

## Mail-SeCure blocks 98.5% of all Spam Including image based Spam!

### Image Spam Defense

Spammers are consistently creating sophisticated new weapons in their arms race with anti-spam technology, the latest of which is **image-based spam**. The number of unsolicited messages containing images has grown significantly throughout 2006, and is expected to continue to grow and spread. Through constant monitoring, PineApp has identified that image-based spam tends to be distributed in massive waves; at one of the distribution peaks, PineApp measured image-based spam as 30% of all global spam. Image-based spam creates bandwidth and storage problems, since the typical image-based spam message weighs more than three times that of a regular spam message. At the image-spam distribution peaks, the bandwidth and storage requirements increase upwards of 70%.

#### Summary

- ✓ Image-based spam is a new and growing problem, leading to loss of productivity and a drain on IT resources.
- ✓ Most anti-spam solutions have problems dealing with image-based spam, and by dealing with it ineffectively, they create other problems along the Way.
- ✓ PineApp has implemented a unique solution to decode images, and treat them with RPD similarly to other types of spam.
  - Improves the already superior spam catch rate
  - Maintains low false positive rate

### Questions & Answers

#### What is Image-Based Spam?

Image-based spam is unsolicited email that contains only images (typically GIF format, but can appear as JPG, PNG, BMP etc.), *with no relevant text or hyperlinks*. The message may appear to be text (see examples below), however in reality it is just an image of text. Often the content of such messages are penny stock “pump & dump” schemes and other malicious types of spam. Since creating image-based spam requires more technical know-how than basic textual spam, it originated in areas such as Russia which have technically advanced spammers. It has rapidly spread to the United States, and is expected to broaden to other locations.

#### What are the Newest Trends in Image-Based Spam?

Lately, spammers have been experimenting with new techniques such as “broken images,” i.e. splitting a single image into smaller images that fit together like puzzle pieces. This technique makes it even more difficult for anti-spam engines to catch and block.

Another technique is to send animated GIFs, with several frames of random noise. These, random pixels act similarly to the randomized images that are not animated, simply with another level of complexity. In some cases, the animated GIFs contain subliminal messages (e.g. “buy... buy... buy”) embedded into frames that flash by very quickly. Animated GIF spam is much heavier, on average, than static image-based spam.

#### Why is Image-Based Spam So Difficult for Most Anti-Spam Engines to Catch and Block?



These unsolicited emails contain no text or hyperlinks, so most anti-spam engines cannot catch this type of spam. Often the message will contain text copied from legitimate books, in order to fool Bayesian filters.

Spammers have figured out a way to foil even those engines that try to analyze the image data itself: they vary the images slightly for each message. They do this easily by changing the shade of the border or background, changing the line spacing or margins, or even adding tiny specks to the background; these types of changes are invisible to the eye (or irrelevant to the reader), but *completely change the way the data appears to most anti-spam engines*. The result is a huge quantity of image-based spam that contains random patterns with almost no repetitions.

None of the traditional anti-spam technologies – content-based, Bayesian, Heuristic, URL Filtering, etc. – have been able to prevent this type of spam on a consistently accurate basis in the past.

## What are Some Technologies Used To Fight Image-Based Spam?

### Optical Character Recognition

Some anti-spam providers have added new features to their technology based on OCR (i.e. Optical Character Recognition, which changes graphic images of text to editable text). OCRbased anti-spam technology has several drawbacks: it requires significant resources and can reduce server performance; and it has difficulty catching spam messages comprised of mostly images, with only a small amount of text within the images.

### Rule Engines

Other methods for blocking image-based spam, such as rules that prohibit attached images of a certain size, or a certain quantity of colors, lead to an unacceptably high number of false positives. In such a scenario, legitimate email messages containing baby pictures or graduation photographs could be considered spam and thus go unseen by their intended recipients.

### Recurrent Pattern Detection

Recurrent Pattern Detection contains an intrinsic mechanism to exact-match recurrent patterns across similar but not-identical messages. However in the case of images, the minute the spammer makes even the smallest changes to an image, the image-encoded data appears completely different. PineApp identified this trend in the earliest days of image-based spam, and made the necessary enhancements to its detection engine in order to defend against this new threat with a sophisticated protection shield. PineApp invested significant resources into implementing a method for decoding the images and then sampling them using the proven RPD approach. The result is a significantly improved spam detection rate, while maintaining the same low false-positive rate.

Example for Image Spam

