WHITE PAPER

Attachment spam – the latest trend

Spammers using common file formats as attachments for pump-and-dump scams

This white paper explains what makes spam such an unbearable problem and how spamming tactics are evolving daily to beat anti-spam software. In the space of two months, spammers have switched from image spam to using PDF, Excel and ZIP file attachments. By using these attachments to send images instead of embedding them in the body of the email message, spammers have taken the cat-and-mouse game with anti-spam software developers to a new level.

Introduction

At one point or another – like the majority of computer users – you have received emails that promise business deals worth millions of pounds, that try to sell products to improve your appearance or that try to convince that it's worth investing your money in a particular company or stock. Dealing with spam (unsolicited email that is not targeted at specific individuals), is one problem that all email users share in common. Research shows that between 65% and 90% of all email received is considered spam.

On an individual user basis, spam is annoying; it is a waste of time and often contains spyware, malware and even pornography. On a company-wide basis, the same threats apply however there is also the financial cost to manage spam that must be taken into consideration.

The evolution of spam

Until a while ago, spam was the domain of text- or html-based emails. For anonymous delivery, these messages traditionally relied on abusing open SMTP relays. When open SMTP relays became less common, spammers switched to proxy servers, dial-up services and more recently, hijacked computers. Spammers designed personalized template emails to deliver their messages and then made use of bulk mailing software for distribution.

To block spam, email service providers and companies often relied on keyword 'detection', and drew up a list of keywords that commonly appeared in most of the spam email. This list would often include keywords such as 'viagra' or 'bank'. However, this method often blocked genuine email and adding more keywords simply resulted in more false positives which in turn blocked legitimate email. But spammers became smarter too, and they addressed keyword blocking by replacing keywords such as 'viagra' to 'v1agra'.

Another attempt at blocking spam includes making use of blacklists that contain a list of IP addresses of known spammers or compromised hosts. However, these lists have to be constantly updated because spammers have learnt to counteract this by rapidly changing the

origin of spam.

New trends: Dynamic Zombie botnets

Botnets can be defined as networks of compromised computers which can be controlled by a single master. The number of nodes (also known as zombies) of these botnets can run into millions and these machines make use of different software vulnerabilities to gain full access to the infected hosts and add it to their existing array of zombies. Computer hackers had long been using botnets to launch DoS (denial of service) attacks and distribute network hacking attacks. Computer criminals had also been using botnets for money-making schemes, such as stealing credit card information and scamming pay-per-click advertising companies.

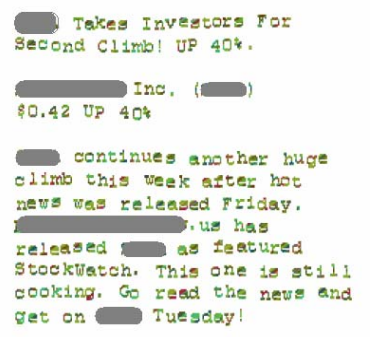
Seeing huge potential in botnets, spammers started financing hackers to make use of zombie machines. Hackers were able to offer services such as renting of botnets for a few minutes or hours and collections of email recipients (spam lists). The anti-virus industry noticed correlations between the spam industry and botnets. Not only were malware writers allowing spammers to make use of their creations, but they were writing malicious code to specifically suit their needs. An unholy alliance had been created.

Image spam

By early 2006, most anti-spam vendors had added Bayesian filtering to their arsenal of spam blocking methods. The fight between spam and anti-spam looked like it was taking a positive turn. However, by the end of 2006, the nature of spam had totally shifted. Whereas spam had been mainly text based, this time spam started looking more graphic in nature. Spammers began making use of images to bypass text-based content filtering, simply by no longer using any text content. By making use of image spam, spammers were attacking the defenses of most anti-spam solutions; while the images displayed text messages to the end-users, the anti-spam software was only able to see pixels.

Some email anti-spam solutions decided to go with OCR (Optical Character Recognition) to turn the images into text that the software could then use. However, spammers took their images to the next level. In an approach usually applied to CAPTCHA (an anti-spam solution that is used on web forums), they started fuzzing (including noise and distortions) images to make it even harder for the machine to recognize text. Although it is possible for the machine to read this text, the process is very CPU intensive – especially when it is handling multitudes of images every few seconds.

The latest trends


[redacted] Takes Investors For Second Climb! UP 40%.

[redacted] Inc. ([redacted])
$0.42 UP 40%

[redacted] continues another huge climb this week after hot news was released Friday. [redacted].us has released [redacted] as featured StockWatch. This one is still cooking. Go read the news and get on [redacted] Tuesday!

Although spammers registered considerable success with image spam (picture, right) the anti-spam software industry had not lost the battle and quickly came out with new counter-measures to stop image spam. Realizing that filters had a problem with images, the answer was to hit spammers at source – that is where the email originated from. This new approach had an immediate positive result and considerably decreased the effectiveness of image spam and gave back to email users some control over their mailbox.

As with every cat-and-mouse game, spammers had to respond and in June 2007, they came up with a new technique that is not only ingenious but even more problematic than image spam. Instead of embedding the image within the email itself, they 'repackaged' it within an attachment using one of the most common file formats in use today – a PDF file.

This move is clever for a number of reasons:

- Email users 'expect' spam to be an image or text within the body of the email and not an attachment.
- Since most businesses today transfer documents using the PDF format, email users will have to check each PDF document otherwise they risk losing important documentation.
- With most anti-spam software products on the market geared towards filtering the email itself and not attachments, spam has a longer shelf-life within a network.
- An attachment that is a PDF file has greater credibility in an email thus making social engineering attacks much easier.
- The ability to send large PDF files could result in a single spam attack causing huge bottlenecks on a company's email server, reducing the quality and amount of bandwidth available.
- By sending PDF attachments, spammers can also resort to phishing by attaching supposedly authentic documents from a bank or service provider.

The use of PDF spam was short-lived as anti-spam software vendors quickly came out with updates and filters that analyzed the body of every PDF file. Not to be defeated, spammers took less than a month to come out with a new option: Microsoft Excel files for push-and-dump scams.

This move was clever for reasons similar to those above for PDFs:

- Email users 'expect' spam to be an image or text within the body of the email and not an attachment.

- Excel is another extremely common file-type in use and users are very familiar with this format.
- Since many businesses use Microsoft Excel for spreadsheets, databases and so on, email users will have to check each document otherwise they risk losing important documentation.
- With most anti-spam software products on the market geared towards filtering the email itself and not attachments, 'Excel' spam has a longer shelf-life within a network.

Taking the game to a new level, in early August 2007, spammers started compressing their text-based and Excel-based spam documents using the ZIP file format. This is effective for two main reasons:

- Companies that do not use anti-virus software on their network could be easy targets for this type of spam.
- Users who may not be aware of security issues surrounding attachments are prone to opening these ZIP files. With spammers and hackers thriving in their unholy alliance, the risk of malicious files being packaged with pump-and-dump spam is all too real.

The use of multiple file format combinations that are most commonly in use by email users appears to be spammers' way forward for spammers.

Solution

Spam continues to be a headache for administrators and end-users because spammers are constantly trying to stay one step ahead of anti-spam software vendors. Using keyword detection methods alone will not solve the problem because new spamming techniques have overcome that hurdle. The solution lies in a product that deploys as many anti-spam techniques as possible, including Bayesian filtering and filtering for images/text embedded in different file-type attachments, while at the same time maintaining false positives at a minimum. Moreover, the package should be easy to install and manage without adding unnecessary administrative burdens and the solution should efficiently handle spam with minimal end-user intervention.

About GFI MailEssentials

GFI MailEssentials offers anti-spam for Exchange server and other email servers and eliminates the need to install and update anti-spam software on each desktop. GFI MailEssentials offers a fast set-up and a high spam detection rate using Bayesian filtering and other methods. With very low false positives, GFI MailEssentials will eliminate over 98% of the spam from your network – including PDF and Excel spam – as well as detect and block phishing emails and hard-to-catch image-spam through a Botnet/Zombie check. GFI MailEssentials also adds email management tools to your mail server: Disclaimers, mail monitoring, Internet mail reporting, list server, server-based auto replies and POP3

downloading.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, Adelaide, Hamburg and Cyprus which support more than 160,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at http://www.gfi.com.

Sources

Viruslist.com (2007), *Contemporary Spammer Technologies* available from: http://www.viruslist.com/en/spam/info?chapter=153350528

NetworkWorld.com (2007), *Spam Calculator* available from: http://www.networkworld.com/spam/index.jsp

SecureWorks (2007), *Storm Worm DDoS Attack* available from: http://www.secureworks.com/research/threats/view.html?threat=storm-worm

The TechWeb Network (2007), *Dutch Botnet Suspects Ran 1.5 Million Machines* available from: http://www.techweb.com/wire/security/172303160

BBC News website (2007), *Criminals 'may overwhelm the web'* available from: http://news.bbc.co.uk/2/hi/business/6298641.stm

Bächer P., Holz T., Kötter M. and Wicherski G. (2007), *Know your Enemy: Tracking Botnets* available from: http://www.honeynet.org/papers/bots/

Computerworld (2007), *Want to rent a botnet?* available from: http://www.computerworld.com/blogs/node/2206