

Zwalczanie wirusów z Windows w Linuksie: filtr ClamAV

# Wirusowa profilaktyka

Złośliwe oprogramowanie (ang. malware) bardzo się ostatnio rozpowszechniło. Mimo że Linux to generalnie system bezpieczny, użytkownicy mający zainstalowany na komputerze także MS Windows wciąż są narażeni na wielkie niebezpieczeństwo zainfekowania wirusem. Filtr antywirusowy jest zatem niezbędnym narzędziem.

MARC ANDRÉ SELIG



Wśród użytkowników komputerów panuje nadal pełna rezygnacji opinia, że najlepszym sposobem zabezpieczenia komputera jest odcięcie go od sieci, a najlepiej wyłączenie

zasilania. No cóż, w dobie wysokowydajnych akumulatorów i sieci bezprzewodowych odcięcie przewodów zasilających i sieciowych może nie wystarczyć do powstrzymania intruza (Ramka 1).

Zapory sieciowe (ang. firewall), regularne aktualizacje systemu operacyjnego i wyłączanie niepotrzebnych usług sieciowych to główne sposoby walki z napastnikami-ludźmi. W niniejszym artykule skupimy się na zautomatyzowanym, autonomicznym złośliwym oprogramowaniu, które potrafi atakować komputery użytkowników bez pomocy człowieka.

Istnieją trzy kategorie oprogramowania tego typu: przede wszystkim wirusy, usiłujące zarazić pliki wykonywalne na komputerze lokalnym lub udostępnione w środowisku sieciowym. Wirusy uaktywniają się w chwili uruchomienia zarażonego programu. Druga kategoria to konie trojańskie (zwane popularnie trojanami), w mniejszym lub większym stopniu wykorzystujące użytkownika do kopiowania i uruchomienia na komputerze ofiary. Trzecią kategorię stanowią robaki (ang. worms), w których posunięto się o krok naprzód – rozprzestrzeniają się one samoistnie, wykorzystując luki w bezpieczeństwie, rozsyłając się

## Listing 1: Instalacja ClamAV i Clamassassin

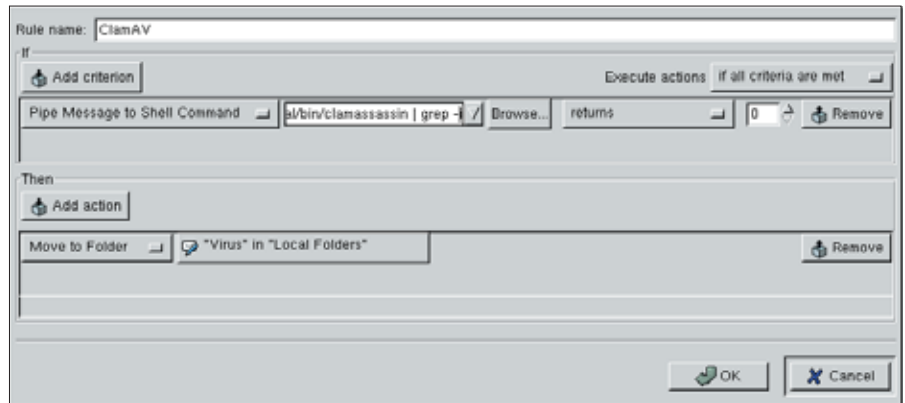
```
$ su
Password: root-password
# groupadd clamav
# useradd -g clamav -s /bin/false clamav
# exit
$ tar xzf clamav-0.70-rc.tar.gz
$ cd clamav-0.70-rc
$ ./configure --sysconfdir=/etc
[...]
$ make
[...]
$ su
Password: root-password
# make install

[...]
# exit
$ cd..
$ tar xzf clamassassin-1.0.0.tar.gz
$ cd clamassassin-1.0.0
$ su
Password: root-password
# install clamassassin /usr/local/bin
# cd /usr/local/bin
# ln -s `which mktemp`.
# ln -s `which formail`.
# exit
$
```

samodzielnie przy pomocy poczty internetowej do nowych ofiar.

Dowolna dystrybucja Linuksa ze wszystkimi aktualizacjami powinna oprzeć się szkodnikom tego typu. Wirusy mają i tak trudny orzech do zgryzienia próbując dostać się do systemów typu Unix. Nieuprawniony użytkownik, który uruchamia dany program, zwykle nie ma praw do jego modyfikacji. Robaki i trojany to już inna sprawa. Na szczęście system Linux jest nadal postrzegany jako nieatrakcyjny (tj. zbyt mało rozpowszechniony) dla działań hakerów, którzy tworzą te złośliwe programy. Ponadto słabe punkty programów Open Source są szybko (w ciągu kilku godzin od odkrycia zagrożenia) usuwane przy pomocy dodatkowych poprawek. Tak więc, jeżeli system jest aktualizowany na bieżąco, nie ma powodów do zmartwień.

W przypadku systemów MS Windows sytuacja nie wygląda już tak dobrze. Luki w oprogramowaniu dla tego systemu są często usuwane (poprzez wydanie poprawek) dopiero po kilku miesiącach, co ułatwia zadanie atakującym. Bez względu na



Rysunek 1: Współpraca ClamAV z Evolution.

to, czy korzystamy z systemu Windows zainstalowanego na drugiej partycji, obok Linuksa, czy też na osobnym komputerze, możemy wykorzystać Linuksa do stworzenia tarczy ochronnej dla tych systemów. Poniżej opiszemy nasze poszukiwania skanera antywirusowego dla systemu Linux. Skanera, który będzie automatycznie sprawdzał przychodzące wiadomości pocztowe lub pliki wykorzystywane wspólnie przez system Windows i Linuksa.

## Bezpłatny skaner antywirusowy

Dla systemu Linux, podobnie jak dla systemu Windows, dostępnych jest wiele skanerów antywirusowych. Niektóre są bezpłatne, inne – komercyjne [4, 5]. Większość z nich zaprojektowano tak, aby chroniły przed wirusami i robakami z systemu Windows.

W niniejszym artykule omówimy program ClamAV [1] – oryginalny produkt

## Ramka 1: Jak uszczelnić systemy operacyjne

Jakie kierunki ataku wybierze wirus, aby przeniknąć przez zabezpieczenia? Najbardziej oczywistym miejscem, z którego możemy spodziewać się ataku, jest usługa dostępu do sieci. Wiele systemów Unix wykorzystuje serwer Apache. Jeżeli serwer taki będzie miał jakiś słaby punkt, haker będzie prawdopodobnie mógł przeprowadzić atak, ustanawiając z nim połączenie umożliwiające przesłanie **exploita**. Użytkownicy komputerów domowych mogą zabezpieczyć się przed atakami tego rodzaju wyłączając lub w ogóle nie instalując usług, które nie są potrzebne.

W zasadzie każde dane pochodzące z ze-

wnątrz mogą zawierać exploit. Po ściągnięciu wiadomości tekstowej czasem wystarczy ją tylko przeczytać, a umożliwi to atakującemu wykorzystanie luki w bezpieczeństwie systemu. Wiele takich luk posiadają programy Outlook, a w szczególności Outlook Express. Dlatego też filtry pocztowe są tak ważnym elementem zabezpieczeń każdego komputera.

Zdarza się, że słabym ogniwem bezpieczeństwa są przeglądarki internetowe, umożliwiające atak w momencie wejścia na (nie)odpowiednią stronę internetową. Niektóre problemy tego typu można rozwiązać przy pomocy **serwera pośredniczącego**, inne – nie.

Dopiero niedawno wirusy i robaki zaczęły rozprzestrzeniać się poprzez sieciowe systemy plików (np. udostępnianie zasobów w systemie Windows). Problem znacznie złagodzone dzięki bardziej restrykcyjnej polityce ustawień domyślnych w systemach Windows oraz wykorzystaniu filtrów pakietów.

Niektóre kierunki ataku są na tyle tajemnicze, że użytkownicy komputerów domowych w zasadzie nie mają możliwości obrony. Tak naprawdę w każdym protokole podstawowym można znaleźć jakąś lukę i ją wykorzystać. W przeszłości dokonano już włamań w protokołach DNS i ICMP.

## SŁOWNICZEK

**Demon SMTP:** Serwer SMTP obsługuje w tle wiadomości wychodzące (w przypadku dostawców Internetu) i przychodzące. SMTP (Simple Mail Transfer Protocol) to skrót oznaczający dosłownie „prosty protokół przesyłania poczty”, czyli „język” komunikacji pomiędzy serwerami pocztowymi.

**groupadd:** Program uruchamiany z wiersza poleceń; umożliwia w naszym wypadku utworzenie nowej grupy użytkowników o nazwie clamav (Listing 1). Aby uruchomić program, musimy podać pełną ścieżkę dostępu

do polecenia `/usr/sbin/groupadd`.

**useradd:** Program uruchamiany z wiersza poleceń; umożliwia stworzenie konta dla nowego użytkownika (przez root-a). Parametr `-g` umożliwia określenie grupy, a `-s` – powłoki logowania dla nowego użytkownika. Wpis `„/bin/false”` na Listingu 1 sprawia, że nikt nie będzie mógł logować się na konsoli na nowe konto clamav. Konto służy wyłącznie do uruchamiania programów.

**install:** Program `/usr/bin/install` kopiuje narzędzie clamassassin do katalogu `/usr/local/bin`.

**procmail:** Rozbudowany program agenta pocztowego, umożliwiający odbieranie wiadomości pocztowych i zapisywanie ich w plikach na dysku. Istnieje wiele możliwości konfiguracyjnych programu, jak np. wyrafinowane sortowanie poczty według określonych kryteriów. Większość nowych dystrybucji Linuksa domyślnie korzysta z procmail (gdy użytkownik utworzy plik `~/procmailrc`). W razie wątpliwości można skorzystać z dodatkowych wskazówek pod adresem [6].

## Listing 2: ~/.procmairc dla ClamAV

```
# Kontrola poczty przychodzącej przy pomocy ClamAV
:0 fw
| /usr/local/bin/clamassassin

# Znalaziono wirusa? Jeśli tak, przechodzimy do virus-found
:0:
* X-Virus-Status: Yes
virus-found

# Inne komunikaty i komentarze
```

Open Source. Jeżeli potrzebna jest kompleksowa ochrona, będzie trzeba użyć również drugiego skanera, ale opisane dalej ogólne metody równie dobrze sprawdzają się w przypadku innych programów antywirusowych.

Instalacja programu ClamAV przebiega standardowo, jak w przypadku większości programów Linuksa. Przy instalacji jedynym problemem jest to, że ClamAV wymaga biblioteki MP [2], której nie ma w standardowych dystrybucjach. Podręcznik użytkownika zawiera wskazówki dotyczące instalacji pakietu z kodem źródłowym, a na Listingu 1 pokazaliśmy procedurę instalacji. Jeżeli korzystamy z komputera autonomicznego (nie podłączonego do sieci lokalnej), warto zainstalować dodatkowo program clamassassin [3]. Dzięki niemu połączymy skaner antywirusowy z systemem poczty elektronicznej, bez konieczności ponownej konfiguracji demona SMTP. Jest to rozwiązanie dużo łatwiejsze, ale też mniej wydajne. Pamiętajmy o znakach ` (znak tyldy) w poleceniach ln -s.

Zaraz po zakończeniu instalacji można

wypróbować program ClamAV. Zakładając, że partycje Windows zostały zamontowane w katalogu /windows, polecenie skanowania dysków będzie miało następującą postać:

```
clamscan -ri /windows
```

## Skanowanie poczty elektronicznej

Najciekawszą z funkcji programu ClamAV jest możliwość automatycznego skanowania przychodzących wiadomości poczty elektronicznej. Stopień integracji programu z istniejącym systemem pocztowym zależy wyłącznie od użytkownika.

Wielu użytkowników konfiguruje prawdziwy serwer pocztowy na lokalnym komputerze z systemem Linux – umożliwia to np. program SUSE YaST. Niewielki program fetchmail pobiera wiadomości przychodzące z serwera dostawcy i przesyła je do lokalnego serwera. Dzięki temu lokalny serwer pocztowy przechowuje wszystkie wiadomości w katalogu /var/mail lub /var/spool/mail, co umożliwia swobodne

manipulowanie pocztą, niezależnie od programu pocztowego.

Najprostszą metodą na dołączenie ClamAV do istniejącego systemu jest wykozystanie programu **procmairc**. Wystarczy, że na początku pliku konfiguracyjnego ~/.procmairc dopiszemy zawartość Listingu 2. Jeżeli w katalogu domowym nie istnieje jeszcze plik ~/.procmairc – po prostu stworzymy go, zapisując w nim kod z Listingu 2.

Użytkownicy korzystający z graficznych klientów poczty, np. Evolution czy KMail, muszą użyć innej konfiguracji, ponieważ w ich wypadku procmairc nigdy nie uzyskuje bezpośredniego dostępu do poczty i cały Listing 2 będzie bezużyteczny. Jedyną metodą jest ustawienie filtra wewnątrz programu pocztowego. Na Rysunku 1 pokazano ustawienie filtra w programie Evolution, można wykorzystać następujący **potok**:

```
sh -c „/usr/local/bin /clamassassin | grep -i 'x-virus-status: yes'”
```

Innymi słowy, wiadomość będzie najpierw przesyłana do clamassassin, a grep przeszuka wiadomość pod kątem słów kluczowych, które mogłyby być śladem wirusa. Jeżeli wyszukiwanie zakończy się sukcesem, zainfekowana wiadomość powędruje do specjalnego katalogu z wirusami.

## Zdążyć na czas

Niektórzy użytkownicy, nauczeni doświadczeniem z systemem Windows, doskonale sobie zdają sprawę, że nawet najlepszy program antywirusowy staje się z biegiem czasu bezużyteczny, jeżeli nie jest na bieżąco

## SŁOWNICZEK

**Cron:** Demon działający w tle i automatycznie uruchamiający programy o określonym czasie. Wpisy do tzw. tabel programu cron zawierają przejrzysty spis zaplanowanych zadań, podzielony na poszczególne konta użytkowników.

**Exploit:** Program wykorzystujący lukę w bezpieczeństwie innego programu, umożliwiając uruchomienie dowolnego kodu na komputerze ofiary.

**Serwer pośredniczący:** Zwany też proxy – jest to program pośredniczący w połączeniu między komputerem lokalnym (np. przeglądarką internetową) a serwerem internetowym. Proxy przyjmuje żądania

z komputera-klienta i przesyła je do serwera. Przesyła także odpowiedzi do komputera lokalnego. Proxy potrafi prowadzić nadzór, korygować lub po prostu buforować pliki, stosować ograniczenia dostępu, a więc ogólnie zwiększa bezpieczeństwo systemu.

**DNS:** Serwer nazw domen (ang. Domain Name Service) zamienia nazwy hostów typu www.abcxyz.com na adresy IP typu 136.199.85.18 i odwrotnie. Jako że większość usług sieciowych wymaga serwera DNS, błędy w serwerach tego typu stanowią szczególnie duże zagrożenie.

**ICMP:** Internet Control Message Protocol

jest wykorzystywany do prowadzenia diagnostyki sieci, np. do kontroli połączenia pomiędzy dwoma komputerami lub do określenia maksymalnego, dopuszczalnego rozmiaru przesyłanego pakietu. Przykładowo, polecenie ping umożliwia stwierdzenie, czy zdalny komputer jest włączony i dostępny w danej sieci – zalewanie zapytaniami ping umożliwiało niegdyś zawieszanie komputerów ze starszymi wersjami Windows.

**Potok:** Przy pomocy znaku | wynik polecenia znajdującego się po lewej stronie znaku jest przetwarzany przez polecenie znajdujące się po prawej stronie znaku.

aktualizowany. Na bieżąco, czyli znacznie częściej niż raz w tygodniu.

Do aktualizacji programu ClamAV służy narzędzie `freshclam` – program automatycznie aktualizuje bazę danych sygnatur wirusów. Mając uprawnienia użytkownika `root` wystarczy mniej więcej co godzinę wykonać polecenie:

```
/usr/local/bin/freshclam --quiet
```

Można oczywiście dopisać to polecenie do pliku `/etc/ppp/ip-up`, dzięki czemu baza danych będzie aktualizowana po każdym nawiązaniu połączenia PPP.

W przypadku korzystania ze stałego dostępu do Internetu najlepiej użyć demona `cron`. Do pliku `/etc/crontab` trzeba dodać następujący wpis:

```
24 * * * * root /usr/local/bin  
/freshclam --quiet
```

W ten sposób baza danych sygnatur wirusów będzie aktualizowana 24 minuty po każdej pełnej godzinie.

Kolejne pytanie, jakie się nasuwa: „Czy skaner antywirusowy jest skuteczny?” Aby na nie odpowiedzieć, możemy przeprowadzić test, pobierając plik fałszywego wirusa EICAR z adresu [7]. Plik ten został specjalnie zaprojektowany na potrzeby testowania programów antywirusowych. ■

## INFO

- [1] ClamAV: <http://www.clamav.net/>
- [2] GNU MP:  
<http://www.gnu.org/directory/GNU/gnump.html> or  
<http://www.swox.com/gmp/>
- [3] Clamassassin:  
<http://drivel.com/clamassassin/>
- [4] Przegląd komercyjnego oprogramowania antywirusowego:  
<http://tinyurl.com/33syb>
- [5] F-Prot firmy Frisk:  
[http://www.f-prot.com/products/home\\_use/linux/](http://www.f-prot.com/products/home_use/linux/)
- [6] Listingi z bieżącego artykułu i dodatkowe wskazówki pomocne przy konfiguracji:  
<http://www.seligma.com/linux-user/virus/>
- [7] EICAR:  
[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)

# Prenumerata Linux Magazine

## Nie przegap takiej okazji!!!



- Zamawiając prenumeratę oszczędzasz!
- Płacisz jak za 9 numerów, a otrzymujesz 12!
- Z każdym numerem DVD lub płyta CD-ROM.

Najszybszy sposób zamówienia prenumeraty:

<http://www.linux-magazine.pl>

Infolinia: 0801 800 105