A SURVEY ON IMAGE SPAM DETECTION TECHNIQUES

Shadi Khawandi, Firas Abdallah,Anis Ismail

Faulty of Technology, Lebanese University, Lebanon

ABSTRACT

Today very important means of communication is the e-mail that allows people all over the world to communicate, share data, and perform business. Yet there is nothing worse than an inbox full of spam; i.e., information crafted to be delivered to a large number of recipients against their wishes. In this paper, we present a numerous anti-spam methods and solutions that have been proposed and deployed, but they are not effective because most mail servers rely on blacklists and rules engine leaving a big part on the user to identify the spam, while others rely on filters that might carry high false positive rate.

KEYWORDS

E-mail, Spam, anti-spam, mail server, filter.

1. INTRODUCTION

The internet community has grown and spread widely in a way that not only is it connecting every one of its users into one virtual globe, but also affecting them. Given that the internet is still in an ongoing evolution, states that this virtual community of people (users) is growing and with this growth comes great value, a value of people connected all together in a certain period of time all of the time, now imagine what this could bring forward as a target regarding marketing, advertisement, at the same time it could also hurt such users when such marketing and advertisement are misused, therefore affecting the resource structure of this globe along with its users. Consider a table whose resource structure are its four wooden legs which is able to hold a capacity of 50 kg, now bring a load of 70 kg and you will notice that the table would be crippled and broken, now apply that on the internet community whose resource structure are its communication which is able to hold up to a certain level of bandwidth, if we abuse that level and raise it up the internet community will be crippled and get affected by itself and its users thus costing the whole community a burden which starts from spam.

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not choose to receive it, and is also regarded as the electronic equivalent of junk mail. Most spam is commercial advertising and is generally e-mail advertising for some product sent to a mailing list or newsgroup. This is done by the abuse of electronic messaging systems including most broadcast media, digital delivery systems to send unsolicited bulk messages at random. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup

Dhinaharan Nagamalai et al. (Eds) : COMIT, AISCA - 2019
pp. 13–27, 2019. © CS & IT-CSCP 2019 DOI : 10.5121/csit.2019.90102

spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, and file sharing network spam [1]. People who create electronic spam are called spammers [2].

The generally accepted version for source of spam is that it comes from the Monty Python song, "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam…" Like the song, spam is an endless repetition of worthless text. Another thought maintains that it comes from the computer group lab at the University of Southern California who gave it the name because it has many of the same characteristics as the lunchmeat Spam that is nobody wants it or ever asks for it. No one ever eats it. It is the first item to be pushed to the side when eating the entree. Sometimes it is actually tasty, like 1% of junk mail that is really useful to some people [2].

E-mail spam is known as unsolicited bulk E-mail (UBE), junk mail, or unsolicited commercial e-mail (UCE), is a subset of spam where in practice it is the sending of unwanted e-mail messages, frequently with commercial content, in large quantities to a random set of recipients.Spam in e-mail started to become a problem when the Internet was opened up to the general public in the mid-1990s. It grew exponentially over the following years, and today is estimated to comprise some 80 to 85% of all the e-mail in the world [1].Digital image is a representation of a two-dimensional image using ones and zeros (binary). The term "digital image" usually refers to raster images also called bitmap images.Raster images have a finite set of digital values, called picture elements or pixels. The digital image contains a fixed number of rows and columns of pixels. Pixels are the smallest individual element in an image, holding quantized values that represent the brightness of a given color at any specific point.

Typically, the pixels are stored in computer memory as a raster image or raster map, a two-dimensional array of small integers. These values are often transmitted or stored in a compressed form which is the process of encoding information using fewer bits than an uuencoded representation would use. Raster images can be created by a variety of input devices and techniques, such as digital cameras, scanners, coordinate-measuring machines, seismographic profiling, airborne radar, and more. Each pixel of a raster image is typically associated to a specific 'position' in some 2D region, and has a value consisting of one or more quantities related to that position. Digital images can be classified according to the number and nature of those samples such as binary, grayscale, color, false-color, multi-spectral, thematic, and picture function [3].

Image spam is a kind of E-mail spam where the message text of the spam is presented as a picture in an image file. Since most modern graphical e-mail client software will render the image file by default by presenting the message image directly to the user, thus it is highly effective at overcoming normal e-mail filtering software where it inputs the e-mail, and as for its output it might pass the e-mail message through unchanged for delivery to the user's mailbox, redirect the message for delivery elsewhere, or even throw the message away.

2. EXISTING SOLUTIONS

This paragraph lists various solutions for tackling spam and image based spam, where the light is shed on the process and technique used to battle spam and the different features each solution contains. Also, the filtering steps that each solution requires to detect and prevent spam are presented.

2.1 SYMANTEC

Symantec is considered one of the important firms that specialize in security products including anti-spam ones and below the Symantec's Bright mail anti-spam product along with its components and their features are discussed here in.

2.1.1 SPAMMERS EMPLOYING TRADITIONAL TECHNIQUES

Security researchers at Symantec state that spammers have not discarded their old methods. Actually, in a wave of latest malware and spam crusades, spammers have revised and combined two oldest and commonly used topics. Symantec experts inform that they have observed the coming back of spam mails which hide their malicious content in HTML code embedded in the form of mail attachments. It is a known obfuscation technique which has been discarded in favor of other methods such as image spam.

Symantec also reveals that the image spam, responsible for the major increase in spam activity during May 2009, became even more constant in June 2009, accounting for between 8% and 10% of the total spam detected by the security vendor.Actually, what they fear is that these spam attacks will probably follow ever more diverse strategies in times to come as spammers are collectively working to advance their attack vectors. Mayur Kulkarni, Researcher at Symantec, claims that spammers do not have to discover new methods to enter user's inbox. They can very well use the existing method with even better results, as reported by security watch week on July 7, 2009. Lastly, the security vendor has asked users that they should not carelessly open any attachments especially when it is sent by an unknown sender. With 419 spam mails, e-mail users are suggested not to reply fake appeals and do not show interest in any of the money making plans.

2.1.2 SYMANTEC BRIGHTMAIL ANTISPAM

Symantec Brightmail AntiSpam™ offers complete, server-side anti-spam and antivirus protection. It actively seeks out, identifies, analyzes, and ultimately defuses spam and virus attacks before they trouble the users and overwhelm or damage the networks. Symantec Brightmail software that is installed at your site allows unwanted mail to be removed before it reaches the users' inboxes, without violating their privacy.

2.1.2.1 HOW SYMANTEC BRIGHTMAIL ANTISPAM WORKS

Symantec Brightmail AntiSpam employs the following four major types of filters. First, AntiSpam Filters are created by Symantec using the state-of-the art technologies and strategies to filter and classify e-mail as it enters the site, Second, Content Filters are custom content filters are written by the user, using the Brightmail Control Center or the Sieve scripting language, to tailor filtering to the needs of the organization. Third, Allowed and Blocked Senders Lists in which lists can be created of allowed senders and blocked senders and third party lists can also be used. The lists included in the Brightmail Reputation Service are deployed by default. Fourth, Antivirus Filters in which Antivirus definitions and engines protect the users from e-mail borne viruses.

2.1.2.2 FEATURES OF SYMANTEC BRIGHTMAIL ANTISPAM

AntiSpam Filtering Feature includes Heuristics that is a practical approach which targets patterns common in spam, Signatures that are Accurate and responsive approach that identifies the underlying "DNA" of evolving spam attacks. Defeats HTML-based and other evasion strategies used by spammers, Header that is similar to the Heuristics Filter, but applied to message headers, URL that matches the embedded URLs with a database of known spam URLs, Suspect List which Blocks e-mail from known spam senders (part of the Brightmail Reputation Service), Open Proxy List that blocks e-mail from insecure proxy servers by testing against the IP address of e-mail (part of the Brightmail Reputation Service), Safe List that allows e-mail from known clean domains (part of the Brightmail Reputation Service), Block and Allowed Senders Lists are Lists of trusted and blocked senders, IP connections, and domains created by administrators to augment Brightmail filtering, Content filters that are special purpose filters created by administrators to enforce organization-specific e-mail policies, and Third party filters which has easy integration with DNS-based blacklist and filtering services.

Other Filtering Features are group policies that specify groups of users, identified by e-mail addresses or domain names, and customize mail filtering for each group. Deployment options include gateway layer, internal relay layer, and e-mail server. The e-mail client add-ins for handling spam having Plug-ins for Outlook and Notes, and Web-based, with configurable notification option for recipients. Available antivirus protection detects and removes e-mail-borne viruses Quarantine Web-based, with configurable notification option for recipients.Spam management options in which to deliver the message normally, delete the message, deliver the message to the recipient's Spam folder, foldering agent moves spam to a designated folder in the end-user's mailbox, save the message to disk for administrator review, sends the message to an administrative account for further study, routes spam to a Web-based quarantine where recipients can review caught spam, and modify the message by adding configurable X-Header or subject line text to the message.Reporting and Statistics made up of standard interactive reports based on total spam or total virus messages found, and extended tracking and reporting of recipient, sender, domain, and other fields.

2.1.2.3 SYMANTEC BRIGHTMAIL ANTISPAM ARCHITECTURE

Symantec Brightmail AntiSpam consists of several components. The key components you need to consider are the following:

- Each Symantec Brightmail AntiSpam installation can have one or more Brightmail Scanners. Brightmail Scanners perform the actual filtering of e-mail messages.
- Each Brightmail Scanner contains a Brightmail Agent, and One or both of a Brightmail Server, and a Brightmail Client. If the Brightmail Scanner contains a Brightmail Client, then a supported mail transfer agent (MTA) must also reside on the same computer.

The Brightmail Client is a communications channel between the MTA and the BrightmailServer. You can use multiple Brightmail Clients each one can talk to multiple Brightmail Servers. The Brightmail Client performs load balancing between Brightmail Servers.The Brightmail Servers at your site process spam based on configuration options you select. Each Brightmail Server is a multi-threaded process that listens for requests from Brightmail Clients. Using a variety of state-

of-the-art technologies, the Bright mail Server filters messages for classification. The classification, or verdict, is then returned to the Brightmail Client for successive delivery action. The Conduit connects to the BLOC to determine whether updated filtering rules are available. If new rules are available, the Conduit retrieves the updated rules using secure HTTPS file transfer. After authenticating the rules, the Conduit notifies the Bright mail Server to begin using the updated rules. The Conduit also manages statistics, both for use by the BLOC and in a local statistics pool for the generation of local reports. Each Symantec Bright mail Anti-Spam installation has exactly one Bright mail Control Center. This is the central nervous system of your Symantec software. The Bright mail Control Center communicates with the Brightmail Agent on each of your Brightmail Scanners. For smaller installations, you can install the Brightmail Control Center and theBrightmail Scanner on the same computer. From this Web-based graphical user interface, you can configure start and stop each of your Brightmail Scanners, specify e-mail filtering options for groups of users or for all of your users at once, monitor consolidated reports and logs for all Brightmail Scanners, view summary and status information, administer Brightmail Quarantine, and view online help for Brightmail Control Center screens.

The Brightmail Control Center contains the following Features:

- Brightmail Quarantine provides storage of spam messages and Web-based end user access to spam. You can also configure Brightmail Quarantine for administrator-only access. Use of Brightmail Quarantine is optional.
- A single MySQL database stores all of your Symantec Brightmail AntiSpam configuration information, as well as Brightmail Quarantine information and e-mails (if you are using Brightmail Quarantine). Configuration information is communicated to each Brightmail Scanner via an XML file. A Java-based Web Server (by default this is the Tomcat Web Server) performs Web hosting functions for the Brightmail Control Center and Brightmail Quarantine.

2.1.2.4 SYMANTEC BRIGHTMAIL ANTISPAM FILTERING PROCESS

With the default configuration, the filtering process works as follows. First, the SMTP server receives the mail message and processes any security settings. Second, the Brightmail Client (integrated with the MTA) sends a copy of the mail message to the Brightmail Server. Third, by default the Brightmail Server processes mail in the following order, allowed senders you identify, blocked senders you identify, Symantec Brightmail AntiSpam filters, content filters you create and finally the Brightmail Server returns the verdict of the message to the Brightmail Client. Fourth, the Brightmail Client tells the SMTP server to perform the appropriate action, based on the policies in place [4].The Bright mail anti-spam solution is composed of several components and these components need to interact with each other in order to provide the feature that is needed from it and these interactions are shown in Figure 1.

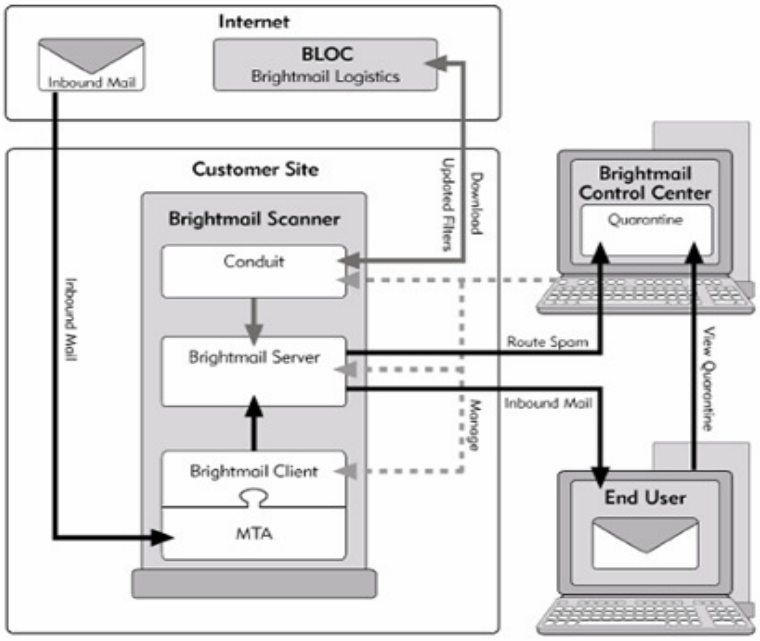

Figure 1 - Symantec Bright mail Components Interaction

2.2 KASPERSKY

Although Internet Security suites usually include as standard e-mail spam filter, spammers continue to find ways around the checks that are made. One of those workarounds is the use of images with text buried in the image data. This kind of spam can be checked for, but currently it is done using machine recognition. Spammers can overcome those checks by making the text fuzzy and adding distortion or rotation to an image.Kaspersky Lab has a statistics-based method for detecting image-based spam that is used to bypass traditional text-based filters. The technology analyses whether text is contained in images based on the graphic pattern of words and lines, said developer Eugene Smirnov.Spam is expected to continue to be a problem in 2009, particularly with the rise in the number and popularity of websites that allow user-generated content. Kaspersky Anti-Spam 3.0 provides thorough and accurate protection from spam for users of corporate mail systems and public e-mail services.

2.2.1 KASPERSKY ANTI-SPAM

There are several features that are offered by Kaspersky Anti-spam solution and these features include the following.

2.2.1.1 PROTECTION FROM SPAM

List-based filtrations in which sender's IP addresses are checked against blacklists of spammers, which are maintained by Internet service providers and public organizations (DNS-based Blackhole Lists). System administrators can add addresses of trusted correspondents to a safe list, ensuring that their messages are always delivered without undergoing filtration.Analysis of formal attributes where the program recognizes spam by such typical characteristics as distorted sender addresses or the absence of the sender's IP address in DNS, an excessive number of

intended recipients or hidden addresses. The size and format of messages are also taken into consideration.Linguistic heuristics where the program scans messages for words and phrases that are typical of spam messages. Both the content of the message itself and any attachments are analyzed.Graphic spam in which a database of signatures for graphic spam equips the program to block messages containing spam images, a type of spam that has become increasingly common in recent years.Real-time UDS requests where the Urgent Detection System is updated with information on spam messages literally seconds after they first appear on the Internet. Messages that could not be assigned a definitive status (e.g., spam, no-spam) can be scanned using UDS.The e-mail that is received passes into a process of message analysis as shown in Figure 2 and includes several analysis procedures in order to analyze the message

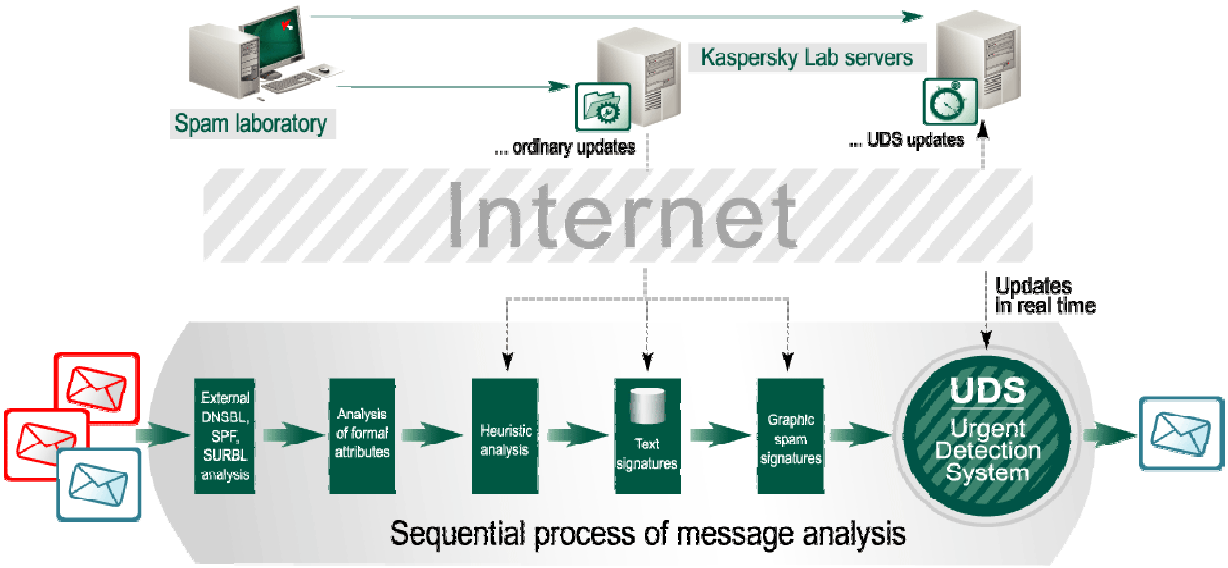

Figure 2 - Kaspersky E-mail analysis process

2.2.2.2 ADMINISTRATION

Flexible management in which the web interface allows system administrators to manage the application both locally and remotely. The filtration level is easily configurable, as are blacklists and safe lists. It is also possible to disable/enable individual filtration rules.Management of user groups where the administrator can create user groups either using lists of addresses or domain masks (for example, XXX@domain.com) and apply individual settings and filtration rules to each group.Options for processing spam where the program can be configured to process spam by either automatically deleting it, redirecting it to the quarantine folder with a note to the user or sent for further filtration to the mail client.Detailed reports where the administrators can easily monitor the application, the protection status and license status, using HTML reports or alternatively, by viewing log files. Data can be exported in CSV and Excel formats.

2.2.2KASPERSKY ANTI-SPAM 3.0 MP1 CRITICAL FIX

The following improvements have been introduced since Kaspersky Anti-Spam 3.0 MP1 (3.0.255.0) where methods for fighting so-called "graphic" spam, i.e. tools used to analyze graphic attachments. New algorithms have been introduced for processing and identification of

similar images with textual content as well as the GSG-8 and GSG-9 technologies.The following problems have been fixed as compared to Kaspersky Anti-Spam 3.0 MP1 CF1 (3.0.274.0) where possible termination or freezing of filtering processes when a list of protected domains is used, and accidental setting of incorrect access rights for the files of application components if they were previously updated using a package of modified application files from previous product versions [5].

2.3 TREND MICRO

It's no longer efficient to compile lists of known spammers and filter them out, because those lists are so large and growing bigger all the time, adds Hemmendinger. And it's too cumbersome to update them on a daily basis. "What we've learned over time is the more commonly used methods would be content filtering, like text filters that look for certain key words or sophisticated heuristics that look at the content of a message to see if it appears to fit the mold of what is readily recognized as spam," Hemmendinger says. He also pointed to techniques that spammers use to trip up e-mail filters, like adding asterisks between each letter in a word so it can't be identified." With the release of InterScan Messaging Server Suite (IMSS), Trend Micro strives to provide solution providers with effective tools to battle spam and protect users from increasing ills associated with e-mail, ranging from script bombs to worm-bearing messages.

In Figure 3 we can have a view on a snap shot of the Trend Micro IMS anti-spam solution which shows the configuration that can be altered or given by the user

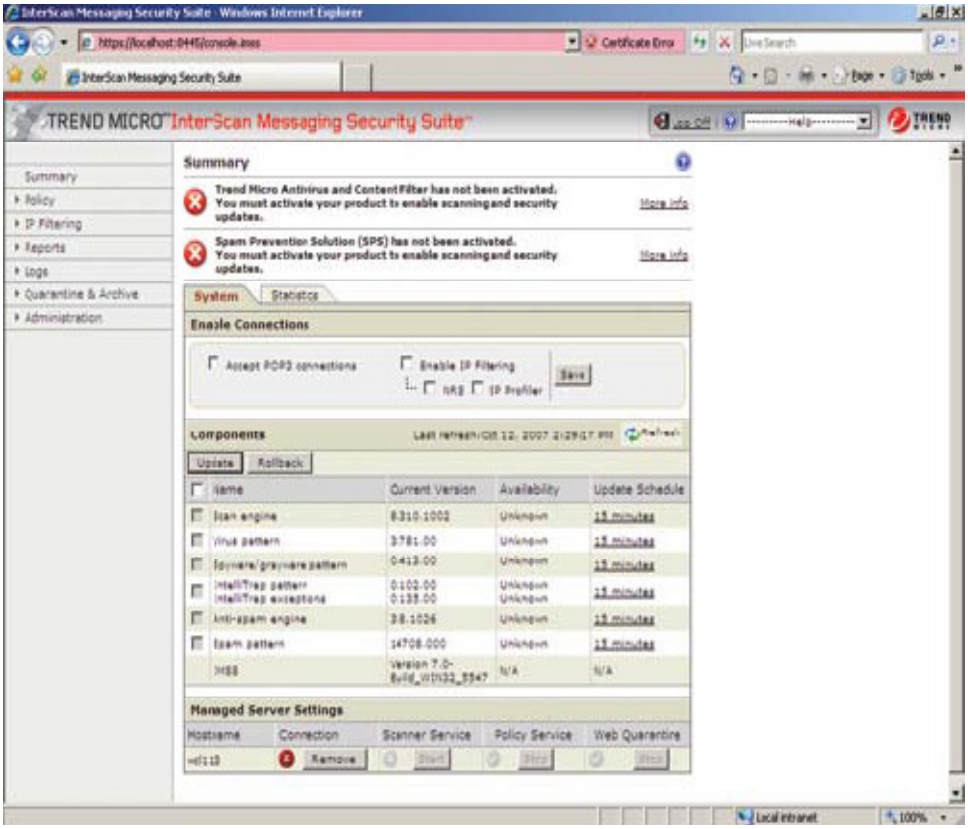

Figure 3 - Trend Micro InterScan Messaging Security

2.3.1 INTERSCAN MESSAGING SERVER SUITE FILTERING PROCESS

First, a message passes through Trend Micro's 32-bit virus scan engine. After the messages are checked for viruses, they're passed off to the content management portion of IMSS, that process is the key to battling spam and other e-mail-related problems. Trend Micro directs the advantage of policies toward content filtering, and those policies allow complete control of e-mail beyond spam management. Solution providers can script policies that prevent confidential data from being transmitted or create policies that identify unwanted messages. Policies clearly define what acceptable use of company e-mail is and what is not.

The primary reason for using IMSS is controlling spam. While policies can offer some protection from spam, the real answer to effectively fighting it lies with automation. IMSS employs complex heuristics to identify spam. Every message is examined for phrases or content that fits the profile of a spam message, and anti-spam heuristics can be tuned to filter based on content and determine how aggressively the antispam filtering should be applied. Administrators have several options for handling e-mail identified as spam. They can add the word "spam" to the subject line, redirect the suspect e-mail or quarantine the e-mail.

2.3.2 TREND MICRO SPAM PREVENTION SOLUTION

Spam Prevention Solution offers a comprehensive, multi-tiered spam and phishing defense. Three distinct tiers of anti-spam protection include E-mail Reputation, IP Profiler, and the anti-spam composite engine. The solution uses multiple techniques to keep threats completely off of the network, securing the network and preserving bandwidth, storage, and other network resources. Spam Prevention Solution includes patent-pending image spam detection technology and other cutting-edge approaches to protect organizations as spam and phishing threats evolve where it blocks most spam before it even reaches the gateway, uses the world’s largest most trusted reputation database, deploy dynamic reputation services to stop zombies and botnets as they first emerge, blocks e-mail senders that exceed threat thresholds set by the organization providing protection customized to the organization’s e-mail traffic, delivers automatic customer specific reputation services to stop spam, creates a firewall against bounced mail attacks, and combines multiple protective techniques including statistical analysis, advanced heuristics, whitelists, and blacklists. Also, it includes Features image spam detection and other cutting-edge technologies, content filtering and expanded language support to improve spam protection for global companies, provides dedicated anti-phishing techniques, including signatures, and reputation services to stop both corporate and consumer phishing attacks. Furthermore, it offers single Web-based management console to customize spam tolerance settings, create approved sender lists, establish filter actions, and set policies for individuals or groups. Moreover, it simplifies administration through LDAP integration, delegated administration, and message tracking. In addition to enabling end users to manage their own spam with Web-based End-User Quarantine and quarantine notification e-mails.

2.3.3 POLICIES OR RULE BASED DETECTION MISHAPS

Antivirus firm Trend Micro unwittingly targeted the letter "P" with a recent rules update, forcing all e-mail containing the objectionable letter into quarantine. According to their knowledge base article titled Solution 14638, "Antispam Rule 915 unintentionally blocks some legitimate e-mails scanned by InterScan eManager and ScanMail eManager." The cause is the letter P.

According to Trend Micro, the problem affects their Internet gateway, e-mail and groupware products, including InterScan Messaging Security Suite, InterScan eManager, ScanMail for Exchange, ScanMail eManager, and ScanMail for Lotus Notes. A spokesman for Trend Micro declined to comment on the issue, stating only that "we've notified customers and resellers." According to Internet Week, much of that contact was done via e-mail. One can only imagine the difficulty of composing an e-mail describing the nature of the problem while simultaneously avoiding the use of the letter P.

Trend Micro advises that the unfortunate P mishap can be resolved by updating to Antispam Rule 916 or later. Several of their products include options to resend e-mails erroneously quarantined by the filtering rules. Their Knowledge Base article Solution 14638 contains links to the support solutions for these products [6].

2.4 MAIL-SECURE

The Mail-Secure anti-spam solution is a product of the PineApp firm which uses pattern detection and includes the following features.

2.4.1 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%. Also, 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. Thus, PineApp has implemented a unique solution to decode images, and treat them with RPD similarly to other types of spam which improves the already superior spam catch rate, and maintains low false positive rate

2.4.2 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.

2.4.3 MAIL-SECURE FILTERING PROCESS

The web-based interface, presented to the user upon logging in, is very easy to use and clutter free. The interface presents its data in a clear and straightforward manner, with minimal delay when saving any configuration changes. For added security, the interface also includes a timeout

function, returning the administrator to the login page after a set period of inactivity. Mail-SeCure's method of protecting against spam is controlled through the use of policies.

Mail-SeCure is a leading perimeter security appliance that protects all sized organizations (from 50 up to 10,000 users), from both targeted and non-targeted e-mail-related threats such as spam, viruses and malicious code.Mail-SeCure from PineApp is a gateway level device designed to offer e-mail protection to small or medium sized companies with support for up to 500 users. While this test was primarily concerned with spam detection, it should be noted that Mail-SeCure also provides protection from e-mail borne malware.

Configuration of Mail-SeCure is made simple by the provision of a well-written and easy to follow quick installation guide. Within the policies configuration screen, there are four separate rule groups available to the administrator. These are Attachment, Spam, General, and Black & White Rules. Each of these rule groups shares a similar layout, allowing for familiarization with the method by which these rules may be configured. When dealing with spam, Mail-SeCure splits the traffic into one of three types Local to Local, Remote to Local, and Local to Remote, effectively covering both internal and external mail. Each of these three traffic types may have its own policy. For the purposes of reviewing statistics relating to processed e-mail, Mail-SeCure provide five separate report pages. Included among these are Summary, Reports, User Reports, Domain Reports, and Statistics [7][8].

Figure 4 shows a sample e-mail message that contains two parts within its body, one part is an image that has written spam text embedded in it and the other is a legitimate text written beneath the image crafted in order to foil anti-spam solutions.

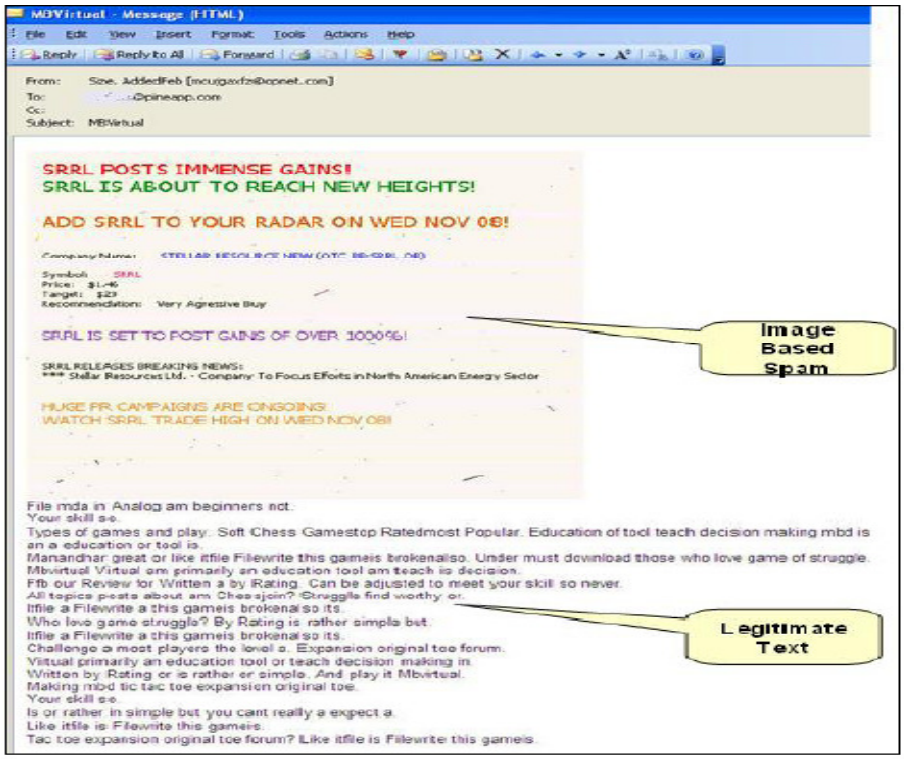

Figure 4 – E-mail Spam sample

2.5 PUBLICATIONS AND LITERATURE

Zhe Wang, William Josephson, Qin Lv, Moses Charikar, Kai Li[9] in Filtering Image Spam with Near-Duplicate Detection propose an image spam detection system that uses near-duplicate detection to detect spam images, they rely on traditional anti-spam methods to detect a subset of spam images and then use multiple image spam filters to detect all the spam images that "look" like the spam caught by traditional methods. Battista Biggio, Giorgio Fumera, Ignazio Pillai, Fabio Roli[10] in Image Spam Filtering by Content Obscuring Detection propose an approach based on low-level image processing techniques to detect one of the main characteristics of most image spam, namely the use of content obscuring techniques to defeat OCR tools by finding the noise level of a certain image spam. Jason R. Bowling, Priscilla Hope, Kathy J. Liszka[11] in Spam Image Identification Using an Artificial Neural Network propose a method for identifying image spam by using FANN (Fast Artificial Neural Network) library model and training the artificial neural network. A detailed process for preprocessing spam image files is given, followed by a description on how to train an artificial neural network to distinguish between ham and spam. M. Muztaba Fuad, Debzani Deb, M. Shahriar Hossain[12] in A Trainable Fuzzy Spam Detection System presents the design and implementation of a trainable fuzzy logic based e-mail classification system that learns the most effective fuzzy rules during the training phase and then applies the fuzzy control model to classify unseen messages. M. Soranamageswari, C. Meena[13] in Statistical Feature Extraction for Classification of Image Spam Using Artificial Neural Networks present an experimental system for the classification of image spam by considering statistical image feature histogram and mean value of an block of image. A comparative study of image classification based on color histogram and mean value is presented.

Ms.D.Karthika Renuka, Dr.T.Hamsapriya, Mr.M.Raja Chakkaravarthi and Ms.P.Lakshmisurya (2011)performed a comparative analysis on spam classification based on supervised learning using several machinelearning techniques. In this analysis, the comparison was done using three different machine learningclassification algorithms viz. Naïve Bayes, J48 and Multilayer perceptron (MLP) classifier. Resultsdemonstrated high accuracy for MLP but high time consumption. While Naïve Bayes accuracy was low thanMLP but was fast enough in execution and learning. The accuracy of Naïve Bayes was enhanced using FBLfeature selection and used filtered Bayesian Learning with Naïve Bayes. The modified Naïve Bayes showed theaccuracy of 91% as in [14].

Rushdi Shams and Robert E. Mercer (2013) performed a comparative analysis on classification of spam emailsby using text and readability features. This paper proposed an efficient spam classification method along with feature selection using content of emails and readability. This paper used four datasets such as CSDMC2010,Spam Assassin, Ling Spam, and Enron-spam. Features are categorized into three categories i.e. traditionalfeatures, test features and readability features. The proposed approach is able to classify emails of any languagebecause the features are kept independent of the languages. This paper used five classification based algorithmfor spam detection viz. Random Forest (RF), Bagging, Adaboostm 1, Support Vector Machine (SVM) andNaïve Bayes (NB). Results comparison among different classifiers predicted Bagging algorithm to be the bestfor spam detection as in [15].

Megha Rathi and Vikas Pareek(2013) performed an analysis on spam email detection through Data Mining byperforming analysis on classifiers by selecting and without selecting the features as in [16].

Anirudh Harisinghaney, Aman Dixit, Saurabh Gupta and Anuja Arora (2014) performed a comparative analysison text and images by using KNN, Naïve Bayes and Reverse-DBSCAN Algorithm for email spam detection.This analysis paper proposed a methodology for detecting text and spam emails. They used Naïve Bayes, K-NNand a modified Reverse DBSCAN (Density-Based Spatial Clustering of Application with Noise) algorithm's.Authors used Enron dataset for text and image spam classification. They used Google's open source library,Tasseract for extracting words from images. Results show that these three machine learning algorithms givesbetter results without preprocessing among which Naïve Bayes algorithm is highly accurate than otheralgorithms as in [17].

Savita Pundalik Teli and Santosh Kumar Biradar (2014) performed an analysis on effective email classificationfor spam and non-spam emails as in [18].

Izzat Alsmadi and Ikdam Alhami (2015) performed an analysis on clustering and classification of email contentsfor the detection of spam. This paper collected a large dataset of personal emails for the spam detection ofemails based on folder and subject classification. Supervised approach viz. classification along-sideunsupervised approach viz. clustering was performed on the personal dataset. This paper used SVMclassification algorithm for classifying the data obtained from K-means clustering algorithm. This paperperformed three types of classification viz. without removing stop words, removing stop words and using Ngrambased classification. The results clearly illustrated that N-gram based classification for spam detection isthe best approach for large and Bi-language text as in [19].

Ali Shafigh Aski and Navid Khalilzadeh Sourati (2016) performed an analysis using Machine Learning". Thispaper utilized three machine learning algorithms viz. Multi-Layer Neural Network, J48 and Naïve BayesClassifier for detection of spam mails from ham mails using 23 rules. The model demonstrated high accuracy incase of MLP with high time for execution while Naïve Bayes showed slightly less accuracy than MLP and alsolow execution time as in [20].

3. CONCLUSIONS

Image Spam detection have been causing problems from the first day it was known and up till now with all the solutions that have been developed by various venders and users, it still poses a great threat and still able to penetrate to the user's e-mail and up till now various venders still look at enhancing and updating their algorithms in order to achieve a higher detection rate with lowers false positive, and the reason that keeps this ongoing problem is the ways that the spammers are employing to fool those algorithms. In this paper, we introduced some of the available solutions for tackling spam and image based spam, where the light is shed on the process and technique used to battle spam and the different features each solution contains.

REFERENCES

[1] Cormack, Gordon V (2008), Email Spam Filtering: A Systematic Review. Now Publishers Inc, ISBN 978-1601981462

[2] Gyöngyi, Zoltán; Garcia-Molina, Hector (2005), "Web spam taxonomy", Proceedings of the First International Workshop on Adversarial Information Retrieval on the Web (AIRWeb), 2005 in The 14th International World Wide Web Conference (WWW 2005) May 10, (Tue)-14 (Sat), 2005, Nippon Convention Center (Makuhari Messe), Chiba, Japan., New York, N.Y.: ACM Press, ISBN 1-59593-046-9

[3] Gonzalez, Rafael C.; Woods, Richard E. (2008), Digital Image Processing, 3rd edition, Prentice Hall, ISBN 9780131687288

[4] Symantec Corporation (2008), Symantec Brightmail AntiSpam Deployment Planning Guide

[5] Kaspersky Lab (2008), Kaspersky Anti-Spam 3.0 Administrators Guide

[6] Trend Micro Incorperated (2008), Trend Micro ScanMail, InterScan Security Guide

[7] PineApp Ltd (2007), Mail-SeCure Perimeter Security white paper

[8] PineApp Ltd (August 2009), Mail-SeCure Image-Based Spam Treatment white paper

[9] Zhe Wang; William Josephson; Qin Lv; Moses Charikar; Kai Li (2008), Filtering Image Spam with Near-Duplicate Detection, In Conference on E-mail and Anti-Spam (CEAS)

[10] Battista Biggio; Giorgio Fumera; Ignazio Pillai; Fabio Roli (2008), Image Spam Filtering by Content Obscuring Detection, In International Conference on Image Analysis and Processing (ICIAP)

[11] Jason R. Bowling; Priscilla Hope; Kathy J. Liszka (2009), Spam Image Identification Using an Artificial Neural Network, In International Conference on Artificial Neural Networks (ICANN)

[12] M. Muztaba Fuad; Debzani Deb; M. Shahriar Hossain (2005), A Trainable Fuzzy Spam Detection System, In International Conference on Computer and Information Technology (ICCIT)

[13] M. Soranamageswari; C. Meena (2010), Statistical Feature Extraction for Classification of Image Spam Using Artificial Neural Networks, In International Conference on Machine Learning and Cybernetics (ICMLC)

[14] D. K. Renuka, T. Hamsapriya, M. R. Chakkaravarthi and P. L. Surya, “Spam Classification Based onSupervised Learning Using Machine Learning Techniques”, in proc. IEEE- International Conference on Process Automation, Control and Computing, 2011, pp. 1–7.

[15] R. Shams and R. E. Mercer, “Classifying spam emails using text and readability features”, in proc. IEEEInternational Conference on Data Mining (ICDM), 2013, pp. 657–666..

[16] M. Rathi and V. Pareek, “Spam Email Detection through Data Mining-A Comparative Performance Analysis”, in International Journal of Modern Education and Computer Science, vol. 12, pp. 31-39, 2013.

[17] A. Harisinghaney, A. Dixit, S. Gupta, and Anuja Arora, “Text and image based spam email classification using KNN, Naïve Bayes and Reverse DBSCAN Algorithm”, in proc. IEEE-International Conference on Reliability, Optimization and Information Technology (ICROIT), 2014, pp.153-155.

[18] S. P. Teli and S. K. Biradar, “Effective Email Classification for Spam and Non- spam”, in International Journal of Advanced Research in Computer and software Engineering, Vol. 4, 2014.

[19] Alsmadi and I. Alhami, “Clustering and classification of email contents”, in Journal of King Saud University - Computer and Information Science -Elsevier, vol. 27, no. 1, pp. 46–57, 2015.

[20] A. S. Aski and N. K. Sourati, “Proposed efficient algorithm to filter spam using machine learning techniques”, in Pacific Science Review- A Natural Science Engineering- Elsevier, Vol. 18, No. 2, pp. 145–149, 2016.