

RISE OF IMAGE SPAM

August, 2006

Contents

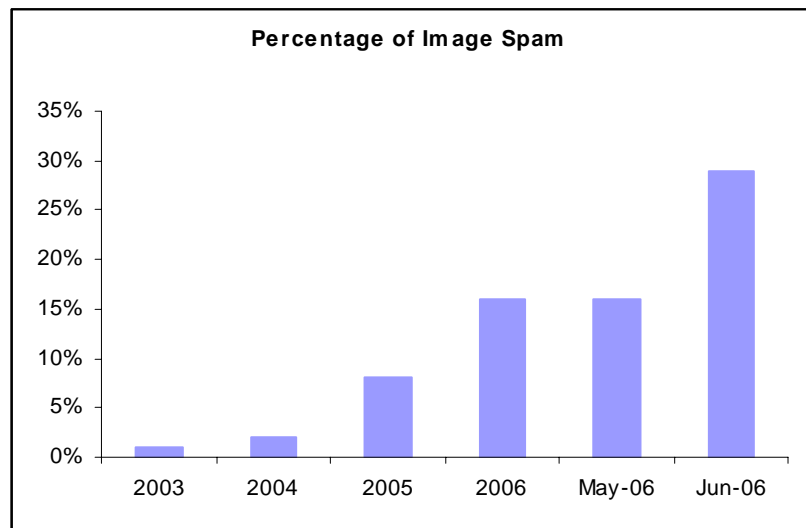
| | |
|---|---|
| What is Image Spam? | 2 |
| Why Image Spam? | 2 |
| Randomization Techniques | 3 |
| Why is image spam a problem? | 6 |
| Effectiveness of MailMarshal against Image Spam | 6 |
| Conclusion | 7 |

This document discusses the rising use of images in spam email, and documents MailMarshal's success in combating this new type of spam.

What is Image Spam?

Image spam is spam with an attached image. Spam with pictures is not new but in the past almost all spam images were actively downloaded from the web by the email client upon viewing.

Spam with an attached image is a relatively new phenomenon, which only started to appear in numbers in the second half of 2005. Image spam exploded in mid 2006. June saw image spam reach almost one in every three spam messages.



Source: Marshal Spam Archives

Why Image Spam?

Why are spammers turning to image spam? To avoid anti-spam devices it seems. Image spam has several advantages for spammers:

- It gets the message across, by-passing anti-spam techniques that scan the message body for spam-like text.
- Pretty graphics allow for a colorful and “professional” message.
- It allows for several new techniques for spammers to randomize each message, again by-passing anti-spam techniques based on signatures.

WHITEPAPER – Rise of Image Spam

It's only "text"

Some images consist only of words; the image below is from a recent spam email:

Hello,

You have been chosen to participate in an invitation only limited time event!

Are you currently paying over **3%** for your mortgage? STOP! We can help you lower that today!

Answer only a few questions and we can give you an approval in under 30 seconds it is that simple!

And stop fighting for lenders, let them fight for you!

Make them work for your business by giving you the lowest rates around!

Two hundred and thirty thousand dollar loans are available for only three hundred and forty dollars/month!

WE ARE PRACTICALLY GIVING AWAY MONEY!

Think your credit is too bad to get a deal like this? THINK AGAIN!

We will have you saving your money in no time!

Are you ready to save your money?

Regards.

Randomization Techniques

To avoid signature-based anti-spam devices, spammers have acquired the ability to randomize each image file on the fly, by subtly altering size, color and inserting random pixels in each file. Here are some examples:

Stock Spots

Note the insertion of colored pixels at random:

Forecast for July, 2006

rice: \$5.50

m Price Target: \$12.00

WHITEPAPER – Rise of Image Spam

Color Streak

Note the multicolored lines of pixels at the bottom of the image:



It's time to save on medicines!
ABSOLUTELY NO PRESCRIPTION! FAST SHIPPING!
**VIAGRA - CIALIS - VALIUM - TRAMADOL - AMBIEN
SOMA - XANAX - PROPECIA - MERIDIA - ATIVAN
CELEBREX - PROZAC - PAXIL - LIPTOR**
Discreet package, to your door! Shipped from Canada!
CLICK HERE AND SAVE 70% ON MEDICINES NOW!

Shades of Gray

Can you see the subtle changes in color between these two images?



BEST SELLING WATCHES

HANDBAGS & PURSES
Beautiful handcrafted luxury items.
[Browse all brands »](#)

TIFFANY & Co JEWELRY
Elegant, day and night. Undeniably chic.
[Browse all models »](#)

NECKTIES
Haute couture neckties, hand-sewn with the finest silks.
[Browse all neckties »](#)

PENS
Superior beauty & elegance carved to the last detail.
[Browse all pens »](#)



BEST SELLING WATCHES

HANDBAGS & PURSES
Beautiful handcrafted luxury items.
[Browse all brands »](#)

TIFFANY & Co JEWELRY
Elegant, day and night. Undeniably chic.
[Browse all models »](#)

NECKTIES
Haute couture neckties, hand-sewn with the finest silks.
[Browse all neckties »](#)

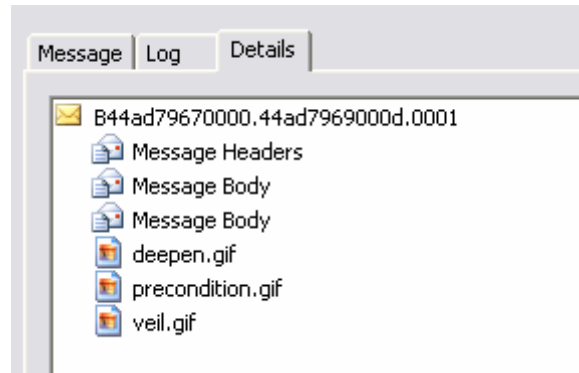
PENS
Superior beauty & elegance carved to the last detail.
[Browse all pens »](#)

WHITEPAPER – Rise of Image Spam

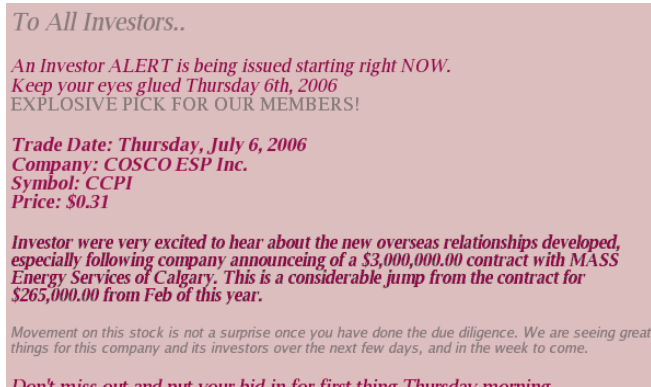
Stock Splits

This new trick, associated with a certain type of stock spam appeared in June 2006. The spammer splits the original image into multiple images, again to avoid signature filters and possibly image scanning software as well.

Note the three attached images, viewed in a MailMarshal Console:



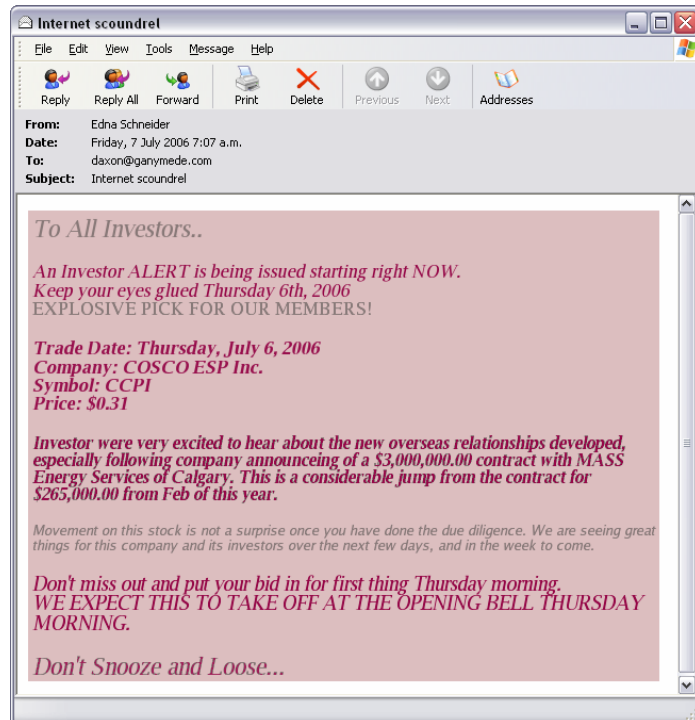
The images are these:



DAY

WHITEPAPER – Rise of Image Spam

The email client re-assembles the pieces when the message is opened:



Why is Image Spam a Problem?

The surge in image spam means one thing: spammers have found some degree of success in by-passing traditional anti-spam technologies. As illustrated above, the mere use of images renders simple text-based scanners useless. The recently acquired ability of spammers to randomize and split images means each image is unique. Systems relying on “fingerprinting” or signatures become less effective.

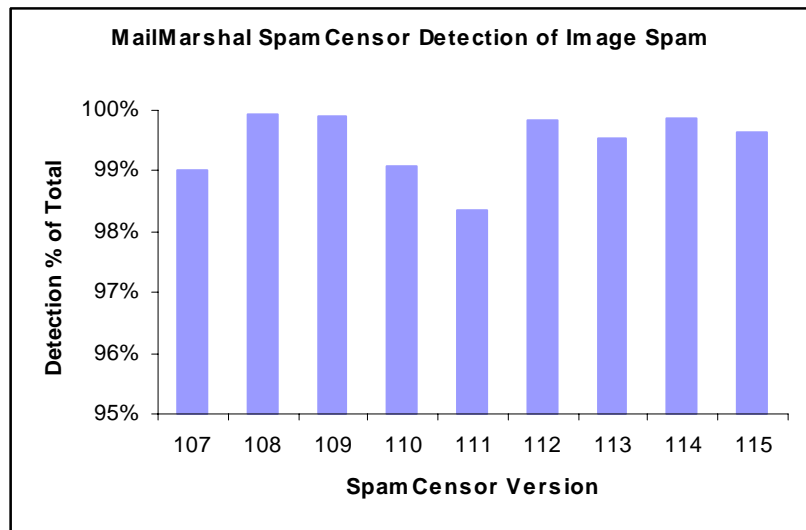
Another issue is impact on bandwidth and email servers. Text-only spam is mostly less than 5KB per message. Image spam is much larger – ranging in size from 12KB to 70KB.

Effectiveness of MailMarshal against Image Spam

MailMarshal has been an effective defense against the flood of image spam. It does not rely solely on text scanning and does not use signature-based detection. Rather, MailMarshal, with its SpamCensor technology, adopts a wide-spectrum approach, utilizing advanced heuristics, header pattern analysis, email-body analysis, URL and IP lookups, message size and composition. The fact that spam includes an image, or that the main idea is encapsulated in an image, is of little significance.

MailMarshal performs exceptionally well against image spam. The graph below shows MailMarshal performance against image Spam during the image spam ‘flood’ in May and June 2006. Only once during this period, did the effectiveness drop below 99%. In six out of the nine weeks the effectiveness was above 99.5%.

WHITEPAPER – Rise of Image Spam



Source: Marshal live "honeypot" streams

Conclusion

Image spam is on the rise. Encapsulating words in an image and new randomization techniques mean spammers are having some success against traditional anti-spam devices, based on simple text scanning and signatures.

Enterprises need a multi-faceted solution that goes beyond the traditional spam detection technologies. MailMarshal provides such a solution, and it has proven effective against image spam.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, MARSHAL LIMITED PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Marshal, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Marshal. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data. This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Marshal may make improvements in or changes to the software described in this document at any time.

© 2006 Marshal Limited, all rights reserved.

U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the U.S. Government is subject to the terms of the Marshal standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

Marshal, MailMarshal, the Marshal logo, WebMarshal, Security Reporting Center and Firewall Suite are trademarks or registered trademarks of Marshal Limited or its subsidiaries in the United Kingdom and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.



Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas
Marshal Inc.
5909 Peachtree Dunwoody Road NE,
Suite 770,
Atlanta,
GA 30328
USA

Phone: +1 404 564-5800
Fax: +1 404 564-5801

Email: americas.sales@marshal.com
info@marshal.com | www.marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com