

EMAIL SPAMMING TECHNIQUES

Introduction

SPAMmers use a variety of techniques to spread SPAM through Email. Some of these techniques exploit the flaws in the specifications of current computer networks and electronic communication systems, and others find workarounds about existing ICT security measures. This article presents a brief about techniques adapted by SPAMmers to spread different types of Email SPAM.

EMAIL SPAMMING TECHNIQUES

SPAMmers collect email addresses by “email address harvesting”. Email address harvesting refers to the techniques used for collecting email addresses without the awareness of the recipients. SPAMmers may:

- Get email addresses from other SPAMmers.
- Setup websites that require registration or websites that offer free subscriptions and collect email addresses.
- Use computer programs that are called “harvesting bots” that surf through websites, blogs, forum and newsgroups and collect email addresses.
- Use dictionary attacks to guess email addresses.

To send their SPAM emails, SPAMmers primarily acquire internet domain(s) and setup one or more mail servers. They then use programs known as “SPAM bots”¹ to send out multiple SPAM emails. SPAMmers tend to hide their identity when sending out SPAM emails by:

- Routing their emails through open mail relays² and open proxies³.
- Spoofing the header of the email message; specifically, spoofing the “Sender/From” field of the email header.
- Spoofing the IP address of their mail servers together with the domain name for each email sent out. Although IP spoofing is complex and not cost-effective for SPAMming, it remains possible that SPAMmers use IP spoofing to fake their sent IP addresses.

SPAMmers may also take advantage of weakly setup mail servers that do not strictly comply with the SMTP protocol specifications and hack into them to send out their SPAM emails. A common example of such incompliance is email servers that do not require user name and password to directly connect to them via telnet. SPAMmers can easily use such servers to send out their SPAM emails which implicitly fake their identities. Additionally,

¹ SPAM bots are programs setup on mail servers to compose and send out SPAM email in bulk quantities. It has been noticed that SPAM bots do not strictly comply with the SMTP protocol specifications.

² Open mail relays are mail servers that are found on public networks (internet). They allow anyone to send emails through them using them as a mail server and hiding the actual mail server's identity.

³ Open proxies are proxy servers that are found on public networks (internet). They except incoming traffic openly (from anywhere) and forward the traffic to another destination showing that the traffic has generated from them. Purposed proxy servers are likely to be abused as open proxies due to misconfigurations or lack of proper access controls. Spammers may send their spam emails through them and hide the actual spamming mail server's identity.

some SPAMmers use Trojans⁴ and control computers on different domains. The Trojans then send the SPAM emails without the awareness of the computer users. In such cases, those computers turn into zombie machines for email SPAMming and the actual SPAMmer remains unknown. SPAMmers may also indirectly send junk emails by spoofing the “Return-Path” header field of an email to hold a legitimate address. Consequently, a legitimate address starts receiving bounced (undelivered) emails, unsolicited replies and error messages that cause major annoyance. Recently, SPAMmers tend to create multiple web-based email accounts on free email services by running a script that contains multiple HTTP POST commands with different user names and passwords. Then, they run a script that contains multiple HTTP POST commands for an email message to send out their SPAM emails. This technique implicitly hides the SPAMmer’s actual identity and allows for bulk distribution of SPAM email without encountering major costs.

SPAMmers mainly compose their emails to contain advertising materials, junk contents, and scam scenarios. It has been noticed in lately that SPAMmers compose their SPAM emails by:

- Embedding their SPAM content in between legitimate contents.
- Placing their unsolicited material on the web and inserting a URL that points to the web location in their SPAM emails.
- Obfuscating the text in the email⁵.
- Embedding HTML code and web-scripts⁶ into the body of the email message.
- Embedding their messages inside a picture attached within the email.

⁴ *Trojans are computer programs that appear to have a certain functionality while in fact it uses that functionality as a cover-up for its real functionality.*

⁵ *Obfuscating text of an email refers to typing a word/words using some non-alphabetic characters. An example is typing the word “Viagra” as “Vi@gra”. This technique is used to type words that give an indication of SPAM contents.*

⁶ *As many email clients support displaying HTML contents, SPAMmers tend to embed HTML code in their email containing links to retrieve content that is located on the web, such as images or websites that contain SPAMming content, scripts to indicate to SPAMmers that an email has been read and such the email account is active, scripts to perhaps download malicious codes and/or scripts to execute malicious codes.*