Cómo bloquear el tipo de contenido basó los juegos de caracteres

Contenido

Introducción

Este documento describe cómo escribir y configurar un filtro para detectar y tomar medidas en los juegos de caracteres basados tipo de contenido en el dispositivo de seguridad del correo electrónico de Cisco (ESA). El documento siguiente se puede utilizar para detectar los caracteres basados en el lenguaje no nativos considerados en los mensajes spam.

Antecedentes

Los administradores ESA pueden recibir una afluencia de los mensajes del correo que contienen los idiomas extranjeros basados carácter que no son correo legítimo para su compañía o dominios. Una manera de dirigir del ESA, tenemos tres opciones:

3. Escriba un filtro usando el lenguaje del mensaje de la condición. (Esta opción es una nueva función para la Seguridad 10.0.0-203 del correo electrónico de AsyncOS y más nuevo.)

Cómo bloquear el tipo de contenido basó los juegos de caracteres

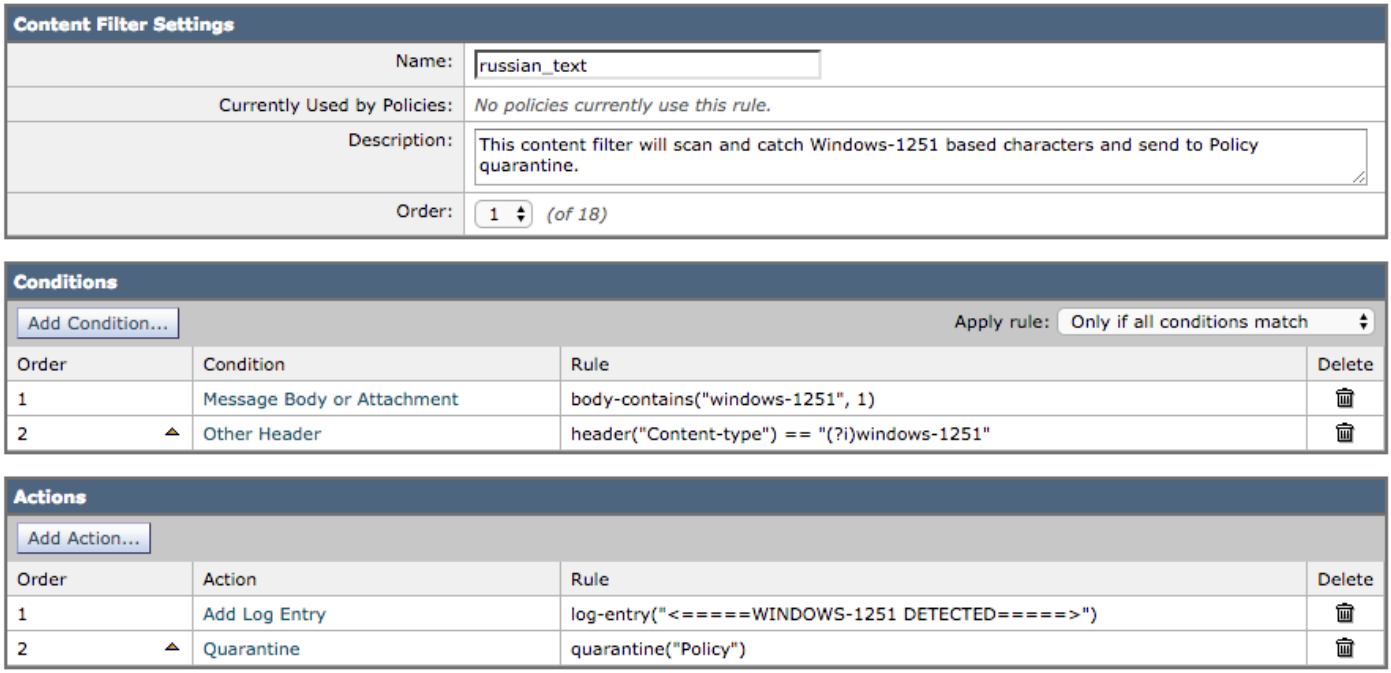
Escriba un filtro para detectar el tipo de contenido

La primera opción está para que el administrador escriba y configure un filtro, y lo asocia a una directiva del correo, según las necesidades.

> Nota: La escritura y configurar de este filtro como filtro del mensaje pueden ser recurso-costosas para analizar el cuerpo de los correos electrónicos para los juegos de caracteres.

Nota: Configurar esto como un filtro contento se sugiere fuertemente, como los filtros contentos ocurren después de la exploración del anti-Spam. Sin embargo, esto se puede escribir y configurar como filtro del mensaje, si es necesario.

El siguiente ejemplo tendrá en cuenta un mensaje del correo contiene los caracteres basados (cirílicos) rusos vía el juego de caracteres basado Windows-1251. Escrito como filtro contento:



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")	

El correo electrónico de la prueba usado contendrá el siguiente en el cuerpo del correo electrónico:

```
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.
```

Con el filtro del contenido configurado como arriba, los registros del correo registrarían similar al siguiente:

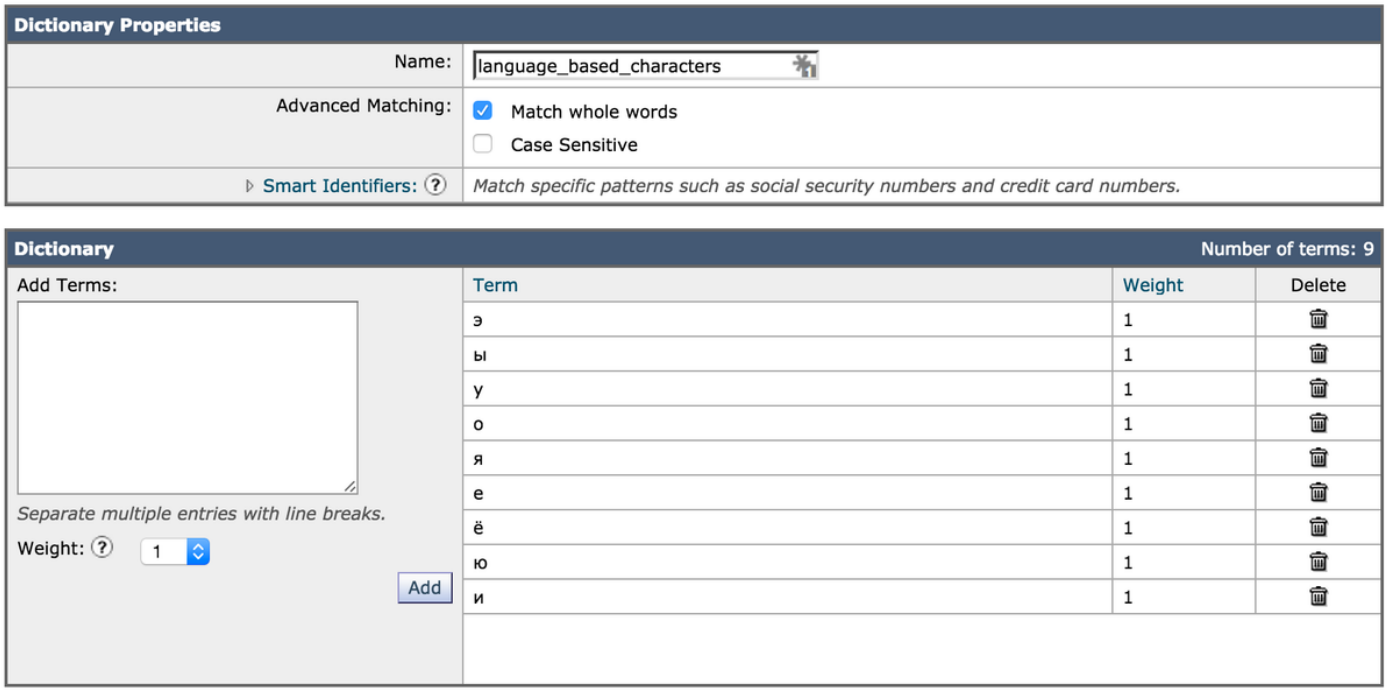
```
Thu Sep 10 14:50:09 2015 Info: Start MID 164993 ICID 266729
Thu Sep 10 14:50:09 2015 Info: MID 164993 ICID 266729 From: <end_user@test.com>
Thu Sep 10 14:50:09 2015 Info: MID 164993 ICID 266729 RID 0 To: <recpient@my_co.com>
Thu Sep 10 14:50:09 2015 Info: MID 164993 using engine: SPF Verdict Cache 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
```

Otros lenguajes y juegos de caracteres pueden ser utilizados. Vea por favor la sección de referencias para la información adicional.

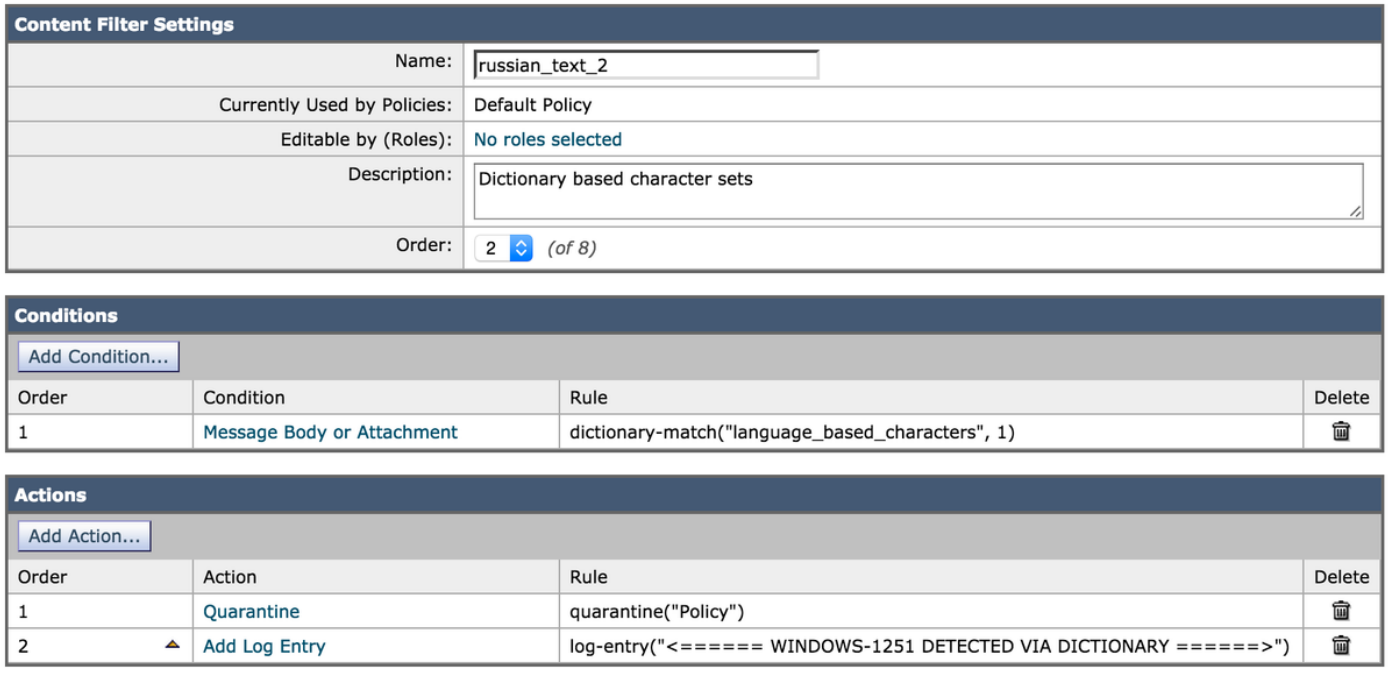
Escriba un filtro para referirse a un diccionario basado carácter

La segunda opción es agregar la lista de juegos de caracteres a un archivo de texto del diccionario y referir a eso en el filtro.

Ejemplo de agregar los caracteres al diccionario:



Los caracteres ahora se asignan al diccionario y el diccionario sí mismo se refiere a los elementos de la condición para el filtro:



Usando el mismo correo electrónico de la prueba que arriba, contiene el siguiente en el cuerpo del correo electrónico:

```
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.
```

Con el filtro del contenido configurado como arriba usando diccionario hace coincidir la condición, los registros del correo registrarían similar al siguiente:

```
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
```

Escriba un filtro contento usando “la condición del lenguaje del mensaje”

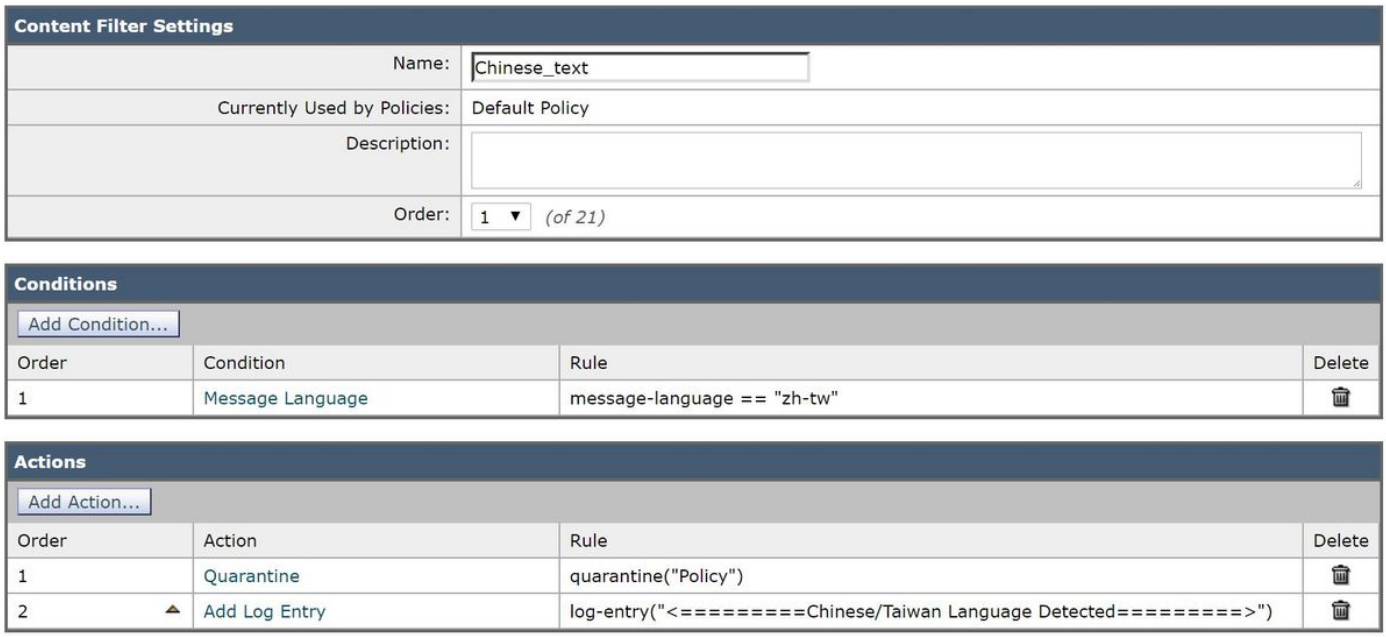
La tercera opción es utilizar “la condición del lenguaje del mensaje”. El ESA utiliza el motor incorporado de la detección del lenguaje para detectar el lenguaje en un mensaje. El dispositivo extrae el tema y al cuerpo del mensaje y lo pasa al motor de la detección del lenguaje.

El motor de la detección del lenguaje determina la probabilidad de cada lenguaje en el texto extraído y la devuelve a la aplicación. El dispositivo considera el lenguaje con la probabilidad más alta como el lenguaje del mensaje. El dispositivo considera el lenguaje del mensaje como “indeterminado” en uno de los escenarios siguientes:

- Si el lenguaje detectado no es soportado por el ESA
- Si el dispositivo no puede detectar el lenguaje del mensaje
- Si el tamaño total del texto extraído enviado al motor de la detección del lenguaje es menos de 50 bytes.

  Nota: Esta opción es una nueva función para la Seguridad 10.0.0-203 del correo electrónico de AsyncOS y más nuevo.

El siguiente ejemplo tendrá en cuenta un mensaje del correo que contenga el chino/el juego de caracteres basado Taiwán. Escrito como filtro contento:



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==========>")	

Con el filtro del contenido configurado como arriba, los registros del correo registrarían similar al siguiente:

```
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
```

Referencias

- Microsoft proporciona los nombres del juego de caracteres (*nombre del .NET*) en sus identificadores de la página de códigos que puedan ser referidos al escribir y configurando los filtros.

  Nota: Las páginas de códigos ANSI pueden ser diferentes en los equipos diferentes, o se pueden cambiar para un solo ordenador, llevando a la corrupción de datos. Para los resultados más constantes, las aplicaciones deben utilizar Unicode, tal como UTF-8 o UTF-16, en vez de una página de códigos específica.

- Mozillazine proporciona los detalles profundizados para el tipo de contenido: encabezado, cartas no nativas, palabras no nativas, y más, en su artículo para el Spam del idioma extranjero

Información Relacionada

- Homoglyph avanzó los ataques del phishing
- Guías del usuario final del dispositivo de seguridad del correo electrónico de Cisco
- Soporte Técnico y Documentación - Cisco Systems