

Usuwanie spamu bezpośrednio z serwerów POP3

Krok naprzód

Jeśli jesteście zasypywani niechcianą pocztą, możecie ją usuwać bezpośrednio z serwera dostawcy internetowego, zanim pobierze ją program pocztowy. Dobrym sposobem walki ze spamem są wyrafinowane filtry i wyrażenia regularne.

TIM SCHÜRMAN



Reklamy, wirusy i wszystkie inne rodzaje śmieci zanieczyszczają codziennie miliony skrzynek pocztowych. Przedstawiamy trzy niewielkie narzędzia: Eremover, Kshowmail i PopWash, które mogą pomóc w pozbyciu się reklam powiększania biustu, Viagry i innych reklam typu: jak za drobną opłatą stać się bogatym w dziesięć minut, nie ruszając się z fotela.

Program taki zachowuje się jak klient pocztowy, ale przechwytuje jedynie temat listu, jego nadawcę i rozmiar wiadomości. Dzięki tym informacjom ofiara spamu może wybrać niechciane wiadomości i pojedynczym kliknięciem usunąć je bezpośrednio na serwerze POP3, zanim znajdą się we właściwym programie pocztowym. Zapobiega to zaśmieszczeniu skrzynki i dysku. Użytkownicy usuwają zatem spam bezpośrednio na serwerze internetowego usługodawcy. Nie tylko zmniejsza to ilość ruchu, ale równocześnie chroni

przed wirusami i zwalcza skutecznie spam.

Zanim skonfigurujemy program usuwający spam, musimy przygotować wszystkie dane dotyczące konta e-mail. Potrzebny jest przede wszystkim adres IP lub nazwa DNS serwera POP3, a także nazwa konta użytkownika na tym serwerze oraz jego hasło.

Dla odważnych: Eremove

Pierwszym kandydatem na zabójcę spamu jest Email Remover (lub krótko Eremove). Jest on oparty na bibliotece GTK, tej samej, na której oparto GNOME. Jednak jego interfejs użytkownika

nie jest tak wygodny jak w KShowmail (omówimy go dalej), będącym aplikacją KDE. Z drugiej strony Eremove dobrze współpracuje z każdym środowiskiem graficznym.

Eremove można pobrać ze strony domowej projektu, zarówno w postaci bi-

narnej jak i źródła. Jeśli wolisz wykorzystać wersję binarną, pobierz i rozpakuj odpowiednie archiwum. Zawiera ono plik wykonywalny eremove.

Eremove ma ograniczoną funkcjonalność. Program usuwa jedynie e-maile z serwera pocztowego. Podczas uruchomienia narzędzia wyskakuje okno pytające o nazwę serwera Server i Username – to jest o nazwę użytkownika serwera POP3 i o hasło Password (Rysunek 1). Ustawienia portu Port można pozostawić domyślne.

Eremove pobiera listę wiadomości z serwera i wyświetla ją w głównym oknie (Rysunek 2). Z tej listy możesz wybrać wiadomości do usunięcia i kasować je klikając Delete. Opcja Select All wybiera całą listę. Kliknięcie na Logout powoduje zakończenie programu.



Rysunek 1: Po uruchomieniu programu Eremove automatycznie pojawia się spartańskie okno konfiguracyjne.



Rysunek 2: Główne okno Eremove zawierające listę wiadomości e-mail.

Zawartość listu można podejrzeć, klikając dwukrotnie na wiadomość. Wywołanie tej funkcji w SUSE Linux powodowało zawieszenie się programu wraz z całym systemem X Window. Dodatkowo, program nie zapewnia właściwej ochrony haseł, które przechowywane w postaci zwykłego tekstu w pliku konfiguracyjnym w katalogu `~/eremove`. Krótko mówiąc, nie polecamy tego narzędzia.

Numer 1: KShowmail

KShowmail, przeznaczony dla KDE, jest najbardziej dojrzałym programem w naszym teście. Wykorzystuje on bibliotekę Qt i doskonale się integruje z pulpitem KDE. Jeśli jesteś użytkownikiem SUSE Linux, możesz bardzo łatwo go zainstalować, używając YaST-a. Jeśli wykorzystywana dystrybucja nie zawiera tego programu, można go pobrać ze strony projektu (Tabela 1).

Ze wszystkich programów, jakie przetestowaliśmy, KShowmail posiada najwięcej funkcji i obsługuje wiele kont POP3. Program może także uaktualniać listę wiadomości w regularnych odstępach czasu. Dzięki temu Kshowmail jest doskonałym, elastycznym i wygodnym narzędziem. KShowmail może być tak skonfigurowany, aby powiadamiał o nowej poczcie.

KShowmail posiada funkcję wysyłania skarg na niechciane wiadomości. Klikając przycisk SPAM, wyślemy wybraną wiadomość do centrum zbierania informacji o spamie. Centra takie często prowadzą dostawcy Internetu, są też projekty globalne – takie jak np. www.spamabuse.org.

Do konfiguracji adresata wiadomości zaklasyfikowanej jako spam w KShowmail potrzebne jest dodatkowe narzędzie, takie jak np.



Rysunek 5: Do określenia informacji wyświetlanych przez KShowmail w głównym oknie programu wykorzystujemy opcję „Display Options”.

spam.pl. Można go pobrać z adresu <http://spam.sourceforge.net/>. Narzędzie to zajmuje się tylko wysyłaniem informacji o spamie w odpowiednie miejsca.

Chcąc wykorzystać spam.pl wraz z KShowmail, wybieramy Setup | User commands, a następnie klikamy w nowym oknie przycisk Add. Wprowadzamy `complain` w górnym polu oraz polecenie uruchamiające program (w polu Command:), który będzie wysyłał informacje o spamie. Skrypt `spam.pl` może być wstępnie skonfigurowany, w takim przypadku w tym polu będzie wpisane polecenie:

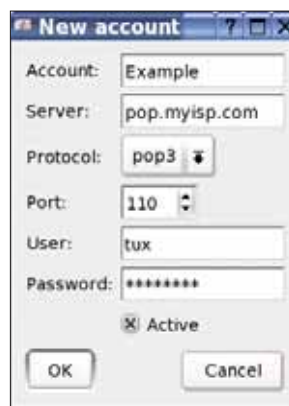
```
spam.pl < <body>
```

gdzie `<body>` jest miejscem, które KShowmail zamienia na zawartość e-mail.

Można użyć tej techniki do wywoływania zewnętrznego programu. Zamiast łańcucha `complain`, wybieramy odpowiedni wpis. KShowmail stworzy odpowiednią pozycję w menu Actions. Można jej używać do uruchamiania programu.

Konfiguracja KShowmail

Aby skonfigurować Kshowmail, wybieramy opcję Setup | Setup accounts, klikamy na Add i wprowadzamy dane swojego konta (Rysunek 3). Wpisujemy tutaj nazwę skrzynki pocztowej w polu tekstowym Account. W polu tekstowym Server podajemy nazwę DNS serwera albo jego adres IP. Opcja Username to nazwa użytkownika na serwerze POP3. Jeśli na tym etapie nie podamy hasła, zostaniemy o nie poproszeni w momencie, gdy pierwszy raz będziemy próbować uzyskać dostęp do tej skrzynki pocztowej. Na koniec klikamy przycisk Ok, aby powrócić do okna ustawień.



Rysunek 3: Używamy tego okna dialogowego Kshowmail, aby wprowadzić dane dla nowego konta. W tym przykładzie konto ma nazwę „Example”, użytkownik to „tux”, a serwer POP3 to „pop.myisp.com”.



Rysunek 4: Zakładka „General Options” w oknie dialogowym ustawień jest wykorzystywana między innymi do określenia odstępu czasowego, w jakim KShowmail będzie sprawdzał, czy są nowe wiadomości.

Można użyć zakładki Action if new mail, aby wybrać sposób, w jaki KShowmail ma powiadamiać o nowej wiadomości. Domyślnie program jest tak skonfigurowany, by wyświetlać okienko i dać sygnał dźwiękowy.

Możliwe jest określenie odstępu czasowego, w jakim KShowmail będzie pobierał pocztę ze skrzynek pocztowych. Analogicznie do zwykłego klienta pocztowego (Rysunek 4) można określić, jakie informacje o każdej wiadomości powinien wyświetlać KShowmail w głównym oknie. Aby skonfigurować te opcje, wybieramy zakładkę Display Options (Rysunek 5).

Klikamy przycisk Ok, aby powrócić do głównego okna zawierającego dwa panele (Rysunek 6). Nasze konta pocztowe są teraz wyświetlane w górnej liście. Symbol zaznaczenia w kolumnie Active nakazuje KShowmail sprawdzanie e-maili dla wybranego w ten sposób konta.

Jeśli nie masz czasu na czekanie, aż program przeprowadzi planowe sprawdzenie, wybierz Actions | Refresh messages lub kliknij na symbol strzałki. Jeśli do tej pory nie skonfigurowałeś hasła, KShowmail poprosi o jego podanie, a następnie wyświetli w dolnej liście głównego okna wszystkie wiadomości znajdujące się na serwerach POP3 (Rysunek 6).

Przytrzymujemy klawisz [Ctrl] i klikamy na wiadomościach, które chcemy usunąć. Klikamy na ikonce gumki lub wybieramy opcję Actions | Delete highlighted messa-



Rysunek 6: Główne okno KShowmail. Konta, z których będzie odbierana poczta, oznaczamy pataszkiem w kolumnie „Active” górnej listy.

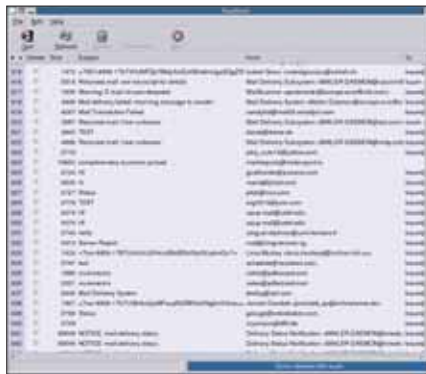


Rysunek 7: Możesz kliknąć znajdujący się w lewym dolnym rogu przycisk „Reply”, aby uruchomić KMail z KShowmail.

ges, aby usunąć wybrane wiadomości z serwera. Opcja Actions | Clear list czyści listę, nie usuwając żadnych wiadomości.

Więcej informacji o e-mailach

Nie zawsze łatwo jest zidentyfikować spam, korzystając tylko z informacji zawartych w treści listu. KShowmail potrafi temu zaradzić, używając rozszerzonego podglądu. Aby go włączyć, najpierw zaznaczamy wiadomość, o której chcemy więcej wiedzieć, następnie wybieramy opcję Actions | Show header of highlighted messages, a KShowmail wyświetli nagłówek wiadomości, czyli nadawcę, datę przesłania oraz serwer pocztowy. Jeśli wybierzemy Ac-



Rysunek 8: Pozbywanie się niechcianych wiadomości w głównym oknie PopWash. Klikając wybieramy wiadomości, a następnie usuwamy je naciskając „Delete”.

tions | Show complete highlighted messages, KShowmail wyświetli zawartość wybranej wiadomości w małym oknie tekstowym bez łączników (Rysunek 7).

Konkurent: PopWash

PopWash jest nowym projektem, stanowiącym wyzwanie dla bardziej znanych konkurentów.



Rysunek 9: W konfiguracji PopWash zostały wykorzystane te same dane konta co w Kshowmail (Rysunek 3).

PopWash znajduje się wciąż w fazie testów (aktualna wersja to 0.3). Wyjątkową cechą tego programu jest fakt, że został on oparty na mieszaninie Tcl i GTK. Dlatego PopWash wymaga nietypowej biblioteki Gnocl, która umożliwia współpracę pomiędzy tymi dwoma światami. Większość dystrybucji nie zawiera tej biblioteki, na szczęście możesz pobrać Gnocl ze strony WWW PopWash (Tabela 1).

Jeśli chcesz samodzielnie skompilować ten program, potrzebne będzie środowisko GNOME oraz dwa pakiety dla programistów:

Tabela 1: Antyspamowe narzędzia dla POP3

Nazwa	Eremove	KShowmail	PopWash
Biblioteki	GTK	Qt, KDE	Gnocl (Tcl, GTK, GNOME)
Zarządzanie wieloma kontami	nie	tak	nie
Automatyczne odświeżanie	nie	tak	nie
Łączy do zewnętrznych programów	nie	tak	nie
Widok nagłówka/zawartości e-maila	nie/nie	tak/tak	nie/nie
Filtry: Czarna lista/Biała lista	nie/nie	tak/nie	tak/tak
Filtry: Wyrażenia regularne	nie	tak	tak
Przechowywanie haseł	tak, niezaszyfrowane	tak, zaszyfrowane	nie
Strona domowa projektu	http://eremove.sourceforge.net/	http://kshowmail.sourceforge.net/	http://www.dr-baum.net/popwash/

Ramka 1: Filtrowanie

Sprawdzenie każdego e-maila jest bardzo męczące. Dlatego do budowy automatycznych filtrów antyspamowych bardzo przydatne są tzw. czarne listy – są to zwykłe listy słów. Filtr po prostu sprawdza każdą wiadomość pod kątem wystąpienia wyrazów z tej listy. Przykładowo, jeśli filtr odkryje słowo „Viagra” w temacie listu, usunie tę wiadomość. Oba programy: KShowmail i PopWash obsługują oczywiście czarne listy.

Program PopWash dodatkowo posiada tzw. białą listę. Działa ona dokładnie w odwrotny sposób: jeśli słowo znajdujące się na liście pojawi się w wiadomości, nie zostanie ona usunięta. Jeśli na listę zostaną wprowadzone zaufane adresy e-mail, to filtr nigdy nie usu-

nie od nich wiadomości, nawet gdy będą one zawierać słowo/słowa z czarnej listy, takie jak np. „Viagra”.

W PopWash konfigurujemy filtry wybierając w oknie konfiguracyjnym opcję String Matching. Następnie wybieramy jedną z zakładek White List lub Black List (Rysunek 10). PopWash będzie przeszukiwał słowa z pól: From (adres nadawcy listu), Subject (temat wiadomości) oraz To (adres odbiorcy e-maila).

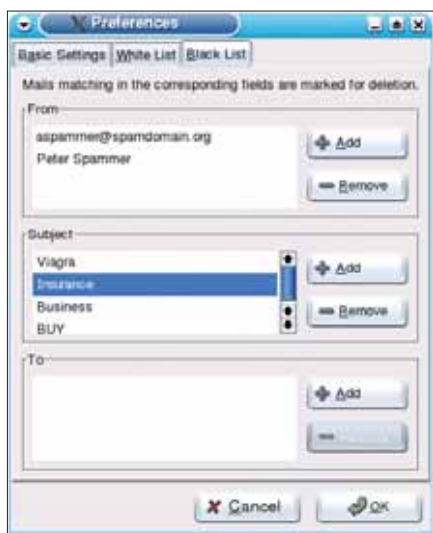
Klikamy przycisk Add, aby do odpowiedniej listy dopisać nowe słowo. Wciskamy [Enter], aby zakończyć wprowadzanie.

W KShowmail należy natomiast wybrać Setup | Filters. W oknie, które się pojawi,

wyberamy opcję Active (Rysunek 11), a następnie klikamy Add, tworząc nową pozycję listy.

Najpierw wybieramy warunki wyszukiwania w ramce Conditions (Rysunek 12), np. według kryterium zawartości tematu listu (opcja Subject), a następnie wpisujemy poszukiwany łańcuch w polu tekstowym. Jeżeli nie zaznaczymy w polu wyboru uwzględniania wielkości liter, KShowmail będzie stosować regułę niezależnie od wielkości liter.

Bardziej szczegółowe przeszukiwanie umożliwiają wyrażenia regularne (Ramka 2). Są one bardzo pomocne w pozbywaniu się spamu, zwłaszcza gdy spamery wykorzystują nietypową pisownię słów kluczowych.



Rysunek 10: Przykładowe filtry w PopWash.

GTK oraz Tcl wraz z biblioteką tellib. Jeśli wszystkie te aplikacje są dostępne, wpisujemy polecenie make w katalogu PopWash, aby uruchomić kompilację. Na koniec poleceniem su przechodzimy na konto root-a, po czym uruchamiamy instalację poleceniem make install. Po zakończeniu instalacji można uruchomić PopWash poleceniem popwash. Od razu można zauważyć, że PopWash posiada, robiący duże wrażenie, zestaw opcji, z wygodnym filtrowaniem e-maili (Ramka 1) na czele.

Wybieramy najpierw opcję Edit | Settings, pokaże się okno dialogowe, w którym zaznaczamy zakładkę Basic Settings (Rysunek 9). Wpisujemy tutaj nazwę serwera w polu tekstowym Pop3 Server oraz nazwę użytkownika w polu User name.

Opcja Default action for mails służy do określenia, co zrobić z wiadomością po jej



Rysunek 11: Okna do dodawania nowych filtrów. Obszar „Filter Status” umożliwia określenie, czy lista filtrów jest włączona, czy nie. W KShowmail można nakazać automatyczne usuwanie spamu.

odebraniu. Jeśli otrzymujesz dużo spamu, najlepiej wybrać też opcję Mark for deletion (zaznacz do usunięcia). Kliknięcie OK spowoduje, że powrócimy do głównego okna aplikacji (Rysunek 8).

Opcja Refresh nakazuje pobranie wiadomości z serwera. Przed naciśnięciem Delete można oznaczyć wiadomości do usunięcia w kolumnie o tej samej nazwie. Zatrzymanie usuwania jest możliwe po natychmiastowym naciśnięciu klawisza [Esc]. Aby cofnąć całą operację, wciskamy Stop.

Kto lepiej pierze brudy?

PopWash i KShowmail to więcej niż tylko proste narzędzia do usuwania spamu ze skrzynek pocztowych. Obydwa programy posiadają możliwość dalszej rozbudowy mechanizmów filtrowania m.in. poprzez wyrażenia regularne. Nieco skromniej prezentuje się na ich tle Eremove. W istocie wybór pro-

gramu jest uzależniony od wykorzystywanego środowiska graficznego oraz od tego, jakiego poziomu funkcjonalności oczekujesz. Ze wszystkich trzech omówionych programów najbardziej wszechstronny wydaje się KShowmail.

Aplikacja jest stabilna, działa w tle i jest doskonale zintegrowana ze środowiskiem KDE. Ponadto KShowmail jako jedyny potrafi obsługiwać kilka kont pocztowych jednocześnie. PopWash posiada niemal wszystkie funkcje, aby móc konkurować z KShowmail, ale jest wciąż aplikacją testową, w dodatku jest trudniejszy do zainstalowania, gdyż wymaga gnocl. W porównaniu do obu tych narzędzi, Eremove to oferta dla prawdziwym minimalistów, nie polecamy go ze względu na liczne błędy i generalny niedorozwój programu. ■



Rysunek 12: KShowmail umożliwia powiązanie dwóch warunków z jednym filtrem. Aby tego dokonać, łączymy warunek z górnej części okna z tym z dolnej części, wybierając logiczny operator z rozwijalnego menu.

Ramka 2: Używanie wyrażeń regularnych

Spamerzy często próbują obejść listę słów zawartych na czarnej liście. To dość proste, np. zamiast słowa „Viagra” wykorzystują jego zmodyfikowaną formę np. „VIA_gra”.

KShowmail i PopWash przeciwdziałają temu, używając w swoich filtrach wyrażeń regularnych. Dzięki temu nie ma potrzeby dodawania do listy wszystkich możliwych form dla słów kluczowych z czarnej listy.

Wyrażenie regularne działa analogicznie jak symbole wieloznaczne * czy? z linii poleceń. Na przykład pic*.jpg oznacza pliki zaczynające się na pic i kończące się na .jpg.

Wyrażenia regularne wyglądają w następujący sposób:

```
[^\b]@\spam\.org
```

Przykład ten oznacza dowolny adres e-mail kończący się na @spam.org. Wyrażenie [^\b] przeszukuje pojedynczy znak przed @spam.org. Sprawdza, czy pasuje on do wzorca w nawiasach kwadratowych. Znak ^ w nawiasach to warunek: „wszystkie znaki z wyjątkiem następującego”. Kombinacja \b oznacza początek lub koniec słowa. Reguła ta pasuje do dowolnego znaku przed @. W ten sposób filtr ten pasuje do wszystkich adresów kończących się na @spam.org.

Aby użyć wyrażeń regularnych w PopWash, wybieramy opcję Advanced regexp z menu Basic settings, a następnie wprowadzamy

stosowne wyrażenia regularne oraz słowa kluczowe (Ramka 1). Natomiast w KShowmail zaznaczamy pole wyboru Regular expression w oknie ustawień filtra (Setup | Filter | Add).

Zanim nauczysz się dobrze wykorzystywać wyrażenia regularne, trzeba nieco czasu i wielu eksperymentów. Jednak warto trochę się wysilić, ponieważ posiadanie podstawowej wiedzy dotyczącej wyrażeń regularnych pozwoli łatwo i szybko pozbyć się większości spamu. Więcej informacji na temat wyrażeń regularnych można znaleźć pod adresem <http://www.selflinux.org/selflinux/html/regex.html>, znajdują się tam także przykłady praktyczne.