Antivirové programy: Co vás skutečně chrání...

Současné virové skenery jsou velmi **KOMPLEXNÍ SYSTÉMY**. K blokování nákazy a útoků na počítač používají různé technologie. Jak efektivní ale ve skutečnosti jsou? Podívali jsme se pod pokličku programům, které uživatelé označují jako „počítačové brzdy“, a prozradíme vám, proč tomu tak je...

ANDREAS MARX

Váš virový skener udržuje vaše nervy neustále napnuté nepochopitelnými varovnými hláškami, častými aktualizacemi a falešnými poplachy – a nakonec se ukáže, že váš počítač byl stejně zasažen nejnovější vlnou virů. Smutná pravda je, že žádný virový skener nenabízí stoprocentní ochranu. I přes tuto skutečnost jsou však všechny „aktuální verze“ nepostradatelnou pomůckou v boji proti počítačovým zločincům.

Souboje s autory virů nebyly nikdy příliš zábavné, ale v současné době je situace ještě horší. Především proto, že většina digitálních parazitů už dávno odrostla „dětským hrám“ typu „veselé nápisy na obrazovce“, které uživatele jen pozlobí. V současnosti jsou jejich nástroje krutými zbraněmi v rukou nelítostných dealerů, které vás mohou stát spousty peněz.

Současné hrozby se od těch starších liší ještě v jednom detailu. Moderní paraziti fungují diskrétně na pozadí, takže uživatel po dlouhou dobu žádnou infekci nepozoruje. Díky tomu mohou autoři malwaru nerušeně „vyčmuchat“ hesla či přístupová data k internetovému bankovnictví či zasílat z počítače uživatele velké množství spamových mailů. Navíc autoři virů očividně své produkty neustále vyvíjejí a výrobci antivirových (AV) řešení se této hry na kočku a myš musí účastnit. To neznamená pouze nekonečné množství signatur, ale také rychlý vývoj nových technologií, aby se dostala armáda virů a podobných hrozeb alespoň zčásti pod kontrolu.

Signatura: „Otisky prstů“ virů

Před dvaceti lety byly virové skenery velice jednoduché programy, které neuměly nic jiného než porovnávat charakteristické řetězce znaků. Skener fungoval na základě příkazového řádku a bez elegantního rozhraní Windows otevřel každý soubor na disketě či na disku a porovnal jeho obsah se známými signaturami (otisky prstů již rozpoznaných virů). Výzkumníci jednotlivých AV společností vytvořili tuto databázi „otisků prstů“ manuálně po komplexních analýzách virů. Pokud se jedna z těchto signatur objevila v prohledávaném médiu, pak byla nahlášena infekce. Výhodou této technologie je skutečnost, že podobné vyhledávací funkce mohou být rozšiřovány téměř libovolně, a pro vyhledávání virů jsou proto důležité i v současné době.

Heuristika: Hlavní pravidla vyhledávání

Nelze však opomenout fatální nevýhodu signatur: skener dokáže najít pouze ty viry, které jsou mu známy – tedy ty, které už byly jednou v laboratoři analyzovány. Proto musela být vyvinuta nová technika, která by si poradila se stále rychleji rostoucím počtem nových virů. Od počátku devadesátých let začaly programy lovit záškodníky pomocí heuristiky. AV nástroje už nevyhledávaly viry jen pomocí přesných signatur specifického viru, ale používaly obecně hledání neobvyklých programových sekvencí.

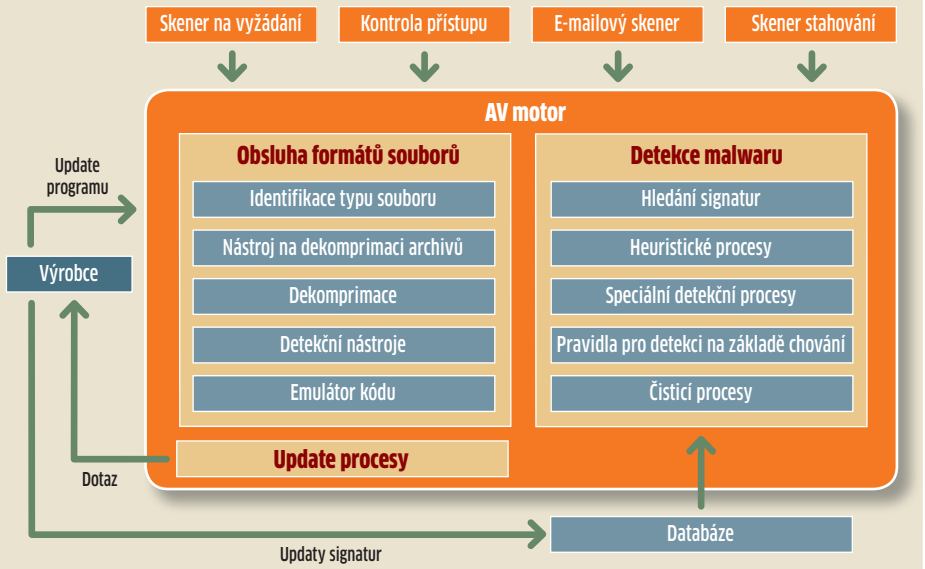
Typický příklad: „Normální“ program se nepokouší vymazat či formátovat disk.

Skenery tedy začaly takovéto funkce hledat v programovém kódu. Avšak i zde lze narazit na určitý stupeň nejistoty, protože i „normální“ programy mohou obsahovat příkazy k mazání souborů, ačkoliv nemají „zlé“ úmysly.

Jako další možnost řešení bylo uvedeno generické vyhledávání viru. Zde je skener „nakrmen“ typickými charakteristikami virů z konkrétní „rodiny“ – ty mohou zahrnovat často používané funkce či obvyklé řetězce znaků. Skener, který je těmito detaily vy-

Struktura virového skeneru

Jádrem virového skeneru je tzv. motor (engine), kterému příslušný skener předává podezřelý soubor. Ve většině případů musí být nejprve „rozbalen“, a až poté ho mohou prozkoumat detekční procesy a případně identifikovat jako malware. Podmínkou dobré detekce je pravidelný update „motoru“ a databází...



baven, pak může snadno ulovit nové varianty škůdce ze stejné „rodiny“.

Emulátory: Testování kódu

Úspěch skenerů byl opět ohrožen po objevení polymorfních virů. Jedním z nejznámějších a nejobtížnějších případů byl v roce 1992 „Tremor“. Autoři viru přišli s nápadem využít výhody skutečnosti, že počítačový program může být navržen celou řadou postupů. Jako jednoduchý příklad lze uvést primitivní sčítání – dvojka může být zadána jako součet dvou jedniček nebo jako podíl osmičky a čtyřky. Můžete dokonce pracovat s derivacemi, integrály a dlouhými komplexními vzorci. A právě to dělá většina zkušených programátorů malwaru až dodnes: konkrétní aktuální škodlivý kód je poté „vypočítán“ při běhu programu.

Pro řešení těchto vzorců a zjištění záměrů škodlivých programů musely antivirové společnosti vyvinout emulátory kódu, které simulovaly úplně každý příkaz programu krok za krokem na virtuálním procesoru ve virovém skeneru. Tímto způsobem mohl být odhalen i ten nejmazanější virus, ale celé toto úsilí stálo spoustu počítačového času a výkonu.

Někteří výrobci – jako například Norman se svým produktem SandBox – šli dokonce tak daleko, že v programu simulovali chování kódu nejen pro vybrané počítačové komponenty, ale také v kompletně vybaveném počítači s diskem, internetovým spojením a operačním systémem Windows. Takové nákladné testy dokáží identifikovat mnohem více malwaru než konvenční metody, ale také vyžadují nesrovnatelně více času…

Jak pracují virové signatury

Základním principem „skenování“ bylo a stále je použití signatur nejrozšířenějších virů.

CHARAKTERISTICKÉ ŘETĚZCE: Nejjednodušší technikou ze všech je detekce na základě statické signatury, jejíž vzorec musí zcela souhlasit se vzorkem uloženým v databázi. Statickou signaturou může být například řetězec „CIH v1.2 TTIT“, který autor viru Win32/CIH (viz obrázek) přidal do svého kódu. Pomocí tohoto řetězce lze tedy identifikovat všechny programy infikované tímto virem.

NÁHRADNÍCI: Vzhledem k tomu, že část výše uvedeného řetězce obsahuje položku 1.2 (což je číslo verze), je možné, že se v oběhu objeví ještě další verze – které budou mít tuto část řetězce jinou. Skener by tedy mohl vyhledávat řetězec „CIH v?.? TTIT“, kde otazníky budou plnit roli „žolíků“ a mohou představovat libovolný znak. Podobné hledání bude mít ale problém v případě verze „1.2a“, kterou bude výše uvedený vyhledávací řetězec ignorovat. Řešení existuje a má následující podobu: CIH v* TTIT“.

Hvězdička v řetězci může zastupovat libovolný počet znaků, a vyhledávácí proces tedy vir objeví nezávisle na jeho verzi. Aby bylo zajištěno, že nepůjde o příliš dlouhý řetězec, lze určit maximální počet znaků, které může hvězdička představovat.

PODROBNOSTI: Po úpravě pravidel by tedy virový skener našel hledaný text i v tomto textu – tedy pokud by ho zde hledal. Pro snížení počtu falešných alarmů a především pro zvýšení rychlosti vyhledávání totiž ukládají AV nástroje do své databáze více podrobností o jednotlivých virech, například jaké typy souborů vir napadá (v našem případě by to byly spustitelné EXE soubory pro Windows) nebo konkrétní část souboru, kterou by skener měl prozkoumat (například začátek souboru nebo posledních 1 024 bajtů).

KONTROLNÍ SOUČET: V našem případě jsme použili velmi krátký řetězec znaků, ale skenery obecně používají řetězec znaků o délce od 32 do 128 bajtů. Ty ale neobsahují přímo textové řetězce, ale určité části virů, které jsou obtížně modifikovatelné. Občas jsou také používány kontrolní součty (například CRC32), které ve srovnání s klasickými řetězci uspoří především místo v paměti…

Typicky – v signatuře se ukládá pouze počáteční bod, délka a samotný kontrolní součet – například:

„od spuštění souboru“, 128 bajtů, „FD CC 34 6F“

Tato sekvence zabere pouze 12 bajtů, místo 32, nebo dokonce 128, které by zabral podrobný popis řetězce. I zde však existuje slabina: stačí, aby se v řetězci znaků změnil jeden bajt, a kontrolní součet nemá žádný efekt.

```
B 69 6C 6C 54 69 6D 65:72 00 55 53 45 52 33 32 : KillTimer USE
E 64 6C 6C 00 00 17 01:77 6E 73 70 72 69 6E 74 : .dll  ‡@wnspr
6 41 00 00 31 00 50 61:74 68 47 65 74 41 72 67 : fA  1 PathGet
3 41 00 00 9E 00 53 48:51 75 65 72 79 56 61 6C : sA  x SHQuery
5 65 45 78 41 00 53 48:4C 57 41 50 49 2E 64 6C : ueExA SHLWAPI
C 00 EB EE 01 5E 10 C6:46 4D 80 EB E5 88 08 88 : l ù¯@^▶ãFMÇùõ
1 C6 00 80 88 08 88 01:C3 97 87 D5 EF 97 87 D5 : ☺ã Çê◘ê☺├ùç¹´
C 0C 44 97 87 D5 EF 97:87 D5 EE C3 00 3A 66 27 : ý¶Dùç¹´ùç¹¯├
3 00 01 00 68 00 40 00:41 00 40 00 32 00 40 00 : $ ☺ h @ A @ 2
3 49 48 20 76 31 2E 32:20 54 54 49 54 00 00 00 : CIH v1.2 TTIT
0 00 00 00 00 00 00 00:00 00 00 00 00 00 00 00 :
```

Rozbalování: Zpátky k originálu

V současné době je mnoho malwarových programů chráněno tzv. „runtime packerem“ – komprimací/dekomprimací v reálném čase. Původně měly tyto nástroje (jako například UPX či WWPack) zajistit, aby programy spotřebovaly méně místa na disku a aby mohly být ihned (například po stažení) funkční. Princip „runtime packerů“ je podobný fungování kompresních programů typu WinZip či WinRAR – ovšem s jedním rozdílem: pro rozbalení a spuštění obsahu už nejsou potřeba externí pomocníci, kteří musí obsah dekomprimovat.

Pro bojovníky proti malwaru má tedy tato technologie nepříjemný důsledek: kompresní proces změní signaturu programu. Výrobci AV programů stáli tedy před novou výzvou.

Ta byla ale mnohem větší, než by se na první pohled zdálo, protože podobných „packerů“ jsou stovky a většina z nich je navíc dostupná v různých verzích a s rozsáhlými možnostmi ovlivňování komprese. Někteří výrobci použili metodu jednoduchého začlenění zapakovaných malwarových souborů do databáze signatur, což se ale neukázalo jako dobrý nápad.

Důvod byl prostý: začalo se objevovat mnoho verzí stejných virových programů, které se lišily pouze v typu „komprimace“. Bylo by tedy nutné pro každou z nich vytvořit novou signaturu...

Jiní výrobci na to šli „od lesa“: nejprve zkusili zrušit „balicí“ proces a poté zkoušeli zkontrolovat skrývající se soubor pomocí obvyklých metod skenu a heuristiky. Nejspolehlivějším způsobem řešení problému „runtime packerů“ je použití emulace kódu. Tato metoda je ale zdlouhavá a náročná, obzvláště tehdy, když musí být simulovány miliony či miliardy operací...

Ve finále se prosadil kompromis: nejoblíbenější a nejčastěji používané „packery“ jsou „podporovány“ zvláštními rutinami ve skeneru, což funguje mnohem rychleji než kódový emulátor.

Aktualizace: Rychlost se počítá

Virové skenery tváří v tvář výzvám „vyrostly“ a postupně se přeměnily do složitých a komplexních nástrojů. Navzdory použití nejnovějších metod, nejpropracovanější heuristiky a používání nejnovějších signatur jsou však autoři malwaru vždy o krok vpředu. Daleko dříve, než nejnovější škůdci přistanou v rukou uživatelů, a mnohem dříve, než se dostanou do laboratoří AV výrobců, je autoři malwaru testují proti co největšímu množství skenerů a sami kontrolují, zda mají šanci je odhalit. Pokud ano, malware je přepsán a nově „zabalen“ – a tento proces je opakován tak dlouho, dokud škůdce nezůstane v utajení před všemi skenery (nebo alespoň před těmi nejrozšířenějšími). Teprve poté je malware vypuštěn a tato snaha by mu měla zajistit komerční úspěch na „černém trhu“. A právě v okamžiku „uvolnění“ začíná závod mezi AV laboratoří (respektive jejími virovými signaturami) a malwarem.

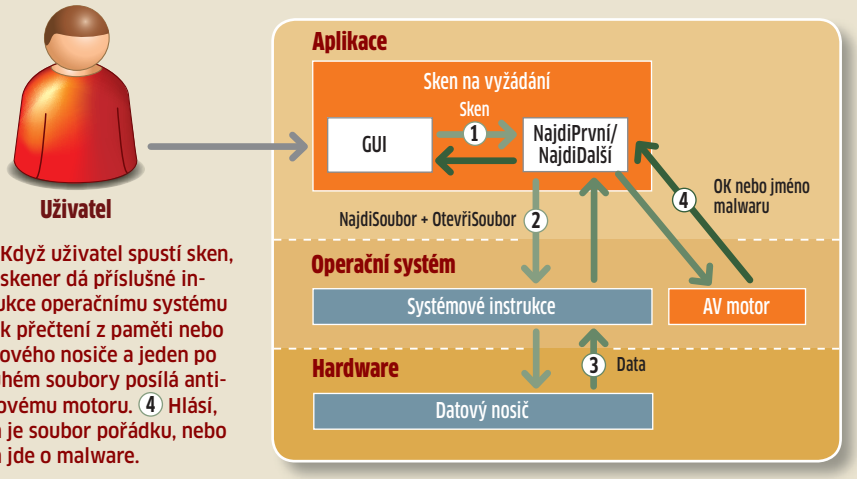
Zajímavé je, že škůdci jsou často naprogramováni a drženi ve skladu a v případě potřeby pravidelně měněni za nové verze, které skenery nedokáží odhalit (a to klidně tisíckrát za den).

Proti této taktice autorů malwaru se AV laboratoře zkouší bránit dvěma rozdílnými technologiemi. Firma Symantec používá ve svých produktech pro rok 2009 tzv. pulzní updaty (známé také jako „streaming definitions“). Tyto definice jsou zaslány uživateli během surfování – každých pět či šest minut dodá laboratoř automaticky nejnovější signatury, které jsou velké pouze 3–5 KB.

„In the cloud scanning“ funguje na odlišném principu: zde lokální počítač zasílá serveru AV společnosti kontrolní součty, nebo dokonce části kódu podezřelých souborů. Na serveru jsou vzorky zkontrolovány, a teprve poté dostane soubor „zelenou“, nebo je vzorek označen jako malware. Obrovskou výhodou této technologie je skutečnost, že na hrozby a virové epidemie lze rychle reagovat a odhalit je téměř okamžitě.

Fungování virového skeneru: Na vyžádání

Při skenování na vyžádání uživatel aktivně vybírá pro kontrolu na obsah malwaru individuální soubory nebo disk v počítači. Své požadavky zadává přes grafické rozhraní antivirového řešení.

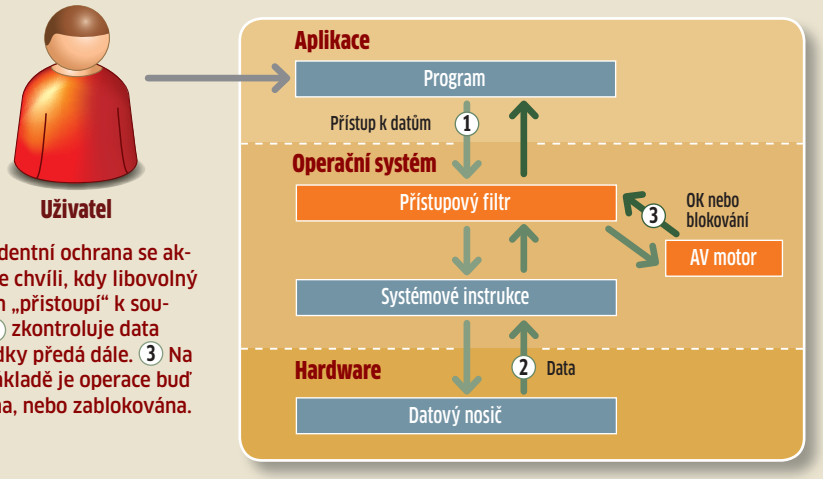


1 Když uživatel spustí sken, 2 skener dá příslušné instrukce operačnímu systému 3 k přečtení z paměti nebo datového nosiče a jeden po druhém soubory posílá antivirovému motoru. 4 Hlásí, zda je soubor pořádku, nebo zda jde o malware.

Proaktivní: Nástroj ThreatFire od firmy PC Tools blokuje software při podezřelých akcích – když mění bezpečnostní nastavení, manipuluje s jinými programy nebo spouští skryté procesy.

Fungování virového skeneru: Rezidentní ochrana

Antivir je stále aktivní „na pozadí“ a pracuje na úrovni operačního systému. V tomto režimu zachycuje všechna data, se kterými pracují aplikace, a kontroluje podezřelé aktivity.



1 Rezidentní ochrana se aktivuje ve chvíli, kdy libovolný program „přistoupí“ k souboru, 2 zkontroluje data a výsledky předá dále. 3 Na jejich základě je operace buď povolena, nebo zablokována.

Je ale jisté, že ne každý uživatel chce, aby „jeho“ antivirová společnost věděla, které programy má nainstalovány či jaké procesy běží na jeho počítači. A to i když jde o „zcela anonymní proces“ a vše je prováděno „nevystopovatelným“ způsobem, jak všichni uživatele ujišťují. Tuto technologii najdete například v nejnovějších produktech pro domácí uživatele od firem F-Secure, Panda a McAfee.

Proaktivní ochrana: Blokujte včas

Ať už se jedná o „pulzní updaty“, nebo o „in the cloud scanning“, obě tyto techniky pouze zkracují čas odezvy – reakce musí vždy následovat. Takže všechny přístupy, které byly doposud představeny, jsou reaktivní, ale nikoliv „proaktivní“. To znamená, že nejsou příliš předvídavé. Řešením je technologie založená na detekci chování (známá také jako „behaviour blocker“), která dokáže odhalit i zcela nové hrozby, které nemohou být odhaleny klasickým způsobem (pomocí signatur). Příkladem mohou být nástroje Norton AntiBot od Symantecu, ThreatFire od společnosti PC Tools nebo DeepGuard od firmy F-Secure.

Příjemným zjištěním je, že i zde jde vývoj mílovými kroky vpřed. První generace těchto nástrojů trpěla některými nepříjemnými vlastnostmi – například kontrolovala pouze jednu „akci“. Mnoho uživatelů bylo také odrazeno častými varovnými hlášeními, podobnými těm od firewallu („Do You Want Application X to Access to Internet?“ nebo „XXX provides server services“). Především proto, že ve většině případů jsou podobná hlášení spíše zmatečná než užitečná – jen málokdo zná interní aplikace Windows a jen zlomek uživatelů je schopen rozpoznat, zda může aplikace X komunikovat s internetem...

Současná druhá generace nástrojů už před jednotlivými akcemi programů nevaruje, ale spíše po určitou dobu kontroluje jejich chování. Během této doby nástroje zaznamenávají jak záporné (potenciálně podezřelé), tak kladné (typické pro „dobré“ programy) body a uživatele varují a aplikaci blokují pouze tehdy, když je překročena nastavená mezní hodnota nebo pokud nastane extrémně kritická (riziková) situace. Obvykle také nekontrolují všechny procesy a všechny zdroje. Systémové procesy Windows, které jsou uvedeny v tzv. whitelistu, stejně jako známé aplikace jsou z kontrol vyňaty.

Vzorce chování: Co je špatné

Opačným extrémem může být například spustitelný program, který se do počítače dostane přes e-mail – ten je považován za potenciálně nebezpečný. Zde však nastupuje na scénu především ochrana pomocí sledování „vzorce chování“ – za podezřelé jsou považovány například následující aktivity:

- po spuštění „exe“ souboru se neobjeví aktivní a viditelné okno;
- program chce ihned zkopírovat něco do systémové složky Windows;
- vytvoření položky v registrech (v sekci Run), aby se program spustil při každém startu systému;
- nástroj se snaží spojit se serverem na internetu.

Jedna akce však „sama o sobě“ není jednoznačným důvodem pro blokování: e-maily ulehčují výměnu dat a někteří uživatelé občas přenášejí i spustitelné soubory. Také spousta hardwarových ovladačů nebo systémových utilit nezobrazuje žádnou informaci na obrazovce, ale funguje diskrétně na pozadí. Některé programy a systémově orientované nástroje se ihned po spuštění zkopírují do systémového adresáře Windows a i neškodný software se často pokouší během instalace vkládat své „spouštěcí“ klíče do registrů. A připojení k internetu? Celá řada programů ho používá ke kontrole nových verzí, doplňků nebo rozšíření...

Ochrana založená na chování jde však dále: blokuje dobré aplikace v tzv. Art Sandboxu a povoluje pouze specifické akce. Tímto způsobem lze systém ochránit i před neznámými útoky, exploity, a dokonce i před tzv. Odays mezerami. Příklad: Aplikace z kancelářského balíku Microsoft Office získává povolení číst a zapisovat soubory DOC a XLS, ale nesmí vytvořit žádné exe soubory na disku. Takové pravidlo spolehlivě chrání před infiltrací systému i přes neznámou „bezpečnostní díru“.

Většina zmiňovaných exploitů pro MS Office funguje ve dvou fázích. Nejdříve využijí díry a podvedou aplikaci pomocí svého programového kódu, který je spustitelný. Tento malý kousek kódu poté na disku vytvoří „velký“ program, který už funguje jako klasický malware.

Dezinfekce: Hluboké čištění

Najít virus je jedna věc, ale vymazat ho je věc druhá. Před několika lety bylo jedním ze zadání skeneru opravit programy poškozené viry. Po komplexní analýze parazita se čisticí příkaz pokoušel vrátit změny, které byly v infikovaném souboru učiněny. Obvykle to fungovalo tak, že antivir zkopíroval originální kód programu zpátky na původní místo nebo zkrátil soubor, aby odstranil virový kód na konci programu. Dnes máme většinou co činit s trojskými koni a červy fungujícími nezávisle na dalším softwaru a s viry nepoškozujícími jiné programy. K dezinfekci většinou stačí smazat malwarové soubory, které byly nalezeny (na disku a paměti), a vrátit zpět změny, které škůdce napáchal v registru. Proto virové skenery nejdříve spustí obecnou čisticí rutinu, kterou většina malwaru „nepřežije“. Pokud základní čištění nestačí, mohou vývojáři antiviru vytvořit pro specifické účely zvláštní dezinfekční rutiny.

Dobře opevněný malware: Tvrdý oříšek

Jakmile jednou malware vnikne do systému a stane se aktivním, má mnoho možností, jak

se bránit. Jednou z možností je nainstalovat do systému rootkit, který pak dokáže manipulovat s přístupem k souborům či registrům. Funguje to takto: Pokud se objeví dotaz s odkazem na malware, rootkit vrátí chybné hodnoty, aby existenci malwaru zamaskoval. Tak se malware stane neviditelným (tzv. stealth malware). S těmito škůdci se dokáží vypořádat pouze zvláštní nástroje, které pečlivě zkoumají paměť a pomocí speciálních postupů i disk. My doporučujeme program Gmer, který patří v oblasti „stopování aktivních rootkitů" ke špičce. Kromě toho doporučujeme občasné skenování systému pomocí tzv. „recovery média" (například takového, které najdete na našem DVD).

Existují ale i jiné metody, kterými dokáže malware ztížit antivirovým nástrojům práci. Například je nepříjemné, pokud má malware agresivní ochranu a zůstává neustále aktivní v paměti. Dokáže simultánně spustit procesy, které se navzájem kontrolují – jestliže jeden z procesů ukončíte, druhý okamžitě spustí jeho náhradníka. Klasickým příkladem této techniky je červ Win32/Sober se svými prostředky „osobní ochrany". V jeho případě nepomáhá odstranění procesů pomocí příkazu „kill" – nejprve je nutné je „uspat" příkazem „suspend".

Vývoj se na straně malwaru bohužel nezastavil, a tak jsou nejnovější škůdci schopni útočit na antivirové nástroje nebo blokovat jejich aktualizace. Existují i specializované nástroje bránící nainstalování nového antivirového programu, nebo dokonce i návštěvě webu antivirové firmy. V tomto případě je jediným řešením použití „záchranného CD" a odstranění škůdců po nabootování čistého systému.

Bezpečnostní balíky: Komplexní ochrana

Jádrem internetového bezpečnostního balíku je virový skener. Balíky však obsahují ještě další komponenty, které dokáží zabránit malwaru v usídlení v systému uživatele. Mezi ně patří například osobní firewall, který filtruje datový tok a rozpoznává podezřelé pakety (a blokuje je, ještě než dorazí k cílové aplikaci). Také spamové filtry pouze nefiltrují reklamu v příchozí poště, ale odstraňují velkou část zavirovaných e-mailů – dokonce i pokud pro ně prozatím nejsou k dispozici virové signatury. Další komponenty blokují pomocí URL filtru podezřelé webové stránky a tak zabraňují uživateli v přímém kontaktu s malwarem. Jiné komponenty zase dokáží uživatele varovat před stránkami s tzv. exploity, které umí malware dostat na počítač uživatele pouhým otevřením nakažené stránky.

Virový skener je tedy jen malou částí ve velké bezpečnostní skládačce a výrobci antivirů jsou nuceni nalézat stále lepší metody, jak ochránit uživatele před novými nebezpečími z internetu.

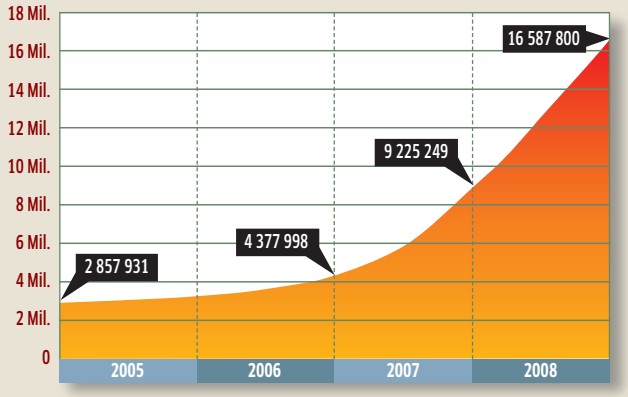
Uživatelé by ale neměli zapomínat, že virové skenery nebo bezpečnostní balíky jsou v boji proti malwaru jen pomocníky. Zdravý rozum a s ním související chování na síti (co bys nedělal v běžném životě, rozhodně nedělej ani na internetu) spolu s pravidelnou kontrolou operačního systému a používaných programů jsou základními kameny zabezpečení každého počítače. S ochranou a kontrolou zmiňovaných oblastí vám může pomoci například nástroj Personal Security Inspector od společnosti Secunia, který jsme vám již několikrát nabídli na našem DVD.

Je pochopitelné, že ani kvalitní bezpečnostní programy nejsou všemocné – a pokud jsou vaše nezazáplatovaná Windows děravá jako ementál a na základě „zaručené" e-mailové zprávy od kolegy jste se rozhodli (při vypnutém antiviru) nainstalovat skvělý přehrávač videí, pak jsou vaše počítače odsouzeny k porážce.

AUTOR@CHIP.CZ

Virová exploze

Malwarová kolekce testovací laboratoře AV-Test.org obsahuje všechny viry, které se objevily – a jejich počet rapidně vzrůstá.



ZDROJ: AV-TEST.ORG

Řetězová reakce: Příčina falešných poplachů

Výrobci antivirových programů pracují pod extrémním tlakem. Jejich programy musí rozpoznat obrovské množství nového malwaru, jehož počet se každý den rapidně zvyšuje. Zároveň se ale musí snažit o co nejmenší počet falešných poplachů, které brzdí operační systém a otravují uživatele.

Důvodem, proč virové skenery stále přináší falešné poplachy, jsou špatně zvolené nebo příliš obecné virové signatury. Častokrát se stane, že kvůli vyšší rychlosti skenování není signatura vytvořena pro „rozbalený" malware, ale jen pro komprimované soubory nebo pouze pro „instalační" data malwaru. Díky tomu je pak možné, že virové signatury nebudou odpovídat pouze malwaru, ale i „dobrému" programovému kódu určenému pro obecné „rozbalení" programu v paměti.

Podobná situace je o to nepříjemnější, že se může stát, že mohou být jako „malware" označeny všechny programy používající podobné „baliče". Bohužel také platí, že prakticky žádný výrobce antivirových programů není v současné době schopen individuálně prozkoumat všechny soubory proudící do jeho laboratoře.

Jen ve výjimečných případech je také na základě jednoho konkrétního souboru automaticky vytvořena signatura a přidána do databáze. Experti tento proces nazývají „VirusTotal fenomén", podle virového skeneru stejného jména (viz obrázek). Výrobci AV programů tedy občas bez náročného testování spoléhají i na výsledky jiných programů. Ale pokud se objeví falešný poplach, zjištěné výsledky se promítnou do produktů až po nějaké době (obvykle až se problém vyhrotí), a teprve poté dojde k odstranění jeho příčin...