معلومات ذات صلة

- هجمات التصيد الاحتيالي المتقدم للحرف المتجانس
- أدلة المستخدم النهائي لجهاز أمان البريد الإلكتروني من Cisco
- الدعم التقني والمستندات - Cisco Systems

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).