SPAM PAL

for Windows

Spis treści

Formalności

Najnowsza wersja dokumentu

Najnowsza wersja tego dokumentu dostępna jest pod adresem http://www.nospam-pl.net/

Prawa autorskie

Dokument powstał przy wykorzystaniu materiałów źródłowych w języku angielskim, których prawa autorskie należą do właściwych autorów. Szczegóły praw autorskich do dokumentów opisuje http://spampal.org/usermanual/credits.html

Licencja

Zastrzeżenie

Informacje o autorze

Adres poczty elektronicznej: mailto:usenet@hoga.pl

Podziękowanie

Szczególne podziękowania należą się Łukaszowi Kozickiemu, za moralne i merytoryczne wsparcie oraz konsultacje w trakcie powstawania niniejszego dokumentu.

Wprowadzenie

Chyba każdy użytkownik poczty elektronicznej spotkał się z problemem spamu. Niechcianych przesyłek od - najczęściej - zupełnie obcych osób, które niepotrzebnie zajmują naszą uwagę, czas, miejsce w skrzynce i przepustowość łącza. Jeśli tych niechcianych przesyłek jest niewiele - 2-3 tygodniowo, uczymy się z tym żyć - używamy klawisza 'Delete' i zapominamy o przesyłce do momentu gdy... pojawi się ponownie kilka dni później!. To zatroskany nadawca poprzedniej przesyłki pyta, czy aby na pewno zapoznaliśmy się z jej zawartością - przecież to niemożliwe, by tak cudowna oferta pozostała bez odpowiedzi!. Kiedy ilość spamu zaczyna wzrastać, zaczynamy poszukiwać metod obrony przed nim - najpierw mozolnie tworzymy regułki w programie pocztowym, które blokują kolejne adresy nadawców... Lista zablokowanych adresów rośnie, lecz ilość niechcianych przesyłek spada tylko na chwilę, by powrócić ze zwiększoną mocą. Wszelkie prośby kierowane do nadawców spamu, przynoszą odwrotny do zamierzonego skutek - spamu jest coraz więcej, bo spamerzy skrzętnie odnotowują fakt, że odbiorca: a. istnieje, b. odbiera pocztę c. czyta ją - nasz adres staje się więc "chodliwym" towarem.. Kiedy ilość spamu przekroczy pewną masę krytyczną (wielkość ta jest różna w zależności od odporności użytkownika), decydujemy się na bardziej drastyczne metody ochrony przed spamem - niechcianą pocztą...
W tym momencie zazwyczaj wychodzi na jaw ułomność systemu Windows... Brak jest powszechnie dostępnych darmowych narzędzi, do walki ze spamem, a te które są - nie przystają do technologicznego zaawansowania metod działania spamerów. Nawet w serwisie NoSpam-PL czytamy (http://nospam-pl.net/obrona1.php), że pierwszym krokiem jest załatwienie sobie konta z dostępem do shella, procmaila itd... Tu pada litania technicznych terminów, które zwykłego użytkownika przyprawiają o zawrót głowy. Nawet jeśli coś te nazwy użytkownikowi mówią, to zazwyczaj może on tylko z zazdrością poczytać o możliwościach takich linuksowych narzędzi jak SpamAssassin, czy BogoFilter. Czy więc biedny użytkownik Windowsów i Outlook Expressa skazany jest na "śmierć przez zaspamowanie" ?. Okazuje się, że na szczęście nie. Pojawiło się ostatnio narzędzie, które pod wieloma względami dorównuje linuksowym rozwiązaniom, a jednocześnie jest na tyle proste w instalacji i konfiguracji, że nawet średnio zaawansowany 'klikacz' da sobie radę. To narzędzie zwie się **SPAM PAL**. Niniejszy dokument ma na celu "oswojenie" problematyki instalacji, konfiguracji i obsługi programu, rozwiązywania codziennych problemów, które mogą pojawić się w pracy z programem.

Co to jest SpamPal?

SpamPal jest narzędziem do wielowątkowej analizy i klasyfikacji przychodzącej poczty, które może pomóc w odsianiu spamu od wartościowych przesyłek.

Czego potrzebuję by używać SpamPal'a?

1. Komputera z Windows 95, 98, ME, NT , 2000 lub XP

2. Skrzynki pocztowej korzystającej z technologii POP3

3. Standardowego programu pocztowego takiego jak MSOutlook, Outlook Express, Eudora, czy TheBat

Spampal nie współpracuje z:

- AOL
- Hotmail
- Yahoo
- Juno
- MSN
- innymi systemami, które umożliwiają czytanie i wysyłanie poczty **wyłącznie** z poziomu strony www obsługiwanej przeglądarką internetową

Jak działa SpamPal?

SpamPal umiejscawia się pomiędzy programem pocztowym, a skrzynką i sprawdza nadchodzącą pocztę w trakcie jej ściągania. Każda przesyłka, którą SpamPal uzna za spam, zostanie **OZNAKOWANA** specjalnym nagłówkiem; do użytkownika będzie należało takie skonfigurowanie programu pocztowego, by ten filtrował pocztę w zależności od tego, czy taki znacznik się w niej znajduje. Możesz na przykład zażądać, by oznakowane przez SpamPala przesyłki, były automatycznie przenoszone do specjalnego katalogu, do kosza tak, by nie mieszały się z pożądanymi przesyłkami., lub od razu kasowane (nie zalecam kasowania, dopóki nie nauczysz SpamPala właściwej oceny przesyłek !!!). Zauważ, iż SpamPal sam z siebie **NICZEGO NIE KASUJE** - jest jedynie doradcą w ocenie przesyłek.

Ale jak to możliwe, że SpamPal wie, co jest spamem, a co nie ? Rozpoznawanie spamu odbywa się na kilka sposobów, jednak najważniejszym jest korzystanie z tzw. **DNSBL** (**DNS-based Blocking List**) lub **RBL** (**Realtime Blackhole List**) czyli mówiąc najprościej - "**czarnych list**" zawierających dane komputerów nadawców spamu. Rozsiane na całym

świecie bazy danych zbierają dane na temat spamu, ich nadawców, zaś zgromadzone i przetworzone dane są udostępniane innym użytkownikom sieci. Jeśli e-mail który otrzymujesz, pochodzi od nadawcy umieszczonego na jednej z takich czarnych list (slangowo mówi się o takich nadawcach, że zostali "**wylistowani**"), to istnieje bardzo duże prawdopodobieństwo, że przesyłka ta **jest spamem**. Niektórzy dostawcy skrzynek pocztowych nauczeni doświadczeniem, zablokowali już **W CAŁOŚCI** niektórych nadawców, czy serwery z których korzystają spamerzy. Ma to swoje odbicie również w owych "czarnych listach" - niektóre z nich "listują" w całości tak popularne w Polsce serwery jak **wp.pl** czy **go2.pl**, które notorycznie "wsławiają się" naruszaniem obowiązujących w internecie norm. Należy więc pamiętać, by przy zakładaniu skrzynki pocztowej na darmowym serwerze, zwrócić uwagę na opinię serwera "w środowisku". Należy unikać zakładania skrzynek na serwerach, które notorycznie są "**listowane**" (docelowo należy rozważyć wykupienie skrzynki na komercyjnym serwerze, który deklaruje ostrą politykę antyspamową - zarówno wobec swoich klientów, jak i przychodzącej poczty). Podobnie przy doborze serwerów DNSBL - metodą prób i błędów należy dobrać taki zestaw "doradców", by z jednej strony wychwytywać maksymalnie dużo niechcianej poczty, z drugiej zaś, liczba **"fałszywek",** czyli błędnie oznakowanych "dobrych przesyłek" (ang. **false-positives**) była jak najmniejsza. W dalszej części dokumentu przedstawię swoje sugestie co do doboru poszczególnych serwerów DNSBL.

Na początek jednak należy zapamiętać jedną ważną rzecz - jeśli ktoś z naszych znajomych korzysta z konta na takim skompromitowanym serwerze, należy zadbać o to, by przesyłki od niego nie były klasyfikowane jako spam. Możemy nakazać SpamPalowi, by przesyłki od określonego nadawcy, nie były poddawane analizie porównawczej z bazami DNSBL, lecz od razu dopuszczane do programu pocztowego. Do wskazywania naszych przyjaciół służy tak zwana "**biała lista**" (ang. whitelist).

Ile to kosztuje ?

SpamPal jest programem darmowym - możesz pobrać go z internetu bez żadnych opłat. Warto zaznaczyć, że oferowany jest pełnowartościowy program, bez jakichkolwiek ograniczeń funkcjonalnych, czy czasowych, bez szpiegujących, czy reklamowych wtyczek. W pełni funkcjonalna wersja programu jest ogólnie dostępna i może być wykorzystana bez żadnych ograniczeń. Jest to bardzo miłe zważywszy, iż znacznie mniejszej funkcjonalności narzędzia dla Windows kosztowały zazwyczaj kilkadziesiąt dolarów, a kompleksowe rozwiązania serwerowe - kilka tysięcy dolarów.

Jakkolwiek, wszelkie datki dla autorów programu są mile widziane.

INSTALACJA PROGRAMU

Instalacja i konfiguracja SpamPala i programu pocztowego do współpracy z nim, będzie wymagała odrobiny wysiłku, jednak z praktyki wynika, iż nie powinno to zająć więcej niż dziesięć minut.

Przedstawię poniżej ogólną instrukcję instalacji i konfiguracji programu pocztowego, jednak w przypadku każdego "klienta" będzie to wyglądało trochę inaczej, ze względu na inne położenie i wygląd poszczególnych opcji programu. Myślę jednak, że znasz już swój program pocztowy na tyle dobrze, że nie będzie problemów ze zlokalizowaniem poszczególnych opcji. Zanim przystąpimy do instalacji, najpierw trzeba ściągnąć program. http://spampal.org/download.html zawiera odnośniki do stron, skąd można ściągnąć program.

Krok pierwszy: Instalacja programu SpamPal

Instalację rozpoczynamy standardowo - od kliknięcia na ikonce instalatora programu SpamPal. Wystarczy odpowiedzieć (lub tylko zatwierdzić) na pytania o miejsce, gdzie chcemy zainstalować program, oraz w którym miejscu Menu Startowego chcemy umieścić odnośnik do programu. Kiedy SpamPal się zainstaluje, automatycznie się uruchomi i umieści swoją ikonkę w zasobniku systemowym - koło zegarka. Rozpoznamy go po różowej parasolce ;-),

Krok drugi: Konfigurowanie programu pocztowego do pracy z SpamPalem

Teraz, kiedy SpamPal już działa, trzeba powiedzieć programowi pocztowemu, jak z niego korzystać. Aby to zrobić, należy zmodyfikować ustawienia programu pocztowego w części dotyczącej serwerów poczty. Szukamy więc w Preferencjach / Opcjach / Ustawieniach programu (różnie się to nazywa w zależności od programu) następujących informacji:

- "**Incoming Mail Server**" lub "**POP3 server**" lub "**Serwer poczty przychodzącej**" lub "**Poczta przychodząca (POP3)"**
  lub podobnie nazwanej opcji dotyczącej nazwy / adresu naszego serwera poczty przychodzącej
- "**POP3 Username**" lub "**Account Name**" lub "**Nazwa użytkownika poczty przychodzącej**"
  lub podobnie nazwanej opcji dotyczącej loginu (identyfikatora / nazwy) jaką podajemy by, zalogować się na serwer celem odebrania poczty

Kiedy już zlokalizujesz powyższe opcje programu, musisz je zmodyfikować w następujący sposób:

Nazwę użytkownika, np. : **jankowalski** mienić na **jankowalski@pop3.serwerpoczty.pl**

(gdzie pop3.serwerpoczty.pl to nazwa właściwego serwera poczty przychodzącej z którego korzystamy). Następnie w pole "**serwer poczty przychodzącej**" zamiast znajdującej się tam informacji (nazwa serwera poczty z którego korzystamy) wpisujemy **localhost** lub, jeśli program się buntuje, wpisujemy tam adres **127.0.0.1**

UWAGA: Użytkownicy programu Netscape / Mozilla zamiast znaczka "@" będą musieli prawdopodobnie użyć znaczka "%" (procent).

Jeśli mamy więcej niż jedną skrzynkę pocztową zdefiniowaną w programie pocztowym, z każdą kolejną postępujemy analogicznie.

Czas na pierwszą próbę !. Wróć do głównego okna swojego klienta poczty i wydaj polecenie sprawdzenia zawartości skrzynki. Jeśli wszystko jest w porządku, to parasolka w zasobniku systemowym powinna się uaktywnić (animowane kolorki) - jeśli coś jednak jest nie tak, trzeba wrócić do okna konfiguracyjnego programu pocztowego i sprawdzić, czy nie popełniliśmy błędu przy wpisywaniu danych - być może wkradła się jakaś "literówka", albo podałeś błędną nazwę serwera i program nie potrafi wykonać polecenia. Jeśli w naszym systemie mamy uruchomioną tak zwaną "zaporę ogniową" (ang. firewall), to najprawdopodobniej otrzymamy komunikat, że program SpamPal chce się połączyć z internetem - jest to jak najbardziej pożądane, więc należy mu na to zezwolić. Jeśli żaden komunikat się nie pojawi, a SpamPal nadal nie będzie mógł połączyć się z serwerem, oznacza to, iż musimy ręcznie stworzyć regułkę w naszym firewallu, przepuszczającą program SpamPal na porcie 110 (jeśli na tym porcie pracuje serwer z którego korzystamy - w większości wypadków tak jest).

Krok trzeci: Konfigurujemy filtry poczty !

Następnym krokiem będzie stworzenie oddzielnego katalogu w obrębie programu pocztowego, do którego wrzucane będą przesyłki uznane za spam. Czynność ta ma na celu oddzielenie spamu (lub czegoś co na spam wygląda) od prawidłowej poczty. Na początku pracy ze SpamPalem, mogą się pojawić problemy z błędną oceną przesyłek - spam zostanie uznany za normalną pocztę, lub list od kolegi z Ameryki może zostać uznany za spam. Tak więc, odrzucone przesyłki należy co jakiś czas kontrolować i ewentualnie pouczyć SpamPala by na przyszłość określonego typu przesyłki traktował inaczej.

A więc najpierw tworzymy katalog - np. **SPAM**, a następnie tworzymy filtr dla poczty przychodzącej, który powie programowi, by w przypadku natrafienia w tytule na ciąg znaków ****SPAM**** (domyślny "znacznik" nadawany podejrzanym przesyłkom przez SpamPala), przenosił przesyłkę do katalogu **SPAM** (warto też nakazać programowi, by zmieniał status przesyłki na 'przeczytane' tak, by rosnąca góra spamu w katalogu nie zaprzątała naszej uwagi - programy pocztowe zazwyczaj zachowują się dość natarczywie, jeśli w którymś z katalogów jest jeszcze jakaś 'nie przeczytana' poczta). Jeśli mamy lepszej klasy program pocztowy, możemy tworzyć bardziej skomplikowane filtry, które np. badać będą nie tylko temat przesyłki, ale też inne elementy nagłówka.

Konfiguracja SpamPala.

Kiedy klikniesz prawym klawiszem myszy na parasolce w zasobniku systemowym, pojawi się menu rozwijalne, które zawiera między innymi "Options" (opcje) które umożliwią nam dostosowanie programu do naszych potrzeb.

Okno opcji podzielone jest na standardowe Windowsowe "Zakładki":

Zakładka"Blacklist"

Jeśli dociera do Ciebie duża ilość spamu z tego samego adresu, a publiczne "czarne listy" jakoś nie kwapią się do napiętnowania spamera, możemy go na własne potrzeby zablokować przy pomocy prywatnej "czarnej listy" (ang. black list) . Mówiąc najprościej - SpamPal porównuje zawartość czarnej listy z adresem nadawcy w polu "From:" (Od:) - jeśli adres się zgadza - SpamPal automatycznie oznacza przesyłkę "łatką" **SPAM** nie zważając na sugestie innych - publicznych "czarnych list". Przykład funkcjonowania naszej czarnej listy:

> # spamerzy z Polski
> dzielny_biznesmen@koalicja.dzielnych.biznesmenow.pl
> marketing@sprzedajemywszystko.com.pl
> lancuszek@wyslijwszystkim.pl
>
> # spam zza granicy
> market@superbiznes.co.kr
> pingpong@ciongpeng.tw

Jak widać, możemy umieszczać własne komentarze do maili, co może być przydatne, kiedy po jakimś czasie będziemy chcieli zrewidować zawartość "czarnej listy". Należy pamiętać, by każdą linijkę komentarza poprzedzić znaczkiem "#". Przy tworzeniu czarnej listy adresów nadawców spamu, możemy wykorzystywać tzw. 'dzikie karty', 'jokery', czyli znaki zastępujące dowolne inne ciągi znaków. SpamPal korzysta przede wszystkim ze znaku "*" który zastępuje dowolny ciąg znaków. Jak to zastosować w praktyce ? Proszę bardzo :

> # cały yahoo.co.kr to spamerzy, więc ignorujmy ich w całości
>
> ***@yahoo.co.kr**
>
> # przeszkadza mi spam 'erotyczny' a spamerzy wykorzystują w adresie słówko '**sexy**'
>
> ***sexy***
>
> # dostaję tony maili od człowieka z adresem jasioXXX@serwer.com gdzie XXX to losowo wybrane znaki

jasio*@serwer.com

Oczywiście pole From: (Od:) może zawierać dowolną bzdurę wymyśloną przez spamera - znacznie skuteczniejsze jest blokowanie przesyłki po adresie IP nadawcy. Służy do tego dodatkowa opcja **Advanced Blacklist** - tu można podawać IP komputerów, zakresy adresów IP lub całe podsieci internetu, jeśli chcemy mieć pewność, że nic z tamtych rejonów nas nie interesuje - bardzo często zdarza się, że spamer po wysłaniu pierwszej partii spamu "przesiada się" na inny adres IP w tej samej sieci i wysyła następną partię spamu... Aby uniknąć zaspamowania innych naszych skrzynek przez tego samego złoczyńcę, możemy na jakiś czas zablokować np. cały zakres IP dostawcy internetu z którego korzysta spamer.

Zakładka "Whitelist"

"Biała lista" jest odwrotnością "czarnej listy". Ma tę samą formę co poprzedniczka, jednak jej przeznaczeniem jest ochrona przesyłek od naszych znajomych, kontrahentów itd. którzy mają pecha i korzystają z tej samej sieci, czy serwera pocztowego, co jakiś spamer. Dopisanie do whitelisty swoich znajomych z którymi utrzymujemy kontakty mailowe, powinno być pierwszą czynnością przy konfiguracji SpamPala ! Zanim zabierzemy się do blokowania i wycinania w pień spamerów, zadbajmy o to, byśmy sami nie ucierpieli przy tym, odcinając się od pożądanych kontaktów!.

```
# tych ludzi, to ja lubie ;-)
jasio@kowalski.com.pl
bardzowaznyklient@bardzowaznafirma.com.pl
```

Oczywiście analogicznie jak przy blackliście, możemy zdefiniować całe grupy adresów, czy serwery, których SpamPal ma nie oznaczać jako spam.

```
# Firmy z którymi współpracuję
*@jakasfirma.pl
*@innafirma.com.pl
```

Co bardzo ważne - wpisy w "białej liście" mają wyższy priorytet, niż wpisy w "czarnej liście" !. Oznacza to, że możemy np. zablokować cały *@hotmail.com, ale zrobić w "białej liście" wyjątek dla jaskowalski@hotmail.com. W tym przypadku, pomimo zdefiniowania filtra negatywnego "na całość" hotmail.com - list od jasiakowalskiego do nas dotrze. Takie ustawienie wzajemnych priorytetów białej i czarnej listy zabezpiecza nas przed omyłkowym "wycięciem" kogoś ważnego.

W tej samej zakładce - analogicznie do zakładki "Blacklist", znajdziemy przycisk przenoszący nas do zaawansowanych funkcji filtrowania. Definiujemy tu adresy IP, zakresy adresów ip, lub całe klasy. Przesyłki zawierające takie dane, nie będą dalej sprawdzane przez porównanie z bazami, lecz od razu przepuszczone bez oznakowania.

Zakładka "Auto-Whitelist"

"Biała lista" jest rzeczą bardzo przydatną i skuteczną w działaniu, wymaga jednak od nas ręcznego dopisywania adresów e-mailowych, adresów ip, itd. SpamPal ceni nasz czas, dlatego umożliwia zautomatyzowanie dopisywania danych do "białej listy". Po uruchomieniu 'automatycznej białej listy" (Auto-Whitelist) SpamPal będzie dopisywał adresy e-mail i/lub adresy IP nadawców przesyłek, które pozytywnie przejdą test porównawczy z publicznymi "czarnymi listami". W przypadku omyłkowego dopisania do whitelisty niepożądanego nadawcy, możemy ręcznie przerzucić go do blacklisty.

Zakładka "Tagging"

Domyślnie, SpamPal oznakowuje spam na dwa sposoby:

- nagłówek "**X-SpamPal: SPAM**"
- ciąg znaków "****SPAM****" dodawany do tytułu przesyłki

Możemy modyfikować sposób działania SpamPala w tym względzie.

Zakładka "Interface"

W tej zakładce możemy zmodyfikować zachowanie interfejsu programu - możemy decydować o tym, czy w czasie analizy nadchodzących przesyłek SpamPal ma wyświetlać okno informacyjne, czy też nie zaprzątać naszej uwagi wykonywanymi czynnościami. Możemy też decydować, które elementy programu pojawią się jako domyślne (czy opcje 'robocze', czy też 'konfiguracyjne'). W tej zakładce decydujemy także jak często program ma pobierać informacje uaktualnieniach zarówno samego programu, jak i listy dostępnych 'czarnych list'

Zakładka "Servers"

Zakładka ta służy głównie do modyfikacji sposobu komunikacji z serwerem POP3 - o ile nasz serwer nie pracuje na jakichś niestandardowych portach, nie należy ustawień modyfikować.

Zakładka "Plug-ins"

Jakby mało było standardowych możliwości SpamPala, umożliwia on ich rozszerzenie o kolejne - poprzez system plug-in'ów (wtyczek). Aktualna lista dostępnych wtyczek znajduje się na stronie http://spampal.org/plugins.html a najważniejsze wtyczki, ich zastosowanie i konfigurację omówię w dalszej części dokumentu.

Zakładka "DNSBL Lists"

Jak już wspomniałem na wstępie, SpamPal pracuje przede wszystkim poprzez porównywanie przychodzących przesyłek z zawartością "czarnych list". W tej zakładce możemy zadecydować, z których czarnych list chcemy korzystać. Przestrzegam przed zrozumiałym w takiej sytuacji entuzjazmem i zaznaczaniem wszystkich serwerów - niektóre z nich są bardzo rygorystyczne i rekomendują blokowanie serwerów, które niekoniecznie są źródłem spamu, a jedynie potencjalnie są jego źródłem, poprzez brak odpowiednich zabezpieczeń. Niektóre listy blokują także W CAŁOŚCI zarówno serwery pocztowe szeroko stosowane w Polsce (wp.pl, go2.pl), jak i rekomendują blokowanie poczty nadawanej np. z sieci sdi.tpnet.pl !!! Oznacza to, że jeśli zaprzęgniemy do współpracy takie czarne listy, możemy nie doczekać się maila od kolegi korzystającego z Wirtualnej Polski, go2.pl, czy "siedzącego" na sdi... Drugim problemem jest czas - jeśli zaznaczymy wszystkie serwery - każda przesyłka będzie analizowana w oparciu o dane z każdego serwera - a to oznacza... czekanie... Oby nie okazało się, że dłużej czekamy na weryfikację maila, niż zajęłoby nam jego odebranie i ręczne skasowanie !. Pamiętaj ! Narzędzie ma pomagać w życiu, a nie je utrudniać !. Zanim wybierzemy jakikolwiek serwer DNSBL do współpracy przy wychwytywaniu spamu, zadbajmy o to, by w naszej "białej liście" znalazły się wszystkie adresy e-mail znajomych, współpracowników, klientów itd., serwerów z których zazwyczaj korzystają. Dopiero kiedy upewnimy się, że nasze stałe kontakty są bezpieczne, zabierzmy się za wycinanie w pień spamerów !

W chwili obecnej SpamPal wykorzystuje następujące "czarne listy"

OSIRU **http://relays.osirusoft.com/** serwer sprawdza, czy otrzymana przez nas przesyłka nie została nadana z serwera, który jest znanym źródłem spamu, lub też pośrednio wspiera spam np. poprzez możliwość nieautoryzowanego wysyłania e-maili (open-relay), reklamowanie usług spamerskich (lub oprogramowania do spamowania). Moim zdaniem serwer ten w polskich warunkach jest zbyt rygorystyczny - nader często przesyłki nadane przez znajomych, korzystających z darmowych serwerów poczty, mogą zostać uznane za spam. **Na początek proponuję nie korzystać z tego serwera.**

SPEWS **http://www.spews.org/** serwer "listuje" serwery wspierające spam, albo powiązane z serwerami, które aktywnie to robią. SPEWS znany jest ze swej "agresywności" w walce ze spamem, dlatego **na początek proponuję nie korzystać z tego serwera** z powodu możliwych **'false-positives',** czyli przesyłek, które dla nas spamem nie są, a są tak oceniane przez publiczne "czarne listy" np. tylko dlatego, że pochodzą z niezabezpieczonego serwera. SPEWS w przypadku powtarzających się przypadków spamu z określonej sieci "listuje" całą klasę adresową providera !!!. Oznacza to, że w sytuacji, gdy w tej samej sieci znajduje się notoryczny spamer i kilka niewinnych firm, to niestety, ale poczta od tychże uczciwych firm także zostanie uznana za spam. Warto o tym pamiętać decydując się na korzystanie ze SPEWS.

SITES **http://www.spamsites.org/** **SPAMSITES** serwer "listuje" przede wszystkim serwery wspierające spam poprzez udostępnianie oprogramowania do spamowania, sprzedaje bazy adresów skradzionych ze stron www, czy grup dyskusyjnych. Sprzedawcy

takich niecnych narzędzi sami zazwyczaj spamują namiętnie, próbując sprzedać swoje produkty. Ponadto SPAMSITES "listuje" także serwery open-relay, niezabezpieczone formularze na www umożliwiające wysyłanie spamu i inne niebezpieczne narzędzia. Jak narazie nie spotkałem się, by w oparciu o SPAMSITES nastąpiła jakaś błędna ocena przesyłki **('false-positive')**. **Proponuję uaktywnić obsługę tego serwera w SpamPalu - Pamiętaj nie kupujemy od spamerów !.**

SBL **http://www.spamhaus.org/sbl/** **Spamhaus SBL** Serwer ten wymienia w swojej "czarnej liście" przede wszystkim notorycznych spamerów, ich stowarzyszenia, oraz firmy, które wspierają aktywnie spam, poprzez udostępnianie spamerom coraz to nowszych zasobów. **Proponuję uaktywnić obsługę tego serwera w SpamPalu**

ORDB **http://www.ordb.org/** Baza "listująca" serwery typu open-relay, które są, lub mogą być wykorzystane przez spamerów do swojej działalności. Należy pamiętać, że takim open-relayem są np. wp.pl, czy go2.pl i prawie na pewno zostaną onet w ORDB "wylistowane". **Jeśli liczysz się z tym, że możesz otrzymywać pocztę z tych serwerów, albo w "zaawansowanej białej liście" wstaw *@*wp.pl, *@tlen.pl (dla pozostałych aliasów tego serwera również), albo nie korzystaj z usług ORDB.**

SPCOP **http://spamcop.net/bl.shtml** **SPAM COP** Dość agresywna czarna lista, która opiera się na raportach składanych przez samych użytkowników poczty. Jest to bardzo skuteczna "czarna lista", lecz ma swoje minusy - podobnie jak ORDB, dość często "listuje" ona polskie open-relay'e - wp.pl i go2.pl w szczególności. Ponadto w związku ze sposobem zbierania informacji przez spamcopa (czyli zgłoszenia od użytkowników) zdarzają się pomyłkowe, lub złośliwe zgłoszenia przesyłek, które spamem nie są. SpamCop, by być skutecznym, natychmiast 'listuje' taką przesyłkę i jej nadawcę, co przez jakiś czas może doprowadzić do zablokowania niewinnego użytkownika, jednak po weryfikacji taki nadawca jest usuwany. **Zalecam mimo wszystko stosowanie tego serwera,** po uprzednim umieszczeniu w 'białej liście" adresów naszych znajomych, albo całych serwerów z których korzystają. Odsetek pomyłek i złośliwych zgłoszeń jest tak niewielki, że nie umniejsza wiarygodności tego serwera.

SPBAG **http://www.spambag.org/** **SpamBag** Czarna lista serwerów, których aktywność może naruszać prywatność użytkowników internetu - spam, mailbombing (bombardowanie tysiącami przesyłek adresów użytkowników), ataki słownikowe (sprawdzanie tysięcy możliwych nazw kont użytkowników w poszukiwaniu istniejących kont, by je zaspamować - czynności takie bardzo obciążają serwer), kradzież adresów e-mail ze stron www, czy grup dyskusyjnych.

FORMAIL formmail.relays.monkeys.com Monkeys serwer listujący serwery udostępniające niezabezpieczone formularze na stronach www, umożliwiających wysłanie niezamówionych przesyłek. Serwer Monkeys nie uznaje 'przedawnienia' win, więc jeśli jakiś serwer zostanie "wylistowany" raz, pozostaje tam na zawsze - nawet jeśli poprawi formularz który był przyczyną zapisania. W efekcie monkeys jest coraz mniej wiarygodny. **Proponuję nie korzystać z tego serwera**

ABL **http://abl.v6net.org/** **ABL** Bardzo agresywna czarna lista, która zawiera adresy IP

znanych spamerów. Siłą rzeczy, wśród wymienionych znajdują się bardzo znane serwery darmowych skrzynek pocztowych (yahoo, hotmail) więc ilość fałszywek może być znaczna. **Na początek odradzam używania tego serwera.**

WIREHUB **http://basic.wirehub.nl/blackholes.html** **Wirehub** Czarna lista adresów IP serwerów notorycznie używanych do spamowania, albo innych czynności naruszających prywatność użytkowników. **Nie spotkałem się jak narazie z "fałszywkami", więc z czystym sumieniem mogę polecić korzystanie z tej listy.**

IPWHOIS **http://www.rfc-ignorant.org** **RFC-Ignorant** Bardzo rygorystyczna lista, która zawiera adresy serwerów, które nie stosują się do "sieciowej konstytucji" jaką są zalecenia RFC. Najczęściej spotykanymi uchybieniami są: brak adresów kontaktowych z właścicielem domeny / serwera, któremu można by się poskarżyć na nadużycia, brak innych danych na temat właściciela domeny. Teoretycznie więc są to serwery ułatwiające życie spamerom, aczkolwiek nie koniecznie !. Niech najlepszym przykładem będzie fakt, iż RFC-Ignorant "listuje" **W CAŁOŚCI** sieć firmy... **TP S.A.** ze względu na nieprawidłowe wpisy rejestracyjne **!. Na początek odradzam więc korzystanie z tej listy.**

NJABL **http://www.njabl.org/** **NJABL** Bardzo skuteczna lista serwerów ułatwiających życie spamerom, oraz samych spamerów. **Nie zauważyłem dotąd "false-positives", więc polecam korzystanie z tej listy.**

BLITZED **http://www.blitzed.org/opm/** **Blitzed.org** Kolejna lista niezabezpieczonych formularzy, serwerów proxy i innych narzędzi ułatwiających życie spamerom. **Polecam tę listę.**

DSBL **http://www.dsbl.org** **DSBL** Kolejna "czarna lista" open-proxy, open-relay i niezabezpieczonych formularzy www. Z powodu kilku fałszywych zgłoszeń mam wątpliwości co do wiarygodności tej listy ale myślę, że na początek można z niej skorzystać, bacznie pilnując wystawianych przez nią ocen.

DNSRBL **http://www.dnsrbl.com/** "Domain Name System Real-time Black List" . Bardzo skuteczna black-lista, która działa w oparciu o tak zwane spam-trapy, czyli pułapki na spam - skrzynki pocztowe w różnych częściach internetu, które nie są używane do normalnej korespondencji, więc teoretycznie nie powinny przychodzić na nie żadne przesyłki - jeśli więc trafią - niechybny to znak, że toczy się zakrojona na ogromną skalę akcja mailingowa. **Zalecam stosowanie tej listy.**

ISOCBG **http://dnsbl.isoc.bg/** **Bulgarian SPAM prevention system.** System zaprojektowany tak, by przede wszystkim bronić użytkowników z Bułgarii, przed spamem pochodzącym z tego kraju. Nam jednak może również się przydać - przecież internet nie zna granic, a spamerzy to raczej niedouczeni ludzie, którzy nie rozumieją, że spam po Bułgarsku przysłany do Polaka, raczej nie podniesie sprzedaży produktu.

SORBS **http://www.dnsbl.sorbs.net/** **SORBS Open Server/Relay System**. SORBS (Spam and OpenRelay Blocking System) - jak łatwo się domyślić, jest to "czarna lista" wszelkiej maści serwerów open-relay, które wspierają spam, oraz adresy komputerów, z

których spam jest nadawany. Ostatnimi czasy na liście SORBS zaczęły pojawiać się adresy komputerów "shackowanych" przez spamerów tak, by były pomocne przy procederze rozsyłania spamu. Potencjalnie więc duża ilość polskich komputerów wyposażonych w system Windows, korzystających ze stałych łącz i pozostawionych bez dozoru (dość częsty proceder w przypadku użytkowników sdi) może zostać umieszczona na liście SORBS ! **Zdarzyło mi się już kilka "fałszywek", więc decyzję o wykorzystaniu tej listy pozostawiam użytkownikom.**

SpamRBL http://www.spam-rbl.com Spam-RBL Bardzo aktywna lista (uaktualniania kilka razy dziennie), zawierająca adresy nadawców spamu. **Zalecam korzystanie z tej listy !.**

CHINA, KOREA, H-KONG, TAIWAN, JAPAN, THAI, ARG (Argentyna), BRASIL, NIGERIA, RUSSIA, MALASIA, SNGPORE (Singapur), http://www.blackholes.us/ Znakomity serwer zawierający poddomeny poświęcone poszczególnym rodzajom "narodowym" spamu. Znakomicie "listuje" jakże uciążliwy spam koreański, nigeryjski. **Zalecam zdecydowanie stosowanie wszystkich list z domeny blackholes.us.**

Jak więc widać, nie ma jednej uniwersalnej listy, która "załatwiłaby" sprawę spamu. Niektóre listy są bardziej rygorystyczne, niektóre mniej. Do nas należy wybór list, z których chcemy korzystać. Na nas też spoczywa odpowiedzialność za ich wykorzystanie. Jeśli wybierzemy zbyt rygorystyczną listę, nie miejmy pretensji do jej administratorów, że "wylistowali" naszych znajomych, czy kontrahentów. To my sami musimy wybrać, jaki styl walki ze spamem jest dla na nas najwłaściwszy.

Zakładka "Advanced"

DNSBL Time-Out interval - Serwery DNSBL są czasami bardzo obciążone - zawdzięczamy to oczywiście "dzielnym" spamerom, którzy bez opamiętania ślą spam w milionach sztuk - im więcej spamu, tym więcej osób wysyła zapytania do serwerów DNSBL. Jeśli obciążenie serwerów spowoduje brak odpowiedzi w określonym okresie czasu, SpamPal nie będzie czekał, lecz przerwie proces analizy w oparciu o DNSBL i poinformuje o tym w nagłówkach maila (czym są nagłówki o tym za chwilę). Przy użyciu opcji **DNSBL Time-Out interval** możemy wydłużyć czas oczekiwania na odpowiedź serwerów DNSBL.

Maximum simultaneous DNSBL queries - umożliwia ograniczenie ilości zapytań do baz DNSBL jakie może jednocześnie generować SpamPal. Im więcej zapytań jednocześnie, tym większe możliwości filtrowania poczty przy obsłudze kilku skrzynek pocztowych jednocześnie. Z drugiej strony - przy słabym łączu, zbyt wiele zapytań na raz, może zwiększyć prawdopodobieństwo wystąpienia zjawiska przekroczenia czasu oczekiwania ('time-out') o którym była mowa wcześniej.

Don't filter mail at all - (w ogóle nie filtruj poczty) umożliwia wyłączenie na jakiś czas funkcji SpamPala

Don't filter mail on automatic whitelists - (nie filtruj poczty przy pomocy automatycz-

nych "białych list") wyłącza filtrowanie, lecz nie wstrzymuje procesu dopisywania adresów do "automatycznej białej listy", jeśli nie wyłączyliśmy tej opcji we właściwym menu.

Remember positive (spam) DNSBL results & **Remember negative (non-spam) DNSBL results** - umożliwia określenie, przez ile dni SpamPal ma pamiętać wyniki "oceny' dokonanej przy pomocy analizy porównawczej z zawartością serwerów DNSBL (RBL). Używanie zbyt długich okresów "przechowywania" wyników, może doprowadzić do sytuacji, że będziemy uparcie blokować nadawcę, który już dawno został "rozgrzeszony".

Extra DNSBL Definitions - umożliwia zdefiniowanie własnych serwerów DNSBL, jeśli uzyskamy zgodę na korzystanie z takiego serwera.

Extra Black- & White-Lists - umożliwia wskazanie dodatkowych plików tekstowych zawierających adresy e-mail/IP zarówno przeznaczonych dla czarnej, jak i białej listy. Jest to przydatne zwłaszcza wtedy, gdy wymieniamy się z innymi użytkownikami danymi na temat spamu. Wtedy w głównych plikach trzymamy własne, sprawdzone wpisy, a w tych dodatkowych - niesprawdzone - jeśli okaże się, że te zewnętrzne listy doprowadzają do 'fałszywek', wtedy bez modyfikowania głównych baz, możemy pozbyć się niechcianych wpisów.

I.P. Configuration - umożliwia zdalny dostęp

ZASADY FUNKCJONOWANIA PROGRAMU

Jak już wspomniałem wcześniej, głównym zadaniem SpamPala jest oznakowywanie przesyłek uznanych za spam tak, by użytkownik, lub odpowiednio skonfigurowany program pocztowy, mógł wyłowić taką przesyłkę i odpowiednio ją potraktować. Podstawową metodą oznakowania, jak już wiemy, jest wstawienie do tematu przesyłki, ciągu znaków ****SPAM****. SpamPal potrafi jednak znacznie więcej. Głównym źródłem informacji jest nagłówek przesyłki, do którego SpamPal wstawia wpisy. Ich zrozumienie ułatwi poniższy opis.

Nagłówek X-SpamPal:

SpamPal oznakowuje podejrzane przesyłki także poprzez dodanie własnych wpisów do nagłówka e-maila. "Czyste" przesyłki oznaczy on nagłówkiem:

X-SpamPal: PASS

Zaś przesyłki podejrzane zostaną opatrzone nagłówkiem:

X-SpamPal: SPAM

Aby obejrzeć nagłówki maila, należy wybrać odpowiednią funkcję programu pocztowego - np. 'Pokaż źródło wiadomości', albo "pokaż wszystkie nagłówki RFC".

Nagłówki poczty są w pewnym sensie elektroniczną kopertą przesyłki - zawierają informację o nadawcy, pośrednikach w przekazie informacji, a także dodatkowe informacje o sposobie w jaki poczta powinna być odczytana (np. tak zwana deklaracja charsetu, czyli informacja w jakim systemie kodowania znaków narodowych przygotowana jest przesyłka).

W większości wypadków, oznakowana jako spam wiadomość, będzie zawierała dodatkowe informacje dotyczące przyczyny takiej, a nie innej decyzji SpamPala.

X-SpamPal: SPAM <kod listy> <adres IP>

Kod listy to pięcioliterowy identyfikator "czarnej listy", która zarekomendowała oznakowanie przesyłki jako spam. Rozszyfrowanie kodu ułatwi lista, o której mówiłem wcześniej, przy okazji opcji konfiguracyjnych programu. Druga informacja przekazywana przez SpamPala, to adres IP nadawcy, który został umieszczony na publicznej "czarnej liście".

Przykładowy wygląd nagłówka

X-SpamPal: SPAM NIGERIA 80.88.150.184

Jak widać, SpamPal zadecydował, że przesyłka jest spamem, gdyż adres nadawcy 80.88.150.184 znalazł się na czarnej liście serwera Nigeria (tak naprawdę jest to serwer www.blackholes.us, który udziela informacji na temat spamu z podziałem na ich źródło: Nigeria, Tajwan, Korea itd... o czym była mowa w dziale 'DNSBL Lists')

Jeśli zablokowałeś kogoś na swojej prywatnej "zaawansowanej czarnej liście" adresów IP, nagłówek X-SpamPal: będzie wyglądał mniej więcej tak:

X-SpamPal: SPAM BLIST <adres IP>

A w przypadku zablokowania na uproszczonej "czarnej liście" adresów e-mail, wyglądać będzie mniej-więcej tak:

X-SpamPal: SPAM BLIST FROM

Jeśli nadawca znajduje się na naszej "białej liście", SpamPal oznakuje przesyłkę następująco:

X-SpamPal: PASS WLIST FROM

"Automatyczna biała lista" nie pozostawia jakichś szczególnych oznaczeń w nagłówku, jednak podstawowa "automatyczna biała lista" (przypominam: opierająca się o adresy e-mail, a nie adresy IP) pozostawia następujący znacznik

X-SpamPal: PASS A-WLIST FROM

Jeśli status przesyłki jest niejasny, bo zapytania do publicznych serwerów DNSBL nie doczekały się odpowiedzi w określonym czasie, SpamPal poinformuje o tym przy pomocy następującego wpisu:

X-SpamPal: PASS TIME-OUT

Jeśli często widzisz w nagłówkach ten komunikat, oznacza to problemy z **komunikacją** z serwerami DNSBL. W tej sytuacji należy wydłużyć czas oczekiwania na odpowiedź - dokonujemy tego oczywiście w panelu sterowania programem**,** a dokładnie: **Options /Advanced / DNSBL queries timeout after : <sekundy>**

Dodatkowe funkcje programu - plug-iny.

Jakby mało było możliwości oferowanych przez standardową wersję programu, mamy możliwość ich rozszerzenia, poprzez system wtyczek (plug-in). W chwili obecnej dostępnych jest kilkanaście wtyczek naprawdę pożytecznych i kilkanaście następnych, które moim zdaniem są już tylko "kwiatkiem do kożucha", gdyż są użyteczne dla bardzo wąskiej grupy maniaków.

Pełna lista dostępnych wtyczek znajduje się pod adresem http://spampal.org/plugins.html

Najbardziej użyteczne moim zdaniem wtyczki to:

Bad Words

Bardzo użyteczny spam do walki np. ze spamem pornograficznym. Umożliwia zdefiniowanie listy "złych słów", których obecność wskazuje na treści, których na pewno nie powinny czytać nasze dzieci. Oczywiście możemy też zdefiniować słowa charakterystyczne dla spamu, który otrzymujemy. Osobiście miałem kiedyś problem ze spamem od członków organizacji FFA (Free For All). Wystarczyło więc do listy "złych słów" dodać FFA i spam tego typu przestał być problemem ;-). Należy jednak bardzo uważać przy doborze "złych słów" - jeśli nieopatrznie dopiszemy popularne słowo np. w języku angielskim, to możemy pozbawić się przesyłek nie będących spamem, a jedynie używających tych samych słów. **Zalecam więc daleko posuniętą ostrożność przy posługiwaniu się tym plug-in'em !.**

Notify
Ciekawy plug-in umożliwiający zdefiniowanie dźwięków powiadamiania o nadejściu poczty - oddzielny dźwięk dla sensownej poczty, oddzielny dla spamu.

Quarantine
Wtyczka, która umożliwia zapisanie każdej przesyłki uznanej za spam do specjalnego katalogu w niezmienionej formie (tzn. bez modyfikacji tytułu, czy dodatkowych. wpisów w nagłówku). Przydaje się to, gdy chcemy np. podzielić się swoimi zbiorami spamu z innymi użytkownikami.

Whitelist Extender
Narzędzie rozszerzające możliwości "białej listy". Standardowe czarne i białe listy kreowane są w oparcie o adres e-mailowy z pola From: (Od:) lub w zaawansowanej wersji - w oparciu o podany adres IP. Extender (rozszerzacz) jak sama nazwa wskazuje - rozszerza możliwości kreowania list w oparciu o inne pola nagłówka - np. 'Reply-to:' (Adres zwrotny).

RegEx Filter
Plug-in jest gratką dla wielbicieli "Regular Expressions" (wyrażeń regularnych) Pearla. Wyrażenia regularne umożliwiają znacznie bardziej elastyczne przetwarzanie danych, niż standardowa '*' zastępująca dowolny ciąg znaków. Szczegółowy opis wtyczki znajduje się na stronie autora http://www.slabihoud.de/spampal/

Gwóźdź programu - 'Bayesian Filter'
Wtyczka udostępniająca nam możliwości, których dotychczas zazdrościliśmy użytkownikom linuksa korzystającym z takich narzędzi jak SpamAssassin, czy BogoFilter.
Wtyczkę możemy pobrać ze strony http://status3.i-r.co.uk/bayesian.htm . Po zainstalowaniu, Bayesian zintegruje się ze SpamPalem i będzie widoczny w menu 'Plugins', a jego konfiguracji będziemy dokonywać z menu 'Options' / 'Plugins' / Properties, Co ciekawe - plug-in jest już spolszczony, co znacznie ułatwi nam pracę.

Bayesian to narzędzie analizy statystycznej, które ma możliwość "uczenia się" z biegiem czasu, właściwej oceny nadchodzących przesyłek. Im więcej przesyłek odbierze i właściwie oceni (z naszą pomocą), tym trafniej w przyszłości wskazywał będzie przydatność przesyłki. Pokrótce proces filtrowania przy pomocy metody Bayes'a wygląda następująco. Każde słowo w nadchodzącym mailu jest oceniane na podstawie jego obecności w poprzednich mailach. Słowo, które pojawiało się wcześniej tylko w mailach uznanych za spam, otrzyma 'ocenę' 0.99. Słowo, które pojawiało się tylko w 'czystych' mailach, otrzyma ocenę 0.00. Wszelkie nieznane słowa otrzymają ocenę 0.2. Następnie zostaną wykonane działania matematyczne oddzielnie dla słów 'spamerskich' i oddzielnie dla słów 'czystych'. Jeśli wynik przekroczy określony wcześniej próg, przesyłka zostaje uznana za spam.
Jeśli nie zgadzamy się z opinią Bayesiana, możemy wskazać mu właściwą ocenę. Dokonujemy tego poprzez wywołanie prawym klawiszem myszy menu programu, następnie 'Plugins', ' Bayesian'. W oknie które się pojawi znajdziemy maile, które zostały przefiltrowane - każdy z nich jest znaczony albo na zielono (jesli mail został uznany za "czysty"), albo na czerwono (jeśli został uznany za spam). Możemy zmienić ocenę zaznaczając tytuł danego maila a następnie klikając na właściwy przycisk przycisk w panelu po lewej stronie. Filtr przyjmie naszą sugestię, dzięki czemu przy następnych przesyłkach nie popełni tego samego błędu. Proces nauki może trochę potrwać - możemy przyspieszyć ten proces poprzez zaimportowanie maili, które sami oceniliśmy. Jak to zrobić ? O tym za chwilę.

Konfiguracja filtra

Z menu głównego programu wchodzimy w 'Options', następnie 'Plugins' , 'Properties' - ukazuje się nam okno konfiguracyjne pluginu 'Bayesian filter'.

Zakładka: Próg reakcji

Próg spamu przez podniesienie progu zmniejszymy ilość fałszywych ocen, przez obniżenie progu zwiększamy czułość filtra. Każde słowo poniżej wyznaczonego progu zostanie uznane za 'czyste'. Domyślnie ustawiona jest wartość '90'.

Uczenie się programu Każde słowo z oceną większą lub równą wyznaczonej, zostanie dodane do bazy danych słów zaklasyfikowanych jako 'spamerskie'. Domyślna wartość '99'

Ustaw ograniczenie przetwarzania wiadomości służy do ograniczenia ilości danych analizowanych przy okazji pojedynczej wiadomości.

Ilość wiadomości do przetwarzania (KB) określa wielkość danych z pojedynczej wiadomości, jaka ma zostać poddana analizie.

Zakładka: Słowa

Ilość słów określa ilość słów kluczowych sprawdzanych w czasie klasyfikowania maila. Im więcej słów analizowanych, tym dłużej to trwa, ale w dłuższym okresie czasu jakość procesu klasyfikacji może znacznie wzrosnąć. Domyślna wartość '10'

Min/ Max długość słowa ogranicza długość słowa poddawanego analizie

Utrata ważności słowa (w dniach) Każde słowo poddane ocenie, zostaje oznaczone datą, a słowa są usuwane z bazy po określonej ilości dni

Minimalna ilość wystąpień słowa dla filtrowania określa minimalną ilość występowania jakiegoś słowa w mailu, zanim zostanie ono uznane za 'kluczowe', umieszczone w bazie i stanie się wskaźnikiem do filtrowania.

Incoming words are case-sensitive zmusza filtr do rozróżniania dużych i małych liter

Zakładka: Opcje

Twórz raport: wymusza tworzenie i uzupełnianie pliku tekstowego z informacjami o przeanalizowanych przesyłkach i ich ocenach

Ucz się (nie zaznaczaj spamu) Plug-in nadal będzie analizował przesyłki, ważył słowa, jednak swoich ocen nie wyrazi poprzez wstawienie nagłówka do przesyłki. Dzięki tej opcji unikniemy sytuacji, gdzie plug-in zanim jeszcze nauczy się rozróżniać nasze przesyłki, będzie już ferował wyroki. Kiedy uznasz już, że filtr wystarczająco dużo się nauczył - wyłącz tę opcję.

Uważaj emaile z Białej listy jako czystą pocztę zmusza wtyczkę do traktowania wszystkich maili od nadawców z "białej listy" jako czyste, niezależnie od ich zawartości

Ucz się z Białej Listy powoduje, że maile od nadawców z 'białej listy' są analizowane, dodawane do bazy danych i służą za wzorzec 'prawidłowej przesyłki' dla następnych, które się pojawią. Jest to dość skuteczna metoda uczenia filtrów, jeśli otrzymujemy dużo maili o określonej tematyce, ale tylko część z nich pochodzi od osób z whitelisty.

Dołącz nagłówki podczas filtrowania powoduje, że analizie zostaną poddane nie tylko słowa z głównej wiadomości, ale także z nagłówków

Select this if you want to include all the emails headers in the Bayesian filtering.

Dodaj nagłówek "X-Bayesian-Words" stanowi ułatwienie do późniejszej oceny skuteczności filtra - widzimy jakie słowa zostały uznane za kluczowe i jaką punktację im przyznano.

Ucz SpamPala spowoduje, że plugin będzie uczył się z 'dorobku' innych pluginów.
(nazwa opcji jest nieco myląca - przynajmniej w wersji polskiej).

Zakładka: Ignoruj

Lista zawiera słowa, które nie powinny być przez Bayesiana traktowane jako słowa kluczowe.

Zakładka: Importuj

Dostępne tu opcje umożliwiają szybki nauczenie Bayesiana właściwej oceny nadchodzących przesyłek. Aby w pełni wykorzystać te opcje, należy wyeksportować z archiwów naszego programu pocztowego do formatu .eml przesyłki - do jednego katalogu spam, do drugiego - czyste przesyłki. Następnie korzystając z przycisków "czysta poczta" i "spam" wskazujemy właściwe katalogi. Program pobierze zawartość plików .eml. podda analizie, wyszuka słowa kluczowe, wystawi oceny i od tej pory znacznie łatwiej będzie mu oddzielać spam od czystej poczty.

Zakładka: Różne

Język umożliwia wybranie języka w jakim plugin ma pracować - na szczęście jest polski.

Konfiguracja

Położenie plików konfiguracyjnych Bayesian Filter i innych plików konfiguracyjnych:

podstawowe pliki konfiguracyjne znajdują się w katalogu programu (e.g. C:\Program Files\SpamPal\plugins\Bayesian), jednak nie powinny być modyfikowane - lepiej, aby w przypadku jakichś pomyłek np. przy imporcie złej/dobrej poczty do filtrów Bayesa było do czego wrócić. Dla każdego użytkownika tworzony jest oddzielny zestaw plików konfiguracyjnych. Ich położenie jest następujące

Windows XP: C:\Documents and Settings\%USERNAME%\Dane Aplikacji\SpamPal\plugins\bayesian

Windows 2k: C:\Documents and Settings\%USERNAME%\Dane Aplikacji\SpamPal\plugins\bayesian

Windows NT: C:\WinNT\Profiles\%USERNAME%\Dane Aplikacji\SpamPal\plugins\bayesian

Windows 98: C:\Windows\Dane Aplikacji\SpamPal\plugins\bayesian
Windows 95: C:\Program Files\Spampal\config\plugins\bayesian

Zawartość tych katalogów należy archiwizować sukcesywnie, oraz w przypadku zaistnienia konieczności reinstalacji systemu.

ZAKOŃCZENIE

SpamPal to dynamicznie rozwijający się, otwarty projekt, którego kolejne wersje zawierają nowe, poprawione narzędzia do walki ze spamem. Niniejszy dokument nie wyczerpuje problematyki związanej z wykorzystaniem programu, dlatego warto korzystać z forów dyskusyjnych oraz innych dokumentów dostępnych na stronie spampal.org. W szczególności polecam

http://www.spampal.org/faqengine/faq.php?list=all&prog=spampal&lang=en