Malware

-Malware je počítačový program určený ke vniknutí nebo poškození počítačového systému.

Výraz malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“ a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Pod souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware. V právní terminologii je malware někdy nazýván počítačová nečistota (angl. „computer contaminant“), například v zákonech států Kalifornie, Západní Virginie a několika dalších členských států USA. Malware je někdy pejorativně nazýván scumware. Jako malware by neměl být označován software, který sice obsahuje chyby, ale byl napsán pro legitimní účely.

V průběhu let autoři psali zákeřný software z různých důvodů. Mnoho dřívějších nakažlivých programů, mezi které patří internetoví červi a velký počet virů napsaných pro operační systém MS-DOS, vzniklo jako experiment nebo žert a většinou se záměrem vůbec neškodit nebo pouze obtěžovat. Mladí programátoři, kteří studovali možnosti virů a techniky jejich psaní, vytvářeli takové programy, aby ukázali, že to dovedou, nebo aby viděli, jak dalece se mohou jejich výtvory rozšířit.

Větší hrozbu představují programy navržené tak, aby poškozovaly nebo zcela mazaly data. Mnoho virů pro DOS bylo napsáno tak, aby smazaly soubory na pevném disku nebo aby poškodily souborový systém zapsáním nesmyslných dat. Síťoví červi, jako například Code Red nebo Ramen, také patří do této kategorie, protože byly napsány, aby vandalizovaly webové stránky.

Motivem pro vznik zákeřného softwaru bývá někdy pomsta. Programátor nebo správce systému, který byl propuštěn ze zaměstnání, může v systému zanechat zadní vrátka (angl. „backdoors“) nebo softwarovou „časovanou bombu“, která mu umožní poškodit v budoucnu systémy bývalého zaměstnavatele nebo zničit jeho vlastní dřívější práci.

S rozšířením širokopásmového internetového připojení vzniklo velké množství škodlivého softwaru zaměřeného čistě na zisk. Například v roce 2003 byla většina nejrozšířenějších virů a červů navržena tak, aby získala kontrolu nad napadeným počítačem pro jeho pozdější podloudné zneužití. Nakažené počítače jsou zneužity pro rozesílání spamu, šíření nezákonného obsahu, kterým je například dětská pornografie, nebo jsou zapojeny v distribuovaných útocích způsobujících nefunkčnost jiných systémů (DDoS, angl. „Distributed Denial of Service“) jako nové formě vyděračství.

Další kategorií malwaru psaného výhradně za účelem zisku je spyware, tedy programy, které monitorují uživatelem navštívené webové stránky, zobrazují nevyžádané reklamy a přinášejí tak autorovi spywaru podíl na zisku. Spyware se nešíří způsobem obdobným počítačovým virům, obvykle se instalují zneužitím bezpečnostních chyb prohlížeče nebo jako trojské koně při instalaci jiného softwaru.

Počítačový virus

Jako virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů.

Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Viry jsou jen jedním z druhů tzv. malwaru, zákeřného softwaru. V obecném smyslu se jako viry (nesprávně) označují i např. červi a jiné druhy malwaru.

Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji. Některé viry mohou být takzvaně polymorfní (každý jeho „potomek“ se odlišuje od svého „rodiče“).

Dnes jsou klasické počítačové viry na jistém ústupu oproti červům, které se šíří prostřednictvím počítačových sítí, hlavně Internetu. Některé antivirové programy se proto snaží chránit počítač i před jinými, nevirovými hrozbami.

Definice

Virus je typ programu, který se dokáže sám šířit tím, že vytváří (někdy upravené) kopie sebe sama. Hlavním kritériem pro posouzení programu jako viru je fakt, že k šíření využívá jiné soubory – hostitele. Virus se mezi dvěma počítači může přenést jedině tím, že někdo přenese celého hostitele, např. nějaký uživatel (obvykle neúmyslně) přenese soubor na disketě či CD-ROM nebo ho pošle prostřednictvím počítačové sítě.

Jako viry jsou někdy nesprávně označovány jiné druhy nebezpečných programů, hlavně červi. Rozdíl mezi červy a virem spočívá v tom, že červ je schopen se šířit sám, bez závislosti na přenosu hostitele. V dnešní době bouřlivého rozvoje Internetu se červi mohou šířit velice rychle. Ale i pro klasické viry je snadnost šíření souborů prostřednictvím Internetu výhodou, takže se rozdíly mezi viry a červy do jisté míry ztrácí.

Druhy virů

Viry je možno dělit podle různých hledisek:

Podle hostitele

Podle toho, prostřednictvím jakých hostitelů se virus šíří, je možné je dělit na několik druhů. Základními typy hostitelů jsou:
Spustitelné soubory – COM a EXE programy v prostředí DOSu, EXE soubory v Microsoft Windows, ELF soubory v UNIXu atd.
Boot sektory disket a diskových oddílů.
Master boot sektor (MBR) pevného disku.
Dávkové soubory a skripty – BAT v DOSu, shellovské skripty na UNIXech.
Dokumenty, které mohou obsahovat makra – např. dokumenty programů Microsoft Office.
Specializované skripty některých konkrétních aplikací.

Podle způsobu činnosti

Podle různých aspektů způsobu činnosti se některé viry označují specializovanými termíny:
Rezidentní/nerezidentní viry

Vir se může šířit dvěma základními způsoby: buď se ve chvíli spuštění hostitele (tzn. ve chvíli, kdy se při spouštění hostitele spustí kód viru) rozšíří do nalezených nenakažených souborů, nebo se pouze uloží do operační paměti počítače, ve které zůstane až do doby vypnutí počítače, a mezitím infikuje soubory (nebo např. diskety), se kterými uživatel pracuje.

První typ se označuje jako nerezidentní vir, druhý jako rezidentní vir.

Stealth viry

Stealth viry se snaží zamaskovat svou přítomnost v souboru tím, že se zachytí na přerušení, kudy prochází veškeré požadavky na čtení dat ze souboru (tedy i požadavky antiviru). Vir si pak kontroluje, zda se požadavek týká i infikovaného souboru, v tomto případě pak vrátí aplikaci data původního neinfikovaného souboru. Poměrně rychle se ale na tento způsob maskování objevila obrana - antivirus si buď kontroluje, zda není adresa přerušení přepsána, případně na čtení používá přímo služby diskového řadiče. Tato technika krytí se převážně týkala operačního systému MS-DOS, pro modernější operační systémy je nutno použít složitějších rootkitů(maskovacích zařízení).

Historie

Historie počítačových virů začíná počátkem osmdesátých let 20. století. V roce 1983 sestrojil jistý Dr. Frederik Cohen první samomnožící program, který začal označovat jako virus. V podstatě se jednalo o neškodný kód, který se uměl pouze sám množit. První skutečný vir, který mohl nějak uškodit, naprogramovali v roce 1986 bratři Basid a Amjad Farooq Alvi, pojmenovali jej Brain (mozek). Objevil se 19. ledna 1986. Sice útočil jen na na určitou část disku, ale na starších počítačích způsobil větší škody. Tím fakticky odstartovala éra virů, které se od té doby dále rozvíjely. Autoři virů si mezi sebou také předávají moderní techniky a mnoho dalších triků, které umožňují virům měnit svůj vlastní kód a být dokonalejšími a lépe se „schovávat“ před antivirovými programy. Současné viry jsou tak mnohem vyspělejší a dokážou zhroutit celou síť počítačů. Proto je nejlepší se jim bránit účinným antivirem.

Důvody vzniku virů

Je několik důvodů vzniku virů.
Vytvářejí je programátoři velkých softwarových firem, kteří byli propuštěni ze zaměstnání. Ti se svým zaměstnavatelům pomstí vytvořením nějakého viru a jeho vpuštěním do jejich lokální (firemní) sítě, aby zničili nebo poškodili firmu.
Vytvářejí je mladí programátoři, kteří si chtějí vyzkoušet své schopnosti. Pokud se takové viry rozšíří, může to být důsledek chyby nebo neuvědomění si celkového dopadu svojí činnosti.
Viry vytvářejí programátoři softwarových firem, které vytvářejí antivirové programy, za účelem zvýšení prodeje svých výrobků.

Viry jsou jednou z cest, jak ovládnout a řídit větší množství počítačů a využívat je např. k rozesílání spamu.
Jsou prostředkem, jak zdiskreditovat platformu, která není schopna sama sebe uchránit před jejich šířením.

Obrana před viry

Některé vyspělé operační systémy (např. z rodiny GNU/Linux, BSD aj.) jsou vůči škodlivým kódům přirozeně velice imunní, tudíž pro svou vlastní potřebu antivirové programy prakticky nepotřebují (výjimkou jsou servery, které tyto programy používají zejména na ochranu svých klientů). I škodlivé kódy, zejména rootkity, pro ně existují, ovšem běžný uživatel se s nimi prakticky vůbec nesetká a když už, většinou se jedná o kódy dávno zneškodněné.

Trojský kůň

Trojský kůň je uživateli skrytá část programu nebo aplikace s funkcí, se kterou uživatel nesouhlasí (typicky je to činnost škodlivá). Název Trojský kůň pochází z antického příběhu o dobytí Tróje.

Trojský kůň může být samostatný program, který se tváří užitečně – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj. Časté jsou spořiče obrazovky s erotikou nebo pornografií. Někdy se trojský kůň vydává za program k odstraňování malware (dokonce jako takový může fungovat a odstraňovat konkurenční malware). Tato funkčnost slouží ale pouze jako maskování záškodnické činnosti, kterou v sobě trojský kůň ukrývá.

V Microsoft Windows může trojský kůň využít toho, že řada programů včetně systémového správce souborů (exploreru) skrývá přípony souborů. Vypadá pak jako soubor s obrázkem, zvukem, archivem nebo čímkoliv jiným, přestože se ve skutečnosti jedná o spustitelný kód. Chce-li uživatel obrázek kliknutím zobrazit, je ve skutečnosti spuštěn program (trojský kůň).

Trojský kůň může být ale také přidán do stávající aplikace. Poté je upravená verze šířena například pomocí peer-to-peer sítí nebo warez serverů. Uživatel stažením kopie aplikace (nejčastěji bez platné licence nebo jako volně šířený program z nedůvěryhodného serveru) může získat pozměněnou kopii aplikace obsahující část programového kódu trojského koně dodaného třetí stranou.

Klíčový rozdíl mezi počítačovým virem a trojským koněm je ten, že trojský kůň nedokáže sám infikovat další počítače nebo programy svojí kopií. Existují však počítačové červy, které na napadeném počítači instalují různé trojské koně nebo vytvářejí trojské koně z programů, které se v napadeném systému nacházejí.

Příklady funkcí trojských koňů
sniffer – odposlouchávání přístupových jmen a hesel, čísel kreditních karet
keylogger – sledování (záznam) znaků zadávaných z klávesnice
spyware - sleduje uživatele a jeho zvyklosti při surfování na Internetu a posílá o tom zprávy
zadní vrátka - trojský kůň obsahuje síťovou službu, kterou může útočník použít pro získání přístupu do systému přes počítačovou síť
spam server – rozesílání nevyžádané elektronické pošty (e-mail) z napadeného počítače

souborový server - trojský kůň nainstaluje souborový server - např. FTP, IRC bota nebo nějaký P2P program - který je poté použit buď pro stahování souborů uživatele, nebo pro ukládání souborů majitelem trojského koně (např. warezu nebo malware).
proxy trojan - maskuje ostatní jako infikované počítače
Security software disabler - zablokuje software pro zabezpečení PC (Firewall,Antivir)
denial-of-service - trojský kůň se účastní DDoS útoku
URL trojan - přesměrovává infikované počítače připojené přes vytáčené připojení k Internetu na dražší tarify

Některé známé trojské koně
Downloader-EV
Pest Trap
NetBus
flooder
Tagasaurus

Spyware

Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele. Někteří autoři spyware se hájí, že jejich program odesílá pouze data typu přehled navštívených stránek či nainstalovaných programů za účelem zjištění potřeb nebo zájmů uživatele a tyto informace využít pro cílenou reklamu. Existují ale i spyware odesílající hesla a čísla kreditních karet nebo spyware fungující jako zadní vrátka. Protože lze jen těžko poznat, do které skupiny program patří, a vzhledem k postoji k reklamě řada uživatelů nesouhlasí s existencí a legálností jakéhokoliv spyware.

Spyware se často šíří jako součást shareware, a to jako adware nebo bez vědomí uživatelů (ale s vědomím autorů programu). Jakmile si takový program nainstalujete a spustíte, nainstaluje se do systému také spyware. Často se to týká například klientských programů pro peer to peer sítě umožňující stahování hudby a videa od ostatních uživatelů.

Spyware patří mezi malware, tedy programy, které na počítači běží bez vědomí uživatele a nějakým způsobem jej poškozují, nebo zhoršují jeho funkci. Spyware představuje z hlediska bezpečnosti dat velkou hrozbu, protože odesílá různé informace (historii navštívených stránek, hesla) z vašeho počítače určenému uživateli, který tyto informace dále zpracovává.

Nejčastějších příznaky výskytu spyware
Nežádoucí domovská stránka (Přesměrování na jinou webovou stránku)
Pomalý start počítače a dlouhé nabíhání internetu
Při surfování na internetu ve zvýšené míře vyskakují reklamy - Pop-up okna
Přesměrování telefonní linky - u vytáčeného připojení - Dialery
Padající Windows (Častý restart, chyby, apod.)
Nové ikony na ploše, které se záhadně objevují

<u>Druhy spyware</u>

Adware - obtěžují při práci na počítači reklamou

Browser helper object - dll knihovna, která umožňuje programátorům změnit a sledovat Internet Explorer
Hijacker - mění domovskou stránku
Dialer - přesměrovává telefonní linku na drahé telefonní tarify
Keystroke Logger - sleduje každý pohyb na klávesnici, některé druhy odesílají uživatelova hesla
Miscellaneous - je to směs spyware
Remote Administration - umožní vzdálenému uživateli ovládat PC

Ochrana proti spyware
Neprohlížet internetové stránky s podezřelým obsahem (pornografie, warez)
Při surfování používat bezpečnější internetový prohlížeč
Používat antispyware
Provádět aktualizace systému
Používat firewall
Neinstalovat podezřelé programy

Spyware může odesílat

části registru systému (uživatelé často pracují pod účtem administrátora)
IP adresu uživatele, někdy i MAC (fyzickou) adresu
Historii prohlížených stránek
Informace o software a multimediálních souborech, které jsou na počítači
Seznam otevíraných souborů
celé dokumenty
uživatelova hesla

Odstranění spyware z počítače

Antivirové programy většinu spyware nenajdou, proto je nutné použít speciální software - antispyware, který si s tím poradí. Je lepší používat více antispyware, protože tyto programy mají různou databázi spyware

Adware

Adware (advertising-supported software) je označení pro produkty znepříjemňující práci s nějakou aplikací reklamou. Ty mohou mít různou úroveň agresivity - od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Další nepříjemnou věcí je např. změna domovské stránky v Windows Internet Exploreru, aniž by o to uživatel měl zájem.

Většinou ale nejsou přímo nebezpečné jako spyware a jsou spojeny s nějakým programem, který je freeware. To se dělá z důvodu toho, že díky těmto reklamám mohou vývojáři financovat dál svůj program. Nebo když se jedné o placený produkt, může se díky těmto reklamám prodávat program se slevou. Nějaký adware je taky shareware, ale není to totéž. Rozdíl mezi adware a shareware je ten, že u adware je reklama podporovaná. Některé produkty nabízejí uživateli možnost odstranění reklam po zaplacení.

Spousta lidí si plete pojmy spyware a adware. Adware velmi často využívá výsledků, které dokázal vyprodukovat spyware,ale není na něm závislý. Adware se instaluje do počítače za souhlasu uživatele. Uživateli je při instalaci hlášeno, že program obsahuje malware a sám má možnost se rozhodnout jestli s tím souhlasí a bude dál pokračovat v instalaci, nebo ne. To je díky licenčnímu ujednání "EULA" (End User License Agreement). Naproti tomu spyware se instaluje do počítače bez vědomí a souhlasu uživatele. Někdy program, který je použit jako reklamní podpora, je spyware - tedy adware instaluje spyware, často se zastíráním detailů činnosti tohoto spyware.

Programy obsahující Adware na rozdíl od spyware neshromažďují tajně informace a neodesílají je přes internet bez souhlasu uživatele.

Existuje velké množství programů, které pomáhají uživatelům vyhledávat a odstraňovat Adaware programy, případně je zachovat, ale zamezit zobrazování reklamy v nich.
Známé Adware programy
TopMoxie
123 Messenger
180 Solutions
180SearchAssistant
Zango
Bonzi Buddy
BlockChecker
ClipGenie
Comet Cursor
Crazy Girls
Cursor Mania
Cydoor
Daemon Tools
Direct Revenue
Aurora
Ebates MoneyMaker
ErrorSafe
Gator
Hotbar
ICQ
Mirar Toolbar
Oemji Toolbar
Xango Toolbar
PornDigger!
Smiley Central
WeatherBug
WhenU
WinFixer
Tag A saurus

Eudora

Eudora e-mailový klient je příklad Adware produktu. Uživatel má nějakou zkušební dobu na otestování programu. Za tuto dobu jsou všechny části programu dostupné. Během této doby si uživatel vybere z jedné volby, buď může bezplatně program používat, ale bude omezen (tzn. že nebudou v něm dostupné všechny jeho funkce), nebo bude dál využívat všechny funkce programu, ale jen s reklamou, nebo zaplatí a bude moc využívat program bez reklam. Když si uživatel vybere druhou možnost tedy bezplatně, ale s reklamou, stává se Eudora Adwarem.

Ochrana

Na ochranu před Adware existuje několik programů. Tyto programy umějí najít adware, odstranit ho z počítače nebo uložit ho do tzv. karantény. Fungují tak, že prohledávají pevný disk, registry i paměť. Obsahují určitou databázi Spywarů a Adwarů. Když najdou něco co odpovídá podle databáze Spywaru a Adwaru, nejenže to detekují a identifikují, ale dokáží to odstranit z počítače. Lepší je ale se před Adware a Spyware chránit. Tuto ochranu tyto program taky umožňují. Aby tyto ochranné programy správně fungovaly, musí se neustále aktualizovat. Neaktualizovaný program je k ničemu, protože neustále vzniká nový Spyware a Adware a bez aktualizované databáze ho nedokáží programy identifikovat.
Nejlepší způsoby jak se bránit před Spyware a Adware jsou tyto:
Neinstalujte žádný program obsahující adware.
Aktualizujte Windows a nainstalujte všechny bezpečnostní záplaty (případně nepoužívejte Windows vůbec).
Používejte alternativní internetové prohlížeče (Mozilla Firefox, Netscape, Opera, atd).
Nainstalujte software blokující reklamy. Pro uživatele používající Firefox existuje rozšíření Adblock, které může blokovat škodlivé a nepříjemné reklamy zobrazené na webu. Uživatelé používající Operu mají tuto funkci zabudovanou do prohlížeče.
Používejte bezplatné alternativní programy, o kterých bezpečně víte, že neobsahují reklamu.
Používejte alternativní operační systémy (Linux, Mac OS X)

Spam

Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging. Používá se též zkratka UBE/UCE (Unsolicited Bulk/Commercial Email).
Pro opak spamu, tj. poštu, která je zaslána konkrétní osobou se specifickým jednorázovým účelem a adresát ji považuje za žádoucí, se řidčeji používá termín ham (anglicky šunka).

Historie spamu (zahraničí)

Internet byl původně armádní projekt a nikdo nepředpokládal, že bude určen k vydělávání peněz. Zřejmě první spam napsal zaměstnanec Digital Equipment Corporation. Byl zaslán 1. května 1978 na adresy tehdejší sítě ARPANET a obsahoval informace o prezentaci produktů této společnosti. Dalším spamem byla zpráva podepsaná jistým Davem Rhodesem a rozeslaná do diskusních skupin sítě USENET. Předmětem této zprávy bylo MAKE.MONEY.FAST!! (vydělávej rychle peníze).

Roku 1993 se muž jménem Richard Depew rozhodl představit svoji novou představu o fungování USENETu. Tato idea nebyla na první pohled špatná. Navrhoval přidat moderátorům konferencí možnost stanovit pravidla a zrušit příspěvky, které je poruší. Koncem března si Richard hrál se svým programem nazvaným ARMM, jehož úkolem bylo spravovat diskuse podle jím navrhnutého způsobu. Bohužel došlo k nehodě a jeho software zahltil diskusní skupinu news.admin.policy více než 200 příspěvky. Samotný Richard Depew se za své počínání omluvil s tím, že se skutečně jednalo o nehodu.

Jedním z dalších spamů byla zpráva zaslaná 18. ledna 1994 s předmětem Global Alert For All: Jesus is Coming Soon (Upozornění pro všechny: Ježíš brzy přijde). Jednalo se o nábožensky laděný text, který ukazoval souvislosti mezi zemětřesením v Los Angeles, Kalifornii, záplavami v Evropě, válkou v Jugoslávii a dalšími katastrofami.

Skutečně masivním spamem byla nevyžádaná zpráva Green Card Lottery, kterou zaslali 5. března 1994 právnická společnost Cantor a Siegel. Zpráva zahltila 6 000 diskusních skupin. V jejich stopách později kráčel další spammer Michael Wolff, který pomocí nevyžádaných zpráv nabízel svoji knihu o internetovém chatu. Každý výskyt spamu doprovázely mohutné diskuse o etice chování na Internetu (tzv. netiquete). Navzdory tomu se spam stal až do dnešní doby hrozbou, kterou řeší nejen známé technologické společnosti, ale také politici.

Historie spamu (Česko), příklady

Zřejmě největší negativní reakci uživatelů vyvolal hromadný spam společnosti Media Online, s. r. o. Firma provozující server o bydlení Tvujdum.cz v něm oznamovala novinky a seznamovala čtenáře se svým webem. Spam obsahoval přílohu ve formátu HTML, což snížilo reklamní dopad celé akce. Uživatele také pobouřila výmluva uvedená v textu e-mailu:

Tento e-mail je Vám zasílán na základě pečlivého výběru a globální rešerše uživatelů, kteří své webové stránky věnují tematice bydlení, stavebnictví. Předem se omlouváme za nevyžádaný e-mail.

Ředitel společnosti se původně pokoušel masivní spamming obhajovat: „Dovoluji si Vás ujistit, že v žádném případě nešlo o masové rozesílání spamů, jak některé servery uvádějí, neboť množství připravených e-mailů bylo vůči českému internetu zanedbatelné.“ Později vydala společnost tiskovou zprávu, v níž se omluvila všem uživatelům. Výkonný ředitel společnosti navíc přislíbil finanční dar v hodnotě 50 000 Kč nadaci Člověk v tísni.

Přesto se uživatelé českého internetu semknuli v boji proti spamu a podle serveru Lupa.cz zaslalo 30 lidí stížnost na společnost Media Online. Některé stížnosti adresované živnostenskému odboru Magistrátu hlavního města Prahy byly podepsány jen přezdívkou. Úřad nakonec udělil spamující firmě pokutu ve výši několika desítek tisíc korun.

Ochrana emailových adres na straně uživatele

E-mailové adresy do spamových databází jsou získávány mj. pomocí robotů, kteří procházejí webové stránky a sbírají e-mailové adresy na nich uvedené. Roboti se zpravidla nezatěžují hlubší analýzou zdrojového kódu a sbírají vše, co vypadá jako e-mailová adresa – tedy posloupnost písmen, číslic, pomlček a teček, která obsahuje zavináč. Proto se doporučuje

vyhnout psaní e-mailové adresy přímo na webovou stránku a raději ji opsat nějakým, pro člověka srozumitelným, způsobem – např. jmeno (zavinac) domena.cz.

Doporučuje se vždy dobře zvážit, zda je vhodné či nutné určitému subjektu svůj e-mail svěřit (týká se především webových stránek, různých registrací, upozorňování). I v případě seriozních subjektů nelze nikdy vyloučit únik informací a zneužití třetí stranou. Pro různé registrace, zasílání informací atd. se doporučuje mít specializovaný e-mail (s případným přeposíláním).

E-mailové adresy pro databáze pro rozesílání spamu můžou být získávány také pomocí virů, je proto důležité znát základní pravidla pro chování na internetu a mít počítač proti virům dobře zabezpečený.

Na adresy, z nichž je spam poslán, by se nemělo žádným způsobem reagovat a neklikat na žádný z odkazů v e-mailu obsažených, neboť tím je spamerovi pouze potvrzeno, že elektronická adresa je funkční a schránku někdo vybírá. Adresa, z níž je spam poslán, často není pravá a často se mění; může jít i o zfalšovanou adresu jiného člověka, jenž s rozesláním e-mailu nemá nic společného.

Spamovací robot však mailové adresy může získat rovněž sledováním odpovědí vzdálených SMTP serverů. Provádějí na vzdálený poštovní server tzv. slovníkový útok, kdy se pokouší doručit e-mail na adresy složené z obvyklých jmen a příjmení, oblíbených názvů a přezdívek (svoboda, novak, standik atd.). Tyto adresy jsou proto ve větším ohrožení, jako protiopatření se doporučuje např. rozšíření adresy o další znaky (xsvoboda).

U tzv. hoaxu (řetězového dopisu obsahujícího často žádost o pomoc a další rozeslání) je vhodné odesílatele upozornit na omyl a e-mail dále nerozesílat (pokud je v e-mailu obsažena žádost o hromadné rozeslání současně s žádostí o pomoc nebo o podporu někoho, nebo něčeho, jde většinou o podvod, nebo hloupý vtip).

Opatření omezující rozesílání spamu

Většina spamu je rozesílána distribuovaně z počítačů napadených počítačovým virem nebo červem. Vir nebo červ často na počítači otevírá tzv. zadní vrátka (backdoor), která umožňují útočníkovi počítač dálkově ovládat a zneužít jej mj. pro rozesílání spamu. Rozesílací robot i databáze adres může být na napadený počítač zaslána ad hoc, rozesílání nemusí probíhat neustále.

Obranou proti distribuovanému rozesílání je klasická antivirová ochrana. Pro správce sítě je důležité, aby uměl napadený počítač lokalizovat a izolovat.

Další možnost jak ztížit rozesílání spamu je neprovozovat SMTP server jako tzv. open relay. SMTP server, který funguje jako open relay, převezme k dopravě jakýkoli dopis bez ohledu na odesílatele i adresáta. Open relay usnadňuje rozesílání spamu tím, že umožňuje přijmout dopis (spam) odkudkoli a dopravit jej kamkoli, často je jeden dopis adresován na stovky cílových adres. Tím jednak snižuje zátěž na straně spammerova rozesílacího robota, jednak se průchodem přes open relay zamaskuje IP adresa, odkud dopis přišel, což silně ztěžuje filtraci spamu na straně cílového SMTP serveru.

SMTP server by měl být konfigurován tak, aby nepřebíral k dopravě dopisy, které přichzejí z vnějšku domény (domén) a nemají adresáta uvnitř domény, kterou server pokládá za „vlastní“. Příklad: SMTP server pro doménu firma.cz propustí pouze dopisy, které v doméně firma.cz začínají nebo končí.

Filtrace podle způsobu dopravy

Blacklisting

Blacklisting rozhoduje, zda dopis je nebo není spam, podle adresy odesílatele (která může být zfalšována), nebo lépe podle IP adresy, ze které dopis přišel na cílový SMTP server. Blacklisty obsahující IP adresy, ze kterých bylo zaznamenáno rozesílání spamu, bývají zveřejňovány nejčastěji pomocí systému DNS. Výskyt adresy v blacklistu může mít za následek buď přímé odmítnutí (nepřevzetí) dopisu ještě během SMTP relace, nebo může být informace z blacklistu použita jako dodatečná informace při následné filtraci podle obsahu.

Greylisting

Greylisting rozhoduje také podle IP adresy a emailové adresy odesílatele a adresáta, ale dělá to dynamicky. SMTP server, který provozuje greylisting, udržuje databázi, kde pro trojici (IP adresa, odesílatel, příjemce) je uvedeno, zda dopis s těmito atributy má být převzat k dopravě, nebo zda jeho převzetí má být dočasně odmítnuto. První dopis je odmítnut a je zaznamenán čas, kdy k tomu došlo. Po určitou dobu (typicky několik desítek minut) pak jsou dopisy s týmiž atributy odmítány. Po uplynutí této doby, pokud se původní SMTP server stále pokouší o odeslání dopisu, je záznam v databázi potvrzen a dopisy jsou naopak přijímány a dopravovány bez zdržení. Po další době (typicky několik málo týdnů) je záznam z databáze odstraněn, takže příští dopis bude opět pozdržen. K odstranění záznamu z databáze dojde také v případě, že v příslušném intervalu, kdy byly dopisy odmítány, se nepokusí původní SMTP server o znovudoručení.

Tato metoda využívá faktu, že protokol SMTP rozlišuje chyby trvalé, jejichž číselný kód začíná číslicí 5, a chyby dočasné s kódem začínajícím číslicí 4. V případě dočasné chyby má odesílající SMTP server dopis uložit do fronty a pokusy o odeslání opakovat (typicky po několika málo desítkách minut). Robot rozesílající spam však často chyby neošetřuje a snaží se všechny dopisy rozeslat co nejrychleji, neboť je možné, že před případným dalším (nebo novým) pokusem o rozeslání, již bude spamerova IP adresa zveřejněna v některém blacklistu. Proto k druhému pokusu již nedojde.

Greylisting se zpravidla používá jako předstupeň před filtrováním podle obsahu a výrazně zvyšuje jeho účinnost. Nevýhodou greylistingu je občasné zdržení dopisu a možnost, že dopisy mohou dojít v jiném pořadí než byly odeslány. Další nevýhodou je, že některé odesílající SMTP servery jsou chybné a neimplementují frontu dopisů k odeslání.

Filtrace podle obsahu dopisu

Automatické rozpoznávání nemůže z principu fungovat dokonale, protože názor, zda konkrétní dopis je spam je individuální. Přesto filtrování podle obsahu dává použitelné

výsledky a hojně se používá. Existují dvě základní metody, některé antispamové programy (např. SpamAssassin) je kombinují.

Filtry založené na pravidlech

Filtry založené na pravidlech vyhledávají v dopisech rysy, které jsou pro spam typické. Jde jednak o některá slova (např. viagra) a slovní spojení, jednak jsou vyhledávány chyby pro spam typické. Příkladem je třeba datum odeslání v budoucnosti, nedovolené znaky v hlavičce, chybně označený MIME-typ zprávy apod. Za každý rozpoznaný rys je dopisu přiděleno bodové ohodnocení, body se zpravidla sečítají a pokud součet přesáhne hranici, je dopis pokládán za spam. Rozpoznávané rysy jsou definovány pomocí pravidel, která je třeba pravidelně aktualizovat a přizpůsobovat praktikám spammerů. K vytváření a údržbě souboru pravidel je třeba mít znalosti, není to práce pro běžného uživatele, laika.

Filtry založené na učení (bayesovské)

Filtry založené na učení (často nazývané bayesovské) využívají triky z oblasti umělé inteligence. V režimu učení se filtru předkládají dopisy explicitně označené jako spam a ham (ne spam), filtr z předložených dopisů extrahuje informace, které si ukládá do databáze. Nejčastěji je dopis rozkládán na slova (popř. jiné úseky textu) a pro jednotlivá slova se statisticky zjišťuje pravděpodobnost, že dopis, který toto slovo obsahuje, je spam. V režimu rozpoznávání pak filtr využívá nashromážděné informace a testovanému dopisu přiřadí pravděpodobnost, že je to spam. Nejčastěji se pro výpočet pravděpodobnosti používá vzorec, který navrhl matematik Bayes. Velkou výhodou je, že filtr může učit i uživatel – laik. Učící se filtry jsou nejúčinnější, učí-li je přímo sami koncoví uživatelé podle svého individuálního názoru, co je spam a co ne. Přesto se bayesovské filtry používají i na serverech, kde učení probíhá pro všechny uživatele serveru společně.

Bayesovský filtr je součástí např. poštovního klienta Mozilla Thunderbird. Příkladem čistě bayesovského filtru pro server je bogofilter.

Počítačový červ

Počítačový červ je v informatice specifický počítačový program, který je schopen automatického rozesílání kopií sebe sama na jiné počítače. Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívá je ke svému vlastnímu šíření.

Popis činnosti

Kromě svého vlastního šíření, které má rozhodující vliv na úspěšnost červa, vykonává obvykle tento v počítači nějakou sekundární činnost, která je červem nesena jako „náklad“ (kód, který tvoří náklad se nazývá anglicky payload).
Typicky se jedná o:
-zneprovoznění počítače, nebo jeho součástí
-odstraňování souborů uložených v počítači
-šifrování souborů uživatele kryptovirálním útokem jako nátlak k zaplacení poplatku, po kterém je přislíbena jejich opětovná dekrypce

-prohledávání počítače za účelem získání osobních dat, která mohou pro autora programu znamenat nějaký profit
-vytváření „zadních vrátek“ do systému (tzv. backdoor), která poté mohou být využita jako přímá cesta k infikování počítače dalšími nákazami
-jako důsledek jiné činnosti způsobují nestandardní chování systému.

Ať už je činnost, kterou takový program vykonává v síti, jakákoli, vždy s sebou nese vedlejší efekty, které jsou důsledkem této činnosti. Téměř vždy je, v případě většího rozšíření červa, těmito infekcemi snižována rychlost průtoku dat mezi jednotlivými počítači (a tím i celý internet) a způsobují menší či větší finanční škody majitelům postižených počítačů – ať už se jedná o soukromé vlastníky, nebo celé firmy. Proto jsou, nezávisle na záměru autora, považovány za malware.

Historie

Slovo červ (anglicky worm) bylo přejato z románu Jezdec na rázové vlně (John Brunner, 1975), v němž byl jako Tapeworm označen program schopný samostatného šíření. Jeho úkolem bylo vyřadit z provozu celou telefonní síť na pokyn svého autora.

První červi

Historicky první počítačové červy vytvořili John F. Schoch a John A. Hupp. Společně je implementovali ve středisku Xerox PARC, kde měli za úkol monitorovat vytížení procesorů počítačů připojených k síti a v případě nečinnosti jim zadat nějakou úlohu. Dosáhli tak optimálního využívání výpočetního potenciálu střediska.

Mezi prospěšné červy patřila rovněž rodina červů Nachi, která odstraňovala ostatní malware, stahovala bezpečnostní aktualizace z webu Microsoft Update a instalovala je na infikovaném počítači. Červi tak záplatovali ty samé chyby, které využívali ke svému šíření. I když bylo jejich úkolem zvýšení úrovně zabezpečení počítačů, způsobovali značné zpomalování sítě a restartování systému po instalaci každé aktualizace.

Můžeme tedy říci, že původním záměrem počítačových červů nebylo škodit, ale pomáhat a celkově zlepšovat práci s PC.

První problémy

Disketa obsahující zdrojový kód červa Morris uložená v Bostonském vědeckém muzeu.

Zlomovým okamžikem byl 2. listopad 1988, kdy se červ označovaný jako Morrisův červ, vytvořený tehdy 23-letým studentem Cornellovy univerzity Robertem T. Morrisem, začal díky chybně naprogramovanému mechanismu šíření nekontrolovaně množit a způsobil tehdejšímu internetu značné škody. Z původně nevinného programu, určeného ke změření rozsahu internetu, se tak stala velmi reálná hrozba.

Současnost

Poté, co si počítačová komunita uvědomila svou zranitelnost, byly podniknuty některé kroky vedoucí ke zvýšení zabezpečení počítačů jako forma prevence před podobnými útoky. Současně s tím se však tyto infiltrace dostávaly na denní pořádek.

V historii nejúspěšnějším počítačovým červem byl červ I Love You, který po svém vypuštění v roce 2000 napáchal škody v řádu desítek milionů amerických dolarů a ochromil provoz některých internetových služeb na několik dnů.

Příkladem červů z nedávné minulosti jsou červi Sasser a Blaster, kteří využívali zranitelnosti operačního systému Microsoft Windows a přerušovali uživatelovu práci s počítačem v důsledku opakovaného vypínání PC.

Typy počítačových červů

Proces zombifikace počítače při útoku typu backdoor.

Stejně jako počítačových virů, i počítačových červů existuje několik druhů. Ty rozlišujeme podle způsobu, kterým se šíří.

E-mailoví červi

E-mailoví červi využívají ke svému šíření elektronické pošty. Poté, co infikují nový počítač, se začnou rozesílat na e-mailové adresy, které získají buď z e-mailového adresáře oběti počítače, nebo prohledáváním obsahu uložených souborů a extrahováním řetězců, které vyhovují tvaru e-mailové adresy. Zvláštním případem jsou sítě botnet, složené z počítačů infikovaných k tomu uzpůsobeným červem, kdy infikované počítače na příkaz autora infekce zasílají hromadně SPAM, nebo uskutečňují útoky typu DDoS na jiné počítače.

Obsah infikované zprávy zaslané e-mailovým červem obvykle obsahuje vlastní škodlivý program jako přílohu, případně odkazuje na webové stránky, které jsou schopny infikovat počítač příjemce.

Výhodou takového přístupu je možnost využít e-mailového účtu oběti a v kombinaci s použitím adres dostupných v adresáři e-mailových adres působit jako věrohodná korespondence.

Internetoví červi

Internetový červ využívá všechny dostupné síťové prostředky počítače ke skenování ostatních počítačů v síti. Pokud najde počítač, který je zranitelný a umí-li této zranitelnosti využít, provede na takový počítač útok a (v závislosti na závažnosti této zranitelnosti) je v ideálním případě schopen spuštění škodlivého kódu a vlastní instalace do systému.

Výhodou tohoto přístupu je fakt, že v případě efektivního využití zranitelnosti počítače je možno jej infikovat bez vědomí nebo přičinení uživatele.

IM a IRC červi

Tyto druhy počítačových červů využívají ke svému šíření sítí pro komunikaci v reálném čase. Zatímco v případě IM červů tito obvykle rozesílají odkazy na webové stránky schopné infikovat počítač příjemce, IRC červi zasílají svůj program jako (spustitelný) soubor. (Z toho plyne jejich menší nebezpečnost, neboť aby mohlo dojít k infekci, musí uživatel potvrdit přijetí souboru, uložit jej a následně spustit.)

Výhodou tohoto přístupu je, stejně jako v případě e-mailových červů, možnost zasílání odkazů a souborů jménem uživatele napadeného systému a působit věrohodně.

Červi využívající sdíleného prostoru

Tento druh kopíruje svůj program jako (spustitelný) soubor do sdílených umístění (typicky na sdílený prostor lokálního počítače), nebo na vzdálený počítač, kdy dává tento soubor k dispozici ke stažení. Po stažení a spuštění takového souboru, který je obvykle pojmenován názvem, který nevzbuzuje žádné podezření, dojde k infikaci počítače.

Výhodou tohoto přístupu je fakt, že dnešní sdílecí sítě jsou využívány ke sdílení nelegálního obsahu a tudíž, v kombinaci s příhodným pojmenováním souboru, přináší poměrně značné možnosti šíření.

Ochrana před počítačovými červy

V podstatě neexistuje ucelený návod, jak uchránit svůj počítač od jakékoli infiltrace přicházející z internetu. Vezmeme-li však v úvahu omezené možnosti šíření počítačových červů, můžeme vyvodit několik jednoduchých kroků, jak se těmto a mnohým podobným infiltracím zcela vyhnout:
neotvírat přílohy e-mailů s neočekávaným typem přiložených souborů, jejichž obsah není přesně znám
nespouštět odkazy na neznámé/podezřelé stránky a ani se po těchto webech nepohybovat
nestahovat sdílený nelegální obshah
používat antivirový a ideálně i antispywarový software, který je schopen nejen zastavit již probíhající infekci, ale v případě správné funkčnosti a nastavení rovněž předejít nakažení počítače
používat firewall
používat vždy nejaktuálnější verzi operačního systému s instalovanými opravnými balíčky.

Vzhledem k faktu, že počítačové infiltrace ze zřejmých důvodů útočí na nejrozšířenější platformy a software, může být používání alternativ částečným východiskem z těchto problémů. Nelze však spoléhat na to, že počítač bude stoprocentně ochráněn, neboť výhoda těchto alternativních platforem nespočívá nutně v jejich vyšší bezpečnosti, ale právě v jejich alternativnosti.

Další způsoby síťové ochrany
Nullrouting
Routery vybavené aktivními ACL
Jiné síťové prvky schopné aktivní ochrany

Antivirový program

Antivirový program je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). K zajištění této úlohy se používají dvě odlišné techniky:
prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi
detekcí podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.Úspěšnost závisí na schopnostech antivirového programu a aktuálnosti databáze počítačových virů. Aktuální virové databáze se dnes nejčastěji stahují z Internetu.

Metody

Virové slovníky/databáze

Při kontrole souboru antivirový program zjišťuje, zda se nějaká jeho část neshoduje s některým ze známých virů, které má zapsány v databázi. Pokud je nalezena shoda, má program tyto možnosti:
pokusit se opravit/vyléčit soubor odstraněním viru ze souboru (pokud je to technicky možné)
umístit soubor do karantény (virus se dále nemůže šířit, protože ho nelze dále používat)
smazat infikovaný soubor (i s virem)

K dosažení trvalého úspěchu ve středním a dlouhém období vyžaduje virová databáze pravidelné aktualizace, které obsahují informace o nových virech. Pokud je antivirový program neaktualizovaný, představují viry přinejmenším stejné nebezpečí, jako kdyby antivir v počítači vůbec nebyl! Uživatelé mohou sami zaslat svůj infikovaný soubor výrobcům antivirových programů, kteří informaci o novém viru začlení do databáze virů.

Antivirový program fungující na platformě databáze virů kontrolují soubory v momentě, kdy je operační systém počítače vytvoří, otevře, zavře nebo je zasílá/přijímá emailem. V takovém případě je virus možné zjistit ihned po přijmutí souboru. Nutno podotknout, že uživatel může naplánovat kontrolu celého systému (pravidelně, nebo na určitý čas). Lze tedy plánovat opakované kontroly všech/části souborů, které se na jednotlivých discích nacházejí. Velmi často je antivirová kontrola naplánována ihned po startu počítače.

Ačkoli lze při kontrole za pomoci virových databází virus spolehlivě zničit, tvůrci virů se vždy snaží být o krok napřed v psaní virových softwarů pomocí "oligomorfních", "polymorfních" a stále častěji "metamorfních" virů, které šifrují část sami sebe nebo jinak upravují vlastní kód jako metodu zamaskování před rozpoznáním virovými databázemi. Dalo by se říci, že jde o jakési dynamické mutace klasických virů, které není vždy jednoduché rozpoznat.

Nebezpečné chování

Metoda zjištění nebezpečného chování se oproti virovým databázím nesnaží najít známé viry, namísto toho sleduje chování všech programů. Pokud se takový program pokusí zapsat data do spustitelného programu, antivirus například označí toto nebezpečné chování a upozorní uživatele, který je antivirovým programem vyzván k výběru dalšího postupu.

Výhodu má tento postup zjištění nových virů v tom, že ačkoli je virus zcela nový, neznámý ve virových databázích, může ho snadno odhalit. Nicméně i tato metoda má své nevýhody. Stává se, že antivirový program hlásí spoustu falešných "nálezů" viru. To může mít za výsledek, že uživatel postupem času přestane vnímat ta "pravá" varování. Pokud tedy uživatel automaticky povolí pokračování programu, je jasné, že v takovém případě antivirus neplní dále svoji funkci varovat uživatele před možným nebezpečím. Z tohoto důvodu tento postup stále více moderních antivirových programů využívá méně a méně.

Další metody

Určité antivirové programy používají další typy heuristických analýz. Například se může pokusit napodobit začátek kódu každého nového spustitelného souboru tak, že ho systém vyvolá ještě před přenosem do tohoto souboru. Pokud se program chová tak, že použije "samo-modifikační" kód nebo se jeví jako virus (pokud například začne hledat další spustitelné soubory), můžeme předpokládat, že virus nakazil další spustitelné soubory. Nicméně i tato metoda může hlásit falešné pozitivní nálezy.

Další metoda detekce virů se týká užití tzv. sandboxu. Sandbox, neboli pískoviště, napodobuje systém a spouští .exe soubory v jakési simulaci. Po ukončení programu software analyzuje sandbox, aby zjistil nějaké změny, ty mohou ukázat právě přítomnost virů. Tato metoda může taky selhat a to pokud jsou viry nedeterministické a výsledek nastane za různých akcí nebo akce nenastanou při běhu - to způsobí, že je nemožné detekovat virus pouze z jednoho spuštění.[1]

Existují také antiviry, které varují uživatele před viry na základě toho, jakého typu soubor je.

Perspektivní metoda která si obvykle poradí s malware je tzv. "whitelisting". Spíše než vyhledávání jen známého zákeřného softwaru tato technika předchází spouštění všech kódů kromě těch, které byly již dříve označeny jako důvěryhodný administrátorem (uživatelem). Navíc aplikace v počítači, které jsou označeny jako malware, mají automaticky zakázáno spouštění jakmile nejsou na "whitelist", tedy seznamu povolených programů. Dnes již existuje velké množství aplikací vytvořených velkými organizacemi, které jsou široce používané a "whitelist" je tedy tvořen především administrátory, kteří software rozpoznávají. Možné provedení této techniky zahrnuje nástroje pro automatické zálohy a whitelist procesy údržby.

Historie

Jsou známa konkurenční tvrzení kdo vlastně vymyslel antivirový software. Pravděpodobně první veřejně známé neutralizování rozšířeného viru byla provedena evropanem Berntem Fixem na počátku roku 1987. Bernd Fix neutralizoval takzvaný Vienna virus. Na podzim roku 1988 vznikl také antivirový software jménem Solomons's Anti-Virus Toolkit (vydal Briton Alan Solomon). V prosinci 1990 bylo na trhu už devatenáct jednotlivých produktů ke koupi, mezi nimi také Norton AntiVirus a VirusScan od McAfee.

Tippett vytvořil několik příspěvků k nadějnému řešení detekce virů. Byl to ambulantní doktor, který zároveň vedl počítačovou softwarovou firmu. Po přečtení článku o tom, že

Lehighovy viry byly první, které se vyvinuly, se Tippett zajímal o Lehigha a ptal se, jestli budou mít stejné charakteristiky virů jako ty jež napadají lidi. Z epidemiologického pohledu byl schopen říci, jak budou tyto viry napadat systémy v počítačích (Boot sektor byl zasažen tzv. Brain virem, .com soubory zase Lehigh virem a .com i .exe sobory virem jménem Jerusalem virus). Tippettova společnost Certus International Corp poté začala vytvářet vlastní antivirové softwarové programy. Společnost se prodala v roce 1992 společnosti Symantec Corp., a Tippett pro ně začal pracovat. Včleňováním softwaru vyvinul produkt Symantecu, dnes velmi známý Norton AntiVirus.

Antivirové programy

Avira antivirus – antivirus německé produkce, vydáván v několika verzích včetně FREE verze ke stažení.
ClamAV – antivirový program šířený pod licencí GNU GPL
AVG (antivirový program) – antivirový systém od české firmy Grisoft. AVG prochází různými nezávislými testy, pravidelnými certifikacemi a obdržel řadu významných ocenění.
Norton AntiVirus – produkt firmy Symantec pro domácí uživatele
Symantec EndPoint Security – antivirové a bezpečnostní řešení pro korporátní sféru
ESET NOD32 Antivirus – slovenský komerční antivirový program, který byl magazínem Virus Bulletin již mnohokrát oceněn jako nejlepší antivir
McAfee Antivirus – klasický antivirový produkt
Kaspersky Antivirus – výrobek ruské společnosti Kaspersky Labs
BitDefender – kvalitní antivirový produkt rumunské společnosti SoftWin
avast! – český antivirový program od firmy ALWIL Software. Pro domácí nekomerční použití freeware. Po nainstalování běží 60denní zkušební doba, po které je nutno program zaregistrovat nebo zakoupit. Program pravidelně získává ocenění VB 100% magazínu. Je však i držitelem ocenění SC Magazine, jako jediný zvítězil v obou částech soutěže (soutěž SC awards se dělí na evropskou a americkou část).
Dr.Web – ruský antivirus
AEC TrustPort – český produkt vyznačující se kvalitní detekcí díky kombinaci dvou antivirových produktů
eScan – kvalitní antivirový produkt z Indie
Sophos antivirus
Norman antivirus
F-Secure antivirus
eTrust antivirus
Zoner AntiVirus - český antivirový systém od společnosti Zoner.