

MailMarshal Stops Bank Hoax Emails

16/6/04

MailMarshal for SMTP stopped recent fraudulent bank hoax emails (also known by the term 'phishing') through MailMarshal for SMTP spam detection. The MailMarshal spam script engine file called 'spamcensor.xml' detected the fraudulent emails with no special customisations made to do so detecting the email as SPAM.

MailMarshal doesn't require a blacklist of known spammers, to detect spam rather using intuitive detection by means of a text censor script. The script uses words, and phrases to trigger a desired score to pull up the offending email. The standard weighting for the spam script is 60. The spamcensor.xml is automatically and continually updated from the web with modifications to cover the ever changing attempts by Spammers to circumvent SPAM detection systems. The spamcensor.xml is a small file that calls it's filter which is only 360KB in size.

MailMarshal for SMTP release 5.5 (released May 2003) has detected the various banking hoax emails for sometime such as the Westpac email shown below & others for such banks as ANZ, Citibank, & NAB.

In November last year in a independent review of spam solutions conducted by RMIT University, MailMarshal came out on top in detection of spam with minimum false positives based on the no customisations.

Below shows MailMarshal with modifications stopping recent Westpac hoax email:

The screenshot displays the NetIQ MailMarshal Console interface. The main window shows a message log for a spam email with the following details:

- Message: B000037b93.00022da5.mml
- Folder: Spam
- From: customerscare@westpac.com.au
- To: qld@virusdefence.com.au
- Subject: [SPAM] Westpac Bank: online account
- Size: 14.5 KB

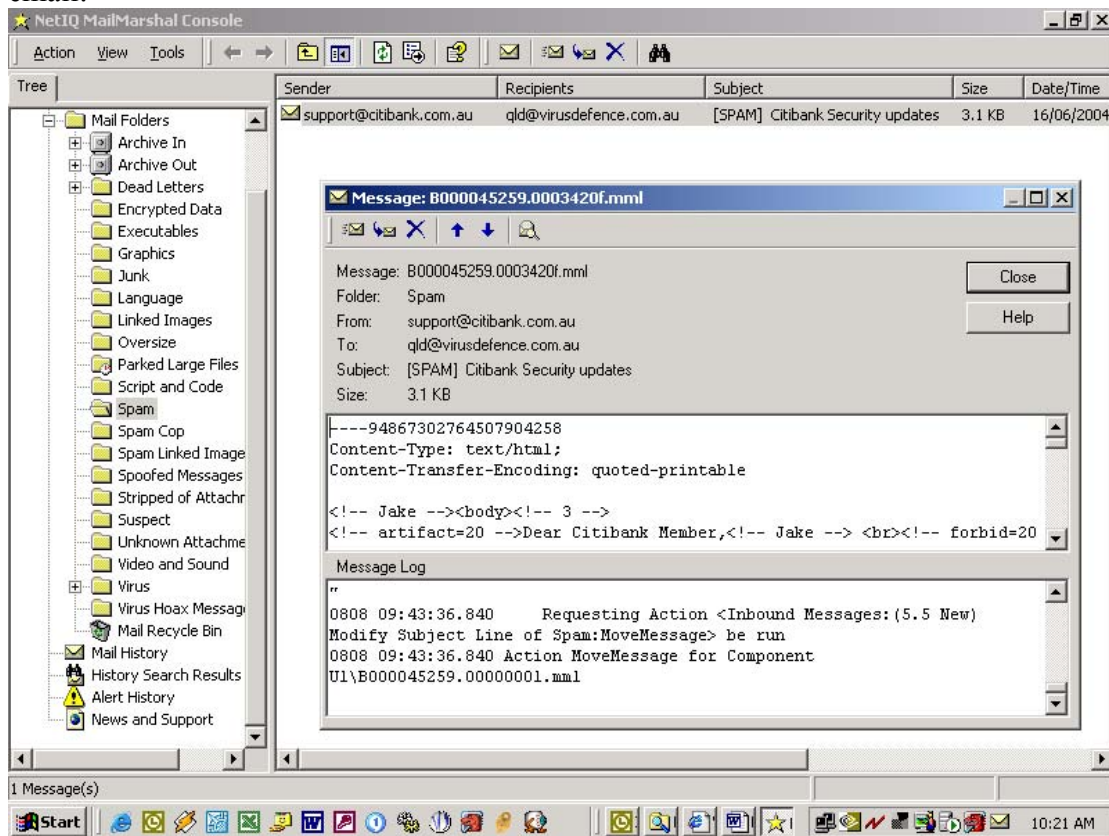
The message content is multipart/alternative with a boundary of "-----8547FF9D2FE1D6". The message log shows the following actions:

- 2784 08:13:02.828 Requesting Action <Inbound Messages: (5.5 New) Modify Subject Line of Spam:MoveMessage> be run
- 2784 08:13:02.828 Action MoveMessage for Component U1\B000037b93.0000001.mml

The console also displays a list of detected spam messages in the background:

From	To	Subject	Size	Date/Time
customerscare@westpac.com.au	qld@virusdefence.com.au	[SPAM] Westpac Bank: online a...	14.5 KB	10/03/2004
misterboo8@hotmail.com	qld@virusdefence.com.au	[SPAM] hispanicgirl69 would like...	2.8 KB	10/03/2004
missy012@hotmail.com	qld@virusdefence.com.au	[SPAM] RE:hispanicgirl69 sent y...	2.6 KB	10/03/2004

Below shows MailMarshal with modifications stopping recent Citibank hoax email:



Further Technical Information

Below is the message log that MailMarshal produced detailing the checks that MailMarshal for SMTP performed on an similar Bank Hoax Email for the ANZ. The below log contents shows how MailMarshal for SMTP looks at the hoax email, and stops the hoax through a variety of means including stopping the hoax by using a non standard port.

```

14:34:13.340 Name=U1\B000047010.00000001.mml (MAIL,1645) False
3104 14:34:13.340 Name=U2\MsgHeader.txt (MHDR,652) False
3104 14:34:13.340 Name=U2\Plain.txt (MBODY,991) False
3104 14:34:13.340 1 user(s) match rule - Block Spam (Asian)
3104 14:34:13.340 Name=U1\B000047010.00000001.mml (MAIL,1645) False
3104 14:34:13.340 Name=U2\MsgHeader.txt (MHDR,652) False
3104 14:34:13.340 Name=U2\Plain.txt (MBODY,991) False
3104 14:34:13.340 1 user(s) match rule - (5.5 New) Modify Subject Line of Spam
3104 14:34:13.360 ----- Category <Spam> evaluation result -----
3104 14:34:13.360 - HTTP_CONTAINS_IP: (1.00) HTTP link contains an ip address
3104 14:34:13.360 - HTTP_LINK: (1.00) HTTP link in message
3104 14:34:13.360 - HTTP_NONSTD_PORT: (27.00) HTTP link contains non standard
port
3104 14:34:13.360 - META_IP_2: (55.00) HTTP link has IP address and is less than 2Kb
3104 14:34:13.360 - MSG_ONLY_HTML: (1.00) Only has HTML body
3104 14:34:13.360 - TC_CLICK_LINK: (0.00) Click on the link below
3104 14:34:13.360 - TC_SCAM_VERIFY_1: (8.00) Possible verification scam
3104 14:34:13.360 - TC_SCAM_VERIFY_4: (18.00) Verify your identity scams
3104 14:34:13.360 - TO_LOCALPART_EQ_REAL: (25.00) To: repeats local-part as real
name

```

3104 14:34:13.360 Total score: (136.0) required(60.0)
3104 14:34:13.360 SpamFilter: Version 35 22-Jun-2004
3104 14:34:13.360 ----- End of Category <Spam> evaluation -----
3104 14:34:13.360 Name=U1\B000047010.00000001.mml (MAIL,1645) TRUE Terminal
3104 14:34:13.360 Requesting Action <Inbound Messages:(5.5 New) Modify Subject Line
of Spam:HeaderRewrite> be run
3104 14:34:13.370 Header Rewrite: Rename Spam Subject field Subject: from " ANZ Bank
Account Verification

" to "[SPAM] ANZ Bank Account Verification
"
3104 14:34:13.370 Requesting Action <Inbound Messages:(5.5 New) Modify Subject Line
of Spam:MoveMessage> be run
3104 14:34:13.370 Action MoveMessage for Component U1\B000047010.00000001.mml