Journal of KONBiN 2(5)2008
ISSN 1895-8281

SAFETY OF CORPORATION ELECTRONIC MAIL SERVERS

BEZPIECZEŃSTWO FIRMOWYCH SERWERÓW POCZTY ELEKTRONICZNEJ

Ireneusz J. Jóźwiak[1], Wojciech Laskowski[2], Artur Szleszyński[3]

(1,2) Wrocław University of Technology, Faculty of Computer Science and Management
Politechnika Wrocławska, Wydział Informatyki i Zarządzania50 -371 Wrocław ul. Łukasiewicza 5
(3) The Tadeusz Kosciuszko Land Forces Military Academy, Wroclaw
Wyższa Szkoła Oficerska Wojsk Lądowych im gen. Tadeusza Kościuszki
51-150 Wrocław ul. Czajkowskiego 109

e-mails: (1) ireneusz.jozwiak@pwr.wroc.pl, (2) wojciech.laskowski@pwr.wroc.pl**,**
(3) artur_szle@gazeta.pl

Abstract. The article describes potential threats for safety of corporation electronic mail servers. Electronic mail servers deliver the corporation the environment to communication with business partners, customers and employees. The unsolicited bulk mail, also known as a spam, can be the cause of improper work of the firm electronic mail system. The spam is one of channel to transmission of the malicious code, which can be used to attack on the corporation local area network. The publication describes potential threats for information security, which is transmitted through the mail servers. The article analyze some methods of reducing the risk of spam strike.

Key words: electronic mail servers, risk reduction, spam, safety of corporation email servers.

Streszczenie: Artykuł opisuje potencjalne zagrożenia dla firmowych serwerów poczty elektronicznej. Serwery poczty elektronicznej dostarczają firmom środowisko do komunikacji z partnerami biznesowymi, klientami oraz pracownikami. Niechciana poczta, nazywana spam, może być przyczyną niepoprawnego działania firmowego systemu poczty elektronicznej. Spam stanowi jeden z kanałów przenoszenia "złośliwego" kodu, który może zostać wykorzystany do ataku na firmową lokalną sieć komputerową. Publikacja opisuje potencjalne zagrożenia dla bezpieczeństwa informacji przesyłanej za pomocą serwerów poczty**.** Artykuł analizuje wybrane metody redukcji ryzyka ataku za pomocą spamu.

Słowa kluczowe: serwery poczty elektronicznej, spam, redukcja ryzyka, bezpieczeństwo firmowych serwerów poczty elektronicznej.

SAFETY OF CORPORATION ELECTRONIC MAIL SERVERS

1. Introduction

The role of electronic mail servers, in contemporary company or institution, is deliver effective way to communication between organization and business partners or customers. The goal of sending unsolicited messages are to offer, the recipient, unwanted goods, services, collecting the information which are needed to overtake the control under the object of attack i.e. computer of employee. The spam, during last year [4], became one of the biggest channel of transmitting the malicious code (trojans, exploits, viruses, etc.). The malicious code, installed in the infected computer, could to steal the sensitive information and to send them to the attacker. Loss of confidential assets like business information, in result of security incident, may be the cause of serious impacts for organization. To group of these impacts belongs: financial losses, loss of market position, loss of good public image of company or legal consequences.
Symantec Internet Security Threats Report presents, that the messages classified as a spam, are responsible for 61% [4] of traffic related with electronic mail services. The most number of malicious code was prepared to steal and disclosure the confidential information win over infected computers. Presented facts are the proof, that the threat of spam attack is the real threat and it should not be treat only as an annoying incident.

2. Filtering unsolicited messages

The question of filtering the unsolicited messages is discussed in many publications. Fight with spam are devoted science conferences organized each year by MIT. In his book J. Zdziarski [5] is described the method based on technique of generating the signal no. 451 “Server is busy now”, which delays receiving the spam messages. This method is effective when the attack is provided by the sending agents, which only tries to send all messages in mail order queue. Different technique is creating black and white lists of sending servers, but described method is less effective. Good results, in spam message filtering, are given by using statistical filtering and the contents classification [1],[2],[5]. The Bayesian method of classification

of text is used by open source and commercial antispam filter solutions [5], [7]. These technique is characterized by good reliability of filtering. In effective spam attack can be used the vulnerability of sending host like open relay. This vulnerability can be used by the attacker to hide the source of spam and can compromised the company which is the owner of the server. The negative impacts of this incident may be cause of serious legal and business consequences.

3. Black and white lists of sending hosts

First strategy in reduction threat of unsolicited bulk mails attack, is to create the black list of sending hosts. Each letter, at its header has a field RECEIVED [3]. Field contains the information about the source of message (IP address of the electronic mail server). When the message is classified as a spam, the information from field RECEIVED IP address, the value of the field is read and compare with records in the database. If the IP address of incoming message is matching to the one from the database, the message is classified as a spam and the letter is deleting from the queue of incoming messages. The disadvantage of this method classification is the probability creation database with large number of records. In testing probe of the 100 letters, classified as a spam, source IP address repeats only two times, rest of 98 IP address occurred, in sample probe, only one time (table 1).

Table 1. The repetition of IP address in the testing probe of spam messages

	Source IP address
The total number of IP address:	100
The number of repeated sending hosts IP address:	2
The number of unique sending hosts IP address:	98

Because each IP address contains the information about network and host identification the next question which should to be consider is – from which class of IP address is coming the biggest number the spam messages? In analyzing testing probe, the most number of spam letter had the A class source IP address (table 2).

Table 2. The distribution of classes IP addresses in testing probe of spam messages

Class of IP Address	A	B	C
Number of repetition	68	8	24

The explanation for that fact is, the most number of IP address belong to the A class of IP addresses, is only first octet is related with the identification of network. The IP address from A class are often used by public Internet providers. This feature gives the potential attacker good possibility to hide a real starting place of sent spam.
Method of filtering the spam messages based on IP addresses is small effective. There is the possibility to built the filter with decision rule based on preliminary IP addresses analysis. The classification rule can describe three values of prior probability of being the spam i.e.: 0.7 for messages with A class IP address, 0.1 for messages with B class IP address and 0.2 for messages with C class IP address.
Different type of filtering incoming messages is based on white list – legitimate – email servers. The destination server accept only the messages sent from the trusted severs. The disadvantage of the white list is reality that the destination server never receive the message from source outside the list. This method is of protection is convenient only in case communication with constant number of servers.

4. Contest analysis and Bayesian filtering

The idea of message analysis is based on the text categorization. The mechanism of filtration is used the words, contained in legal and spam mails, to comparative the number of repetition each word in two categories of electronic letters. The result of the process of analysis is decision matrix, which classified the words. Decision matrix contains the information about the estimated value of the word. The estimation of value the word is made with the usage of mathematical formula (1)[5],[6], evaluate to categorize the word to class of legitimate or spam messages. The evaluate value is mean by the letter P. If the value P is more than 0.5 it suggest the word often were used in spam messages, the conclusion, message is probably a unsolicited mail. If the value of parameter P is less 0.5, the word is categorized to group of legitimate mails, the conclusion, message is probably legal mail. If the value of parameter P is more than 0.5, which mean that the word is often present in spam than the legal messages, word is attached to group of spam messages. The example of these kind of words are: viagra, replica, watches,

etc. To good categorization each examined word should occur minimal in five spam or legal letters.

$$P = \frac{SH \cdot TS}{(SH \cdot TS) + (IH \cdot TI)} \tag{1}$$

where:
SH – number of repetition the word in spam messages,
IH – number of repetition the word in legal messages,
TS – total number of spam messages,
TI – total number of legal (innocent) messages.

The parameter P can take value from 0 – for innocent letter – to 1 – for spam messages. In testing probe the most frequent word was the words "the" which occur 37 times, "and" 27 repetition. The taking this kind of words as the spam indication words is mistake, because these words could be the part of legal letters to. The words which the best identify the spam messages are: "boyfriend" – 7 repetitions, "cock" – 4 repetitions, "medication" – 4 repetitions, "sex" and "sexual" together 6 repetitions, "girls" – 3 repetitions, etc. Chosen words do not belong to the group of words used in business correspondence. These kind of words well identified the unsolicited character of the message. The shown words could be used to built the decision matrix. Then the filter is searching inside the header and the body of letter words classified as the spam identifier. The auxiliary words like article "the" or "and" would get the value parameter P around 0.4 [5]. The problem, which can be find, related with text categorization is using in spam messages separation marks in place of the letters i.e.: word "He110" than the word "Hello". The text searching engine, which analyses the messages, has to recognize the proper shape of masked words. The probe of built the analysis engine on typical programming construction like "***if … then …***" is to require constant changes in the software, which helps the filter in proper recognition the example words: "\/iagara" and "V1agra" and "V_I_A_G_R_A" and "V\1\A\G\R\A" as the word viagra. That's why classification engine should be based on the artificial intelligence technique like i.e. artificial neuron network filtering (ANNF). The filter used the technique ANNF can quickly recognize words typical for spam mails. There is needed the process of training the neuron network, but after the process of learning (or self learning) network can find out new words characterized the spam messages.
There was no examined the question of spam messages in languages different than English language. This is the result of lack the unsolicited

messages in testing probe, which were written in Polish or Spanish language. We can expect, that this kind of classification will be need completely new decision matrix with new words in characterized the unsolicited message in different languages. The first step in examination of the content of the message will be identify the language, which was used email, then chose the proper decision matrix.

5. Summary

The probe of built of filter on the black list junk mails host is less effective, in sample probe only one IP address was repeated. Building the big matrix (data base) which contains potential sources of unsolicited messages, may have the influence on effective work of spam filter.
The analytical engine should to use the techniques of artificial intelligence, which will be useful in recognition the modification of typical shape of the word. The problem which is expected to occur, if there would be used the technique of artificial neuron network, is the process of training the network. Well trained network can recognize the changed shape of the words and properly classified the recognized word to the group of spam.
There was not analyzed the question of wrong classification of letters. Incorrect classification can be the result Bayesian poisoning attack [5],[6], and there was no analyze the question of multi language spam classification.

References

[1] Graham P., *Better Bayesian Filtering*, January 2003, www.paulgraham.com/better.html.
[2] Graham P., *Plan for Spam*, August 2002, www.paulgraham.com/spam.html.
[3] RFC-822, *Standard For The Of ARPA Internet Text Message*.
[4] *Symantec Internet Security Threats Report Trends for January-June 07*, Volume XII, http://www.symantec.com/business/theme.jsp?themeid=threatreport
[5] Zdziarski J., *Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification, [in polish]*, PWN, Warszawa 2005.
[6] Zdziarski J., *Bayesian Noise Reduction: Contextual Symmetry Logic Utilizing Pattern Consistency Analysis*, 2004, http://www.zdziarski.com/papers/bnr.html
[7] Yerazunis W., *Sparse Binary Polynomial Hashing and the CRM114 Discriminator*, http://crm114.sourceforge.net/.

BEZPIECZEŃSTWO FIRMOWYCH SERWERÓW POCZTY ELEKTRONICZNEJ

1. Wprowadzenie

Zadaniem serwerów poczty elektronicznej, we współczesnej firmie lub instytucji, jest dostarczenie efektywnego sposobu do komunikacji pomiędzy organizacją, a partnerami biznesowymi oraz klientami. Celem niechcianych wiadomości jest oferowanie, odbiorcy, niepotrzebnych towarów, usług, zbieranie danych przydatnych do przejęcia kontroli nad obiektem ataku np. komputerem pracownika. Spam, w ciągu ostatniego roku [4], stał się jednym z największych kanałów przesyłania „złośliwego kodu" (koni trojańskich, exploitów, wirusów, itp.). Złośliwe oprogramowanie, zainstalowane w zaatakowanym komputerze, może wykraść wrażliwe dane przesyłając je do atakującego. Utrata poufnych zasobów, jakimi są informacje biznesowe, w skutek wystąpienia incydentu w bezpieczeństwie, może być przyczyną niekorzystnych następstw dla organizacji. Należą do nich: straty finansowe, utrata pozycji rynkowej, utrata dobrego wizerunku firmy lub pozwy do sądu.
Raport firmy Symantec dotyczący zagrożeń występujących w sieci Internet podaje, że wiadomości klasyfikowane jako spam, stanowią 61% ruchu odpowiedzialnego za wymianę pocztową [4]. Większość złośliwego kodu przygotowana jest w celu kradzieży oraz rozpowszechnienia poufnych informacji pozyskanych z zaatakowanych komputerów. Przedstawione dane są dowodem, że atak przy użyciu spamu jest rzeczywistym zagrożeniem i nie powinien być odbierany tylko jako irytujący incydent.

2. Filtracja niechcianych wiadomości

Kwestia filtracji niechcianej poczty opisywana jest w wielu publikacjach. Walce ze spam poświęcone są coroczne konferencje naukowe organizowane przez MIT. W swojej książce J. Zdziarski [5] opisuje metodę wykorzystującą sygnał nr 451 „Serwer aktualnie jest zajęty", który opóźnia odbieranie spamu. Metoda jest skuteczna w przypadku ataków przeprowadzanych za pomocą agentów wysyłkowych, które próbują wysłać wszystkie wiadomości znajdujące się w kolejce. Inną techniką jest tworzenie czarnych i białych list serwerów poczty elektronicznej, jednak

przedstawiona metoda jest mało skuteczna. Dobre wyniki, w filtracji niechcianej poczty, uzyskiwane są poprzez wykorzystanie filtracji statystycznej oraz klasyfikacji zawartości [1],[2],[5]. Bayesowska klasyfikacja tekstu wykorzystywana jest przez filtry antyspamowe open source oraz komercyjne [5],[7]. Technika ta charakteryzuje się wysoką niezawodnością. Do skutecznego ataku niechcianą pocztą może zostać wykorzystana podatność serwera poczty elektronicznej jaką jest przekazywanie. Podatność może posłużyć atakującemu do ukrycia źródła spamu oraz do kompromitacji firmy będącej właścicielem serwera poczty elektronicznej. Negatywnymi skutkami wymienionego incydentu mogą być problemy prawne i biznesowe firmy.

3. Czarne i białe listy serwerów poczty elektronicznej

Pierwszą strategią w redukcji ryzyka ataku za pomocą niechcianej poczty, jest przygotowanie czarnej listy serwerów poczty elektronicznej. Każdy list, w polu nagłówka posiada pole RECEIVED [3]. Pole przechowuje informację o źródle wiadomości (adres IP serwera nadawcy). Kiedy wiadomość poddawana jest procesowi klasyfikacja do spamu, wartość pola zostaje odczytana i porównana z rekordami umieszczonymi w bazie danych. Jeżeli, adres IP przychodzącej wiadomości, odpowiada, któreś z wartości umieszczonej w bazie danych, wówczas wiadomość klasyfikowana jest jako spam i wiadomość zostaje usunięta z kolejki listów przychodzących. Wadą opisanej metody jest prawdopodobieństwo utworzenia bazy danych zawierającej dużą ilość adresów IP serwerów rozpowszechniających niechcianą pocztę. W próbie testowej 100 listów zaklasyfikowanych, jako spam, taki sam adres IP wystąpił tylko dwa razy, pozostałe 98 adresów IP wystąpiły tylko jeden raz (tabela 1).

Tabela1. Powtarzalność adresów IP w próbie testowej, wiadomości spam

	Adres IP serwera nadawcy
Całkowita liczba adresów IP w próbie:	100
Liczba powtórzeń adresów IP:	2
Liczba niepowtarzalnych adresów IP:	98

Ponieważ każdy adres IP zawiera informację o numerze sieci oraz komputera, kolejną kwestią, którą można rozważyć jest ustalenie, z której klasy adresów IP pochodzi największa liczba listów typu spam? W analizowanej próbie badawczej, największa liczba adresów należała do klasy A adresów IP (tabela 2).

Tabela 2. Rozkład klas adresów IP w badanej próbie poczty typu spam

Klasa adresów IP	**A**	**B**	**C**
Liczba wystąpień	**68**	**8**	**24**

Wytłumaczenie tego faktu jest następujące. Największa liczba serwerów nadawców wiadomości typu spam należy do klasy A, ale tylko pierwszy oktet identyfikuje sieć. Ta cecha pozwala potencjalnemu atakującemu na skuteczne ukrycie rzeczywistego miejsca rozpoczęcia ataku. Metoda wykorzystującą w procesie filtracji adres źródła wiadomości jest mało skuteczna. Istnieje możliwość zbudowania filtra z regułą decyzyjną wykorzystującą wstępną ocenę adresu IP. Reguła decyzyjna mogłaby klasyfikować wiadomości jako spam z wagami: 0,7 – dla adresów IP klasy A, 0,1 – dla adresów IP klasy B, 0,2 – dla adres IP klasy C.
Innym rodzajem filtrowania dostarczanej poczty jest wykorzystanie białej listy – akceptowanych – serwerów poczty elektronicznej. Serwer odbierający przesyłkę akceptuje tylko te wiadomości, które pochodzą od zaufanych serwerów poczty. Wadą metody białej listy jest odrzucanie przez serwer docelowy wiadomości, których źródło nie zostało umieszczone w liście. Opisana metoda jest użyteczna w przypadku komunikacji z niezmienną liczbą serwerów.

4. Analiza zawartości i filtracja Bayesowska

Pomysł analizy wiadomości oparty jest na kategoryzacji tekstu. Mechanizm filtracji korzysta ze słów umieszczonych w treści wiadomości, legalnych i niechcianych, do porównania ilości powtórzeń każdego ze słów w obu kategoriach wiadomości. Wynikiem procesu analizy jest macierz decyzyjna klasyfikująca słowa. Macierz decyzyjna zawiera informacje o szacowanej wartości słowa. Szacowana wartość słowa obliczana jest na podstawie wzoru (1)[5],[6]. Ocenia on przynależność słowa do klasy wiadomości legalnych lub niechcianych. Szacowana wartość oznaczana jest literą P. Jeżeli wartość parametru P jest mniejsza niż 0,5, słowo jest klasyfikowane do grupy wiadomości akceptowanych. Również wiadomość może być

traktowana jako wiadomość akceptowana. W przypadku, gdy wartość parametru P jest większa niż 0,5, co oznacza, że słowo częściej występuje w poczcie niechcianej niż legalnej, słowo jest przypisywane do grupy spamu.

$$P = \frac{SH/TS}{(SH/TS) + (IH/TI)} \tag{1}$$

gdzie:
SH – liczba wystąpień słowa w przesyłce poczty niechcianej,
IS - liczba wystąpień słowa w przesyłce akceptowanej,
TS – liczba wiadomości niechcianych,
TI – liczba wiadomości legalnych.

Przykładami tego typu słów są: „viagra", „replica" i „watches", itp. Żeby proces klasyfikacji przebiegł poprawnie każde sprawdzane słowo musi wystąpić co najmniej 5 razy w przesyłkach legalnych lub spamie.
Parametr P może przyjmować wartości od 0 – poczta akceptowana – do 1 – poczta niechciana. W badanej populacji wiadomości najczęściej powtarzającymi się słowami były słowa „the" - 37 wystąpień, „and" - 27 wystąpień. Przyjęcie wymienionych słów, jako wskaźników spamu jest błędne, ponieważ wymienione słowa będą występować w legalnej poczcie. Słowami, które jednoznacznie identyfikują przesyłki spamowe są: "boyfriend" – 7 wystąpień, "cock" – 4 wystąpienia, "medication" – 4 powtórzenia, "sex" i "sexual" w sumie 6 powtórzeń, "girls" – 3 powtórzenia, itp. Przedstawione słowa nie należą do grupy słów używanych w korespondencji biznesowej. Wymieniona grupa słów umożliwia identyfikację niechcianej poczty, które zostaną wykorzystane do tworzenia macierzy decyzyjnej. Filtr poszukuje w nagłówku i ciele wiadomości słów umieszczonych w macierzy. Wyrazy posiłkowe takie, jak „have", „and" itp. będą posiadały wartość parametru P = 0.4. Problemem, z jakim można się spotkać, w kategoryzacji tekstu jest obecność znaków rozdzielających w miejscu liter np. „He110" zamiast „Hello". Silnik analityczny, przeszukujący wiadomość, musi rozpoznać właściwe postać ukrytych słów. Próba zbudowania silnika analitycznego w oparciu o konstrukcję instrukcji warunkowych „***if .... then ...***" wymaga ciągłych zmian w oprogramowaniu, które pozwolą filtrowi na właściwe rozpoznanie przykładowych słów: "\/iagara" and "V1agra" and "V_I_A_G_R_A" and "V\1\A\G\R\A" jako słowo viagra. Dlatego zaleca się budowanie silnika analitycznego filtra w oparciu o techniki sztucznej inteligencji np. sztucznych sieci neuronowych. Konieczny jest proces treningu sieci w celu właściwego

rozpoznawania słów charakterystycznych dla niechcianej poczty.
Nie badano kwestii niechcianej poczty wysyłanej w językach innych niż język angielski. Jest to wynikiem braku niechcianych wiadomości, w badanej próbie, napisanych w językach np. polskim lub hiszpańskim. Można oczekiwać, że ten rodzaj kategoryzacji będzie wymagał nowej macierzy decyzyjnej zawierającej słowa charakteryzujące niechciane przesyłki w różnych językach. Pierwszym krokiem w analizie wiadomości będzie ustalenie języka, użytego do napisania listu elektronicznego, a następnie wybranie odpowiedniej macierzy decyzyjnej.

5. Podsumowanie

Próba zbudowania filtra na bazie czarnej listy serwerów niechcianej poczty jest nieskuteczna, w badanej próbie, powtórzył się tylko jeden adres IP. Tworzenie dużej macierzy (bazy danych) zawierającej potencjalne źródła niechcianej poczty, może być przyczyną nieefektywnego działania filtra.
Silnik analityczny powinien korzystać z technik sztucznej inteligencji, który będzie skuteczny w rozpoznawaniu zmienionej postaci słów. Problemem, który może pojawić się w przypadku korzystania z techniki sztucznych sieci neuronowych, jest proces uczenia sieci. Właściwie wytrenowana sieć jest wstanie rozpoznać zmienioną postać poprawnie klasyfikując słowo do grupy przesyłek niechcianych.
W publikacji nie analizowano błędnych klasyfikacji wiadomości. Błędna klasyfikacja może być wynikiem ataku określanego terminem „zatruwania" filtra [5],[6]. Nie analizowano kwestii rozpoznawania języka wiadomości i kategoryzowania ich do grupy spamu lub poczty akceptowanej.

Literatura

[1] Graham P., *Better Bayesian Filtering*, 2003, [on-line], dostępny w World Web Wide: www.paulgraham.com/better.html.

[2] Graham P., *Plan for Spam,*2002, [on-line], dostępny w World Web Wide: www.paulgraham.com/spam.html.

[3] RFC-822, *Standard For The Of ARPA Internet Text Message*.

[4] *Symantec Internet Security Threats Report Trends for January-June 07, Volume XII, 2007,* [on-line], dostępny w World Web Wide: http://www.symantec.com/business/theme.jsp?themeid=threatreport

[5] Zdziarski J., *Spamowi stop! Bayesowskie filtrowanie zawartości i sztuka statystycznej klasyfikacji języka*, PWN, Warszawa 2005.

[6] Zdziarski J., *Bayesian Noise Reduction*: *Contextual Symmetry Logic Utilizing Pattern Consistency Analysis,* 2004, [on-line], dostępny w World Web Wide: http://www.zdziarski.com/papers/bnr.html

[7] Yerazunis W., *Sparse Binary Polynomial Hashing and the CRM114 Discriminator,* [on-line], dostępny w World Web Wide: http://crm114.sourceforge.net/.

Ireneusz J. Jóźwiak is a Profesor at Institute of Applied Informatics in Wrocław University of Technology. He is a chief of computer security section in the Institute. He is interested in problems of reliability and security of information systems. He does research in functional and structural reliability.

Wojciech Laskowski is a PhD student at Institute of Applied Informatics in Wrocław University of Technology. He also works as a consultant in computer security domain. He is interested in problems of computer security, especially in managing security.

Artur Szleszynski is a Lecturer in The Tadeusz Kosciuszko Land Forces Military Academy. He also works as Local Area Network administrator. He is interested in problems of computer security, especially in security requirement managements.