

# Andrzej Kobyliński, Stanisław Lipski

---

## Analiza skuteczności programów antywirusowych

---

Ekonomiczne Problemy Usług nr 87, 404-413

---

2012

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

ANDRZEJ KOBYLIŃSKI, STANISŁAW LIPSKI

Szkoła Główna Handlowa

## ANALIZA SKUTECZNOŚCI PROGRAMÓW ANTYWIRUSOWYCH

### Wprowadzenie

Wprawdzie wszyscy są świadomi tempa, w jakim powiększa się zakres popularności Internetu, ale dane liczbowe dotyczące tego procesu są naprawdę imponujące. W ostatnim czasie Intel rozesłał bardzo interesującą infografikę<sup>1</sup> (do której autorzy artykułu dotarli poprzez stronę Marka H. Goldberga<sup>2</sup>), która obrazuje rozwój Internetu. Liczba urządzeń sieciowych, poprzez które korzystać można z zasobów Internetu, osiągnęła już liczbę mieszkańców Ziemi i szacuje się, że zostanie podwojona za 3 lata. Co minutę (!):

- przez Internet przesyłanych jest prawie 640 TB danych,
- do YouTube ładowanych jest kolejnych 30 godzin materiału filmowego, a 1,3 mln użytkowników ogląda zgromadzone tam już materiały,
- 6 mln osób przegląda Facebooka,
- Google udziela odpowiedzi na ponad 2 mln zapytań,
- wysyłane są 204 mln listów elektronicznych<sup>3</sup>.

Oczywiście znaczną część przesyłanych e-maili stanowi spam, w ostatnich latach stanowi on 80–85% wszystkich przesyłek elektronicznych, a według ostatnich danych dostępnych autorom podczas pisania artykułu wynosił on 80,6%<sup>4</sup>. Każdy niezamawiany list<sup>5</sup> o charakterze handlowym stanowi pewną uciążliwość dla

<sup>1</sup> [http://mhgoldberg.com/blog2/wp-content/uploads/2012/01/infographic\\_600\\_intel.jpg](http://mhgoldberg.com/blog2/wp-content/uploads/2012/01/infographic_600_intel.jpg)

<sup>2</sup> <http://mhgoldberg.com/blog/?p=5321>

<sup>3</sup> Czyli ok. 42 dziennie na każdego mieszkańca Ziemi.

<sup>4</sup> <http://www.viruslist.pl/news.html?newsid=691#9>

<sup>5</sup> Zgodnie z art. 10 Ustawy o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (DzU nr 144, poz. 1204) „1. Zakazane jest przysyłanie niezamówionej informacji handlowej

odbiorcy, który traci swój czas na określenie jego charakteru, a następnie ewentualne usunięcie go, ale o wiele gorsze jest to, że aż w 3% korespondencji znajdują się szkodliwe pliki<sup>6</sup>. To one w ostatnich latach stanowią podstawowe źródło infekcji: otwarcie zawirusowanego pliku dołączonego do listu elektronicznego, pobranie i uruchomienie zainfekowanego programu komputerowego, wejście na zawirusowaną stronę internetową – to są najczęstsze sposoby zarażenia wirusem komputerowym. Duża grupa wirusów przenoszona jest tradycyjnie – poprzez urządzenia pamięci zewnętrznej dołączane wprost do komputerów: płyty CD i DVD, przenośne twarde dyski, a przede wszystkim urządzenia typu *pendrive*.

Na szczęście od lat na rynku dostępnych jest wiele programów antywirusowych, zarówno rozprowadzanych komercyjnie, jak i bezpłatnych. Świadomość zagrożeń, jakie niesie brak ochrony antywirusowej, jest już na szczęście na tyle wysoka, że rzadko spotyka się komputery pozbawione jakichkolwiek zabezpieczeń. Z drugiej strony nadmierna bywa ufność użytkowników oprogramowania antywirusowego w skuteczność stosowanych mechanizmów. Na zainstalowaniu programu antywirusowego często kończy się cała aktywność użytkownika związana z zabezpieczeniem komputera; niekiedy użytkownicy zapominają przedłużyć licencję, co skutkuje brakiem aktualizacji baz sygnatur wirusów; w jeszcze innych przypadkach użytkownicy świadomie wyłączają oprogramowanie antywirusowe, które ich zdaniem niepotrzebnie spowalnia pracę systemu komputerowego. Ale nawet wykorzystywanie stale aktualizowanego oprogramowania antywirusowego nie zawsze wystarcza – skuteczność programów antywirusowych nie jest stuprocentowa. Często użytkownikom wydaje się, że gdy zainstalowali i wykorzystują oprogramowanie antywirusowe, to są w pełni chronieni, wydaje im się, że antywirusy wykryją wszystkie zagrożenia i zapewnią pełne bezpieczeństwo. Niestety, przekonanie to należy uznać za nadmiernie optymistyczne.

Celem pracy jest zbadanie wybranych programów antywirusowych pod kątem skuteczności w wykrywaniu szkodliwego (złośliwego) oprogramowania (*malware*).

## 1. Rodzaje zagrożeń powodowanych przez szkodliwe oprogramowanie

Historia szkodliwego oprogramowania sięga już 40 lat. W latach 70. XX wieku w sieci Arpanet (będącej protoplastą Internetu) wykryto pierwszego wirusa – o nazwie Creeper; w 1981 roku miała miejsce pierwsza w historii epidemia wirusów na większą skalę – wirus Elk Cloner zaatakował system operacyjny komputerów Apple II; w 1983 termin „wirus” został po raz pierwszy użyty przez L. Adle-

---

skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej”.

<sup>6</sup> <http://www.viruslist.pl/news.html?newsid=691#9>

mana, a rok później spopularyzowany przez F. Cohena; w 1986 roku miała miejsce pierwsza ogólnościatowa infekcja wirusa Brain; w 1988 R.T. Morris uruchomił wirusa, który w przeciągu kilku godzin praktycznie sparaliżował działanie całego Internetu<sup>7</sup>. W początkowym okresie jedynym wykorzystywanym rodzajem szkodliwego oprogramowania były wirusy. Stopniowo pojawiały się kolejne grupy złośliwego oprogramowania: robaki, trojany, expoity, dialery, spyware, szkodliwe adware itd. Klasyfikacji i powiązań rodzajów szkodliwego oprogramowania można doszukać się co najmniej kilka. Nie faworyzując żadnej z nich, zdefiniujemy krótko poszczególne, najczęściej aktualnie występujące rodzaje szkodliwego oprogramowania<sup>8</sup>:

- wirusy – programy komputerowe posiadające zdolność samopowieliania, modyfikujące nośnik danych (nosiciela),
- robaki (*worm*) – samopowielający się program, podobny do wirusa, lecz przenoszący się poprzez sieć, niepotrzebujący nosiciela (wspomniany wcześniej Creeper był właśnie robakiem),
- konie trojańskie (tzw. trojany) – programy, które wydają się użyteczne i zachęcają użytkownika do ich uruchomienia ze względu na oferowane funkcjonalności, po czym wykonują różnego rodzaju szkodliwe działania (np. instalowanie *backdoora*, szpiegowanie itp.),
- *backdoor* – rodzaj trojana, który przejmuje kontrolę nad zarażonym komputerem, umożliwiając włamywaczowi zdalne administrowanie systemem operacyjnym komputera poprzez sieć, który wykonuje te czynności bez wiedzy i woli ofiary,
- programy szpiegujące (*spyware*) – szkodliwe oprogramowanie zbierające informacje o użytkowniku komputera, takie jak hasła dostępne lub dane o odwiedzanych stronach itp., niekiedy również wykonujące działania bez wiedzy użytkownika,
- *adware*<sup>9</sup> – programy, które bez zgody użytkownika wyświetlają niechciane reklamy, robiąc to w sposób utrudniający korzystanie z komputera, czasami zawierają fragmenty złośliwego kodu szpiegującego użytkownika.

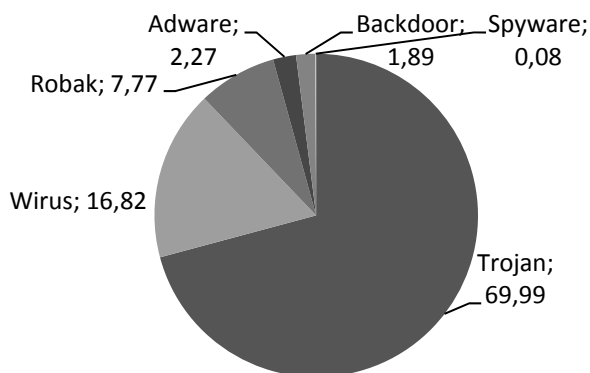
Te akurat typy oprogramowania zostały powyżej wspomniane, gdyż one właśnie, według badań przeprowadzonych przez Panda Security, firmy oferującej rozwiązania antywirusowe, stanowią większość aktualnie spotykanych rodzajów szkodliwego oprogramowania. Obrazuje to rysunek 1.

---

<sup>7</sup> <http://www.viruslist.pl/encyclopedia.html?chapter=articles&id=1>

<sup>8</sup> [en.wikipedia.org](http://en.wikipedia.org)

<sup>9</sup> Jest też drugie znaczenie tego terminu, oznaczające typ licencji na oprogramowanie, w którym użyteczne oprogramowanie rozpowszechniane jest bezpłatnie, ale za to użytkownik godzi się na wyświetlanie reklam podczas wykorzystywania takiego programu.



Rys. 1. Powszechność występowania poszczególnych kategorii szkodliwego oprogramowania (%)

Źródło: *Creation of New Malware Increases by 26 Percent, Reaching More than 73,000 Samples Every Day, According to PandaLabs*, <http://press.pandasecurity.com/usa/news/creation-of-new-malware-increases-by-26-percent-reaching-more-than-73000-samples-every-day-according-to-pandalabs/>

Pod względem powszechności występowania wirusy zostały wyprzedzone przez trojany już w 2003 roku<sup>10</sup>. Trend ten obserwowany jest do dnia dzisiejszego. Według doniesień z laboratorium Panda Security obecnie trojany stwarzają już 70% zagrożeń, podczas gdy wirusy niespełna 17%<sup>11</sup>. Co więcej, jak wynika z tego samego źródła, w pierwszym kwartale 2011 roku (z tego okresu pochodzą najświeższe dane) nastąpił 26-procentowy przyrost nowych zagrożeń w porównaniu do podobnego okresu w roku 2010. W I kwartale 2011 roku laboratorium Panda Security identyfikowało codziennie 73 000 nowych odmian złośliwego oprogramowania.

Oczywiście jak zawsze we wszystkich dziedzinach życia, akcja pociąga za sobą reakcję. Pierwszy znany przypadek neutralizacji wirusa wystąpił w 1986 roku, gdy B. Fix znalazł antidotum na wirusa Vienna, stając się w ten sposób prekursorem współczesnych ekspertów z dziedziny programów antywirusowych. W kolejnych latach wiele osób zajęło się tym problemem, początkowo powstało dużo małych, 2-3-osobowych zespołów, część z nich przekształciła się w firmy, które wydawały cieszące się znaczną popularnością programy antywirusowe. Pierwszy komercyjny program antywirusowy pojawił się w 1987 roku, a był nim AntiVirusKit

<sup>10</sup> <http://www.viruslist.pl/encyclopedia.html?chapter=articles&id=17>

<sup>11</sup> <http://press.pandasecurity.com/usa/news/creation-of-new-malware-increases-by-26-percent-reaching-more-than-73000-samples-every-day-according-to-pandalabs/>

niemieckiej firmy G Data Software AG<sup>12</sup>. Obecnie rynek programów antywirusowych jest bardzo dobrze rozwinięty. Działa na nim kilkudziesięciu graczy o zasięgu globalnym, na rynkach lokalnych próbują działać mniejsi producenci (np. w Polsce od końca lat 80. XX wieku do chwili obecnej powstają kolejne wersje programu mks\_vir<sup>13</sup>).

## 2. Opis eksperymentu i uzyskane wyniki

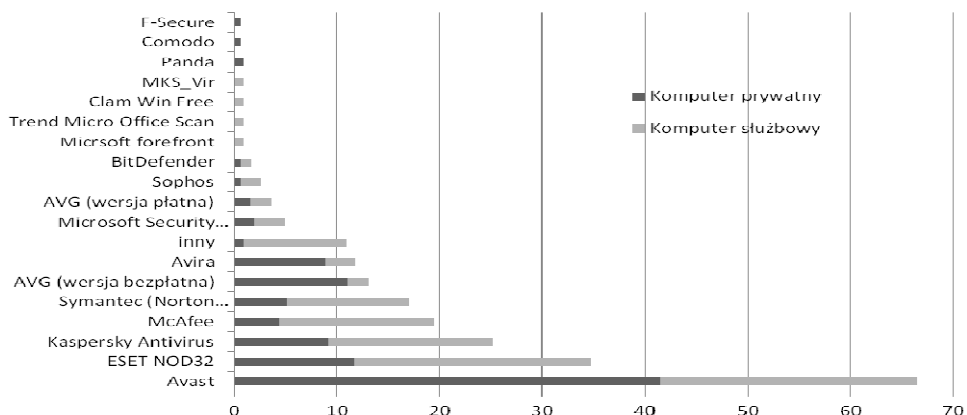
Jeden z autorów artykułu, zbulwersowany faktem, że każdorazowa wizyta z *pendrivem* w punkcie druku skutkowałą zarażeniem kolejnymi wirusami, postanowił gromadzić znaleźiska (było to o tyle bezpieczne, że korzysta on z systemu operacyjnego Linux, a odmienna architektura systemu GNU/Linux pozwalała na bezpieczne składowanie znajdujących na nośnikach plików uruchamialnych, bez zagrożenia zawirusowaniem komputera). W ten sposób na przestrzeni lat 2008–2011 udało się zebrać 33 podejrzane pliki (tabela 1). Jednocześnie we wszystkich punktach deklarowano, że mają zainstalowane oprogramowanie antywirusowe. Podejrzanie zatem można było skierować na skuteczność oprogramowania antywirusowego.

Pierwszym etapem systematycznego badania było określenie, które programy antywirusowe są najczęściej wykorzystywane w Polsce. Ponieważ niechęć pracowników punktów do udzielania odpowiedzi można uznać za zrozumiałą, przeprowadzono badanie ankietowe dotyczące popularności tego typu programów wśród studentów i absolwentów szkół wyższych. Uzyskano 369 poprawnie wypełnionych ankiet, odpowiedzi udzieliły osoby w wieku od 15 do ponad 40 lat, w większości (78%) studenci wszystkich typów uczelni (technicznych, ekonomicznych, humanistycznych, medycznych, przyrodniczych, artystycznych). Osoby aktywne zawodowo (zarówno absolwenci, jak i studenci) stanowiły 38%. Rozróżnienie na osoby pracujące i niepracujące jest o tyle istotne, że respondenci pytani byli odrębnie o programy antywirusowe wykorzystywane w pracy i w domu. Uzyskanej próby statystycznej nie można uznać za reprezentatywną, aczkolwiek odpowiedzi respondentów znajdują dobre odzwierciedlenie w rzeczywistości i mogą zostać uznane za niezły materiał do badań. Nie miało to jednak żadnego znaczenia w kontekście właściwego badania, tutaj chodziło wyłącznie o to, by do dalszych badań użyć wyłącznie programy najpopularniejsze. Rozkład popularności poszczególnych programów antywirusowych, z zaznaczeniem zastosowania na komputerach prywatnych i służbowych, przedstawiony został na rysunku 2.

---

<sup>12</sup> <http://www.gdatasoftware.co.uk/security-labs/news/news-details/article/1532-g-data-presents-security-first.html>

<sup>13</sup> <http://www.mks.com.pl/>



Rys. 2. Popularność poszczególnych programów antywirusowych

Źródło: opracowanie własne.

W dalszych badaniach użyto 7 programów o największej popularności oraz ClamAV (gdyż jest on używany na serwerach i jest rekomendowany przez znaczące firmy informatyczne. Badaniu poddano wszystkie zgromadzone 33 podejrzane pliki (tabela 1).

Tabela 1

Lista podejrzanych plików

| Nazwa             | Wielkość  | Nazwa         | Wielkość   |
|-------------------|-----------|---------------|------------|
| 2id9.exe          | 112,64 KB | jwgvksq.vmx   | 168,6 KB   |
| 9xf8.exe          | 113 KB    | kraljevic.exe | 121,5 KB   |
| bajrami.exe       | 154 KB    | kure.exe      | 68 KB      |
| cgaqyi.exe        | 111 KB    | macuru.exe    | 92,5 KB    |
| dogyx90.exe       | 113,31 KB | opgde.exe     | 107,15 KB  |
| dryq.pif          | 167,5 KB  | p6xebmnt.exe  | 110 KB     |
| ehthumbs_vista.db | 1840 KB   | q3kku.exe     | 113,14 KB  |
| etaklp.exe        | 656,45 KB | rane.exe      | 1445,96 KB |
| ewqij.bat         | 110,1 KB  | Recycle.exe   | 1445,96 KB |
| findproc.dll      | 473,55 KB | spoolsv.exe   | 31 KB      |
| fzgykr.exe        | 470,23 KB | tgt.exe       | 93,5 KB    |
| ggpw.exe          | 130,5 KB  | tornado.exe   | 99,5 KB    |
| gpaswp.exe        | 802,38 KB | UFO.exe       | 17,5 KB    |
| hladi.exe         | 134,5 KB  | usbdrive.exe  | 1468 KB    |
| installer.exe     | 1736 KB   | veza.exe      | 145,5 KB   |
| iqosrtk.bat       | 102,02 KB | yqg8eqil.exe  | 112,5 KB   |
| jwgvksq_v2.vmx    | 164,42 KB |               |            |

Źródło: opracowanie własne.

Tabela 2

Rezultaty badania podejrzanych plików programami antywirusowymi

| Plik/program             | ClamAV | Kaspersky | AVG  | Avast | Avira | NOD32 | Norton | McAfee |
|--------------------------|--------|-----------|------|-------|-------|-------|--------|--------|
| 2id9.exe                 | -      | +         | +    | -     | +     | -     | +      | +      |
| 9xf8.exe                 | -      | +         | +    | -     | +     | -     | +      | +      |
| bajrami.exe              | +      | +         | +    | +     | +     | +     | +      | +      |
| cgaqyi.exe               | +      | +         | +    | +     | +     | +     | +      | +      |
| dogyx90.exe              | +      | +         | +    | +     | +     | +     | +      | +      |
| dryq.pif                 | +      | +         | +    | +     | +     | +     | +/-    | +/-    |
| ehthumbs_vista.db        | -      | -         | -    | -     | -     | -     | -      | -      |
| etaklp.exe               | +      | +         | +    | -     | +     | +     | +      | +      |
| ewqij.bat                | -      | +         | +    | -     | +     | -     | +      | +      |
| findproc.dll             | -      | -         | -    | -     | -     | -     | -      | -      |
| fzgvkr.exe               | +      | +         | +    | +     | +     | +     | +      | +      |
| gppw.exe                 | -      | +         | +    | +     | +     | +     | +      | +      |
| gpaswp.exe               | +      | +         | +    | -     | +     | -     | +      | +      |
| hladi.exe                | -      | +         | +    | -     | +     | -     | +      | +      |
| installer.exe            | -      | -         | -    | -     | -     | -     | +      | +      |
| iqosrtk.bat              | -      | +         | +    | -     | +     | -     | +      | +      |
| jwgkvsq_v2.vmx           | +      | +         | +    | -     | +     | -     | +      | +      |
| jwgkvsq.vmx              | +      | +         | +    | -     | +     | -     | +      | +      |
| kraljevic.exe            | +      | +         | +    | -     | +     | -     | +      | +      |
| kure.exe                 | -      | +         | +    | -     | +     | -     | +      | +      |
| macuru.exe               | -      | +         | +    | -     | +     | -     | +      | +      |
| opgde.exe                | +      | +         | +    | -     | +     | -     | +      | +      |
| p6xebmnt.exe             | +      | +         | +    | -     | +     | -     | +      | +      |
| q3kku.exe                | -      | +         | +    | -     | +     | -     | +      | +      |
| rane.exe                 | +      | +         | +    | -     | +     | -     | +      | +      |
| Recycle.exe              | +      | +         | +    | -     | +     | -     | +      | +      |
| spoolsv.exe              | +      | +         | +    | -     | +     | -     | +      | +      |
| tgt.exe                  | +      | +         | +    | -     | +     | -     | +      | +      |
| tornado.exe              | -      | +         | +    | -     | +     | -     | +      | +      |
| UFO.exe                  | +      | +         | +    | -     | +     | -     | +      | +      |
| usbdrive.exe             | -      | +         | +    | -     | +     | -     | +      | +      |
| veza.exe                 | -      | +         | +    | -     | +     | -     | +      | +      |
| yqq8eqil.exe             | +      | +         | +    | -     | +     | -     | +      | +      |
| <b>Wykryto zagrożeń</b>  | 18     | 30        | 30   | 6     | 30    | 7     | 30     | 30     |
| <b>Falszywe wykrycia</b> | 0      | 0         | 0    | 0     | 0     | 0     | 1      | 1      |
| <b>Pominięto</b>         | 0      | 0         | 0    | 0     | 0     | 0     | 1      | 1      |
| <b>Punkty</b>            | 18     | 30        | 30   | 6     | 30    | 7     | 28     | 28     |
| <b>Wynik</b>             | 60%    | 100%      | 100% | 20%   | 100%  | 23%   | 93%    | 93%    |

Źródło: opracowanie własne.



Zasadnicza część badań polegała na przeskanowaniu wszystkich podejrzanych plików 8 programami antywirusowymi (w różnych wersjach i konfiguracjach), i to zarówno w trybie ochrony rezydentnej, jak i skanowania uruchamianego na żądanie. Wykrycie zagrożenia co najmniej w jednym z tych trybów pracy zaznaczone zostało w tabeli 2 za pomocą znaku „+”, jako skuteczne wykrycie wirusa. Proces skanowania przeprowadzany był pod systemem operacyjnym Microsoft Windows XP, uruchomionym na tzw. maszynie wirtualnej emulowanej przez oprogramowanie Oracle VirtualBox. Taka konstrukcja środowiska miała uniemożliwić wirusom wyrządzenie ewentualnych szkód. Celem skanowań było zarówno zidentyfikowanie zagrożeń zawartych w zebranych plikach, jak i porównanie skuteczności programów antywirusowych. Sumaryczne wyniki badań zawarte są w tabeli 2.

W próbie 33 podejrzanych programów znajdowało się 30 programów szkodliwych. **Kaspersky, AVG, Avira wykryły je bezbłędnie.** Natomiast Norton i McAfee wykryły wprawdzie 30 zagrożeń, ale w jednym przypadku były nadgorliwe – podejrzany plik *installer.exe* uznały za szkodliwy (pomimo że ten wcale taki nie był – zaznaczono to cyfrą 1 w wierszu „Fałszywe wykrycia”), a nie zauważyły szkodliwości pliku *dryq.pif* (a właściwie zauważyły to, lecz nie podjęły żadnych kroków prewencyjnych – w tabeli 2 zasygnalizowano to symbolem „+/-” we właściwym wierszu, a następnie na dole tabeli 2 cyfrą 1 w wierszu „Pominięto”). Te dwa uchybienia obniżyły punktację tych programów do 28. Ale szczególnie niepokój może budzić fakt, że 2 najpowszechniej stosowane programy antywirusowe (patrz rysunek 2), Avast i NOD32, wykazały tak słabą skuteczność, wykrywając zaledwie niewiele ponad 20% zagrożeń.

## Podsumowanie

Badanie wykazało, że niektóre programy antywirusowe znacząco górują nad innymi pod względem skuteczności wykrywania szkodliwego oprogramowania. Co ciekawe, właśnie to wyraźnie mniej skuteczne oprogramowanie cieszy się większą popularnością wśród użytkowników. Z czego może wynikać ten paradoks? Prawdopodobnie z tego, że skuteczność w działaniu (wykrywalność) to nie jedyna cecha jakościowa, która jest interesująca dla użytkowników. Równie istotne mogą być takie kwestie, jak zdolność do zreperowania zarażonych plików, użyteczność (przyjazność, łatwość użycia, intuicyjność, dobre domyślne opcje konfiguracji, czytelność raportów, możliwość zapisywania raportów w postaci plików zewnętrznych, np. tekstowych, linki do stron z informacjami o wykrytych zagrożeniach itp.), czas potrzebny do przeskanowania podejrzanych plików i obciążenie wykorzystywanych zasobów (procesora i pamięci operacyjnej). Istotna dla użytkownika może też być kwestia możliwości wyboru trybu skanowania (rezydentna lub na żądanie) – nie wszystkie badane programy miały opcję skanowania rezydentnego. Warto przy

okazji zauważyć, iż badania wykazały, że skanowanie na żądanie było zawsze skuteczniejsze od rezydentnego. Pewien wpływ na popularność może też mieć fakt, że niektóre programy mogą być rozprowadzane jako rozwiązania autonomiczne, inne zaś jako element większego pakietu zabezpieczenia komputera, w skład którego może dodatkowo wchodzić np. *firewall*. W pełniejszym badaniu należałoby uwzględnić te dodatkowe cechy. A nie można też zapomnieć o względach marketingowych. Niektóre antywirusy są dołączane w wersjach próbnych (np. miesięcznych) do nowo zakupywanych komputerów, co przyzwyczajają użytkownika, który potem już się nie zastanawia, czy ten antywirus jest skuteczny. Pogłębione badania powinny uwzględnić większy zbiór programów antywirusowych, dodatkowo w różnych wersjach (komercyjnych, próbnych, bezpłatnych), celem stwierdzenia, czy rozwiązanie darmowe ustępuje komercyjnym.

Opisany w artykule test skuteczności nie może być uznany za w pełni miarodajny. Oprócz zasygnalizowanego już niedostatku, polegającego na szczupłości zestawu przebadanych programów antywirusowych, jeszcze większe wątpliwości można mieć w stosunku do liczności zbioru zainfekowanych plików. Użyta próbka z całą pewnością nie była reprezentatywna i można sądzić, że w przypadku zastosowania innej bazy próbek wyniki mogłyby być nieco odmienne.

## Literatura

1. G Data Software AG, <http://www.gdatasoftware.co.uk> (15.01.2012).
2. Goldberg M., *In an internet minute*, <http://mhgoldberg.com/blog/?p=5321> (15.01.2012).
3. MKS Sp. z o.o., <http://www.mks.com.pl/> (15.01.2012).
4. Press Panda Security, <http://press.pandasecurity.com/> (15.01.2012).
5. Viruslist.pl – wszystko o bezpieczeństwie, <http://www.viruslist.pl> (15.01.2012).
6. Wikipedia, [en.wikipedia.org](http://en.wikipedia.org) (15.01.2012).

## PERFORMANCE ANALYSIS OF THE ANTIVIRUS SOFTWARE

### Summary

The development of computerization and the Internet affected the increase in the scale of threats involved. One of the most common are computer viruses. Users fight them using antivirus programs. The effectiveness of these programs can be questioned. The research described in the paper was to determine which antivirus programs are the

most popular, and then examine the effectiveness of the most popular antivirus software for detection and removal of viruses.

*Translated by Andrzej Kobyliński*