

Una insidiosa red de bots spammers ataca a Charly

BOT ATTACK

Mientras realizaba sus tareas habituales, el colaborador de Linux Magazine, Charly Kühnast fue víctima de un malvado ataque. Su servidor antispam, ubicado como defensa ante su servidor de correo, le salvó de la avalancha de emails.

POR CHARLY KÜHNAST



Era un martes soleado de julio. Estaba tranquilamente escribiendo mi columna Sysadmin para Linux Magazine. Son las 2:00 pm cuando le hecho un vistazo al monitor que me ofrece la última información de la carga y el tráfico de datos de los servidores sensibles que administro. De buenas a primeras, la línea de la gráfica de rechazo del filtro de spam se disparó (véase la Figura 1). El artículo tendrá que esperar.

El servidor estaba rechazando grandes cantidades de correos en una etapa temprana del diálogo SMTP. Sospeché de una ola de spam con direcciones falsificadas. Eso no es nada nuevo, por cada email legítimo que recibo, tengo como mínimo dos mails de spam. Pero aún así decidí abrir una conexión SSH al filtro antispam, que se ejecuta en otra máquina, y no podía dar crédito cuando descubrí 140 conexiones SMTP paralelas. Eso es unas diez veces el nivel habitual. Y es raro que el servidor simplemente ignore las conexiones de esa manera.

La curiosidad saca lo mejor de mí mismo, y decidí echarle un vistazo al archivo de logs. Como me esperaba, cada mensaje provenía de una fuente distinta. Dos tercios de las direcciones IP pertenecían a proveedores de acceso de Europa, y el resto de EEUU y Brasil. Los ordenadores proporcionaban amablemente sus nombres en el mensaje HELO, y ni siquiera parecía que fuera spoofing, lo cual es realmente raro, ya que los HELOs falsificados son la norma en spam.

Los Atacantes son Víctimas

Lancé un nmap y escané algunos puertos. También ejecuté nmap con `—osscan-guess` para descubrir los sistemas operativos de las máquinas spammers. Lo que quería saber era si eran relays abiertos, máquinas secuestradas, servidores de correo mal configurados, servidores Web infectados o simplemente ordenadores de usuarios con troyanos. La respuesta de nmap fue clara: esta última opción. Las máquinas que investigué funcionaban todas bajo Windows XP, y nadie usa Windows XP como servidor Web o de correo. Acababa de conocer en mis carnes lo que es una red de bots.

Una red de bots es un grupo de máquinas independientes con una cosa en común: el malware que los ha infectado permite a un hacker controlarlos desde una ubicación remota. A los ordenadores de una red de bots se les denomina habitualmente leafbots o zombies. Considerado individualmente, un zombie no es demasiado dañino, pero juntos pueden convertirse en un arma peligrosa.

Afortunadamente la red de bots que me atacaba parecía tener apenas 200 máquinas.

Unas Palabras de Nuestros Patrocinadores

Aún no había podido volver a ponerme a terminar el artículo para Linux Magazine, pues los intervalos en los que llegaba el spam se estaban haciendo cada vez más cortos. Como había restringido el número de procesos SMTP simultáneos, existía el peligro de que los correos auténticos no entrasen debido a la falta de recursos para atenderlos. Le eché un vistazo a la carga del sistema: el filtro antispam aún tenía algo de margen. Eliminé el límite, y la red de bots pisó a fondo el acelerador: unos minutos más tarde ya tenía 580 conexiones SMTP simultáneas (véase la Figura 2).

De algún modo estos correos estaban superando mi graylist. El graylist le indica al servidor que rechaze un correo con un mensaje de error (*450 please try later*) y que acepte los correos al segundo intento.

Nótese que las redes de spam no tienen normalmente una cola para guardar correo no entregado temporalmente hasta un nuevo intento. Parece que el graylistening se ha convertido en algo tan común que los spammers han empezado a pensar en cómo saltárselo. El Listado 1 muestra el efecto que tuvo en mi sitio. La línea 1 del archivo de log muestra cómo un zombie se conecta a mi servidor. *greylist=update* en la línea 2 muestra al zombie intentándolo por segunda vez tras el rechazo inicial de mi servidor con un mensaje de error.

Verificación de la Dirección del Remitente

Volvamos al log: el remitente infinito es siempre el mismo, esto es, < >, remitente nulo. La ventaja de esta dirección de remitente para el spammer es que cualquier servidor de correo que cumpla el RFC lo aceptará. Y muchas medidas antispam que confían en verificar la dirección del remitente, como el SAV (Sender Address Verification), son inútiles si tenemos un remitente nulo.

Pero las direcciones de destinatario que enviaba la red de bots eran incluso más interesantes: ninguna existía, y todas ellas eran palabras de algún dialecto Coptico ya extinto, o más bien eran cadenas generadas aleatoriamente. Esto explica por qué el filtro antispam descartaba los correos antes de que el diálogo SMTP llegase a la fase del comando *DATA*. El filtro lleva a cabo el Recipient Address Verification, que es el complemento al SAV.

El Recipient Address Verification se basa en un sencillo principio: si el servidor de entrega cita la dirección de destinatario en *RCPT TO:*, el filtro antispam verifica primero a dónde tiene que llegar el correo, es decir, a mi servidor de correo (*mail.kuehnast.com* en la línea 3 del Listado 1). Abre un diálogo SMTP y verifica la respuesta a *RCPT TO:*. Esta es *user unknown* en el caso de los zombies. Esto causa que el filtro antispam finalice el diálogo (línea 4), lo que se refleja en la multitud de rechazos en la gráfica.

Ahora comenzaba a comprender por qué el filtro antispam estaba relativamente tranquilo, aunque tenía en marcha 500 procesos SMTP. Ninguno de estos procesos realmente conseguía entregar un correo, ya que el Recipient Address Verification los estaba bloqueando antes de esa etapa. Si hubiese alimentado a Spamassassin con estos correos antes de verificar la dirección de destino, el filtro antispam habría mordido el polvo debido al volumen de los correos entrantes. Mi consejo a los administradores de correo: el Recipient Address Verification hará tu vida algo más tranquila.

Interceptores

Decidí capturar algunos de los correos spam entrantes porque quería saber cuál era el mensaje que ese ejército de bots había intentado colar por mi filtro antispam. Me esperaban las sandeces de costumbre más algún troyano disfrazado como

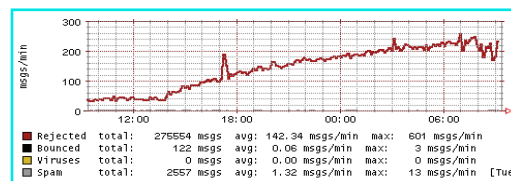


Figura 1: La línea de rechazo en la gráfica del filtro antispam se dispara de repente. Estaba siendo atacado por un ejército de spambots.

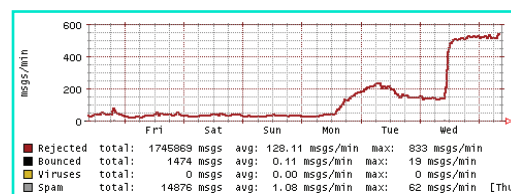


Figura 2: Tras eliminar el límite SMTP, los zombies intensificaron el ataque al servidor. *loadavg* marca 0.3 y todo está correcto.

GIF o PDF. O los habituales anuncios de ayudas para la erección, fiestas con drogas o aumentos de pecho (desafortunadamente, parece que nadie ha descubierto el tratamiento para las barrigas cerveceras). Pero lo que encontré fue simplemente un revoltijo de caracteres ASCII. O el spammer estaba intentando cabrearme o realmente no sabía lo que era MIME. Me imaginé que era esto último, e incluso estaba considerando pasar esa sopa de letras por un decodificador Base64. Pero, ¿necesitaba saber el precio del Viagra esa semana? Pensé que era mejor que me concentrara en el archivo de log y observar los correos que salen del filtro antispam. Siempre puedo terminar el artículo por la noche.

Listado 1: Extracto del Archivo de Log

```
01 May 12 04:16:07 spamfilter2
    postfix/smtpd[32629]: connect
    from
    hcm-ms-185.vnn.vn[203.162.4.185]
02
03 May 12 04:16:07 spamfilter2
    policyd: rcpt=598727,
    greylist=update,
    host=203.162.4.185
    (hcm-ms-185.vnn.vn),
04 from=<>,
    to=shaynsimo@kuehnast.com,
    size=5228
05
06 May 12 04:16:07 spamfilter2
    postfix/smtpd[29010]: NOQUEUE:
    reject: RCPT from
    hcm-ms-185.vnn.vn[203.162.4.185]
:
07 550 <shaynsimo@kuehnast.com>:
    Recipient address rejected:
    unverified address: host
    mail.kuehnast.com[80.190.243.62]
    said:
08 550 <shaynsimo@kuehnast.com>:no
    such user (in reply to RCPT TO
    command); from=<>
    to=<shaynsimo@kuehnast.com>
09 proto=ESMTP
    hello=HCM-MS-185.vnn.vn]
10
11 May 12 04:16:07 spamfilter2
    postfix/smtpd[32629]: disconnect
    from
    hcm-ms-185.vnn.vn[203.162.4.185]
```