

Fighting Spammers With Honey pots: Part 2

Laurent Oudot 2003-11-26

[continued from [Part 1](#)]

Most of the time, a spammer connecting to the open proxy server will try to send an initial email in order to check how the proxy is working. This moment can be crucial if you want to fool him properly.

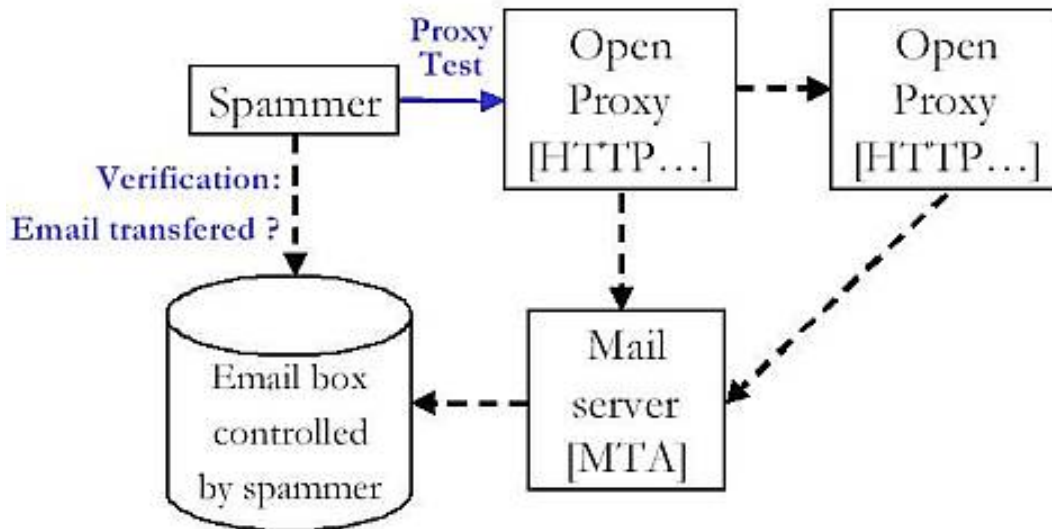


Figure 3: Phase one - spammer checks the open proxy

Here is an example of a TCP session from a spammer who connected to my fake Web proxy (port 8080). You will see that he tried to bounce to an SMTP server (CONNECT ?.:25) and then tried to send an email. The body of the mail is quite ridiculous because it tries to fool a potential recipient of the email by saying that it's for a meeting. Who could really think that such an email -- sent over a TCP session on a lost proxy server -- is a real one?

```

$ cat /var/log/snort/192.168.1.66/SESSION\ :8080-4087
CONNECT 204.2.aa.bb:25 HTTP/1.0

Helo Google.com
MAIL FROM:<RDaniels@zzzz.com>
RCPT TO:<rich003@xxxxx.com>
DATA
From: "Daniels" <Daniels@yyyyyy.com>
To: <rich003@xxxxx.com>
Subject: John want you to call Daniels.
Content-Type: text/plain;
      charset="Windows-1252"
Content-Transfer-Encoding: 7bit
  
```

```

Just wanted to remind you about our meeting at 1D9808AFD:8080:6 o'clock.Thanks,
Rodney

.
QUIT

```

The spammer probably used automatic tools to gather information on the Internet : D9808AFD (in hex) was the IP address of the fake temporary proxy, and 8080 was the TCP port. Proxypot proposes a tool to send a caught email like this: *deliverone*. With this tool, you can decide whether or not you want to send the email. It can be funny to send the test email of a spammer (check that this is not dangerous) because he will think that the proxy is really open.

When the spammer is sure he has good open proxies, he will try to reach open relays or a usual MTA, by bouncing through the open proxies. If he uses a chain of open proxies, and your fake open proxy is one of the links, you will even be able to guess other open proxies by looking at the TCP sessions. For example:

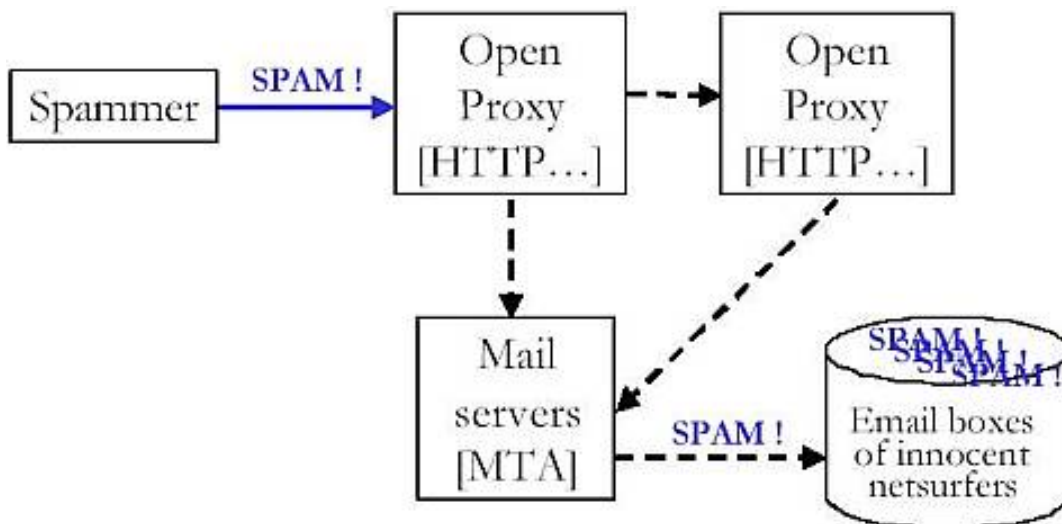


Figure 4: Phase two - Spam! Spam! Spam!

That's why the use of fake open proxies may help in detecting spammers, slowing spammers (by slowing down the network dialogs) and even blocking spammers (by simulating and avoiding the sending of real spam).

One of the funniest spam emails I blocked was destined to the honeynet project itself:

```

Return-Path: <wewqurjm9c@nm.ru>
Delivered-To: <project@honeynet.org>
Received: from xxxxxxxx.abo.wanadoo.fr ([213.248.aaa.bbb]) by gate
        with SMTP via SOCKS4 id "12816,1068543435,1"
        (attempted proxy to 66.93.112.231);
        Tue, 11 Nov 2003 10:37:17 +0100
From: =?koi8-r?B?9G9wx2/XwdEgzchSy8EgIk7PdsEi?= <wewqurjm9c@nm.ru>
To: ycgfdspwlcbtj <ycgfdspwlcbtj@honeynet.org>
Subject:=?koi8r?B?83nXZc51cM7B0SDQcG/E1cvDddEg0M8gY81l287ZzSDDZc7BzS4gICAg
ICAgICAgICAgICAgICAg?==?koi8r?B?ICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
AgICAgICAgICAgICAgICAgICAgICAgIMXB?==?koi8-r?B?x8XX1c/UIM/Pz9jczyDJ08rP?=
Date: Tue, 11 Nov 2003 12:40:02 +0400
Reply-To: wewqurjm9c@nm.ru
Mime-Version: 1.0
Content-Type: text/html; charset="koi8-r"
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-Priority: 3
X-MSMail-Priority: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
<html><head></head><body bgcolor=#ffffff>
<table width="98%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td align="center"><b><font size="2" face="Arial, Helvetica, sans-serif">
.: 177-82-09, 177-44-11, 778-15-25</font></b></p>
  <center>
    <p style="font:30px Arial"><font color=red><b><i>
"Nova"</i></b></font></p>
  (...)

```

2.3 Honey pots and open relays

We know that spammers try to find open relays to route bulk emails. Would it be so difficult to create a fake mail server? Definitely not; we'll discuss a couple of examples.

An interesting solution from Brad Spencer is to transform an unused sendmail daemon to fool spammers [[ref 11](#)]. This can be easily done by asking sendmail to accept relaying and to queue every email without ever sending one email out. This configuration offers a service that looks like a real open relay. Such a sendmail configuration may log and block incoming emails.

I tried this with sendmail 8.12.3-6.6 by reconfiguring the sendmail.mc file :

```
FEATURE(`promiscuous_relay')dnl
define(`confDELIVERY_MODE', `queue')
```

As explained by the author of this idea, you just need a running `sendmail -bd`. But be careful because some `sendmail` options can be forgotten (mail may be de-queued automatically because of MSP, etc).

An excellent way to verify the configuration of such a `sendmail` server is to use a free service that remotely checks if you are playing the role of a mail relay server. You should see their emails in the directory of queued messages.

```
$ /bin/cat /var/spool/mqueue/dfhAC1djJB008617
```

This is a test message to check for open mail relay servers.

You are probably receiving this message as the Postmaster of a mail server. We tried to relay a message through your mail server; because you are reading this message, your mail server probably did not relay the message, which is good.

If this message does not reach the recipient stated in the header, your mail server is not an open relay.

```
##
## RUN=2003111234316.2443
## HOST=80.13.a.b
## FROM=<>
## TO=
## REQ=
## KEY=b30628d6ff9c89c3910591add7476afe
##)
```

```
$ /bin/cat /var/spool/mqueue/qfhAC1djJB008617
```

V7

T1068601187

K0

G0

Y0

N0

P30092

Fbs

\$_Mail.TM.Odessa.UA [195.66.200.105]

```

$rESMTP
$localhost.localdomain
${daemon_flags}
${if_addr}192.168.1.66
S<>
rRFC822; spam@tm.odessa.ua
RPFID:<spam@tm.odessa.ua>
H?P?Return-Path: <g>
H??Received: from localhost.localdomain (Mail.TM.Odessa.UA [195.66.200.105])
    by gate.intranet (8.12.3/8.12.3/Debian-6.6) with ESMTP id hAC1djJB008617
    for <spam@tm.odessa.ua>; Wed, 12 Nov 2003 02:39:47 +0100
H?D?Date: Wed, 12 Nov 2003 02:39:47 +0100
H?M?Message-Id: <200311120139.hAC1djJB008617@gate.intranet>
H??To: <spam@tm.odessa.ua>
H??Subject: open relay test message
H??User-Agent: ortest (1.0)
.)

```

Of course, you may want to relay some specific emails, such as test emails used by spammers to check if you are a real open relay. This may be accomplished easily with: `sendmail -qRuser@destination`.

One other great solution is a daemon called Spamd [ref 12] coming from the OpenBSD team [ref 13]. Spamd is a tarpit (sometimes called *teergrub* which is originally a Deutsch word). This daemon simulates a sendmail-like server which rejects false mail. Used in conjunction with *pf* [ref 14], the goal is to waste the time and resources of the spam sender. If you have never checked out the Web page maintained by Daniel Hartmeier [ref 13], you definitely should.

Of course, Honeyd is another easy solution to create fake mail servers that simulate the relaying of spam. Now we will talk about architectures, with a great example of using Honeyd.

2.4 Architectures

If you look at the Web page titled *Honeyd Research: Spam* [ref 15] you will find a perfect way to use Honeyd in the tremendous struggle against spammers. Niels Provos will release more details in the near future about this research.

The following network diagram taken from *www.honeyd.org* shows the architecture proposed by Niels Provos. This is an excellent example of a real network with honeypot farms [ref 16].

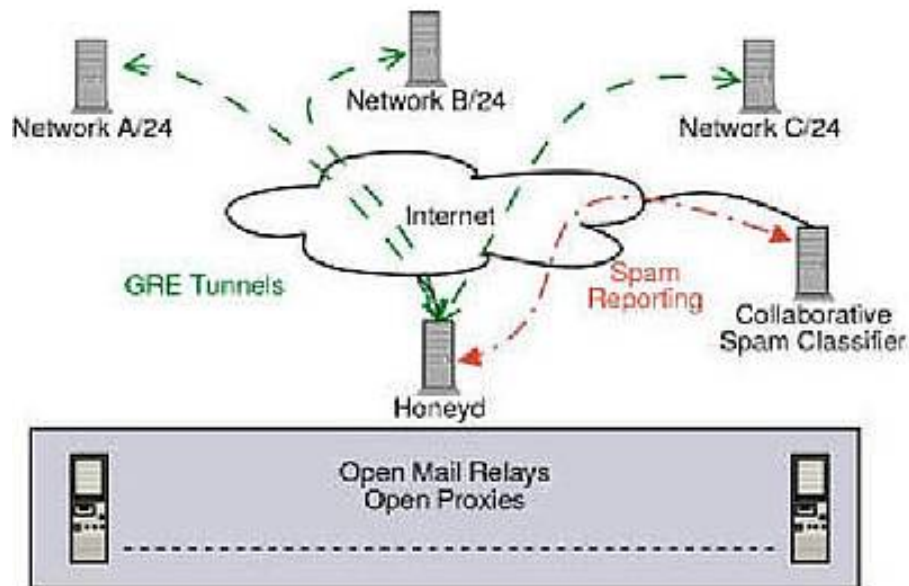


Figure 5: Honeyd farms proposed architecture for fake spam relays

Remote administrators working with Niels redirect ugly incoming spam traffic to one Honeyd daemon over GRE Tunnels (examples: redirecting unused IP addresses, or incoming TCP traffic to ports 25, 3128, etc which are not supposed to run those services). This daemon will then be able to simulate a fake proxy or a fake open relay, and will answer over the tunnel too. Honeyd is able to behave differently depending on the computer it simulates (IP Stack behavior, opened services, etc). In this case, a remote spammer attacking different sites will not realize that this is the same Honeyd daemon that replies to him, and he will not be able to understand where it is located (thanks to GRE).

The collected logs obtained on the Honeyd daemon -- that simulate multiple hosts with open relays and open proxies -- can be used to report spam abuses to official spam classifiers (for updating their blacklists). Therefore, this example of a successful architecture shows that there are ways to fight off spam on the Internet, owing to Honeyd.

2.5 Results

By using Proxypot on a single temporary DSL box, the French Honeyd Project received thousands of emails per day coming always from the same countries. On the Web site of Proxypot, you can also find a tool called *spamstat*. It may be used to generate statistics about spamming activities.

As a small example, during the weekend of November 8th and 9th, we caught 14,789 spam emails destined to 84,243 different users. Here is a sample taken from the logs :

```

/24 statistics:
213.248.57/24 sent 7571 messages
  total 44599919 bytes to 28680 recipients
212.46.2/24 sent 6616 messages
  total 72901704 bytes to 55862 recipients
213.148.180/24 sent 265 messages
  total 732527 bytes to 265 recipients
210.17.198/24 sent 166 messages
  total 255617 bytes to 830 recipients
207.69.200/24 sent 39 messages
14789 messages from 21 distinct /24s

Grand totals:
  14789 messages sent
  total 118773379 bytes to 85808 recipients
Report completed at Mon Nov 17 23:32:19 2003)

```

It's probably nothing compared to the huge amount of spam spreading around the cyber world, but what would happen if plenty of annoyed administrators decide to move and fight spammers with honeypots? The Internet would not be so safe and easy for spammers.

Another interesting result obtained by Niels Provos is the fingerprinting of hosts spreading spam. By using passive OS fingerprinting (included in next version of Honeyd, 0.7), he was able to guess that 43% of spammers used Linux boxes. Check the next figure coming from www.honeyd.org:

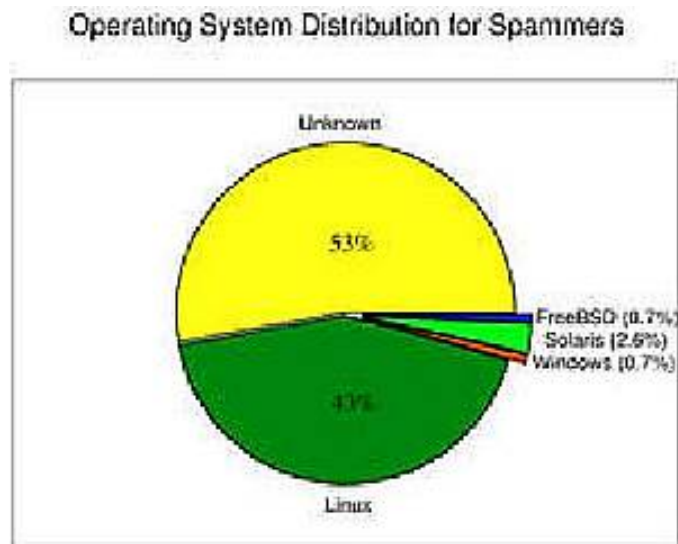


Figure 6: Operating system distribution for spammers

Another excellent chart shows that spammer activity has grown during the last few months, especially in October 2003 where many spam emails were caught.

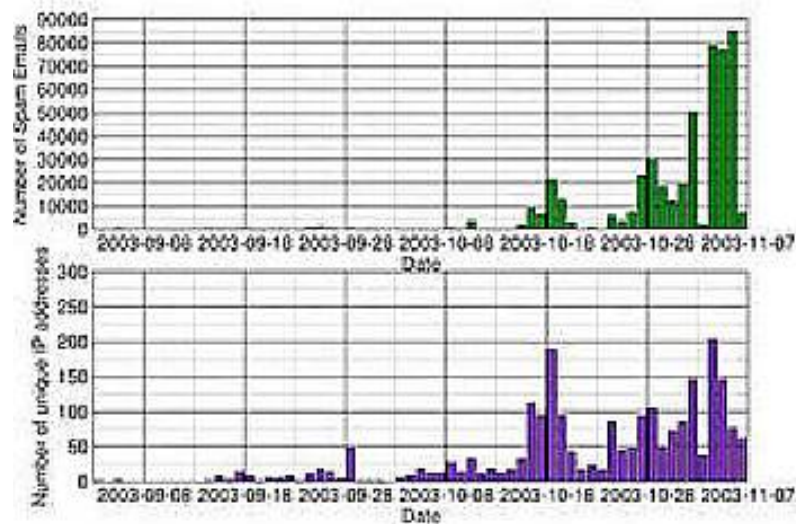


Figure 7: Spammer activity in recent months

These kind of results show that honeypots are valuable in the fight against spammers, though they should not be considered as the only solution.

3.0 Conclusion

This year, new mail threats have been discovered and spammers have started to use nasty new techniques.

At the beginning of November 2003, different versions of a worm called MiMail [ref 17] were launched, and some performed a Denial Of Service attack on Web servers that were dedicated to the fight against Spam. Those worms targeted the Web sites from spews.org, spamhaus.org and spamcop.net [ref 18].

By the end of October 2003, a new backdoor called Hogle (Proxy-Regate) [ref 19] was found. Its sole purpose is to infect Windows computers and to install a SMTP proxy service (running on TCP port 3355) that will be used by remote spammers. This example is not the only one, and this type of threat continues to grow very quickly (Kalshi, etc) [ref 20].

Should we consider this the end of the use of open proxies? Evil spammers spread worms all around the world to control millions of zombies hosts, and those hosts may be used to launch spam at anytime. It appears to be a dark future for netsurfers.

How valuable could honeypots be in this new kind of struggle? My previous article tried to explain what could be done to fight worms with honeypots [ref 21]. We could even imagine a new type of honeypots, active honeypots, that would be able to simulate an infected computer, claiming it is infected and waiting for remote orders. That would help us with understanding the new techniques and motivations used by this new kind of dark spammer.

This sounds like an unofficial cyber war. Even commercial tools are created by spammers to fight the honeypot makers [ref 22] in order to support their unwanted bulk mail activities.

To conclude this article on a more positive note, let's summarize. This paper explained how typical spammers work, as well as how honeypots could be used to detect spammers, slow spammers, or even block spammers. If people ask themselves if it is worth using honeypots and similar tools in the fight against spam, let's consider the alternative. Just look at the new worms used to attack legitimate anti-spam supporters -- they are the proof that spammers are annoyed by any attempt that defend against spam. The spammer's miscreant desire to attack legitimate organizations that defend the Internet appears to stem from their desire to make money at any cost.

Honeypots, toward a cleaner Internet.

Credits

Thanks to Niels Provos for his ideas and reviewing.

About the Author

[Laurent OUDOT](#) is a computer security engineer employed by the Commissariat a l'Energie Atomique in France. On his spare time, he is a member of the team [Rstack](#) with other security addicts. Concerning honeypots, Laurent is an active member of the [French Honeynet Project](#) which is part of the [Honeynet Alliance](#).

View [more articles by Laurent Oudot](#) on SecurityFocus.

References for Page 2

[ref 11] Brad Spencer, [Sendmail used as a honeypot](#)

[ref 12] [Spamd Daemon from OpenBSD](#)

[ref 13] Daniel Hartmeier, [Annoying spammers with pf and spamd](#)

[ref 14] [pf is the firewall brick that appeared starting with OpenBSD 3.0](#)

[ref 15] [Honeyd Research about Spam](#)

[ref 16] Lance Spitzner, [Honeypot Farms](#), 2003

[ref 17] Norton Anti-Virus, [MiMail.F version](#)

[ref 18] [SpamHaus attacked by a worm](#)

[ref 19] Norton Anti-Virus, [Hogle Backdoor](#)

[ref 20] Norton Anti-Virus, [Trojan.Kalshi](#)

[ref 21] [Fighting Worms with Honeypots](#), Laurent Oudot, October 2003

[ref 22] [Honeypot Hunter](#), this tool first seen on the [honeypots mailing list](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus