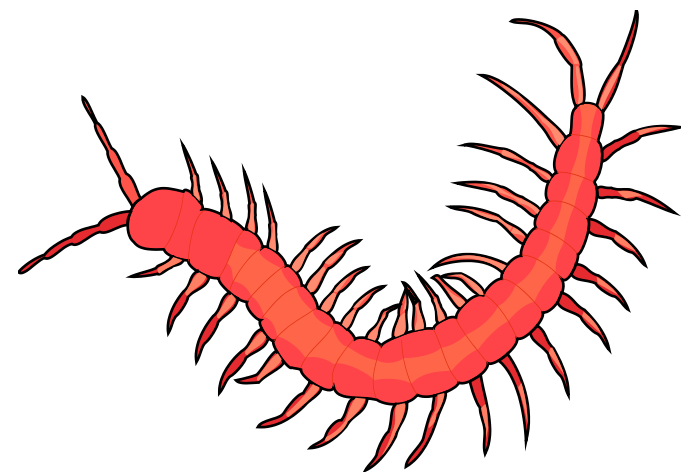


WIRUSY



Lub: **MALWARE** (Mal-Ware) –
WIRUSY, Phishing, ROBAKI I INNE KONIE TROJAŃSKIE

Wirus komputerowy

Nazwa „wirus” powstała prawdopodobnie w 1984 roku i pochodzi bezpośrednio od biologicznego „protoplasty”, który jest także mały, rozmnaża się samodzielnie i nie może funkcjonować bez organizmu tworzącego jego środowisko.



Wirus

- Komputerowy program, który potrafi sam się replikować. Termin wirus jest używany zamiennie zarówno w odniesieniu do wirusów, jak i robaków, co z technicznego punktu widzenia jest niepoprawne.
- Przenosi się przez nośniki (USB i inne), Sieć (P2P 66%) IM i inne.

Wirusy i robaki (Worm'y)

Wirus podszywa się/ukrywa np. pod nazwą podobną do znanego programu.

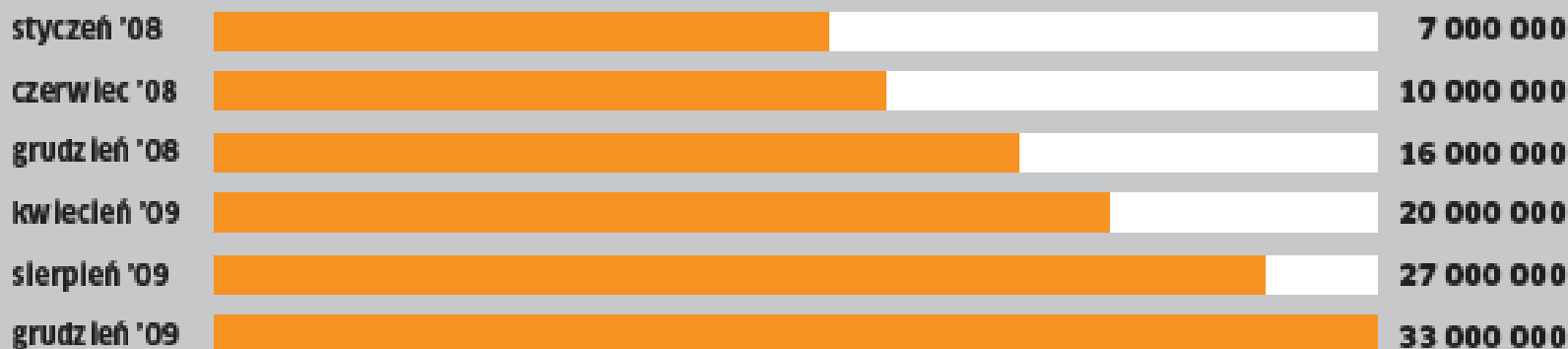
Jest to mały program, który nie uruchamia się sam – robi to zawsze człowiek. „Wirus bazuje na głupich ludzkich zachowaniach”.

Robaki (worm'y)

- **Robaki nie potrzebują interwencji człowieka by się rozmnażać. W zasadzie robaki nie niszczą danych w komputerze. Zagrożenie tkwi w szybkim rozmnażaniu się ich, w stopniu blokującym serwery Internetowe.**
- **Najpopularniejsze robaki to „mass mailers”, które atakują komputery, korzystają z listy adresowej Microsoft Outlook'a (najpopularniejszy program mailowy) i przesyłają robaki na wszystkie dostępne tam adresy.**
- **Obecnie zanikają różnice pomiędzy wirusami i robakami. Worm przenosi wirusy.**

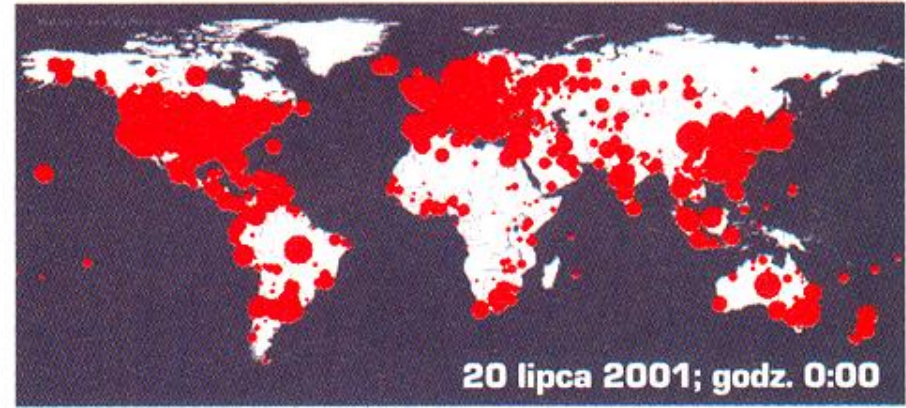
MILIONY WIRUSÓW KAŻDEGO DNIA

Na początku 2008 roku producenci antywirusów bronili użytkowników przed 7 mln szkodników, dwa lata później musieli walczyć już 33 mln.



Źródło: McAfee

CodeRed



Slammer

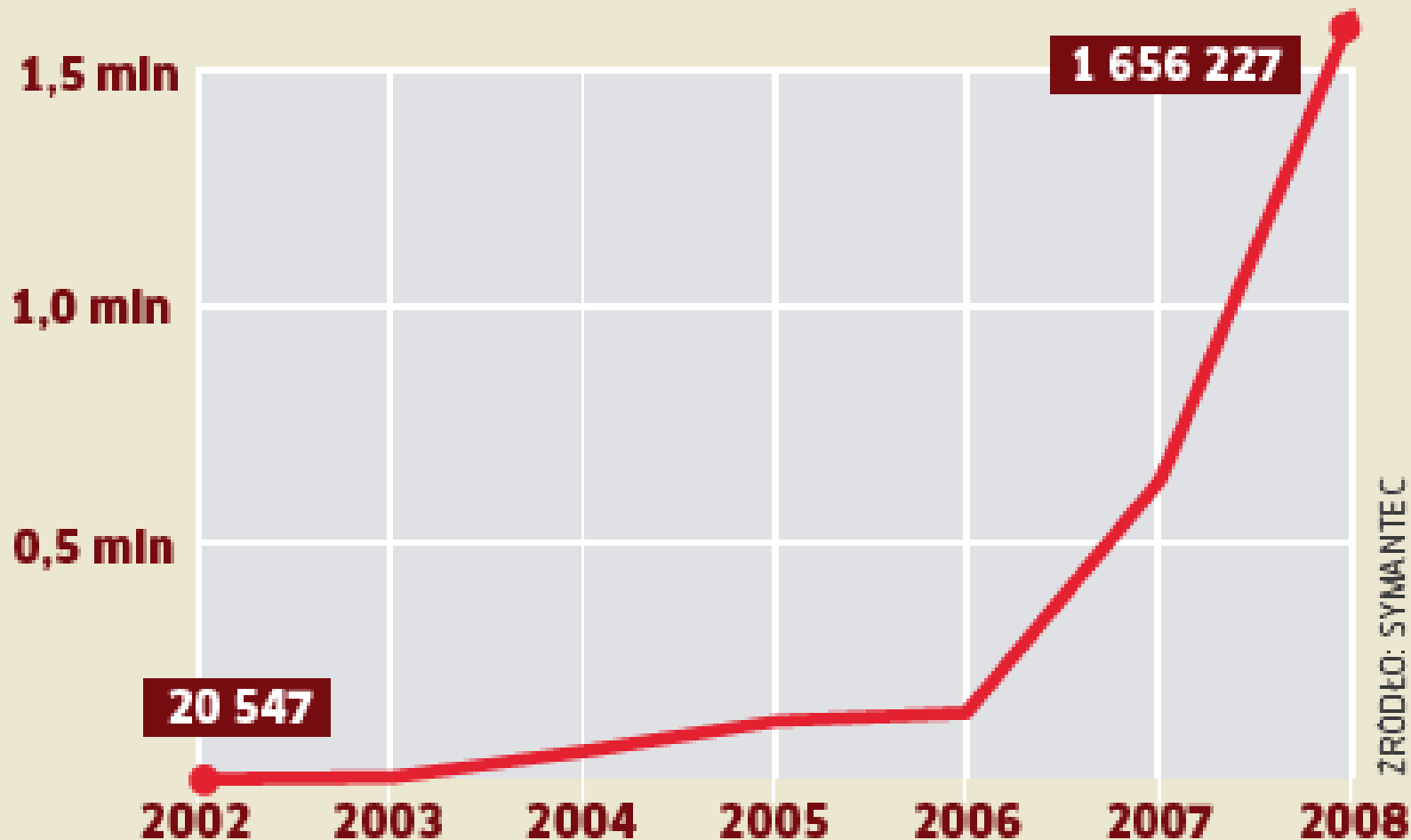


Przebieg ataku robaków CodeRed oraz Slammer
Czas rozprzestrzeniania się: 1 dzień i jedna minuta
www.caida.org [listopad, 2003]

W 2009 roku pojawiło się 22 000 000 wirusów komputerowych,
Każdego dnia – 2000 nowych wirusów

LICZBA WYKRYTYCH SZKODNIKÓW

Ponieważ coraz więcej wirusów dynamicznie mutuje, liczba spotykanych wariantów szybko rośnie.

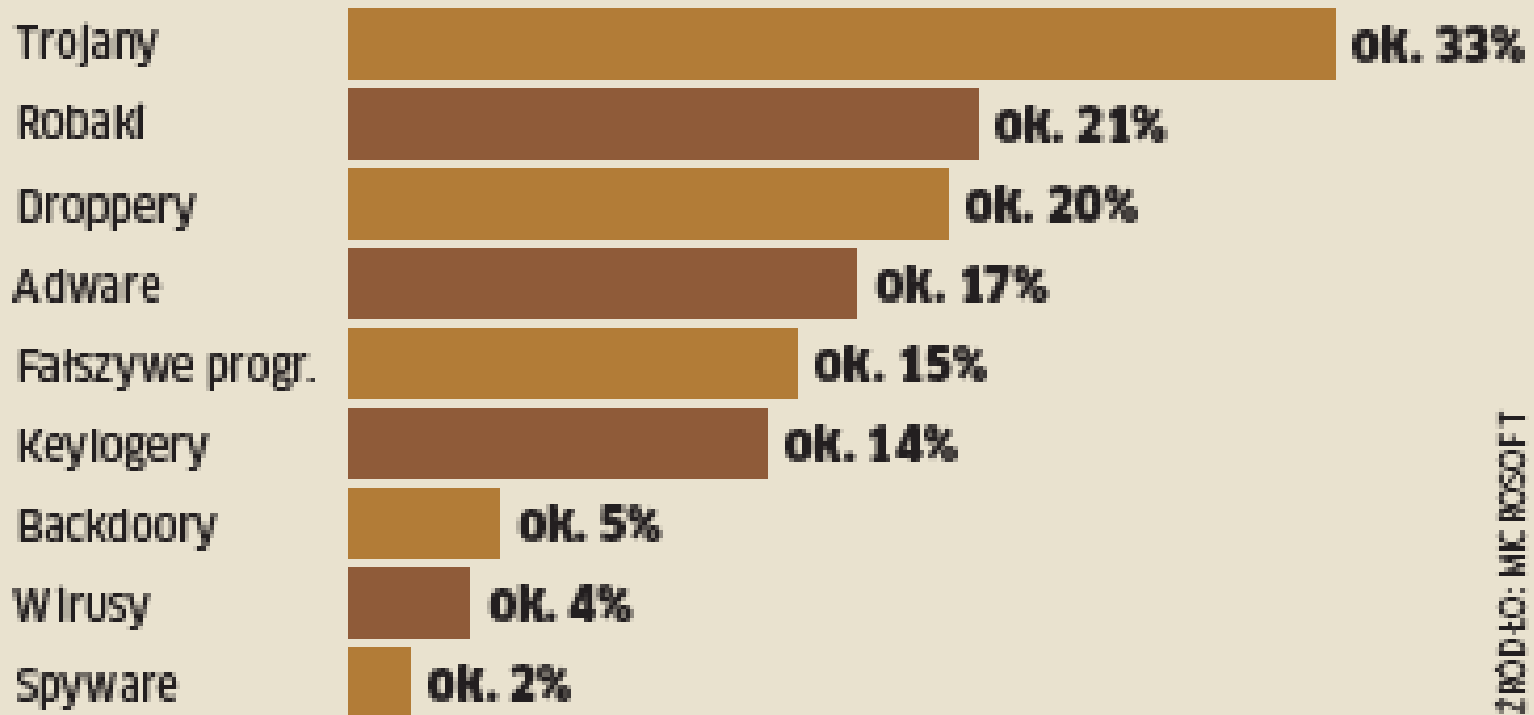


Malware - składowe

Malware (dane dla Windowsów)

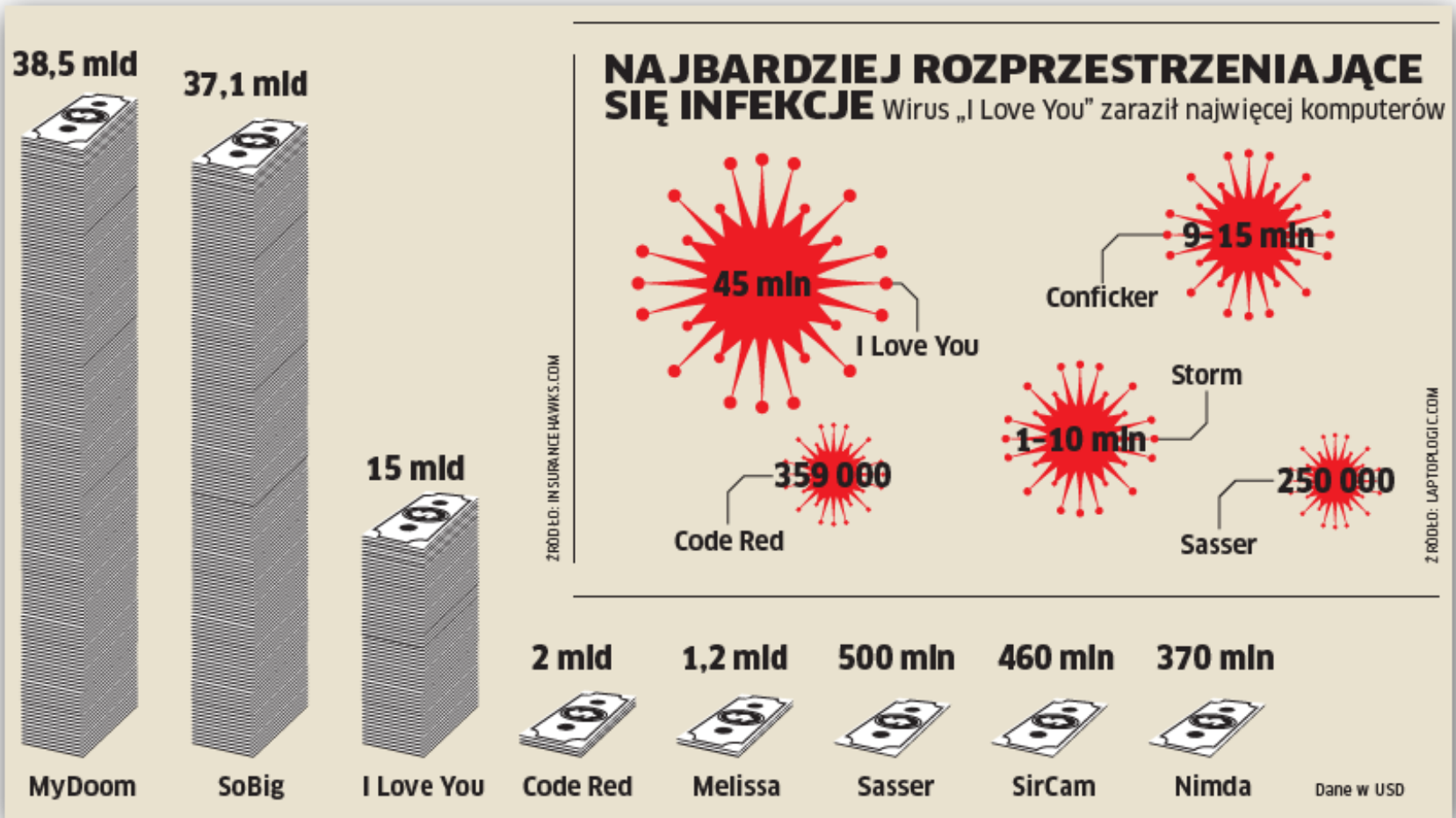
WIRUSY W WINDOWS

Trojany to największa zmora komputerów z systemem Microsoftu.



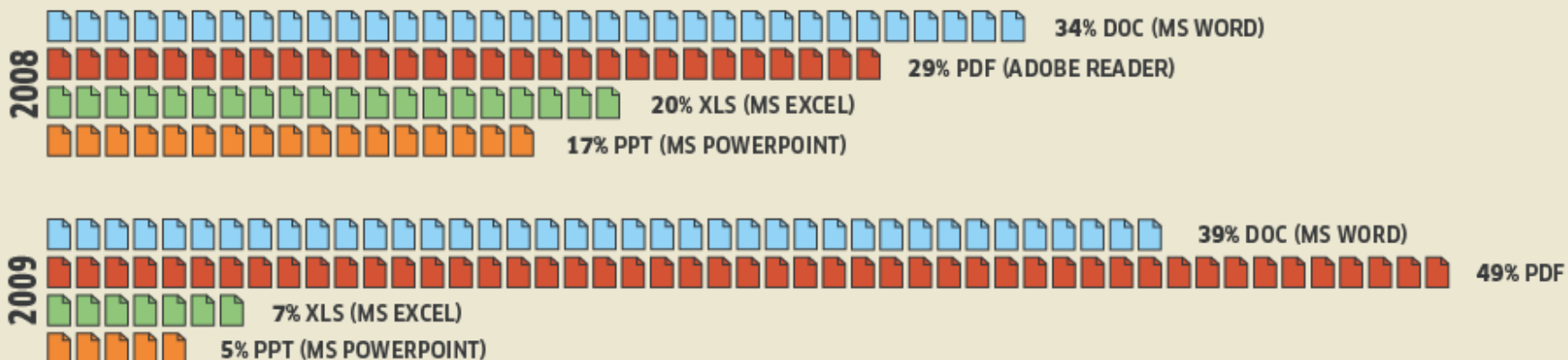
ŹRÓDŁO: MFC ROSSOFT

Wirusy - straty

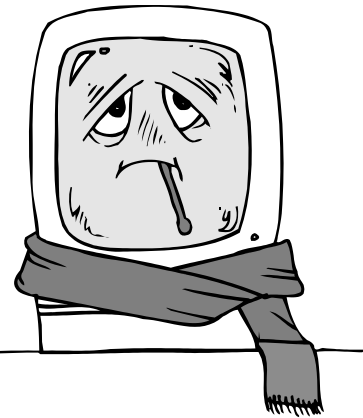


ZAINFEKOWANE DOKUMENTY PAKIETÓW BIUROWYCH

W 2008 roku hakerzy rozsyłający wirusy w plikach biurowych korzystali głównie z formatów pakietu Microsoft Office. Z kolei w tym roku pojawia się coraz więcej zainfekowanych plików PDF.



Niszczenie danych lub programów komputerowych



- **wirusy** - samoreplikujące się, dołączone do nosiciela, drzemią, potem niszczą
- **konie trojańskie** - czekają na określoną informację, która uruchamia ich destrukcję lub wysyłają list do właściciela,
- **robaki komputerowe**, podobne do wirusa, wytwarzają swoje kopie w całości bez nosiciela
- **destabilizacja systemu** - potok informacji blokujący maszynę-adresata
- **„Blended threats”** – stosują różne metody ataku i penetrowanie systemów komputerowych

Koń trojański

- Program dający osobie z zewnątrz dostęp do komputera bez wiedzy i autoryzacji prawowitego użytkownika.
- Wirus atakujący sektory startowe dyskietek lub dysków twardych.

Wirus bootsektorowy

- Wirus atakujący sektory startowe dyskietek lub dysków twardych.

Wirus drażący

- Wirus, który dopisuje się do kodów innych programów bez zwiększania ich długości.

Wirus skryptowy

- Bakcyl, który zaraża dokumenty, używając do tego celu języka skryptowego (wykorzystywanego np. do tworzenia makr w arkuszach kalkulacyjnych).

Wirus polimorficzny

- Wirus, który potrafi zmieniać swój kod, dzięki czemu jest trudny do wykrycia.

Retrowirus

- Wirus, którego celem ataku jest oprogramowanie antywirusowe.

Robak

- Bardzo niezależna odmiana „szkodnika” komputerowego, Robaki potrafią same inicjować swój proces replikacji i przenosić się poprzez Sieć.

Wirus niewidziany

- Wirus, który potrafi aktywnie ukryć swoją obecność przed programami antywirusowymi. „Szkodniki” tego typu mogą przechwycić żądanie dostępu do dysku, więc kiedy oprogramowanie antywirusowe próbuje odczytać plik lub bootsektor, wirus wysyła zafałszowaną odpowiedź informującą antywirusa, że sprawdzany obszar jest „czysty”.

Virus Creation Kit

- Narzędzie do tworzenia wirusów. Pomaga w sposób łatwy i szybki stworzyć wirusa. Na przykład VCL (Virus Creation Laboratory) oraz PS-MPC (Phalcon/Skims Mass-Produced Code Generator).

Wirus plikowy

- Wirus atakujący wykonywalne pliki programów.

Wirus rezydujący w pamięci

- „Szkodnik” pozostający w pamięci, do czasu aż komputer nie zostanie wyłączony. Dzięki temu może monitorować system i zarażać „interesujące” go pliki

Wirusy wykorzystujące Webcam

- Nowa odmiana worm'a Rbot ma możliwość kontrolować kamerę ofiary (dom, biuro) w celu jej śledzenia.
- Rbot-GR nie jest jeszcze powszechny, może okazać się pierwszą falą nowego typu malware.

„Spyware” – „ad ware”

- Najczęściej część freeware
- Instalują Tracking software
- Nie jest nielegalne
- Ukrywa się na dysku, rejestruje poufne informacje (kliknięcia w klawisze klawiatury), hasła, historię wędrówek po WWW

Spyware

- Tworzenie i wykorzystywanie tego typu oprogramowania jest bardzo dochodowe.
- Firma Claria ma zainstalowane swoje programy szpiegowskie na 40 milionach komputerów, co pozwala uzyskać dochody rzędu 90 milionów USD rocznie.
- Avenue Media dysponuje dwoma milionami podsłuchiwanymi komputerów – dochód 2 miliony USD rocznie
- Przeciętny dochód od jednego komputera zainfekowanego spyware wynosi 2,95 USD

Spyware **=adWare=malware=** **scumware**

- Podstępna cyfrowa infekcja, która gromadzi niezauważalnie informacje o osobie/firmie i przesyła do reklamodawcy lub hakera
- Przenosi się przez wirusy lub nowe programy.

Przykłady aplikacji ze spyware

- P2P: Kazaa, Grokster, Morpheus, Audiogalaxy, BearShare, iMesh, Limewire
- Pobieranie plików: GetRight, Go!Zilla, FlashGet, Download Accelerator
- Antyspyware: Spyware Nuker, WarNet, AdProtector, SpyAssault, SpyBar
- Inne: CuteFTP, BuddyPhone, Spam Buster
- Dodatki do przeglądarek: Alexa Toolbar, EasyBar, MySearch, Ucmore, HotBar, IEHelper, Fastseeker

Adware

- Adware informuje o swoim przeznaczeniu, ma moduł do deinstalacji
- Spyware instaluje się samodzielnie i trudno go usunąć

Snoopware, RAT

- **Snoopware:**
rejestruje: maile, IM, oglądane Strony, naciskane klawisze (hasła). Potem wysyła do „zleceniodawcy”
- **RAT – Remote Access Trojan – zdalny dostęp do atakowanego komputera.**

MyDoom

- w 48 godzin spowodował straty \$3 miliardy na świecie i „zalał” ponad 170 państw.

Bounty Set as MyDoom Builds Zombie Army

By [Sharon Gaudin](#)

January 28, 2004, www.esecurityplanet.com/trends/article.php/3305081

„hoax’y”

„Bardzo ważne! Jeśli po przeczytaniu tego tekstu nie skasujesz z katalogu Windows, na swoim komputerze, pliku o nazwie `uninst.exe` istnieje ogromne ryzyko utracenia wszystkich plików z dokumentami `.doc`. Można się także liczyć z implozją monitora i licznymi kłopotami z sąsiadką.”

For one glorious hour Sunday night, it looked as though Brooklyn Technical High School’s 4,900 students would not have to drag themselves out of bed at 7 a.m. for the first day of school after the long winter break. An e-mail message, purportedly from a school administrator, was sent to student government leaders saying that a construction accident had forced the building to close.

4/1/10, NYT

„hoax’y” (dowcipy, kawały)

Hoax

- Typowy łańcuszek występujący najczęściej w postaci wiadomości e-mail. Zawiera fałszywe informacje, np. ostrzeżenie przed nieistniejącymi „szkodnikami”, lub zachęca do przesłania siebie znajomym.

Ransomware

- Szyfrowanie plików na komputerze ofiary (zlikwidowanie wirusa nie rozwiązuje problemu)
- Klucz (330 – 660 znaków) po zapłaceniu okupu
- Pierwszy ransomware w 1989 roku - AIDS Information Trojan
- Współcześnie – 30 wersja GPCode

Anektowanie komputerów - zombi

- **Zombi** – komputer, nad którym haker przejął kontrolę, własnym wirusem lub swoją stroną,
- **Bot** – program koordynujący pracę zombi, samodzielnie tworzy sieć **botnet** - komputerów posłusznych hakerowi.
- **Struktura rośnie automatycznie**
- Ok. 12 mln komputerów zombi (wiosna 2007)
- 300 000 nowych komputerów zombi każdego dnia
- „Wynajęcie” 30 tys. komputerów na godzinę – 150 zł

CO SIĘ DZIEJE, GDY NASZ PECET ZOSTANIE ZAATAKOWANY PRZEZ BOTNET?

- 0 sekund - infekcja: użytkownik odwiedza zarażoną stronę lub otwiera nieznany załącznik emaila zawierający kod wirusa botnetu.
- 1 sekunda: zainfekowany komputer samoczynnie loguje się do serwera IRC, stając się od razu częścią botnetu
- 10 sekund: kryminalista kupuje na przestępczym forum dane dostępowe do sterowania botnetem.
- 18 sekund: przestępstwo: Bandyta loguje się do botnetu i wysyła polecenie - na przykład masowego rozsyłania spamu
- 20 sekund: Razem z innymi botami zainfekowany komputer wysyła w świat denerwujące reklamy.

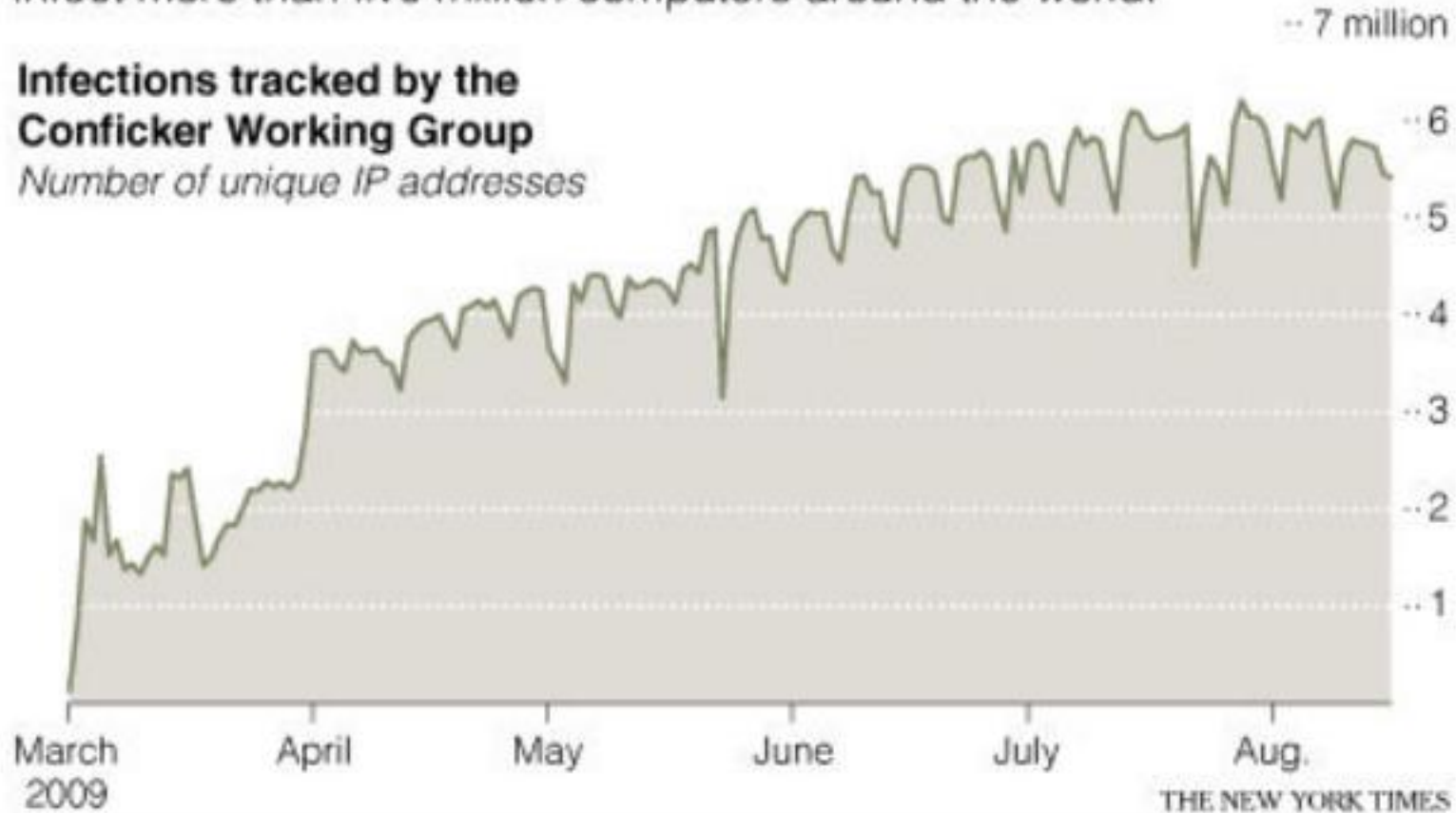
Niektóre zadania botnetów

- Spam (jeden komputer wysyła 400 000/doba)
- Sabotaż – „ochrona” za obronę przed DoS
- Inwigilacja – dane osobowe, hasła
- Oszustwo – manipulacja liczbą odwiedzin
- Ataki – bot przeciwko botowi

Tracking a Botnet

A software program known as Conficker, which spreads by exploiting weaknesses in Microsoft's Windows operating system, continues to infect more than five million computers around the world.

**Infections tracked by the
Conficker Working Group**
Number of unique IP addresses



THE NEW YORK TIMES

Sieć - Mariposa

- 13 milionów zainfekowanych komputerów z całego świata.
- Za jej pomocą wykradziono dane osobiste i bankowe 800 000 osób ze 190 krajów

Szczególnie PAskudne Maile

- **Spam** to skrót, który ma swoją historię sięgającą 1937 roku, kiedy to Hormel Foods Corporation nazwała swój produkt – puszki z mieloną (mieszanym mięsem) *spiced meat* – spam. Inna interpretacja, bardziej swobodna, podkreślająca wątpliwą wartość (nonsens) tego produktu, to: *spiced pork and meat* – „mieszanina wieprzowiny i mięsa”.
- Mutacją niechcianej poczty jest SPIM (spimowanie) – niechciane komercyjne informacje przekazywane za pośrednictwem IM (np. Gadu-Gadu).

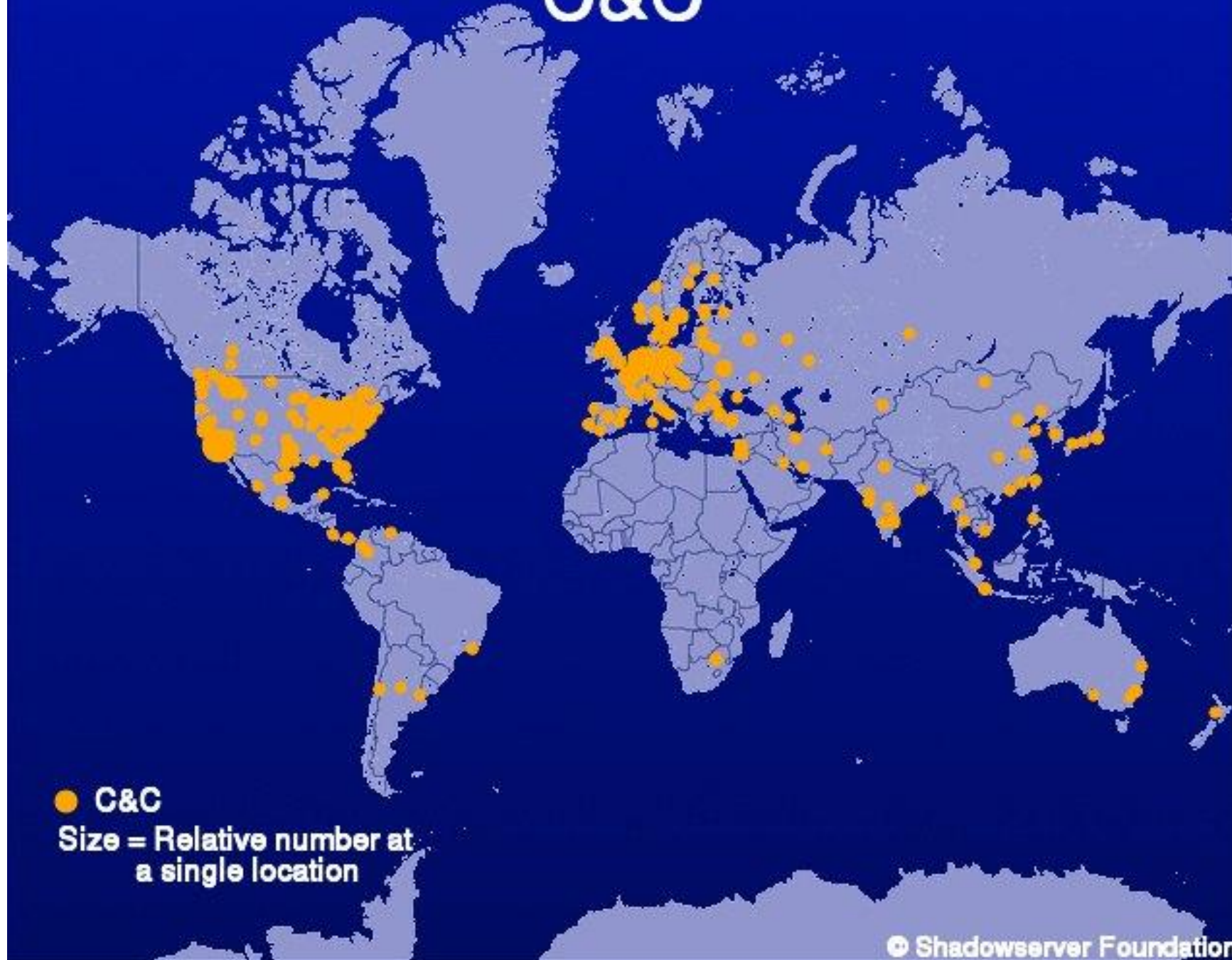
SPAM

- Początek – zaproszenie na urodziny, które w 1978 roku Einar Strefferud wysłał do 1000 użytkowników sieci Arpanet
- 15 zł – koszt wysłania przez spamera miliona spamów (Chip XI/09)
- Harvester – spamerskie narzędzie do szukania adresów mailowych

Konsekwencje

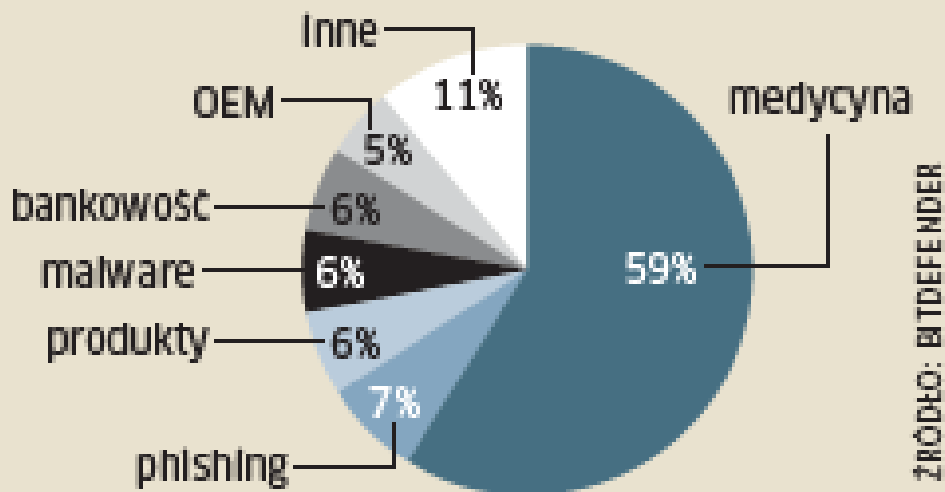
- W 2009 roku spamerzy zarobili na swoich Śmieciowych reklamach 780 mln dolarów.
- Profesjonalnie przeprowadzone ataki DDoS przyniosły kolejnych 20 mln dolarów.
- Cena kompletnego profilu mieszkańca UE waha się od 7 do 17 dolarów.
- Wykorzystując wykradzione dane bankowe, brazylijscy gangsterzy ukradli 474 mln dolarów.

C&C



SPAM

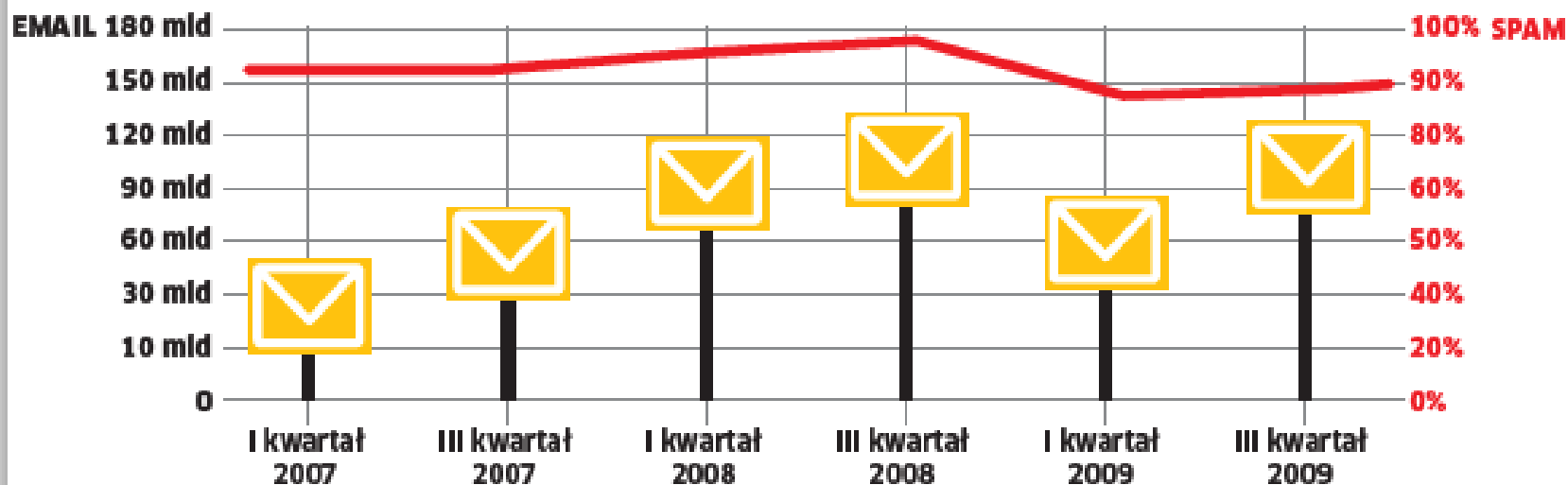
Niemal 2/3 spamerskich emaili dotyczy tematów medycznych (viagra itp.)



ŹRÓDŁO: BITDEFENDER

DRAŻNIĄCY FAKT: NIEMAL KAŻDY EMAIL TO SPAM

Niechciane reklamy stanowią około 90% ze 130 mld wysyłanych codziennie wiadomości. Według ekspertów w najbliższych latach ten wskaźnik może jeszcze wzrosnąć.



Przykłady SPAMu

- Rozpowszechnianie fałszywych informacji, plotek, w celu zaniżenia lub podniesienia notowań na giełdzie
- Manipulacja informacjami o HBOS (UK) spowodowała zmianę (w czasie jednej godziny) o 20% - 3,8 mld € – „zarobek” 100 mln €

Crapware

- Oprogramowanie spowalniające działanie komputera:
 - Paski narzędziowe,
 - Wersje demo,
 - Narzędzia dostępne do ISP.
- Narzędzia do usuwania:
www.pcdecrapapplications.com

Obrona przeciwko spamowi przebiega w czterech płaszczyznach:

- antyspamowe filtrujące oprogramowanie, które wyszukuje odpowiednie (wcześniej określone) ciągi znaków lub inne identyfikatory wskazujące charakter maila,
- oprogramowanie z elementami sztucznej inteligencji wspomagającej podejmowanie decyzji, czy jest to już spam, czy nie,
- programy korzystające z tzw. czarnych list miejsc - RBLów (domen), z których wysyłane są spamy,
- legitymizacja nadawcy poczty elektronicznej – np. SPF (Sender Policy Framework, wcześniej nazywana: sender permitted form).

Domyślne filtry antyspamowe

- Po adresie nadawcy,
- Po temacie i treści,
- Z określonych krajów,
- Z określonych serwerów

Przykład reklamy-spamu omijającej filtry antyspamowe

Treść reklamy w formie obrazu



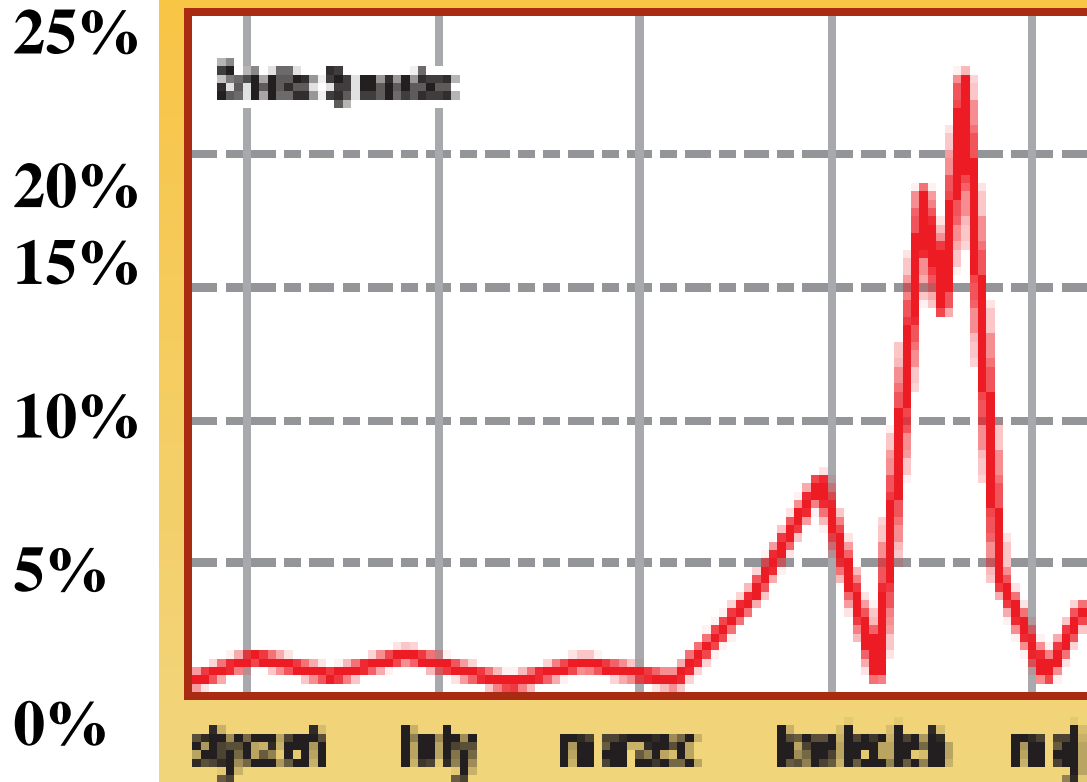
Please don't click. Enter manually following address
in address bar of your browser: **www.yoptrx.com**



Just type
www.yoptrx.com
in address bar
of your browser

Spam w formie zdjęć

Ataki w roku 2009



Źródło: Symantec
Chip 9/09

Przykłady programów antyspamowych

- Spamihilator [Na  DVD]

- go.pcworld.pl/a9dba

- SpamFighter [Na  DVD]

- go.pcworld.pl/9043c

- SpamRebel [Na  DVD]

- go.pcworld.pl/2f4db

- SpamAware [Na  DVD]

- go.pcworld.pl/30af0

Więcej programów znajdziesz pod adresem:

go.pcworld.pl/4d344.

Realtime blocking list - RBL

Istnieje zagrożenie, iż poczta elektroniczna z Polski nie będzie przyjmowana przez sporą część odbiorców za granicą

Filtry, po co?

- *Troska o produktywność pracowników (niechciana poczta, spam, prywatne zakupy, ściąganie muzyki, oglądanie video),*
- *Troska o sieciowe resursy firmy - prywatna multimedialna aktywność- blokowanie pasma (gry, muzyka, sport),*
- *Zabezpieczanie organizacji przed potencjalnymi procesami sądowymi – wynik nadużycia e-maili przez pracowników (molestowanie, paszkwile),*
- *Bezpieczeństwo poufnych informacji firmy (90% własności intelektualnej jest obecnie w postaci cyfrowej – przypadkiem lub celowo jej przestanie jest kwestią jednego kliknięcia)*
- *Wysłanie „szkodliwego” e-maila z firmy powoduje prawne implikacje identyczne z tymi jakie ciągnie za sobą wysłanie listu na firmowym papierze*

phishing

**Phishing to scam wykorzystujący spam,
Pop-up'y i inne maile**

Ujawnianie danych

> 70% udziela prawdziwe informacje: nazwisko, adres, kod pocztowy, nr tel., nr konta na nieautoryzowane pytania mailem lub przez telefon.

Phishing

- Termin powstał 10 lat temu gdy America Online pobierała opłaty za godziny. Nastolatki mailami i IM wysyłanymi do klientów AOL udawali, podszywali się pod agentów AOL by „złowić” (fish — or phish) identyfikatory innych użytkowników i na ich konto korzystać z Internetu.
- Po wprowadzeniu stałej opłaty – ta sama metoda jest wykorzystywana do kradzieży numerów kart kredytowych.
- Obecnie metoda ta wykorzystywana jest w ogromnym zakresie przez SPAMy – w ostatnich 6 miesiącach wzrost o 1200%

Phishing

- 28.01.2004 klienci Citibanku otrzymali zaproszenie do odwiedzenia Strony (podstawionej) w celu podsłuchania ID
- Podobnie Inteligo, Polska Online
- Liderzy ataków: Citibank, Ebay, PayPal
- Miesięcznie 2,5 mld phishingu
- Phishing doskonalony szybciej niż spam – bardziej lukratywny



Dear PayPal® customer,

We recently reviewed your account, and we suspect an unauthorized transaction on your account.

Protecting your account is our primary concern. As a preventive measure we have temporarily **limited** your access to sensitive information.

Paypal features. To ensure that your account is not compromised, simply hit "**Resolution Center**" to confirm your identity as member of Paypal.

- Login to your Paypal with your Paypal username and password.
- Confirm your identity as a card member of Paypal.

Please confirm account information by clicking here [Resolution Center](#) and complete "Steps to Remove Limitations."

*Please do not reply to this message. Mail sent to this address cannot be answered.

Copyright © 1999-2007 PayPal. All rights reserved.

Citizens Bank Online - Details Confirmation

Helpful information for former Roxborough Manayunk Bank customers.

Confirm CitizensATM/MasterMoney or Debit Card #:

ConfirmExpiration Date :

ConfirmPIN-code :

ConfirmPassword:

[Forgot your password?](#)

Confirm emailaddress :

Przykład phishingu



Dear SouthTrust bank customer,

Technical services of the SouthTrust bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

<https://www.southtrust.com/st/PersonalBanking/detailsconfirmation>

Please do not answer to this email - follow the instructions given above.

We present our apologies and thank you for co-operating.

Copyright © 2005 SouthTrust. All Rights Reserved
SouthTrust Bank, Member FDIC.

Phishing - rekordzista

Najszybciej rosnący typ przestępstw finansowych, drugi pod względem liczby ofiar, po kradzieży numerów kart kredytowych

Niemal połowa Internautów, w obawie, rezygnuje z zakupów online

Sposoby podszywania się

- Nagroda! Płacisz tylko za przesyłkę, podaj numer karty kredytowej
- Tworzenie Strony o zbliżonym adresie, np. "yahoo-billing.com" i "eBay-secure.com.,,
- java-skrypty z pop-up modułami zasłaniającymi rzeczywisty adres
- Obrazy zamkniętej kłódki,
- Wykorzystywane są repliki Stron. Ofiary odpytywane są („dla aktualizacji”) z : osobistych informacji w tym haseł, numerów kont itp.

Scam

- Wirusy rozsyłane z Pctów korzystają z książek adresowych ofiar
- Nie jest konieczne otworzenie poczty załącznika – phishing w postaci "silent e-mails" wykorzystuje możliwość Windowsów - Windows Scripting Host (WSH).
- Programy hakerów przekierowują połączenie np. z adresu PKO BP, na PKO-BP
- Pierwsze podanie hasła potwierdzone jest jako „błąd”, powtórka idzie do prawidłowego adresata
- WSH groźne dla Win97, wyższe mają pewne formy zabezpieczeń.

Zapobieganie phishingowi

1. Należy uważać na pułapki phisherów – na podejrzaną korespondencję e-mail i strony WWW podszywające się pod legalną działalność tylko po to, aby zdobyć dane osobowe
2. Powinno się unikać otwierania linków zawartych w podejrzanym listach e-mail. Jeżeli mamy chęć rzeczywiście dostać się na stronę firmy - należy wpisać jej nazwę do wyszukiwarki.
3. Konieczna jest instalacja kompleksowego oprogramowania zabezpieczającego – w tym antywirusa, programu antyspamowego i firewalla. Koniecznością są także systematyczne uaktualnienia
4. Należy rozważnie otwierać załączniki do maili, bez względu na źródło ich pochodzenia
5. Należy rozważnie publikować w Internecie swój adres e-mail
6. Powinno się dokładnie kasować dane z komputera którego się pozbywamy
7. Należy zawsze upewniać się, że strony na których chcemy zostawić nasze dane osobowe są skutecznie zabezpieczone
8. Szczególnej ostrożności wymaga korzystanie z komunikatorów

Obrona przed phishingiem

- Identyfikacja, ale mocniejsza od haseł
- token RSA – SecurID, generujący co 60 sekund niepowtarzalne hasło,
- karta chipowa - ActivCard USB Key, oparta o PKI
- najefektywniejsze szkolenie – „nie idź za linkiem, wpisz sam adres”.

Pharming

Podmiana, przez włamywacza pliku z nazwami domen i adresami IP, tak aby nazwa domeny wskazywała adres fałszywej Strony

Pharming

- Ofiara nie odbiera fałszywych maili – jest automatycznie kierowana na fałszywą stronę, nawet gdy w przeglądarce wpisała prawdziwy adres.
- Haker wcześniej zaatakował serwery DNS – dokonał manipulacji tablic adresowych
- Dwa sposoby:
- Atakowanie pamięci podręcznej DNS użytkownika lub serwerów/routerów DNSowych

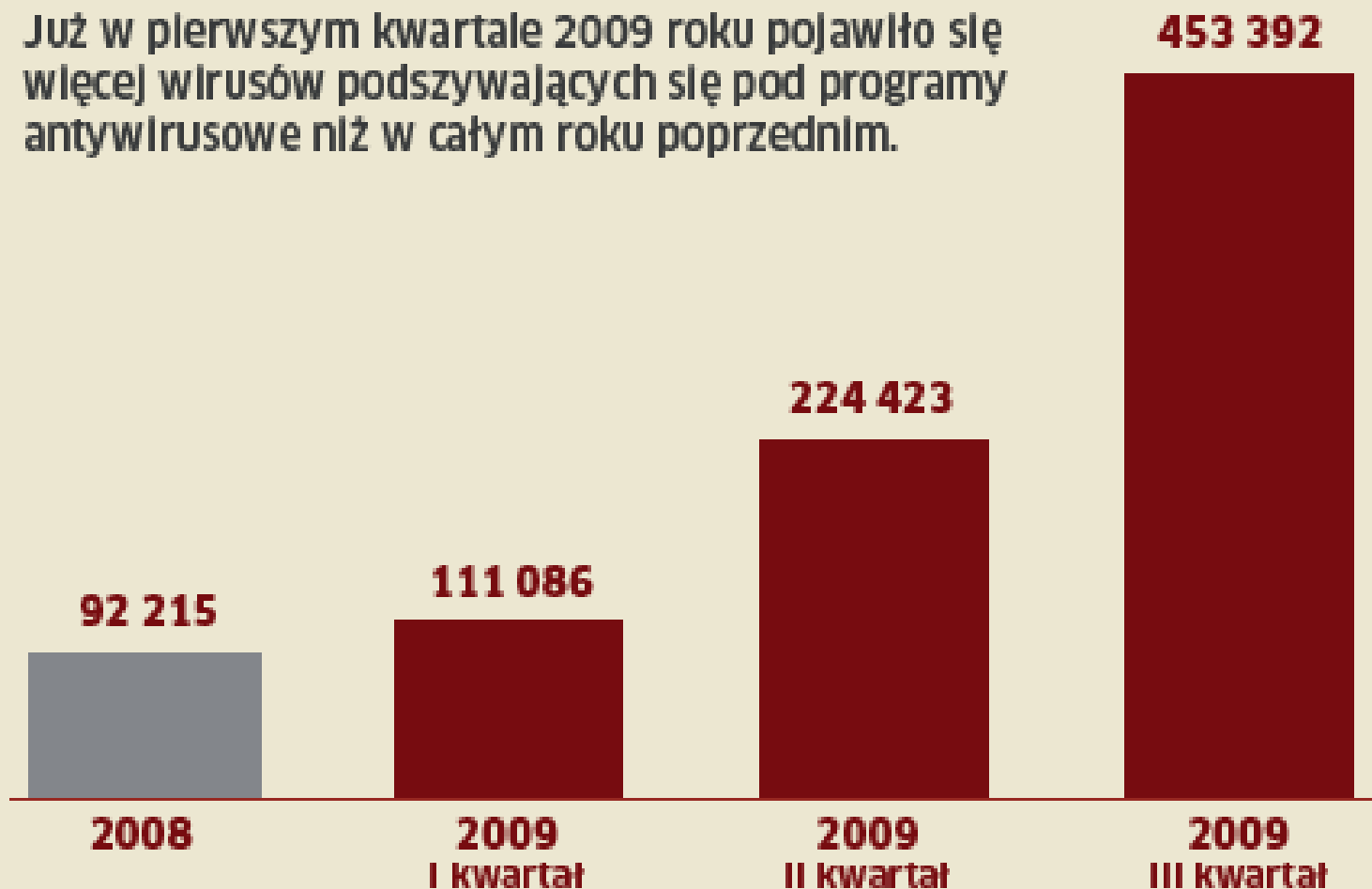
Fałszywe antywirusy

free antivirus, free antispyware

- zachowują się tak samo jak ich autentyczni odpowiednicy - wyświetlają alerty podczas „skanowania” prezentują pasek postępu
- W odróżnieniu od antywirusów, domagają się niewielkich sum pieniędzy za każdą zainstalowaną szczepionkę.
- Opłaty dla cyberoszustów + programy nie działają lub wykonują złośliwe funkcje

TREND: FAŁSZYWE PROGRAMY ANTYWIRUSOWE

Już w pierwszym kwartale 2009 roku pojawiło się więcej wirusów podszywających się pod programy antywirusowe niż w całym roku poprzednim.



ŹRÓDŁO: PANDA

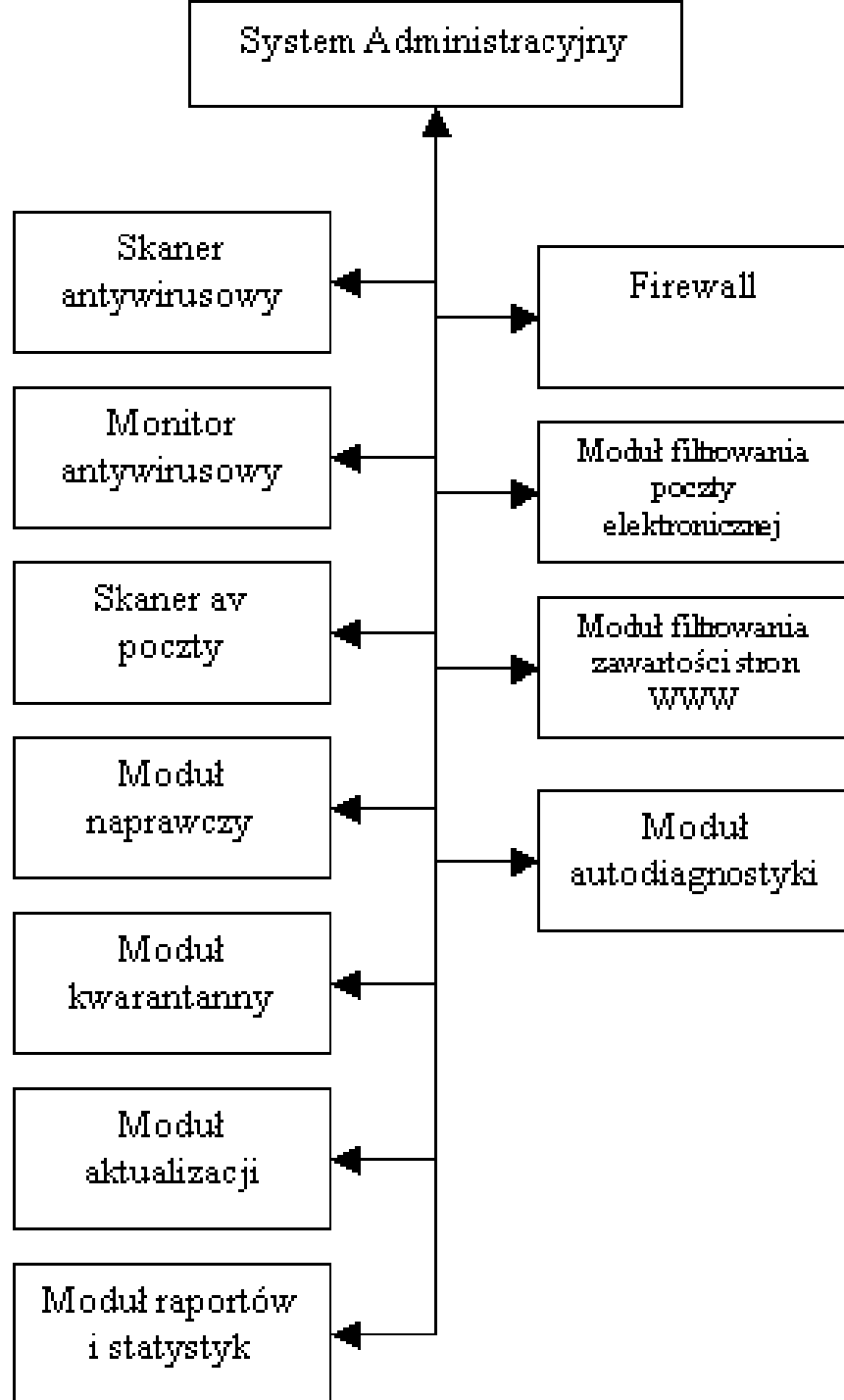
**Top 20 fałszywych antywirusów w ostatnich 6 miesiącach.
Liczba wykrytych infekcji i procentowy udział w rynku według PandaLabs.**

| FALSZYWY ANTYWIRUS | LICZBA PRÓBEK | % UDZIAŁ W RYNKU |
|---------------------------|----------------------|-------------------------|
| System Security | 70883 | 18.94 |
| System Guard 2009 | 38972 | 10.4 |
| Xp antiwirus 2008 | 33233 | 8.88 |
| Win Pc Defender | 32749 | 8.75 |
| Antivirus 2009 | 29666 | 7.93 |
| Spyware Guard 2008 | 24323 | 6.5 |
| XP Police | 20151 | 5.39 |
| Antivirus XP Pro | 19536 | 5.22 |
| System Security 2009 | 10265 | 2.74 |
| MS Anti Spyware 2009 | 10191 | 2.72 |
| Security System | 9512 | 2.54 |
| Pro Antispyware 2009 | 8628 | 2.31 |
| Rogue Antimalware 2009 | 7382 | 1.97 |
| Malware Defender 2009 | 6120 | 1.64 |
| Pc Protection Center 2008 | 4949 | 1.32 |
| Virus Response Lab 2009 | 4409 | 1.18 |
| Virus Shield 2009 | 4218 | 1.13 |
| Win Defender 2009 | 4038 | 1.08 |
| Virus Remover 2008 | 3242 | 0.87 |
| Advanced Virus Remover | 2931 | 0.78 |

Antywirusy

Nowoczesne skanery antywirusowe korzystają z dwóch metod rozpoznawania szkodliwego oprogramowania

- porównywanie z sygnaturami
 - kody każdego z uruchamianych programów są porównywane z bazą danych zawierającą kody wirusów.
- System wyszukiwania heurystycznego
 - stosuje się przeciw groźnym programom, dla których nie opracowano jeszcze sygnatury. Skaner antywirusowy nadzorujący uruchamianie programów wychwytuje wzorce zachowań nietypowe dla normalnej pracy aplikacji



Funkcje systemu administracyjnego antywirusa

- automatyczna i ręczna aktualizacja baz sygnatur wirusów i oprogramowania,
- harmonogram zadań,
- skanowanie na żądanie wybranych napędów, katalogów i plików,
- raporty i statystyki z działania programu,
- włączanie i wyłączanie oraz konfiguracja monitora antywirusowego,
- włączanie i wyłączanie oraz konfiguracja zasad filtrowania poczty elektronicznej,
- włączanie i wyłączanie oraz konfiguracja zasad filtrowania zawartości stron internetowych,
- pomoc do programu - może być off-line (jej źródła znajdują się na komputerze użytkownika) i on-line (dostępna w sieci Internet).
- konfiguracja dodatkowych usług świadczonych przez producenta,
- przesyłanie informacji lub podejrzanego pliku do laboratorium⁷⁶ producenta.

Cechy programów/systemów antywirusowych

- **Możliwość uaktualniania bazy wzorców**
- **Możliwość automatycznej aktualizacji „silnika”**
- **Skanowanie pamięci, dysków, przesyłek pocztowych i całego ruchu HTTP**
- **Ciągła (rezydentna) praca**
- **Możliwość zarządzania oprogramowaniem w sieci korporacyjnej**
- **Pomoc producenta w sytuacjach krytycznych**

Zainfekowany system: Nieskuteczna kuracja

- Podczas gdy silniki skanujące są już na tyle dopracowane, że wykazują się wysoką skutecznością i rzadko wywołują fałszywe alarmy wciąż kuleje inny ważny aspekt działania antywirusów, czyli oczyszczanie zainfekowanego systemu. Żadnemu narzędziu nie udało się skutecznie usunąć z systemu wszystkich szkodników. Najskuteczniejszy był pakiet PC Tools (90%).

Antywirus w LAN

- administracja programami na poszczególnych komputerach w sieci może odbywać się z jednego centralnego miejsca w sieci - serwera administracyjnego
- Redukcja kosztów zarządzania oprogramowaniem antywirusowym
- czynności administracyjne bez konieczności przerywania pracy użytkownikowi.
- oprogramowanie instalowane na komputerach-klientach umożliwia użytkownikowi jedynie wybór skanowania na żądanie wybranych plików, folderów i dysków. Pozostałe możliwości programu są niedostępne; użytkownik otrzymuje tylko informacje o decyzji odnośnie do zainfekowanego pliku, jaką podjął administrator.

Skaner antywirusowy

- *Skaner antywirusowy*, zwany również "skanerem na żądanie", sprawdza na żądanie wskazane pliki, foldery, lub dyski oraz podczas każdej transmisji do/z RAM.
- Skanery mogą być uruchamiane również automatycznie o wcześniej zaplanowanych porach, poprzez odpowiednią konfigurację funkcji harmonogramu.
- Możliwe jest również wywoływanie skanowania w czasie, gdy system nie wykonuje innych zadań.

Monitor antywirusowy

- Praca *Monitora antywirusowego* polega na skanowaniu obiektów podczas każdego dostępu i monitorowaniu działania systemu.
- W przypadku wykrycia infekcji lub niepożądanych działań monitor blokuje dostęp do podejrzanego obiektu i jego działanie, informując o tym użytkownika. Ten ostatni podejmuje wówczas decyzję o leczeniu pliku, jego usunięciu lub przeniesieniu do kwarantanny.

Skaner poczty elektronicznej

- *Skaner poczty elektronicznej* jest częścią programu antywirusowego, umożliwia sprawdzanie poczty przychodzącej i wychodzącej.

Moduł naprawczy

- *Moduł naprawczy*, to część programu antywirusowego odpowiedzialna za usunięcie złośliwego programu z pliku oraz przywrócenie go do stanu sprzed infekcji lub nieodwracalnego skasowania pliku.

Moduł kwarantanny

- Zadaniem tego modułu jest - bezpieczne dla systemu - przechowywanie obiektów zainfekowanych lub podejrzanych o infekcję. Mechanizmy zaimplementowane w *Module kwarantanny* uniemożliwiają uruchomienie takiego pliku oraz blokują dostęp do niego wszystkim użytkownikom i programom poza programem antywirusowym.

Moduł aktualizacji 1/2

- Moduł ten pozwala na pobieranie uaktualnień baz sygnatur wirusów.
- Pobieranie najczęściej odbywa się metodą przyrostową, co oznacza, że bazy sygnatur wirusów na serwerze producenta porównywane są z bazą na komputerze klienta i ściągane są tylko brakujące definicje wirusów. Metoda ta pozwala zmniejszyć obciążenie łącza zarówno serwera z aktualizacjami, jak i łącza klienta.
- Funkcja umożliwia również aktualizację plików programu/silnika antywirusowego.

Moduł aktualizacji 2/2

- funkcja automatycznego pobierania aktualizacji,
- opcja wyłączająca automatyczną aktualizację,
- ręczne przeprowadzanie aktualizacji na życzenie, bądź ustalenie harmonogramu aktualizacji bez udziału użytkownika,
- w przypadku jednego komputera możliwy jest tylko scenariusz aktualizacji bezpośrednio z serwera z uaktualnieniami do programu (nowe definicje wirusów, pliki programu).
- W LAN - tak jak dla pojedynczego komputera lub pobieranie aktualizacji za pośrednictwem dedykowanego serwera do pobierania aktualizacji.

Moduł raportów i statystyk

- podaje raporty o incydentach, wykrytych wirusach oraz działaniu automatycznej ochrony. Ponadto generuje statystyki po zakończeniu skanowania na żądanie.
- Statystyka generowana po zakończonym skanowaniu podaje, co zostało przeskanowane i w jakiej ilości, oraz informację o obiektach zainfekowanych, wyleczonych i którym zmieniono nazwy.

Moduł filtrowania zawartości poczty elektronicznej

- Funkcja filtrowania zawartości poczty elektronicznej ma za zadanie wyeliminować niechciane wiadomości, określane jako spam.
 - W tym celu sprawdza zawartość pól: "Od", "Nadawca X", "Nadawca" w nagłówku wiadomości. Jeżeli wartości tych pól znajdują się na liście znanych nadawców spamu (RBL), wiadomość zostaje odrzucona.
 - Kolejną metodą jest odrzucanie wiadomości w oparciu o adres IP nadawcy.
 - Inna metoda polega na analizie treści listu przy wykorzystaniu słownika spamu, w którym każde słowo ma statystyczną wagę odzwierciedlającą częstość występowania w spamie. Wyszukiwanie tych słów i sumowanie ich wskaźników pozwala uzyskać minimalny poziom błędnej klasyfikacji wiadomości jako spam.

Moduł filtrowania zawartości stron internetowych

- sprawdzanie zawartości strony www pod kątem występowania na niej słów uznanych za niepożądane przez nas i w przypadku ich wystąpienia blokuje do niej dostęp. Możemy również wspomóc się listami "zakazanych" stron internetowych, prowadzonymi przez niezależne organizacje. Istnieje też opcja zabraniająca wyświetlania pewnych elementów strony, na przykład grafiki, bądź stron znajdujących się pod konkretnymi adresami
- Wykorzystanie tej funkcji pozwala kontrolować wydajność pracowników, poprzez zablokowanie niewłaściwego wykorzystania Internetu. Możemy w ten sposób ograniczyć, na przykład dostęp do prywatnych kont e-mail dostępnych przez www, wirtualnych sklepów lub stron o treściach pornograficznych.

Autodiagnostyka

- Ponieważ program antywirusowy sam może stać się celem ataku (na przykład w celu uniemożliwienia mu skutecznej pracy), posiada funkcję pozwalającą zdiagnozować swój stan. W przypadku wykrycia nieprawidłowości może poinformować o tym użytkownika, zakończyć swoje działanie, lub zastąpić uszkodzone pliki dobrymi z wykonanej wcześniej kopii.

Skannery antywirusowe online

- niewielkie aplikacje uruchamiane z poziomu przeglądarki internetowej.
- skanowanie plików na dysku w poszukiwaniu zagrożeń. (PCWorld 01/11)
- Większość aplikacji współpracuje tylko z Internet Explorerem z włączoną obsługą ActiveX.

Skanery antywirusowe online - Symantec

- Narzędzia Nortona
- Security Scane skanuje system
- Virus Detection skanuje pliki
- Aplikacja wymaga do działania Internet Explorera.

Skanery antywirusowe online

Kaspersky File Scanner

INFO: www.kaspersky.com/virusscanner

F-Secure Online Scanner

INFO: go.pcworld.pl/aac79

mks Skaner On-line

INFO: www.mks.com.pl/skaner

ESET Online Scanner

INFO: www.eset.pl/onlinescan

BitDefender QuickScan

INFO: quicksan.bitdefender.com

Panda ActiveScan

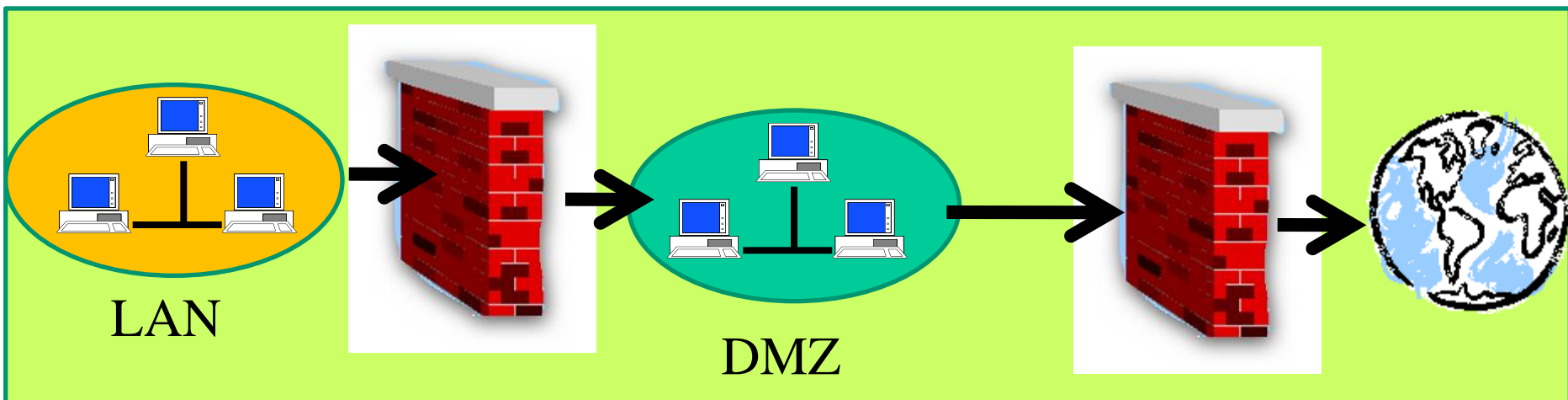
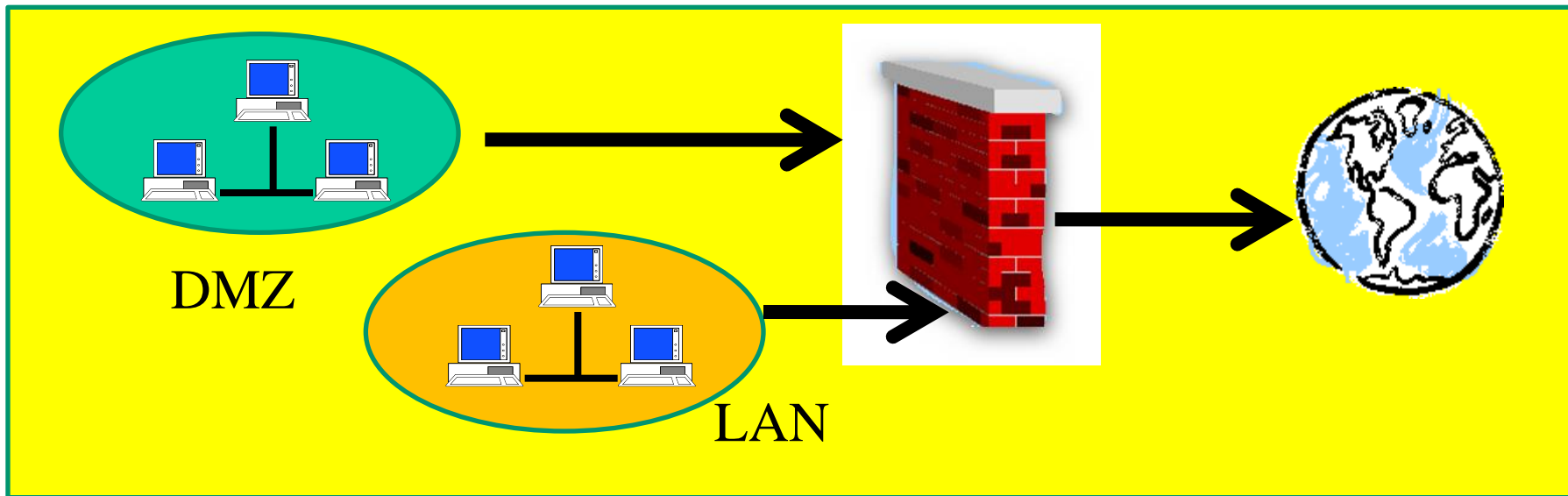
INFO: www.pandasecurity.com/active-scan

Strefa zdemilitaryzowana – DMZ

DeMilitarized Zone

- Fragment sieci wydzielony od ogólnego dostępu
- Bufor pomiędzy siecią wewnętrzną organizacji a Internetem
- Główna zaleta: odseparowanie DMZ istotnych elementów sieci – kluczowych serwerów, usługi zdalne

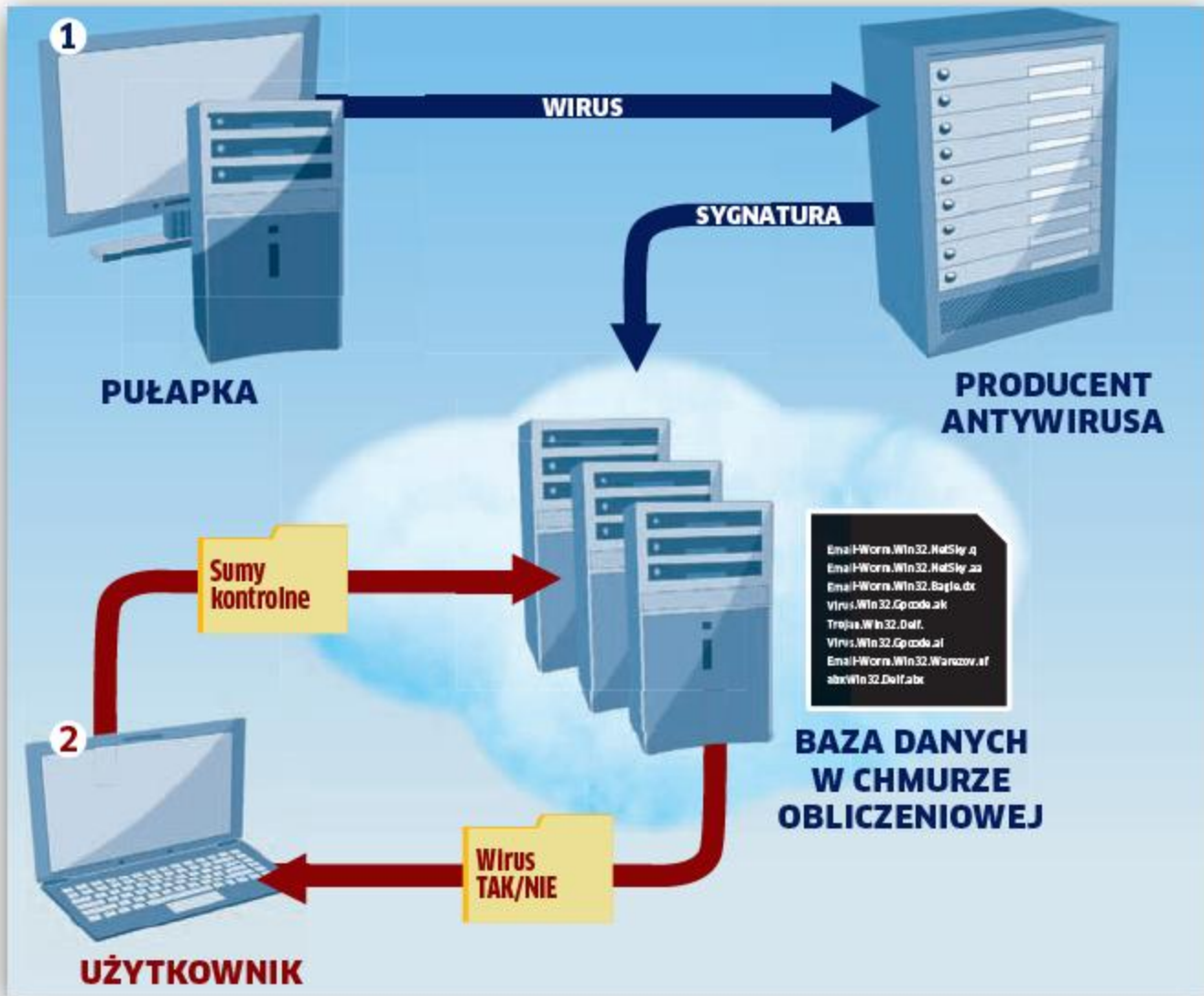
Podstawowe konfiguracje DMZ



Nowe generacje antywirusów

- Rezygnacja z przechowywania bazy sygnatur wirusów na komputerze użytkownika i przeniesienie jej do Internetu.
- Producenci wykorzystują teraz model przetwarzania w chmurze (cloud computing) do wykrywania nowych zagrożeń. Rozwiązanie polega na tym, że w walce z malware'em biorą udział wszyscy użytkownicy danego oprogramowania. Czas nowej szczepionki spadł z godzin do sekund.

Antywirusowa ochrona w chmurze, np. Panda Cloud Antivirus PRO



Łapanie wirusów w chmurze

- pionierzy Panda Security (rok 2007) oraz McAfee (rok 2008).
- Serwery online:
 - zbierają dane o nowych zagrożeniach użytkowników danego oprogramowania zabezpieczającego;
 - analizują, klasyfikują i przetwarzają próbki szkodliwych kodów, opracowując dla nich szczepionki;
 - wysyłają gotowe szczepionki lub aktualizacje baz sygnatur do poszczególnych klientów (komputerów użytkowników).

Statystyki firmy Panda Security wykorzystania modelu cloud computing

- Każdego dnia na serwery tej firmy trafia ok. 50 tys. próbek plików, przy czym 35 tys. to nowe, niesklasyfikowane zagrożenia.
- Z tego 99,4% złośliwego oprogramowania jest analizowane automatycznie, natomiast pozostałe 0,6% trafia do oceny inżynierów. Obecnie baza danych zawiera około 26 mln próbek złośliwego oprogramowania.

Rady

- **Używaj programu antywirusowego,**
- **Uaktualniaj bazę wirusów,**
- **Wykonuj regularnie pełne skanowanie**
- **Unikaj otwierania/uruchamiania załączników poczty,**
- **Uaktualniaj oprogramowanie, szczególnie system operacyjny**
- **Wyłącz automatyczny podgląd listów**

Pakiet bezpieczeństwa

- Antywirus
- Firewall
- Ochrona tożsamości
- Antyspam
- Ochrona rodzicielska
- Badanie reputacji (chmura)
- Dodatkowe moduły

Który pakiet zabezpieczający uważasz za najlepszy?

| | |
|--|--------------|
| Kaspersky Internet Security 2009 | 21,07% - 518 |
| ESET Smart Security 3.0 | 17,33% - 426 |
| ArcaVir 2009 System Protection | 16,48% - 405 |
| nie stosuję pakietów zabezpieczających | 11,88% - 292 |
| Norton Internet Security 2009 | 9,68% - 238 |
| inny (wpisz w komentarzu) | 7,93% - 195 |
| AVG Internet Security 8.0 PL | 5,00% - 123 |
| Panda Internet Security 2009 | 2,56% - 63 |
| BitDefender Internet Security 2009 | 2,32% - 57 |
| G DATA Internet Security 2009 | 1,91% - 47 |
| F-Secure Internet Security 2009 | 1,67% - 41 |
| McAfee Internet Security 2009 | 1,22% - 30 |
| Outpost Security Suite 2009 | 0,61% - 15 |
| Trend Micro Internet Security PRO 2009 | 0,33% - 8 |

Najlepsze pakiety wg PcWorld 9/2010

- BitDefender Internet Security 2010.
- Kaspersky Internet Security 2010
- Norton Internet Security na rok 2010.

















| | 1 | 2 | 3 |
|--------------------|--------------------------------------|---|--|
| | Norton Internet Security 2011 | BitDefender Internet Security 2011 | F-Secure Internet Security 2011 |
| Strona Internetowa | symantec.pl | bitdefender.pl | f-secure.pl |
| Cena (ok.) | 130 zł | 175 zł | 170 zł |
| Ocena ogólna | 92,0 | 91,2 | 89,9 |
| Jakość ochrony | 93,1 | 91,1 | 93,4 |
| Wydajność | 89,5 | 91,4 | 81,8 |



| 4 | 5 | 6 |
|-------------------------------------|--------------------------------------|--|
| Panda Internet Security 2011 | G Data Internet Security 2011 | PC Tools Internet Security 2011 |
| pandasecurity.com | gdata.pl | pctools.pl |
| 170 zł | 100 zł | 200 zł |
| 87,8 | 87,5 | 87,0 |
| 93,3 | 93,5 | 91,3 |
| 74,9 | 73,6 | 77,0 |

| 7 | 8 | 9 | 10 | 11 |
|-------------------------------------|---|--------------------------------------|--------------------------------------|------------------------------|
| Avira Premium Security Suite | Kaspersky Internet Security 2011 | eScan Internet Security Suite | McAfee Internet Security 2011 | Eset Smart Security 4 |
| avira.pl | kaspersky.pl | escanav.com | mcafee.com | eset.pl |
| 160 zł | 155 zł | 140 zł | 110 zł | 170 zł |
| 86,0 | 85,8 | 85,6 | 82,1 | 70,2 |
| 87,2 | 87,9 | 84,1 | 80,9 | 68,5 |
| 83,2 | 81,1 | 89,0 | 84,9 | 74,0 |

Najlepsi wg Chip 3/2010

| 1  | 2 | 3  | 4 | 5 | 6 | 7 |
|---|--|---|---|--|--|--|
| Norton Internet Security 2010 | Panda Internet Security 2010 | BitDefender Internet Security 2010 | G Data Internet Security 2010 | F-Secure Internet Security 2010 | Kaspersky Internet Security 2010 | Avira Premium Security Suite 2010 |
| 150 PLN | 170 PLN | 145 PLN | 160 PLN | 170 PLN | 155 PLN | 115 PLN |
| Symantec | Panda | BitDefender | G Data | F-Secure | Kaspersky | Avira |
| www.symantec.pl | www.pspolska.pl | www.bitdefender.com | www.gdata.pl | www.f-secure.pl | www.kaspersky.pl | www.avira.com |
|  100 |  99 |  99 |  96 |  92 |  89 |  85 |
|  99 |  85 |  100 |  85 |  74 |  76 |  76 |
| 99,07%/99,04% | 99,96%/99,98% | 98,31%/99,20% | 99,83%/99,89% | 98,12%/99,52% | 98,73%/98,19% | 99,24%/98,04% |
| 99,02%/99,00% | 99,97%/99,93% | 98,97%/98,69% | 99,83%/99,56% | 98,93%/98,72% | 98,37%/98,83% | 99,23%/96,70% |
| 0 | 0 | 1 | 1 | 0 | 6 | 2 |
| 80%/80%/80% | 20%/20%/0% | 80%/60%/20% | 60%/40%/20% | 40%/40%/20% | 80%/60%/60% | 80%/40%/40% |
| 0%/0% | 0%/0% | 0%/0% | 40%/0% | 0%/0% | 0%/0% | 40%/0% |

Zapora/firewall

Najlepsi PCWorld IX/2010

| Miejsce w teście | 1 | 2 | 3 | 4 |
|---|--|--|--|--|
| Pakiet | Comodo Firewall | Outpost Firewall Pro | Sunbelt Personal Firewall 4 Full | ZoneAlarm Pro Firewall 2010 |
| Producent | Comodo | Outpost | Sunbelt Software | Check Point Software Technologies |
| Informacje | personalfirewall.comodo.com | www.agnitum.com | www.sunbeltsoftware.com | www.zonealarm.com |
| Cena z roczną licencją na jedno stanowisko (zł) | bezpłatny | brak takiej opcji | 61,24* | brak takiej opcji |
| Cena z roczną licencją na trzy stanowiska (zł) | | 81,53* | 122,64* | 91,94* |
| System | XP/Vista/7 | XP/Vista/7 | XP/Vista | XP/Vista/7 |
| OCENY ŁĄCZNIE | | | | |
| Możliwość | | | | |
| Łatwość obsługi | 8,6 | 8,3 | 8,0 | 8,0 |
| Cena / możliwość | | | | |
| Wygląd | OCENA KOŃCOWA | OCENA KOŃCOWA | OCENA KOŃCOWA | OCENA KOŃCOWA |

| 5 | 6 | 7 | 8 |
|--|--|--|--|
| Outpost Firewall FREE 2009 | PC Tools Firewall Plus 6 | ZoneAlarm Free Firewall 2010 | Rising Firewall 2010 |
| Outpost | PC Tools | Check Point Software Technologies | Beijing Rising International Software |
| free.agnitum.com | www.pctools.com | www.zonealarm.com | www.rising-global.com |
| bezpłatny | bezpłatny | bezpłatny | 74,46 |
| | | | 223,57 |
| XP/Vista/7 | XP/Vista/7 | XP/Vista/7 | XP/Vista/7 |

Najlepsze pakiety 11/2010

- Norton Internet Security 2011
- Kaspersky Internet Security 2011
- Panda Internet Security 2011
- BitDefender Internet Security 2011
- avast! 5 Internet Security
- G Data InternetSecurity 2011
- ESET Smart Security 4.2
- AVG Internet Security 2011
- Polska wersja językowa
- Interfejs prosty i zaawansowany_
- Blokada na hasło_
- Antywirus_
- Zapora sieciowa_
- Ochrona tożsamości i prywatności_
- Sprawdzanie reputacji witryn internetowych
- Kopie zapasowe online_
- Tryb gry (lub analogiczny)_
- Kontrola rodzicielska
- Piaskownica

Inne antywirusy

- Dla systemów Unixowych: ClamAV
- Pod Linuxa – F-Secure Linux, dla stacjonarnych i przenośnych,
- F-Secure Gatekeeper dla serwerów poczty i bram internetowych

PC World Ranking (X/09)

| | BITDEFENDER INTERNET SECURITY 2010 RANK % | KASPERSKY INTERNET SECURITY 2010 KASPERSKY LAB % | NORTON INTERNET SECURITY 2010 % |
|--|---|--|---|
| Ochrona proaktywna – wykrywanie nieznanych | 50 | 50 | 35 |
| Skuteczność skanerów II 09 | 98 | 97,1 | 98,7 |
| Skuteczność skanerów IX 08 | 97,6 | 98,4 | 98,7 |
| | | | |

| vendor | detected | total | percent |
|------------------|-----------------|--------------|----------------|
| AntiVir | 20,563,779 | 22,354,559 | 91.99% |
| F-Secure | 20,091,169 | 22,354,559 | 89.88% |
| Avast-Commercial | 19,481,906 | 22,354,559 | 87.15% |
| BitDefender | 18,797,996 | 22,354,559 | 84.09% |
| NOD32 | 18,741,120 | 22,354,559 | 83.84% |
| Ikarus | 17,819,794 | 21,311,870 | 83.61% |
| DrWeb | 18,072,789 | 22,354,559 | 80.85% |
| Kaspersky | 17,464,531 | 22,354,559 | 78.13% |
| McAfee | 16,645,006 | 22,354,559 | 74.46% |
| VBA32 | 16,015,200 | 22,354,559 | 71.64% |
| Sophos | 14,104,840 | 21,321,563 | 66.15% |
| Norman | 14,516,433 | 22,354,559 | 64.94% |
| F-Prot6 | 13,982,668 | 22,354,559 | 62.55% |
| Clam | 13,666,038 | 22,354,559 | 61.13% |
| AVG7 | 13,441,713 | 22,345,352 | 60.15% |
| Vexira | 13,207,560 | 22,354,559 | 59.08% |
| TrendMicro | 12,218,206 | 22,354,559 | 54.66% |
| QuickHeal | 9,531,648 | 21,179,613 | 45.00% |
| Panda | 7,688,849 | 22,354,559 | 34.39% |
| VirusBuster | 3,799,237 | 22,354,559 | 17.00% |
| G-Data | 3,419,218 | 21,321,563 | 16.04% |

<http://www.shadowserver.org/wiki/pmwiki.php/Stats/VirusYearlyStats>
 26/12/09

Bezpłatne antywirusy online

- Kaspersky.com
- Skaner.mks.com.pl
- Bitdefender.com
- Panda Cloud Antivirus (www.cloudantivirus.com) – „pierwszy w „chmurze”
- Housecall.trendmicro.com
- Security.symantec.com
- eset.pl/onlinescan (sprawdzony VII.2010)

Wirusy w komórkach

- „Cabir” – szkodnik działający pod Symbianem. Rozsiewa się przez Bluetooth, po włączeniu komórki (głównie Nokie).
- SEXXY i Gavno (2KB trojan).
- Gavno i Camtimer rozsiewane Cabir’em przez Bluetootha.

Konsekwencje ochrony

- Moc komputera
- Opóźniony start
- Wolniejsze pobieranie plików