A taste of honey: Reducing spam

Nick Wallingford
Bay of Plenty Polytechnic, New Zealand
nick.wallingford@boppoly.ac.nz


Abstract

In computing terminology, a 'honeypot' is a computing software system used to identify or deflect unauthorised use of the system, often using an email address not used for any other purpose. Email users, as well as organised groups of users, set up 'trap' email accounts to attract Unwanted Commercial Email (UCE, also known as spam) and then identify the sources and nature of the mail received. All email users are affected by UCE, through cluttered inboxes, network congestion, and the cost of transport involved in delivery. The use of honeypots reveals some of the methods that spammers use to obtain email addresses, and also identifies some of the steps that can be taken to avoid having one's address become a target of UCE. An understanding of ‘How did they get my email address?’ is of interest and value to all users, as well as being part of the process of UCE reduction. This paper describes efforts being made by individuals and organised projects to utilise honeypots to better identify the means by which spammers obtain email addresses.

Keywords

Spam, email, UCE, honeypots, spambot, Project Honey Pot

1. Introduction and Background

It is a rare Internet email user who receives no unwanted commercial email (UCE), or spam, at all. For most users it has become both a significant problem and a topic that generates strong debate, including such comments as:

“The uncontrolled proliferation of spam is taking one of the most important new forms of communication and killing its effectiveness” (Oliva, 2004).

and

“Spamming is the scourge of electronic-mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on an individual’s e-mail system.” (Cerf, V., cited by Cournane and Hunt, 2004).

Cournane and Hunt (2004) categorised the problems created by UCE as:

- **Cost shifting** - the recipients of email are forced to pay the costs of delivery that the advertiser has avoided,
- **Fraud** - misleading subject lines (to encourage a user to open what would otherwise be deemed to be unwanted email) and misrepresentation of the origin and routing of messages,
- **Resource wastage** - network congestion created by the routing and delivery of UCE,
- **Displacement of legitimate mail** - overfull inboxes that exceed size limits set may mean ‘real’ mail is rejected and lost, and
- **Black lists** - the banning of servers and domains may impact on users who were not necessarily responsible for the abuse of email systems.

Knowledge of how UCE originates - how the spammers get your email address - allows an email user to make informed choices about where and how an email address is published. By restricting
the publication of one's email address, or by allowing it to appear but making it 'unavailable' to spammers, an email user can effectively restrict the amount of unwanted emails received.

On a wider scale, users can participate in organised projects that are intended to identify spammers and spamming techniques. Again, such participation has the potential to ultimately reduce the incidence of UCE.

For many email users, the issue is emotive and highly-charged - they simply wish it would all go away, along with the people who produce and distribute the unwanted emails. This paper describes one component of the on-going efforts to deal with UCE by technical means: the use of honeypot addresses to attract UCE with the longer term aim of reducing the overall amount of unwanted email.

1.1 "Project Honey Pot"

Biever (2005) describes Project Honey Pot well:

"Webmasters who want to help fight spam can download Project Honey Pot's software, which is designed to turn their website into a magnet for harvesters. If the site detects that a crawler [ a program that visits Web sites and reads their pages and other information] is visiting it the software generates a fake email address for the crawler to grab, and records the address of the crawler and the time and date."

The fake address then vanishes from the site, but remains valid as a mailbox. Because it is a fake, no one will send it legitimate mail. If any mail arrives it can only have come from the spammer who grabbed it off the Honeypot site, and this fingers the computer that crawled the site as belonging to the spammer.

The project is then able to provide both individual site and collective statistics on the numbers of email address harvesters that have visited the site and the quantity of UCE that resulted from the harvesting.

The results are shared with anti-spam developers and researchers with the intent that it will assist in the development of tools to ultimately reduce the quantity of UCE. (Project Honey Pot, 2005)

1.2. Example: A Personal Honeypot

David Harris, author of the Pegasus Mail and Mercury Mail Transport programs, utilises a honeypot to attract, identify and ultimately 'blacklist' spammers.

In the footer of his webpages, he includes a simple '|' character that has an email link to the address "shibboleth@pmail.gen.nz". Alternative text is displayed if a mouse moves over the character and warns "Never, ever use this link - it is a honeypot address" (Harris, 2005).

Harris is a self-proclaimed lover of words - his use of 'shibboleth' for the email account carries an intentional irony. A shibboleth is a word or phrase that by its pronunciation or use indicates that a person is a member of a particular group (Kemmer, 2004). In this case, the use of the address reveals anyone who writes to it as a spammer!

Harris reports that within 1 1/2 hours of first placing the honeypot address on his website, he began to receive UCE at the address. He currently receives approximately 30,000 email deliveries per month.

Harris chooses to reject the deliveries before they occur, and adds the sender to his 'blacklist', refusing to accept any further mail from that server/address (Harris, 2005).

2. Project Overview

This research was specifically directed at the potential for addresses on a website to be harvested as targets for UCE. It investigates several of the methods that can be used to restrict the harvesting, but does not attempt to categorise content or identify the source of the UCE that was received.

Three particular aspects were examined:
• How email addresses appearing on websites are harvested,
• How dictionary attacks are used to generate spam, and
• How Project Honey Pot operates to identify spam.

One of the primary means of obtaining email addresses for UCE is by taking them from where they appear on websites. The software used for this harvesting, sometimes called ‘spambots’, crawl from one webpage to another, collecting and collating anything that appears to be a validly-formatted email address.

Addresses that appear on websites are there to make it easy for website users to address emails, allowing the user to simply click on the link rather than having to type an email address into their email client program. It is this convenience, however, that leads to the majority of address harvestings.

Munging is a term referring to either making an email address technically invalid, but still potentially usable by the website visitor, or, by a process of obfuscating the address in some way, so that it appears visually and performs technically as expected, but is not likely to be picked up by the automated harvesting software.

Another means of obtaining email addresses is to target email accounts with common names, or use a 'brute force' method to find variations on those names. Delio (2003) refers to users stating that “... within a day of creating a new Hotmail account the spam starts flowing in”, blaming dictionary attacks for the harvesting of the addresses.

Dictionary attacks involve the submission of a large number of random email addresses to a mail server, recording which are "live" based on the server's response. Common names (john@domain.com) and variations on them (john01@domain.com, john02@domain.com) are typically targeted by the software, resulting in an increased likelihood of success with those email address formats.

Cook (2004) described such an attack from the viewpoint of the recipient of the 'catch all' mail account - the account to which any misaddressed mail to the domain is delivered. He suggests that in some cases, it may be that a spammer's list of addresses has been inflated by simply making up account names before on-selling the list of email addresses.

3. Project Methodology

Registering a site with Project Honey Pot involves creating a webpage that will contain code provided by the project and registering that page's Universal Resource Indicator (URI, sometimes referred to as a URL) with the project.

As part of the research, a page on the server used for the research was set up and monitored for harvesters' visits and UCE received at the addresses it promulgated to the Internet.

The BCS server (the Bachelor of Computing Systems at Bay of Plenty Polytechnic, New Zealand: http://www.bcs.net.nz) was used to create a series of email accounts (Table 1) which were used for the primary research work. A page on the BCS server was set up using the instructions provided by Project Honey Pot. The page was named with an innocuous name (studentlist.php) and links to the page were made from the footer of each of the pages on the BCS website. Below are the different types of accounts described.

Common first names - Twenty email accounts were created using common first names. Those email addresses were not placed on any webpages or advertised in any way. Any mail received by them would have been generated simply with the expectation that there might be an account with that name on the server involved.

A further 18 accounts were created with randomly generated names of the form 'aaa###' where 'a' is a random letter A-Z and '#' is a random digit 0-9.

Controls accounts - Three of the 18 addresses were not advertised on any website in order that they might remain as controls.

The remaining addresses, in sets of three, were placed in the footer of each page of the BCS server.
'As is' - Three of the email addresses were written into the text of the footer, such as: xsw572@bcs.net.nz.

'mailto:' - Three were included as properly formatted mailto: links, such as <a href="mailto:ute938@bcs.net.nz">Email</a>.

'Munged with AT' - Three were 'munged' by replacing the @ character with AT in a mailto: link, such as <a href="mailto:wtnt222 AT bcs.net.nz">Email</a>.

'HTML encoded' - Three were obfuscated with HTML entities, obtained using an online generator (Neumüller, 2005). While long and unreadable to the eye, when the page was viewed with a browser, they appeared and acted like normal mailto: links. An example was: <a href="&#109;&#97;&#105;&#108;&#116;&#58;&#103;&#111;&#53;&#53;&#51;&#64;&#98;&#99;&#115;&#46;&#110;&#116;">Email</a>.

'Hex encoded' - The final 3 addresses were similarly obfuscated using the same online tool, but were instead encoded with hexcode entities. An example was: <a href="%64%6B%76%36%33%31%40%62%63%73%2E%6E%65%74%2E%6E%7A">Email</a>.

<table>
<thead>
<tr>
<th>Type</th>
<th>No.</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common first names</td>
<td>20</td>
<td>Net published on a web page</td>
<td><a href="mailto:xjpa289@bcs.net.nz">xjpa289@bcs.net.nz</a></td>
</tr>
<tr>
<td>Controls</td>
<td>3</td>
<td>Unformatted text on web page</td>
<td><a href="mailto:xsw572@bcs.net.nz">xsw572@bcs.net.nz</a></td>
</tr>
<tr>
<td>mailto:</td>
<td>3</td>
<td>Clickable email link on web page</td>
<td>&lt;a href=&quot;mailto:ute938@bcs.net.nz&quot;&gt;Email&lt;/a&gt;</td>
</tr>
<tr>
<td>Munged with AT</td>
<td>3</td>
<td>@ sign replaced with AT on web page</td>
<td>&lt;a href=&quot;mailto:wtnt222 AT bcs.net.nz&quot;&gt;Email&lt;/a&gt;</td>
</tr>
<tr>
<td>HTML encoded</td>
<td>3</td>
<td>HTML entities instead of ASCII characters on web page</td>
<td>&lt;a href=&quot;%64%6B%76%36%33%31%40%62%63%73%2E%6E%65%74%2E%6E%7A&quot;&gt;Email&lt;/a&gt;</td>
</tr>
<tr>
<td>Hex encoded</td>
<td>3</td>
<td>Hex encoding instead of ASCII characters on web page</td>
<td>&lt;a href=&quot;%64%6B%76%36%33%31%40%62%63%73%2E%6E%65%74%2E%6E%7A&quot;&gt;Email&lt;/a&gt;</td>
</tr>
</tbody>
</table>

Table 1. Summary of email accounts created

To summarise, email accounts were created for the 20 most common first names, 10 male and 10 female (Lusby, 2005). In fact, the names are those that appear most often within the latest US census; no attempt was made to incorporate names from other cultures or countries.

Addresses were 'munged' by replacing the @ symbol in the address with the word AT (with the expectation that a genuine user would reinstate the symbol before using the address to send email).

Addresses were also obfuscated through the use of HTML entity substitution and hexcode entity substitution. In each of these methods, the address when rendered by an Internet browser will still appear 'normal'. The coding that generates the address, however, consists of a string of characters that may (hopefully) not be recognised by address harvesting software.

4. Results

After advertising all of the addresses for 25 days (allowing them to appear on webpages on the BCS server), the addresses were removed from the site.

The accounts were monitored and the number and size of messages received by each account
were recorded at the point the addresses were removed from the website. A final summary of activity was done after 6 months had elapsed (5 months after the advertising of the addresses had ceased).

Unwanted emails began to arrive at the test account addresses four days after they were first advertised on the website. For most of the accounts, UCE continued every two to three days, even after the advertising of the addresses stopped, and a further 5 months have elapsed since that time.

The mailboxes most badly affected have received approximately 1MB of UCE each. This continues in spite of the fact that the addresses no longer appear on any website in any form.

4.1. Munging and Obfuscation

Of the methods used in the research, 'munged with AT' and 'Hex encoded' were the only two that did not receive any UCE during the term of the research.

Most of other categories received a similar level of UCE. All of the 'As is' and 'mailto:' addresses had similar results, with the number of messages from 36-40, and the total size for each account ranging from 209kb to 284kb.

Each of the addresses 'HTML encoded' received one message - with the same sender, subject and message body. While HTML encoding of email addresses to appear on websites is described as effective (Center for Democracy & Technology, 2003), these results would indicate otherwise. After six months, however, no further emails have been received at those addresses.

4.2. Dictionary Attacks on Common Names

No mail was received by any of the 20 'common name' accounts, indicating that no specific dictionary attack was apparent to target the mail server being utilised.

During the same period, however, the server was under attack with attempts to login to SSH (Secure Shell server) using a series of common names. In one 24 hour period of the initial 25 days, 384 attempts were made, using a series of common first names, hoping there might be accounts with those names that had insecure passwords. These dictionary attacks on the SSH server targeted 8 of the 20 names that were being used in the research.

| Summary of Addresses after Initial 25 Days (While Appearing on the Website) |
|-------------------------------------------------|-------|-----|
| Treatment                   | Number of emails | Size(KB) |
| Control                     | 0     | 0    |
| Common names                | 0     | 0    |
| As is                       | 36-40 | 209-284 |
| Mailto:                     | 25-37 | 207-239 |
| Munged with AT              | 0     | 0    |
| HTML encoded                | 1     | 7    |
| Hex encoded                 | 0     | 0    |
| Total                       | 233   | 1.526MB |

| Summary of Addresses after Six Months (5 Months after Being Removed from Website) |
|-------------------------------------------------|-------|-----|
| Treatment                   | Number of emails | Size(KB) |
| Control                     | 0     | 0    |
| Common names                | 0     | 0    |
| As is                       | 135-140 | 833-999 |
| Mailto:                     | 136-141 | 849-979 |
| Munged with AT              | 0     | 0    |
| HTML encoded                | 1     | 7    |
| Hex encoded                 | 0     | 0    |
| Total                       | 233   | 5.352MB |

During the initial period of the research, only one suspected spambot email address harvester visited the page set up for Project Honey Pot on the BCS server. Of the 27 email addresses that
had been presented on that page through the course of the research, only 1 had been the recipient of UCE, according to the Project Honey Pot statistics.

After six months, four "harvesters" had visited the 'honeypot', resulting in 11 spam messages. With three of those in the last week, it would appear that the site was beginning to attract the attention of more harvesters.

With the first UCE arriving 10 days after first setting up the Project Honey Pot page, the BCS server would appear to have been 'found' earlier than the Project's average of 29 days.

4.3. Other Research Opportunities Using the Data

No effort was made in this research to examine the nature or origins of the UCE received by the accounts. Such further work, however, might provide some interesting insights into the characteristics and motivations of the sending agents.

A preliminary look at one mailbox gave the following categorisations:

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stocks and Shares</td>
<td>20%</td>
</tr>
<tr>
<td>Nigerian Scams</td>
<td>17%</td>
</tr>
<tr>
<td>Viral Content</td>
<td>15%</td>
</tr>
<tr>
<td>Contests and Prizes</td>
<td>13%</td>
</tr>
<tr>
<td>Jobs</td>
<td>9%</td>
</tr>
<tr>
<td>Drugs</td>
<td>0%</td>
</tr>
<tr>
<td>Pornography</td>
<td>0%</td>
</tr>
<tr>
<td>Other/Non-obvious</td>
<td>5%</td>
</tr>
<tr>
<td>Software</td>
<td>5%</td>
</tr>
<tr>
<td>Retail</td>
<td>3%</td>
</tr>
<tr>
<td>Phishing Attempts</td>
<td>1%</td>
</tr>
</tbody>
</table>

(n=152)

Further analysis could be carried out utilising the headers of the messages to identify aspects of misrepresentation to facilitate delivery and maintain the sender’s anonymity. Wallingford (2002) provided some examples of the methodologies that could be employed for such research.

Of the email received in one account, for instance, the following results were obtained. It must be borne in mind that these 'From' addresses were almost certainly bogus:

<table>
<thead>
<tr>
<th>Origin</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotmail</td>
<td>12%</td>
</tr>
<tr>
<td>Yahoo</td>
<td>11%</td>
</tr>
<tr>
<td>Netscape</td>
<td>5%</td>
</tr>
<tr>
<td>MSN</td>
<td>3%</td>
</tr>
</tbody>
</table>

(n=164)

Other work could attempt to analyse the real origins of the emails. Again, this information is generally available through a close scrutiny of the full set of email headers received with the messages.

5. Discussion and Conclusion

This research utilised a similar methodology to that of the Center for Democracy & Technology (2003). In that work, email addresses were placed on web pages, placed in USENET postings, submitted using online forms to individual sites, and placed into the WHOIS database of domain registrations. As much as 97% of the unwanted emails received came after an email address appeared on a public web page. As a potential source of spam for an ordinary email user, it is clear that this aspect is one that should be carefully considered if one wishes to keep spam to a minimum.

The results of the project described here were similar in most respects, but differed in one way. In the previous work, the amount of spam dropped rapidly after the address was removed from the web page. This research found that the level of spam remained relatively constant after the
removal of the address.

Both sets of research supported the desirability of obscuring an email address in some way as an effective means of reducing UCE to one's email address.

Email users can adopt strategies that will assist in the reduction of unwanted emails received. The use of honeypots can be used to both confirm and quantify the effectiveness of the strategies, as well as provide information that can be used to reduce spam in a broader context.

Honeypots can be used effectively to attract UCE with the purposes of identifying sources and could provide source data for the analysis of the nature of the emails. Such projects as Project Honey Pot are active in identifying the sources of spam, with the ultimate goal of stopping the spam before it is sent to the ordinary user, providing the ability to blacklist operators who originate the UCE.

This research examined aspects of email address harvesting from webpages and dictionary attacks on common names using a personal honeypot. Other means such as the misuse of email addresses collected as part of web-based registration services may also contribute to the collection of addresses by the originators of spam.

Email users should be particularly wary of allowing their email address to appear on webpages in any form that might leave them open to harvesting by spambots. From this and similar research, it is evident that an email address appearing on a web page in a form capable of being harvested will attract unwanted emails, and will continue to do so. Email users need to be cognizant of the dangers to their future use of an email address in order to protect its on-going effectiveness as a means of communication.

This research identified subsequent research that could be carried out using similar datasets. Content analysis and origin analysis of UCE could be used to complement this source analysis, with the material for examination already available to the researcher. Only a preliminary attempt was made in this research to examine the content of the messages received, but further work could both categorise the nature of the mail, and potentially correlate the origins with the nature.

Acknowledgements

This article represents a reviewed and extended version of a paper presented at the 18th Annual NACCQ Conference (Wallingford, 2005).

References


NACCQ to publish this document in full on the World Wide Web (prime sites and mirrors) and in printed form within the Bulletin of Applied Computing and Information Technology. Authors retain their individual intellectual property rights.

Copyright ©2005 NACCQ.
Krassie Petrova, Michael Verhaart & Tim Hunt (Eds.)
An Open Access Journal, DOAJ # 11764120,

✓zotero