

## Scans de la red

Aproximadamente 250 scans diarios son efectuados por los hackers sobre nuestra red. No podemos bloquearlos, pero podemos protegernos.

Existen diferentes scans que tienen por finalidad detectar diferentes fallos.

## Smtplib

```
Nov 2 08:06:40 ping postfix/smtpd4747: 5ED2B3BB3C: reject: RCPT from
102.50.233.64.transedge.com64.233.50.102: 554 <smtps1@cox.net>: Relay
access denied; from=<ejl@au.ru> to=<smtps1@cox.net> proto=ESMTP
helo=<Post.sk>
Nov 2 08:06:40 ping postfix/smtpd4745: 8727B3BB3F: reject: RCPT from
102.50.233.64.transedge.com64.233.50.102: 554 <smtps1@cox.net>: Relay
access denied; from=<grjg@orgio.net> to=<smtps1@cox.net> proto=ESMTP
helo=<mx2.mail.spray.net>
Nov 2 08:06:41 ping postfix/smtpd5029: 0169C3BB40: reject: RCPT from
102.50.233.64.transedge.com64.233.50.102: 554 <smtps1@cox.net>: Relay
access denied; from=<dnkldngl@terra.com.hn> to=<smtps1@cox.net>
proto=ESMTP helo=<Exit.de>
Nov 2 08:06:44 ping postfix/smtpd4747: DB5DB3BB3C: reject: RCPT from
102.50.233.64.transedge.com64.233.50.102: 554 <smtps1@cox.net>: Relay
access denied; from=<dfkdsnlkfn@chanteur.com> to=<smtps1@cox.net>
proto=ESMTP helo=<mail.ru.ru>
Nov 2 08:06:47 ping postfix/smtpd5029: 992C73BB3C: reject: RCPT from
102.50.233.64.transedge.com64.233.50.102: 554 <smtps1@cox.net>: Relay
access denied; from=<cvnlkjn@netposta.net> to=<smtps1@cox.net>
proto=ESMTP helo=<terra.com.pa>
Nov 2 08:06:53 ping postfix/smtpd4747: 1F0B03BB3C: reject: RCPT from
102.50.233.64.transedge.com64.233.50.102: 554 <smtps1@cox.net>: Relay
access denied; from=<lxknlvk@lycos.co.jp> to=<smtps1@cox.net> proto=ESMTP
helo=<mail.ru.ru>
```

Es un intento de envío de email por fuerza bruta desde un servidor smtp. El objetivo es comprobar si no hay fallos en lo que concierne a la opción de **relay** en el servidor smtp que permitan eventualmente enviar el spam.

## Web

Un ejemplo de scan de **fuerza bruta** de las diferentes url. Este scan tiene por objetivo encontrar los fallos de los diferentes scripts eventualmente alojados. Vemos rápidamente que se trata de scripts bajo windows. El hacker comprueba si los scripts están presentes. Si es el caso, se trata de una máquina bajo windows y que puede ser eventualmente hackeada. El error 404 nos muestra que el script no se encuentra en la máquina.

```
81.49.172.135 - - 02/Nov/2003:13:35:46 +0100 "GET
/_vtti_bin/owssvr.dll?UL=1&ACT=4&BUILD=2614&STRMVER=
4&CAPREQ=0 HTTP/1.1" 404 797 "-" "Mozilla/4.0 compatible; MSIE 6.0;
Windows
NT 5.1)"
81.49.172.135 - - 02/Nov/2003:13:35:46 +0100 "GET
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=2614&STRMVER=
4&CAPREQ=0 HTTP/1.1" 404 797 "-" "Mozilla/4.0 compatible; MSIE 6.0;
Windows
NT 5.1)"
81.49.172.135 - - 02/Nov/2003:13:35:47 +0100 "GET
/_vtti_bin/owssvr.dll?UL=1&ACT=4&BUILD=2614&STRMVER=
4&CAPREQ=0 HTTP/1.1" 404 797 "-" "Mozilla/4.0 compatible; MSIE 6.0;
Windows
NT 5.1)"
81.49.172.135 - - 02/Nov/2003:13:35:47 +0100 "GET
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=2614&STRMVER=
4&CAPREQ=0 HTTP/1.1" 404 797 "-" "Mozilla/4.0 compatible; MSIE 6.0;
```

Windows  
NT 5.1)"

El mismo tipo de scan sobre **formail.pl** y sus clones puede ser efectuado sobre los sitios. El objetivo es encontrar los scripts formail.pl sin protección que permiten a los spammers enviar el spam.