INSTRUCTIVO DE CONFIGURACIÓN
McAfee Email Gateway 7.**x**

PREPARADO POR:
Pablo Schivo – Analista en Seguridad Informática
pschivo@ransecurity.com
RANSecurity

Buenos Aires, 2019

INSTRUCTIVO DE CONFIGURACIÓN
McAfee Email Gateway 7.**x**

Contenido

Resumen ejecutivo 2
Introducción 2-3
Descripción de tareas a realizar 3-3
Recomendaciones y observaciones 7

Resumen ejecutivo

Solución gestionada	Versión
McAfee Email Gateway	7.x

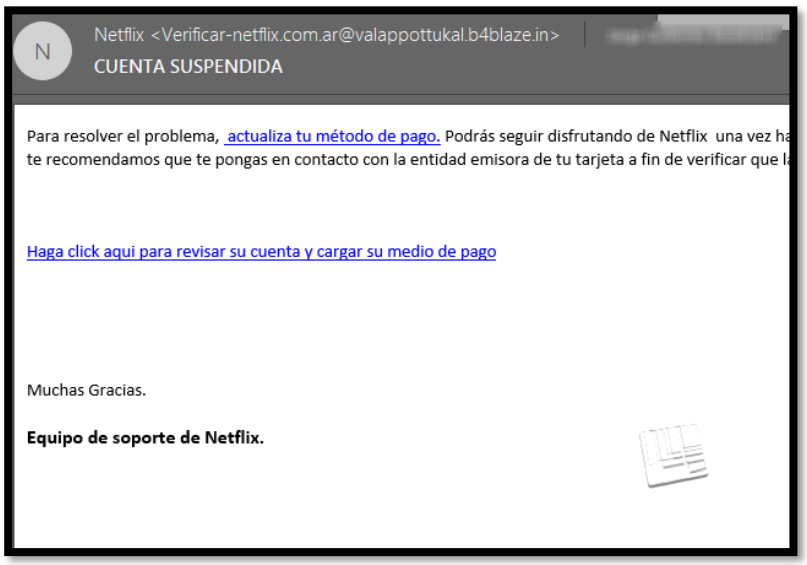
El presente instructivo tiene como objetivo la creación y configuración de reglas contra EMOTET para McAfee Email Gateway 7.x.

Introducción

EMOTET es un troyano polimórfico que es distribuído mediante campañas masivas de SPAM/Phishing y usualmente se camufla como un e-mail legítimo con adjuntos Word y/o PDF simulando ser una factura, notificación de pago, etc.

Para poder frenar este tipo de ataques, necesitamos entender qué información necesitamos obtener del **Header** de los mensajes. A continuación, veremos el header de una muestra del troyano en cuestión.

Así luce una muestra de EMOTET:



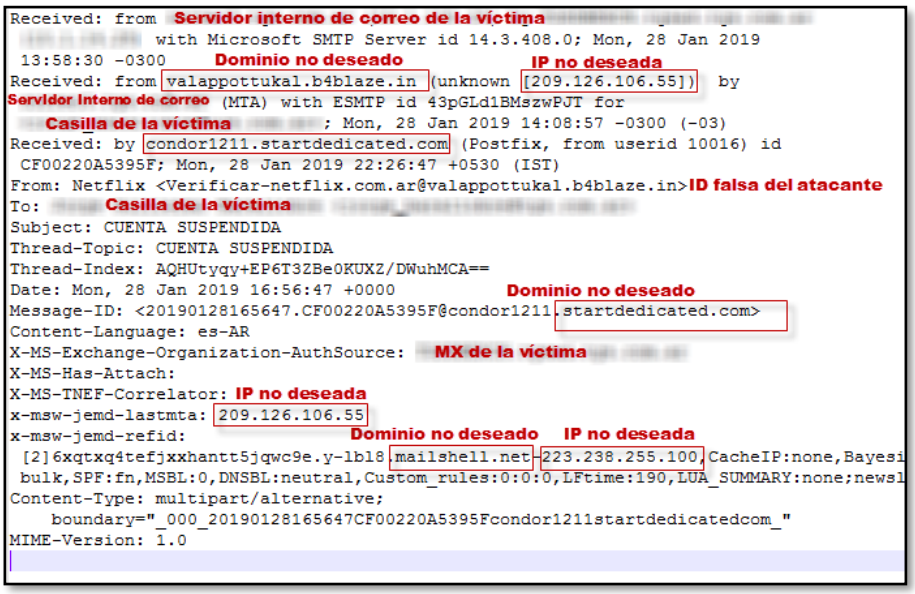
ARGENTINA
Rivadavia 877 Piso 5°
(C1002AAG) · CABA · Argentina
tel/fax (+54 11) 5353 9999

CHILE
San Sebastián 2812 Oficina 312
Las Condes · Santiago de Chile · Chile
tel/fax (+56 2) 3223 9532

PERÚ
Los Zorzales 160 Piso 3°
San Isidro · Lima · Perú
tel/fax (+51 1) 712 4764

www.ransecurity.com
expertos@ransecurity.com
LINKEDIN /RANSecurity
TWITTER @RANSecurityv

Así luce el **Header** de la muestra anterior:




```
Received: from
 with Microsoft SMTP Server id 14.3.408.0; Mon, 28 Jan 2019
 13:58:30 -0300
Received: from valappottukal.b4blaze.in (unknown [209.126.106.55]) by
 (MTA) with ESMTP id 43pGLd1BMszwPJT for
 ; Mon, 28 Jan 2019 14:08:57 -0300 (-03)
Received: by condor1211.startdedicated.com (Postfix, from userid 10016) id
 CF00220A5395F; Mon, 28 Jan 2019 22:26:47 +0530 (IST)
From: Netflix <Verificar-netflix.com.ar@valappottukal.b4blaze.in>
To:
Subject: CUENTA SUSPENDIDA
Thread-Topic: CUENTA SUSPENDIDA
Thread-Index: AQHUtyqy+EP6T3ZBe0KUXZ/DWuhMCA==
Date: Mon, 28 Jan 2019 16:56:47 +0000
Message-ID: <20190128165647.CF00220A5395F@condor1211.startdedicated.com>
Content-Language: es-AR
X-MS-Exchange-Organization-AuthSource:
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
x-msw-jemd-lastmta: 209.126.106.55
x-msw-jemd-refid:
 [2]6xqtxq4tefjxxhantt5jqwc9e.y-lb18.mailshell.net-223.238.255.100,CacheIP:none,Bayesi
 bulk,SPF:fn,MSBL:0,DNSBL:neutral,Custom_rules:0:0:0,LFtime:190,LUA_SUMMARY:none;newsl
Content-Type: multipart/alternative;
    boundary="_000_20190128165647CF00220A5395Fcondor1211startdedicatedcom_"
MIME-Version: 1.0
```

Nuestro objetivo es bloquear **todos los dominios y las IP que provienen de fuentes no confiables** luego de haber analizado el Header.

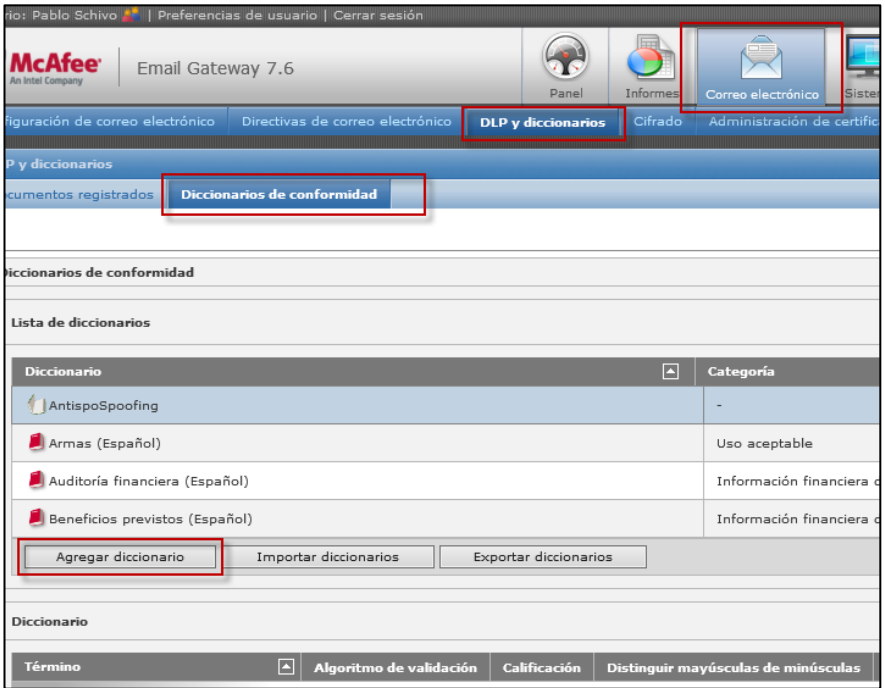
Nota: si usted no está seguro de lo que tiene que bloquear, por favor contactarse con el Soporte de RAN Security para su asistencia.

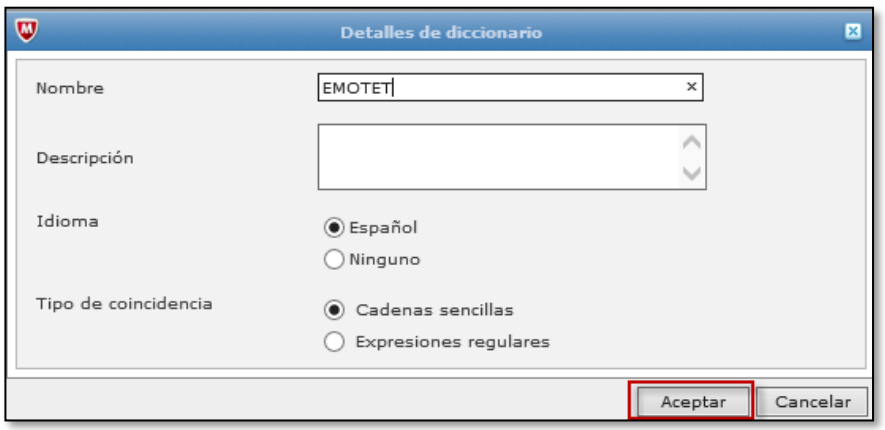
Descripción de las tareas a realizar

Usaremos a continuación como ejemplo los datos que obtuvimos del Header anteriormente analizado.

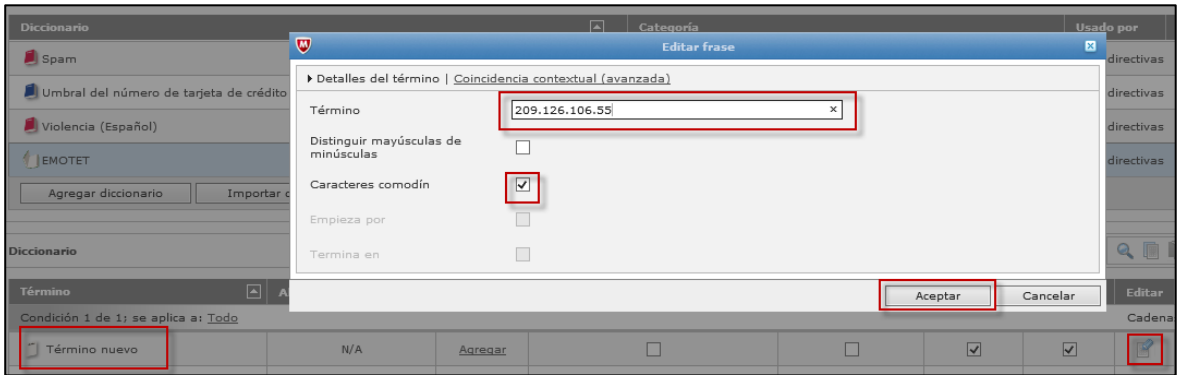
1) En primer lugar vamos a ingresar a la consola web del MEG con nuestras credenciales de administrador.

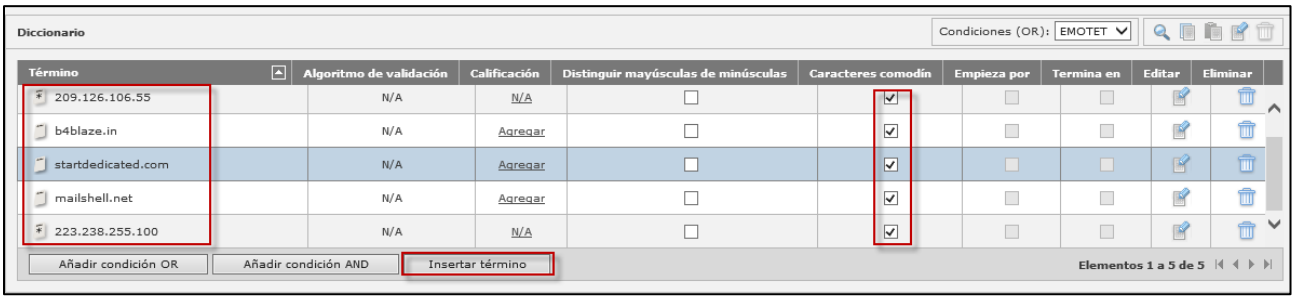
2) Vamos a proceder a crear un **Diccionario de Conformidad** para poder detectar patrones en el Header del correo que llamaremos **EMOTET**.

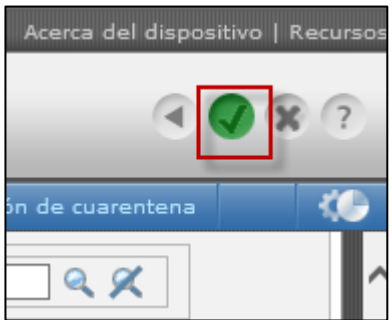




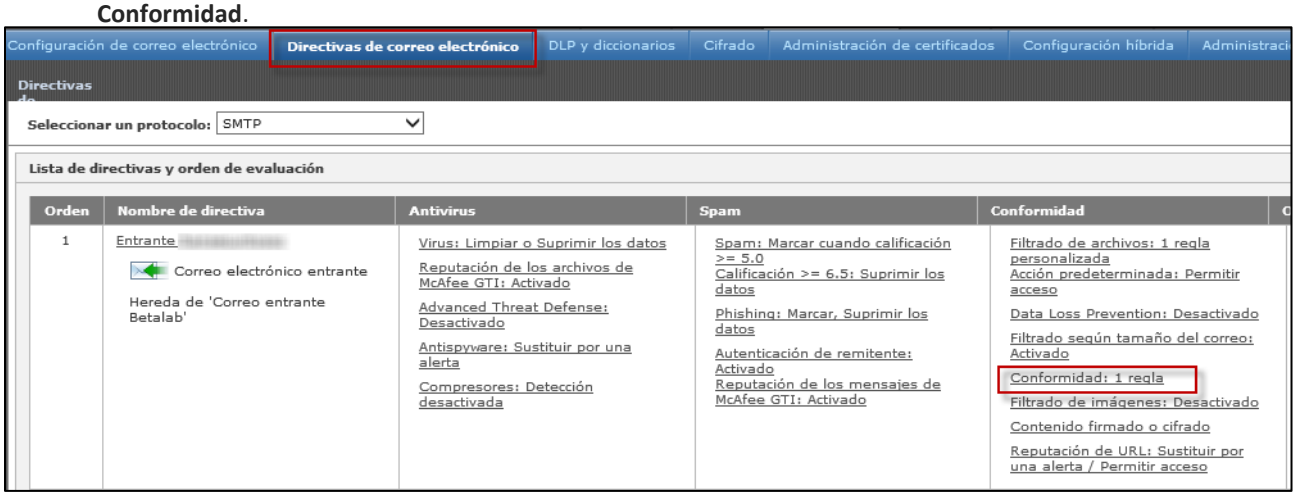
3) Editamos el **Término nuevo/Insertamos un nuevo término** y cargamos el primer valor que es la IP de donde se originó el mensaje y clickeamos en **Aceptar**. Repetiremos este paso con todas las IP y Dominios que deseamos bloquear. Guardamos los cambios clickeando el tilde verde.



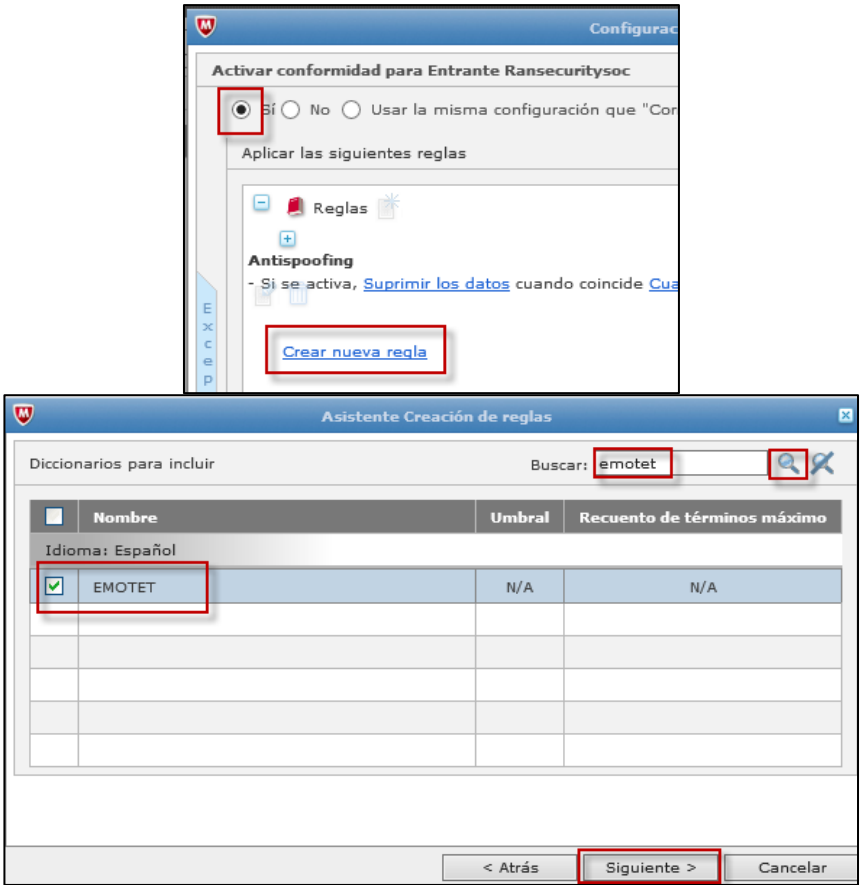




4) Una vez aplicados los cambios, editaremos nuestra regla principal de **Correo entrante** en la sección **Conformidad**.

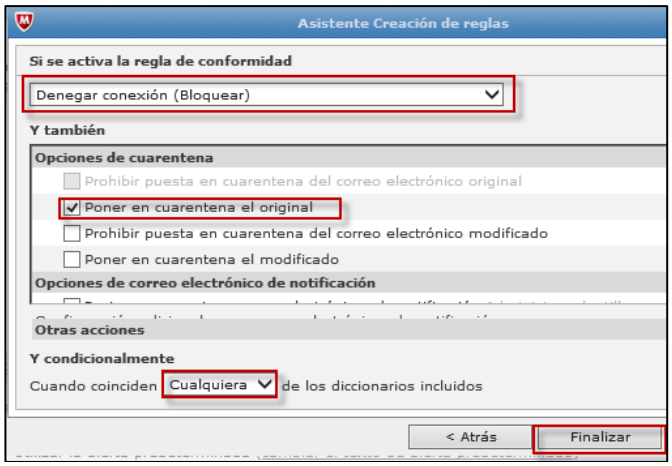


5) Creamos una nueva regla de Conformidad. La llamaremos **Detección EMOTET** y luego buscamos nuestro Diccionario creado anteriormente, llamado **EMOTET**. Clickeamos **Siguiente** dos veces.

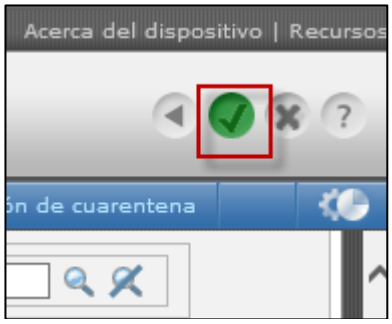


6

6) Le indicamos a la regla que deniegue la conexión, que ponga en cuarentena el mail original y que coincida con cualquiera de los diccionarios incluídos. Clickeamos en **Finalizar** y luego en **Aceptar**.



7) Guardamos los cambios clickeando el tilde verde.



Recomendaciones y observaciones

- Se recomienda que el Administrador de la plataforma Anti-Spam verifique en los próximos días la cuarentena para descartar que no haya falsos positivos.

ARGENTINA
Rivadavia 877 Piso 5º
(C1002AAG) · CABA · Argentina
tel/fax (+54 11) 5353 9999

CHILE
San Sebastián 2812 Oficina 312
Las Condes · Santiago de Chile · Chile
tel/fax (+56 2) 3223 9532

PERÚ
Los Zorzales 160 Piso 3º
San Isidro · Lima · Perú
tel/fax (+51 1) 712 4764

www.ransecurity.com
expertos@ransecurity.com
LINKEDIN /RANSecurity
TWITTER @RANSecurityv