Тимирясова Элина

Борьба со спаммерами с помощью honeypots.

В наши дни актуальной проблемой стали груды писем с коммерческой рекламой каждый день рассылаемые неутомимыми ребятами - спаммерами. Как показывают социологические исследования, каждое утро офисные работники вынуждены просматривать сотни ненужных писем, так как до сих пор не существует надежных фильтров. Это занимает рабочее время и, кроме того, очень раздражает. В данном докладе я хочу представить способ борьбы со спаммерами с помощью технологии honeypots.

Узнаем противника.

Рассмотрим подробнее, за что спаммер получает деньги. Для успешной рекламной деятельности в сети посредством массовой электронной рассылки необходимо:

- **накопить базу данных работающих электронных адресов;**
- **найти анонимные прокси - серверы для безнаказанной рассылки тысяч писем;**
- **иметь доступ к серверу, который позволяет отправлять массу электронного мусора;**

Кроме того, для рассылки спама используются взломанные компьютеры и серверы. Но в данной статье я не буду рассматривать методы защиты от хакеров с помощью honeypot, так как это очень обширная тема и по ней существует уже множество публикаций.

Наиболее простые способы получить базу данных e-mail адресов жертв: во-первых, используя автоматические программы, просматривающие Web-страницы в поисках адреса автора. Во-вторых, просто написать программу, которая будет вытаскивать адреса из заголовков писем, посылаемых в UseNet. И, наконец, недостаточно хорошо настроенные легальные рассылки могут снабдить злоумышленника полной базой электронных адресов.

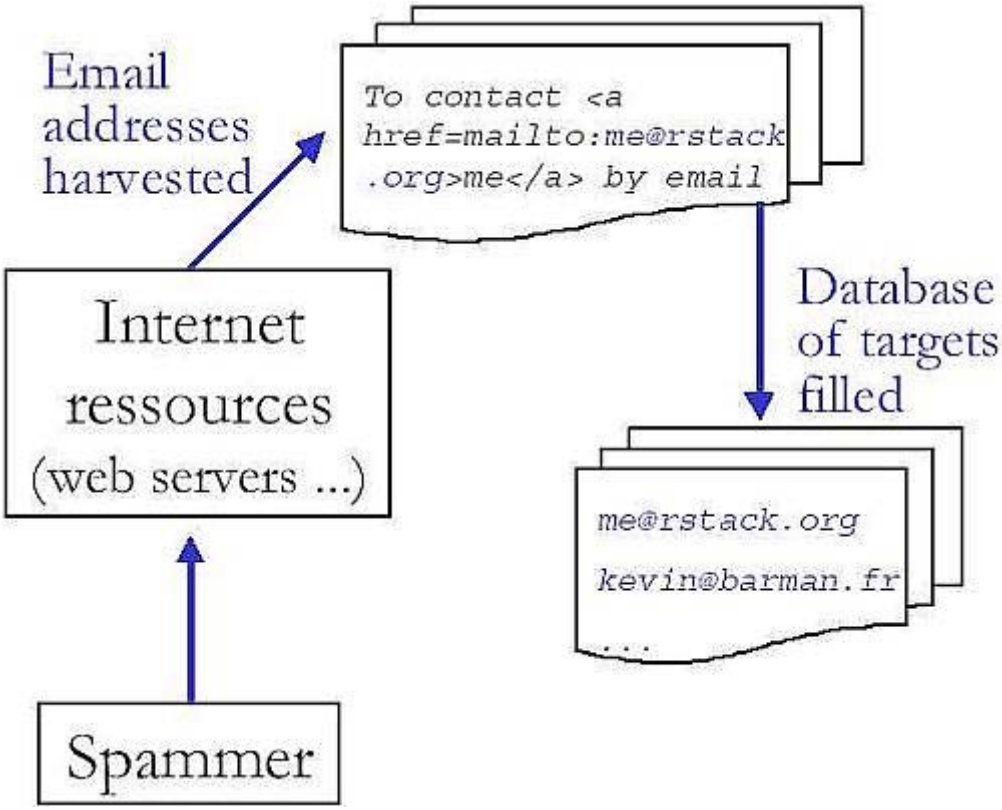
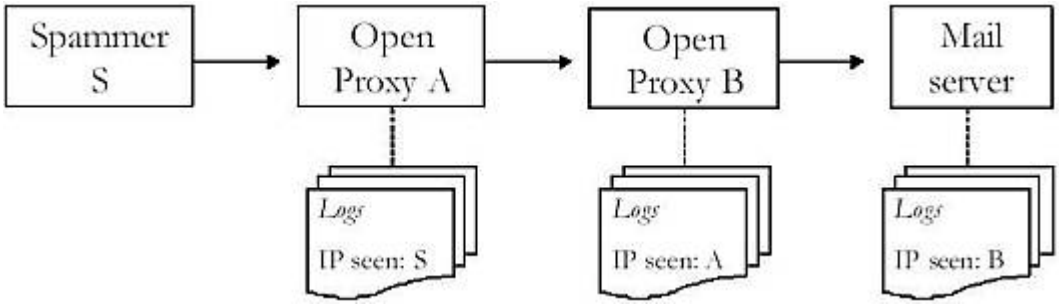


Рисунок 1. Ссылка с интернет страницы на адрес автора.

Для того чтобы оставаться безнаказанными при соединении с удаленным почтовым сервером спаммеры используют общедоступные прокси - серверы(open proxy). Во всех журналах на mail -сервере остается только IP адрес прокси – сервера и выследить источник рассылки становится почти невозможно, так как большинство прокси – серверов не ведут журналов соединений. Далее представлен пример TCP сессии клиента, использующего прокси, и SMTP:

```
$ cat /var/log/snort/192.168.1.66/SESSION\:8080-4072
CONNECT 207.69.200.120:25 HTTP/1.0

HELO [217.128.a.b]
MAIL FROM:<openrelay@abuse.earthlink.net>
RCPT TO:<spaminator@abuse.earthlink.net>
DATA
Message-ID: <36af800461754252ab1107386a9cd8eb@openrelay@abuse.earthlink.net>
To: <spaminator@abuse.earthlink.net>
Subject: Open HTTP CONNECT Proxy
X-Mailer: Proxycheck v0.45

This is a test of third-party relay by open proxy.

These tests are conducted by the EarthLink Abuse Department.
EarthLink, by policy, blocks such systems as they are discovered.

Proxycheck-Type: http
Proxycheck-Address: 217.128.a.b

36af800461754252ab1107386a9cd8eb

Proxycheck-Port: 8080
Proxycheck-Protocol: HTTP CONNECT

This test was performed with the proxycheck program. For further
information see <http://www.corpit.ru/mjt/proxycheck.html/>

.
QUIT
```

Но так как спаммеры должны быть осторожны, для уверенности в собственной безопасности они используют несколько прокси – серверов, но при этом увеличивается задержка:



И, наконец, на последнем шаге рекламные агенты используют, так называемые, open relays, то есть почтовые серверы, которые передают электронные письма, не относящиеся к их локальным пользователям. Обычно это происходит из-за неправильной конфигурации почтового сервера, и активно используется злоумышленниками.

Honeypots.

Новая и интересная технология honeypot или система - приманка позволит нам нанести существенный удар по деятельности назойливых распространителей рекламы. Так как система-приманка гибкое и простое орудие, его можно использовать для борьбы на всех этапах деятельности спаммеров.

При накоплении базы своих жертв основной целью спаммера является отыскать как можно больше действующих e-mail адресов, так как эффективность рекламы прямо пропорциональна количеству ее получателей. Мы же постараемся подсунуть автоматическим программам, сканирующим Web-страницы, как можно больше фиктивных адресов. Обычно такая программа следует по всем ссылкам, найденным на web-странице, поэтому легко подсунуть ей ложные ссылки на страницы – приманки, генерирующие тонны ложных электронных адресов. Такие ссылки можно сделать невидимыми для человека (например, белые буквы на белом фоне или

ссылка, спрятанная за надпись), однако программа-бот не сможет распознать подмены. Примеры подобных скриптов уже существуют и активно используются. Но можно поступить еще более хитро и генерировать не случайные e-mail адреса, а включающие в себя информацию о распространителе. И как только неосмотрительный спаммер воспользуется подобным адресом для рассылки, его IP станет известным.

```
<?
// PHP example taken from the frenchhoneynet Web site
// replace by your domain, add recipients filtering on your MTA
(mimedefang...)
echo '<a href="mailto:'.$REMOTE_ADDR.'_'.date('y-m-j').'-
spamming@frenchhoneynet.org"
title="There is no spoon">For stupid spambots';
?>
```

Такой скрипт будет генерировать фиктивный электронный адрес, содержащий IP web – клиента и текущую дату. Например:

```
<a href=mailto:80.13.aa.bb_03-11-17-spamming@frenchhoneynet.org>...
```

Затем администратор mail – сервера может фильтровать входящие письма и извлекать из них IP адреса попавшихся на уловку источников спама.

```
# Example of a simple recipient filtering with Mimedefang
http://www.mimedefang.org/]
# Will filter incoming email containing a recipient address in the form
# of those created by the latter PHP example.
sub filter_recipient {
        my ($recipient, $sender, $ip, $hostname, $first, $helo) = @_;
        if($recipient =~ /^<.*-spamming@frenchhoneynet\.org>?$/i)
        { return ("REJECT", "Spamming activity"); }
        return ("CONTINUE", "ok");
}
```

Следует, конечно, отметить, что подобный трюк пройдет только с простыми программами. В то время как профессиональные спаммеры не пострадают.

Рассмотрим теперь прокси – серверы, которые являются прикрытиями для назойливых распространителей рекламы. Как нетрудно догадаться, можно обмануть спаммера, настроив honeypot как фальшивый прокси сервер.

Итак, рассмотрим, как это сделать. Интересные для злоумышленника порты:

- **1080 socks proxy server**
- **3128 squid proxy server**
- **8080 web caching service**

Найти открытые прокси серверы очень легко. Достаточно набрать в любом поисковике “open proxies List”. Затем, после подсоединения к TCP порту, отправка нескольких пакетов может помочь понять, является ли найденный ресурс открытым прокси сервером или нет.

Что, если попробовать установить honeypot, который будет отвечать на входящие запросы? Вероятно, мы сможем обмануть некоторых спаммеров.

Для этой цели можно использовать Honeyd, как наиболее универсальное и удобное OpenSource решение, разработанное Нильсом Провосом(Niels Provos). Такая приманка может не только эмулировать какой-то сервис, но и целую операционную систему. То есть злоумышленник будет видеть машину как Cisco роутер, WinXP веб-сервер или Linux DNS сервер, где эмулирование ведется не только на уровне сервиса. Так как в этом случае определить настоящую операционную систему машины было бы достаточно просто с помощью печатей fingerprints. Honeyd позволяет эмулировать операционную систему на уровне ядра, то есть изменяет поведение стека IP протокола. И тогда на запросы таких утилит как Nmap или Xprobe приманка генерирует ответы, соответствующие фальсифицируемой операционной системе.

Рассмотрим конфигурирование системы-приманки на основе Honeyd. Настроим его на симулирование почтового сервера, пересылающего любые письма и поддерживающего открытые прокси:

```
create relay
set relay personality "OpenBSD 2.9-stable"
add relay tcp port 25 "sh /usr/local/share/honeyd/scripts/sendmail.sh $ipsrc
$sport $ipdst $dport"
add relay tcp port 3128 "sh /usr/local/share/honeyd/scripts/squid.sh $ipsrc
$sport $ipdst $dport"
add relay tcp port 8080 "sh /usr/local/share/honeyd/scripts/proxy.sh $ipsrc
$sport $ipdst $dport"
set relay default tcp action block
set relay default udp action block
bind 192.168.1.66 relay
```

Легко понять, что такая приманка будет вести себя как компьютер с операционной системой OpenBSD 2.9, IP адресом 192.168.1.66 и тремя открытыми портами: 25, 128, 8080. На любой входящий запрос по данным портам система будет фальсифицировать соответствующий сервис: sendmail.sh, squid.sh, proxy.sh. Взаимодействие ведется через два потока STDIN и STDOUT. Если интересно посмотреть, что же пытается разослать спаммер, достаточно просто читать данные с потока STDIN. Для обмана необходимо симулировать часть или весь диалог с подключившимся пользователем.

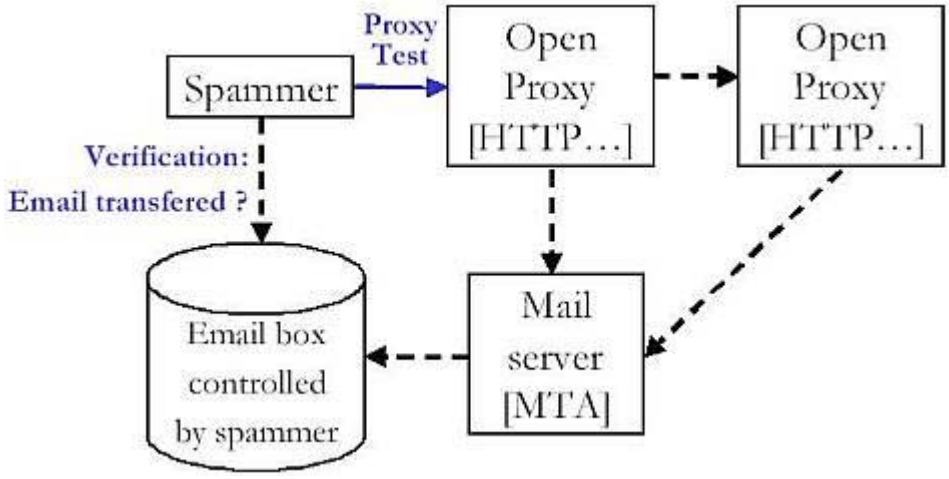
Но для данной цели можно использовать и другой маленький и удобный honeypot, созданный специально для симулирования открытого прокси - сервера, - это Bubblegum Proxypot. Возможности данной приманки этим и ограничиваются, в отличие от Honeyd, который может использоваться для фальсификации большого множества различных сервисов и оперативных систем.

После установления соединения с открытым прокси некоторые спаммеры просто проверяют, является ли он действительно открытым, в то время как другие, более продвинутые, так же проверяют правильную работу прокси. Время для спаммера - критический показатель, поэтому он не хочет тратить его впустую.

В Proxypot существует три режима работы:

- **smtp1:** Вся сессия SMTP – соединения симулируется.
  Плюсы: нет никакого исходящего SMTP трафика, поэтому ваша сеть не засоряется;
  Минусы: такая приманка легко распознается и, кроме того, можно выбрать только один вид SMTP сервера;
- **smtp2:** Соединяется с реальным SMTP сервером и читает его идентификационную строку и HELP команды для адекватного ответа на входящие запросы.
  Плюсы: если спаммер отслеживает корректность ответов сервера, то в этом случае он ничего не заподозрит;
  Минусы: появляется исходящий трафик. Нужно быть более осторожным, применять дополнительную защиту от взлома. К тому же, если отслеживать трафик, проходящий через SMTP и почтовый сервер, на который идет рассылка, то легко можно заметить несоответствие и распознать honeypot.
- **smtp3:** Соединяется с реальным SMTP сервером и пересылает все команды за исключением DATA, EXPN. RCPT и VRFY контролируются и пересылаются ограниченно.
  Плюсы: эта симуляция является наиболее правдоподобной, и сделать лучше honeypot невозможно, так как иначе он станет действующим открытым прокси сервером.
  Минусы: остается вероятность, что опытный спаммер распознает подлог.

В большинстве случаев спаммер сначала попытается проверить корректность работы открытого прокси сервера и на этом этапе очень важно правильно отвечать на приходящие запросы. Ниже приводится примерная схема такой проверки:

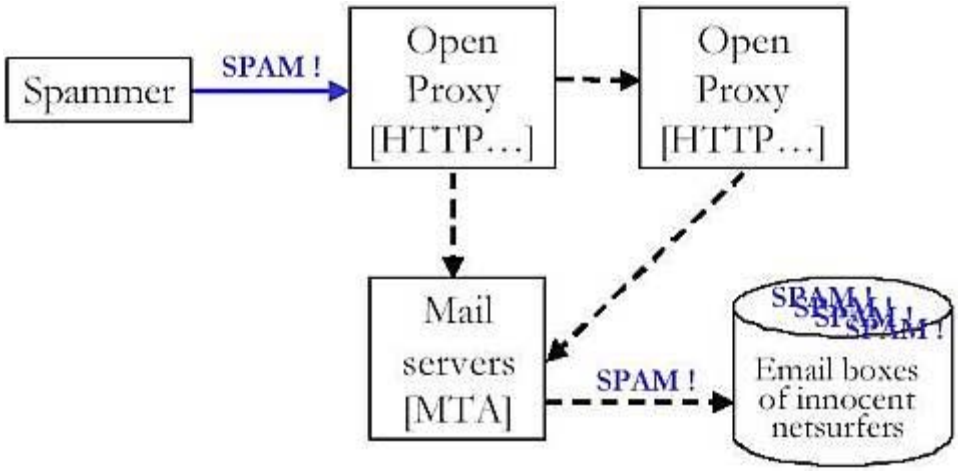


Рассмотрим пример сессии злоумышленника и системы – приманки, симулирующей Web-proxy (порт 8080) .

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

Hello Google.com
MAIL FROM:<RDaniels@zzzz.com>
RCPT TO:<rich003@xxxxx.com>
DATA
From: "Daniels" <Daniels@yyyyyy.com>
To: <rich003@xxxxx.com>
Subject: John wants 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
```

Мы видим соединение с 25 портом SMTP – сервера и попытку отправить письмо с достаточно бессмысленным содержанием. Можно предположить, что в данном случае используется какая – то программа для автоматической проверки, поэтому в тексте письма указывается в 16 – тиричном формате IP проверяемого прокси - сервера и порт 8080. В Proxypot существует возможность отправлять или не отправлять подобные одиночные письма. Если вы пропустите такое письмо, то спаммер будет думать что нашел реальный открытый прокси – сервер.

Теперь, когда он относительно уверен в том, что нашел нужный сервис, он попытается установить соединение с почтовым сервером для пересылки тонны мусора в наши ящики. Он может использовать один или цепочку открытых прокси - серверов.



На этом этапе мы можем обнаружить потенциального источника спама, затормозить его работу или же вовсе заблокировать (симулируя отправку мусора).

Теперь можно рассмотреть конфигурацию honeypot, фальсифицирующего почтовый сервер для пересылки большого количества писем. Бред Спенсер(Bred Spencer) первый предложил использовать для этого настоящий почтовый сервис. Нужно только настроить его на прием входящего трафика и блокировку исходящего. Симуляция получается очень реальной, и поэтому нет необходимости использовать какое - то дополнительное программное обеспечение. Пример конфигурации сервиса sendmail 8.12.3-6.6 в sendmail.mc файле:

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

Автор идеи предлагает теперь просто запустить sendmail –bd, однако следует быть осторожным, так как некоторые неучтенные опции сервиса могут быть использованы злоумышленником. Для надежности можно использовать удаленный сервис, который будет периодически проверять состояние sendmail – сервера. Так как все отправленные с этого сервера письма должны находиться в папке с заблокированными сообщениями. Сообщения могут быть подобного вида:

```
$ /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=<SPAM@TM.ODESSA.UA>
## REQ=
## KEY=b30628d6ff9c89c3910591add7476afe
##)
```

```
$ /bin/cat /var/spool/mqueue/qfhAC1djjB008617
V7
T1068601187
K0
G0
Y0
N0
```

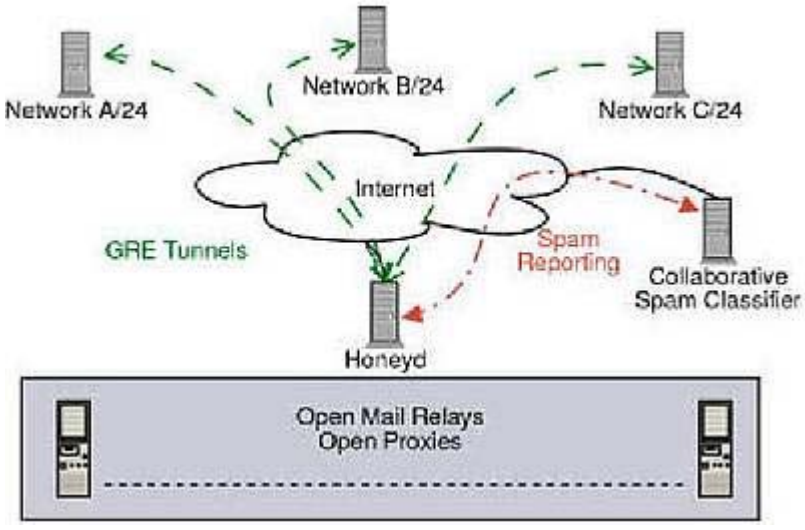
```
P30092
Fbs
$_Mail.TM.Odessa.UA [195.66.200.105]
$rESMTP
$slocalhost.localdomain
${daemon_flags}
${if_addr}192.168.1.66
S<>
rRFC822; spam@tm.odessa.ua
RPFD:<spam@tm.odessa.ua>
H?P?Return-Path: <g>
H??Received: from localhost.localdomain (Mail.TM.Odessa.UA [195.66.200.105])
        by gate.intranet (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)
.)
```

Стоит отметить, что для правдоподобности нужно пропускать тестовые сообщения спаммера, что нетрудно реализовать, например, таким способом: -qRuser@destination.

Другим решением может стать honeypot, называемый Spamd и разработанный командой OpenBSD, или Honeyd. Задача любой такой приманки – заставит спаммера бессмысленно тратить свое время и ресурсы.

Исследования в области борьбы со спамом.

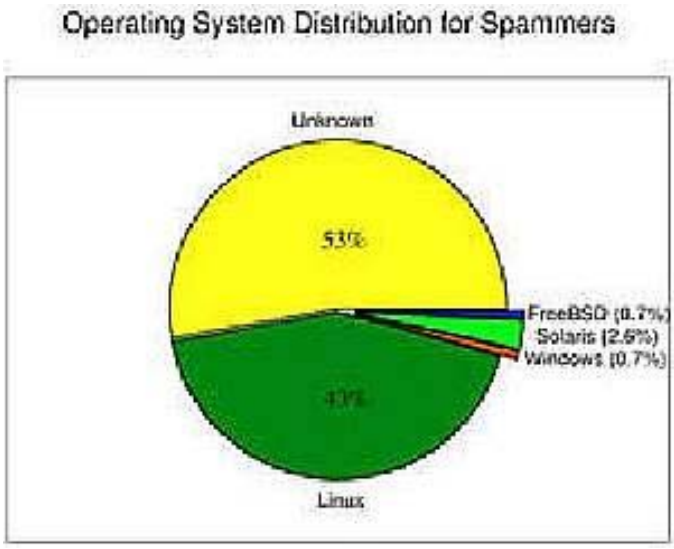
В настоящее время ведутся обширные исследования в области борьбы со спамом. Один из них является “Honeyd Research:Spam” под руководством Нильса Провоса (Niels Provos). В рамках данного проекта строится сеть как показано на рисунке:



Администраторы удаленных сетей, сотрудничающие с Нильсом, пере направляют опасный трафик на один сервер-приманку с установленным Honeyd по GRE Tunnels. Этот сервис затем симулирует прокси или почтовый сервер и отвечает тоже по GRE каналу. Honeyd может вести себя по – разному, в зависимости от сервиса, который он симулирует. В этом случае злоумышленник, атакующий различные сайты не подозревает о том, что на все его запросы отвечает один и тот же Honeyd. И благодаря GRE каналам он не сможет распознать реальное местоположение сервера.

Собранная таким образом информация может использоваться для составления черных списков спаммеров.

Так же получена интересная статистика относительно источников рассылки рекламы. Например, около 43% спаммеров используют оперативную систему Linux:



В заключение, стоит отметить, что борьба со спаммерами активно ведется в последнее время различными методами. И пока ни один способ не может полностью защитить нас от назойливых рекламных писем. Однако технология honeypot вместе с другими техниками может помочь сократить их количество. Эффективность использования приманок уже доказана на практике и будет распространяться в будущем.

Использованы картинки:

1. **Fighting Spammers With Honeypots: Part 1**
   by Laurent Oudot
   < http://www.securityfocus.com/infocus/1747 >
2. **Fighting Spammers With Honeypots: Part 2**
   by Laurent Oudot
   < http://www.securityfocus.com/infocus/1748 >

Использованная литература:

1. **Fighting Spammers With Honeypots: Part 1**
   by Laurent Oudot
   < http://www.securityfocus.com/infocus/1747 >
2. **Fighting Spammers With Honeypots: Part 2**
   by Laurent Oudot
   < http://www.securityfocus.com/infocus/1748 >
3. **Brad Spencer, Sendmail used as a honeypot**
   http://www.tracking-hackers.com/solutions/sendmail.html
4. **Lance Spitzner, Honeypot Farms, 2003**
   http://www.securityfocus.com/infocus/1720
5. **Niels Provos, Honeyd-Network Rhapsody for You.**
   http://www.citi.umich.edu/u/provos/honeyd/