Nejrychlejší antiviry

Udeří-li nový virus, jsou dnešní skenery často příliš pomalé. Škůdce totiž dokážou odhalit až po aktualizaci signatur, tedy v lepším případě teprve po několika hodinách. To má změnit nová **ANTIVIROVÁ SUPERZBRAŇ:** analýza založená na chování viru. Chip novinku otestoval. VALENTIN PLETZER

Vkradou se k vám jako nepolapitelné e-maily, pomocí podvržených webových stránek nebo zmanipulovaných downloadů si podmaní váš počítač – počet virů, trojských koní a jiného malwaru dramaticky narůstá. Vloni se podle údajů bezpečnostní laboratoře AV-Test objevilo skoro 5,5 milionu nových škodlivých souborů. Pětkrát více než ještě v roce 2006 – a měsíčně tolik, kolik škůdců přibylo za celý rok 2005!

Této záplavě teď výrobci antivirového softwaru chtějí čelit novou zbraní: analýzou vycházející z chování záškodníka. Nové speciální nástroje mají maligní programy rozpoznat podle jejich počínání, a ne jen podle vzhledu, signatury nebo statické heuristiky (viz rámeček). Důvod pro vznik nové strategie antivirových specialistů je zřejmý: exploze malwaru v loňském roce ukazuje, že autoři virů se pokoušejí přelstít skenery stále rychleji se šířícími variantami svých zvrhlých výplodů. Než pak bezpečnostní firma stačí reagovat, už je na světě jiná verze škůdce.

Chip nyní testoval, zda nová zázračná zbraň skutečně přináší něco pozitivního. Co totiž člověku připadá snadné, to se musí počítač teprve naučit.

Malý příklad: Jestliže nějaký program bez ověřovacího dotazu manipuluje s bezpečnostními nastaveními Windows, jde s poměrně velkou pravděpodobností o malware. Pokud však program taková nastavení mění na přání uživatele, mohlo by se také jednat o tuningový nástroj. Rozlišit takové případy je velice nesnadný úkol, kterého se analytické nástroje musí úspěšně zhostit.

Rozpoznání chování: Nový prostředek v arzenálu lovců virů

K našemu testu jsme do laboratoře poslali osm moderních bojovníků proti virům. Kde to bylo možné, šlo o nové nástroje, které sázejí výhradně na metodu analýzy chování. Většina výrobců však novou zbraň zařadila do svého stávajícího arzenálu – jako doplněk k tradiční heuristice a identifikaci signatur. Rozhodli jsme se proto v testu zohlednit jen ty výsledky, které přinesla analýza chování. To pro nás byla opravdová výzva, neboť u kompletních řešení se neustále za-

Nebezpečí zažehnáno: I bez jakékoli signatury poznal Norton AntiBot hrozbu a podezřelý soubor zablokoval.

Dosud: Tak dlouho jste museli čekat na nové signatury virů

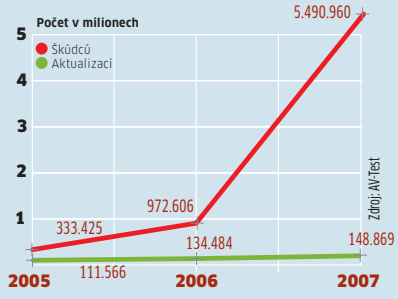
Nyní: Analýza chování reaguje takřka okamžitě

ZÁVĚR

Odhalit neznámé viry jen podle jejich počínání není vůbec snadné. Mnozí výrobci proto ještě mají s touto technikou problémy: většinou jejich skenery obviní příliš mnoho podezřelých, nebo naopak příliš málo. V tomto směru se programy musí rozhodně polepšit. Co všechno nová metoda dokáže, to ukazuje vítěz našeho testu, Norton AntiBot.

PŘÍVAL ŠKŮDCŮ

Objem malwaru exponenciálně stoupá, databanky signatur nestačí držet krok.



INFO

SIGNATURA

Záškodnické programy jsou i dnes z valné části odhalovány touto metodou. Ta má tu přednost, že podobně jako u otisků prstů je test rychlý a jednoznačný. Ovšem čím více signatur je v databance uloženo, tím déle kontrola trvá. Proto nyní výrobci antivirů pro rozpoznání malwaru hledají nové cesty.

HEURISTIKA

Programátoři virů nepíší pokaždé úplně nový kód, často se škodlivé programy liší jen v detailech. Rozpoznat tyto podobnosti je právě úlohou heuristiky. Jestliže nějaký soubor obsahuje například rutinu pro infikování souborů, s největší pravděpodobností jde o virus.

ANALÝZA CHOVÁNÍ

Podobně jako u heuristiky je úkolem analýzy poznat neznámý malware. Namísto vyhodnocování statických charakteristik zde však antivirový program sleduje chování softwaru. Podezřelé programy jsou pak obratem zablokovány. Na rozdíl od porovnávání signatur však v tomto případě už musí být škůdce v činnosti.

pojovala i signatura nebo firewall (viz tabulka), které bylo třeba odfiltrovat.

Časová osa s čekacími dobami na virové signatury (dole) ukazuje, jak je důležité odhalit diverzanta i bez signatury. Platí to zejména pro ty kandidáty, kteří na aktualizaci signatur potřebují delší dobu. Například Kaspersky dodá update velmi rychle a díky tomu není na analýzu chování tolik odkázán. Naproti tomu firmy jako Symantec, u nichž to trvá déle, mají více důvodů sázet na novou metodu.

Viděno z tohoto zorného úhlu pak není překvapením jasný vítěz v rozpoznávání chování: Norton AntiBot. Technologie, kterou před rokem koupil Symantec od Sana Security, se evidentně osvědčuje. Stoprocentní rozpoznání jako AntiBot dokázal v testu už jen Mamutu.

Jak užitečné by bylo kombinovat tradiční a nové technologie, to ukazuje další účastník ze stáje vítěze testu: Norton AntiVirus pracuje ještě s technologií vyvinutou samotným Symantecem. V testu sice vyhlásil poplach u 80 % všech hrozeb, ale jen ve 35 % si byl software skutečně jist a vetřelce zablokoval. Ještě horší je, že pouze 20 % útočících virů bylo ihned vyhodnoceno jako natolik nebezpečných, že byly automaticky odstraněny.

Ostatní kandidáti zde byli vesměs svědomitější. Tak například Prevx odhalil rovněž 80 % škůdců a 65 % ihned zlikvidoval. Nebo třeba nástroj Safe'n'Sec: 75 % identifikoval ihned, pouze u jednoho útočníka si musel vypomoci dotazem. Kéž by se takovým poměrem mohli pochlubit všichni výrobci!

Zdroj: AV-Test

CHIP PLNÉ VERZE

Na Chip DVD tentokrát najdete i dva programy z kategorie „proaktivní ochrany“ zdarma. O netradiční zabezpečení dat před útoky škodlivého softwaru se postará Safe'n'Sec, který chrání soubory před manipulací nedůvěryhodnými programy. Komplexní zabezpečení nabídne program Kaspersky Internet Security…

KASPERSKY INTERNET SECURITY 7.0 CZ

- ► Win 2k/XP/Vista
- ► licence 31.12.2008
- ► www.kaspersky.cz

SAFE´N´SEC PERSONAL 2.5

- ► Win 2k/XP/Vista
- ► On-line registrace
- ► www. safensoft.com

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **ODBLOKOVÁNÍ VIRŮ.**

Bezpečná Windows jsou pomalejší

Falešné poplachy: Příliš ostrá nastavení vadí systému i programům

Existují však dobré důvody pro to, aby antivirové programy nevymazávaly hned všechno, co považují za nebezpečné. Analýza chování je totiž dosud poměrně často příliš podezřívavá. Dokazuje to zkouška falešných poplachů: tak špatné výsledky jsme u obvyklých testů signatur nikdy nezaznamenali. Za problematický výsledek se zde považuje už více než jedno promile.

Kdybychom tuto laťku nasadili u metod analýzy chování jako jediné kritérium, většina kandidátů by zcela propadla. Tak třeba Mamutu od firmy Emsi Software, nástroj, který se pyšní stoprocentním rozpoznáním, diskvalifikovalo 70 % falešných hlášení – přes polovinu domnělých nebezpečí nástroj navíc ihned zablokoval. Jenom Norton AntiBot a AntiVirus 2008 firmy F-Secure se nenechaly znervóznit a nevyvolaly jediný falešný poplach. Pro AntiBot to spolu s 90 % bezprostředně zablokovaných škůdců znamenalo jasné vítězství v testu. Zbývá jen doufat, že Symantec technologii AntiBot co nejdříve integruje do všech svých produktů.

Tato přídavná ochrana však nemá jen pozitivní stránky: antivirový software musí být v tomto případě neustále aktivní – jinak by chování softwaru v počítači nemohl trvale zkoumat. To samozřejmě stojí systémové prostředky. Ve sporných případech tolik, že uživatel už nemůže plynule pracovat – a nakonec ve stresu nástroj deaktivuje. Nicméně v testu jsme nemohli zatížení systému srovnatelným způsobem hodnotit. Testovací pole je totiž příliš různorodé. Postavit proti sobě kompletní bezpečnostní řešení a štíhlé speciální nástroje by nebylo fér. Přesto jsme měřili alespoň obsazení operační

CENOVÝ TIP 07/2008
VÍTĚZ TESTU 07/2008

PŘEHLED	1. MÍSTO	2. MÍSTO	3. MÍSTO	4. MÍSTO	5. MÍSTO	6. MÍSTO
Produkt	**Norton AntiBot**	**F-Secure Antivirus 2008**	**PrevX 2.0**	**Safe´n´Sec Personal Pro**	**Kaspersky Anti-Virus 7.0**	**Mamutu**
Cena (cca)	30 eur	1 200 Kč	20 eur	900 Kč	1 100 Kč	20 eur
Internet (www.)	symantec.com	f-secure.com	prevx.com	safesoft.com	kaspersky.com	emsisoft.de
Počet licencí	3	1	1	1	1	1
Hodnocení zabezpečení	95	80	77	76	71	68
	■■■■■	■■■■□	■■■■□	■■■■□	■■■□□	■■■□□
Zabezpečení						
Rozpoznávání podle chování	**100 %**	50 %	80 %	75 %	20 %	**100 %**
Rozpoznávání podle signatur	0 %	30 %	0 %	0 %	20 %	0 %
Jiná hlášení (např. od firewallu)	0 %	0 %	0 %	0 %	30 %	0 %
Celkem: rozpoznáno	**100 %**	80 %	80 %	75 %	70 %	**100 %**
Celkem: rozpoznáno a zablokováno	**90 %**	60 %	65 %	70 %	65 %	85 %
Celkem: rozpoznáno, zablokováno a odstraněno	70 %	50 %	65 %	50 %	40 %	70 %
Falešných poplachů / zablokováno	**0 % / 0 %**	**0 % / 0 %**	30 % / 10 %	40 % / 0 %	10 % / 10 %	**70 % / 40 %**
Výkonnost						
Doba bootování* (Vista a antivirus)	47 sekund	70 sekund	40 sekund	45 sekund	39 sekund	34 sekund
Obsazení operační paměti „private bytes“ (exkluzivně vyhrazeno)	30 MB	160 MB	104 MB	42 MB	55 MB	17 MB
Obsazení operační paměti „working set“ (podle Správce úloh)	46 MB	69 MB	17 MB	10 MB	9 MB	34 MB
Ergonomie						
Srozumitelnost hlášení poplachu	velmi dobrá	velmi dobrá	dobrá	dobrá	dobrá	dobrá
Podrobnější nápověda	detailní informace jen anglicky	všechny informace jen anglicky	směs anglických a německých zpráv	téměř žádná	zčásti i německá nápověda	všechny informace v němčině
Konfigurovatelnost	málo voleb	mnoho expertních voleb	mnoho expertních voleb	mnoho expertních voleb	mnoho expertních voleb	mnoho expertních voleb
Přídavné funkce	–	mj. HTTP skener	–	–	mj. HTTP skener	–

Špičková třída (100–90) Vyšší třída (89–75)
Střední třída (74–45) Nelze doporučit (44–0)
Všechna hodnocení v bodech (max. 100)

● ano – ne
údaj nejlepší údaj
údaj nejhorší údaj

* čerstvá instalace Visty: 30 sekund

paměti a zpoždění při nabíhání Windows. Podle tabulky se tak každý může rozhodnout, co je pro něj důležitější.

Pro srovnání: Náš testovací počítač, s čerstvě nainstalovanou Vistou, nabíhal bez přídavného softwaru v průměru za 30 sekund. To se s prvním bezpečnostním softwarem prudce mění. Nejnevinnější je v tomto ohledu Mamutu, který spuštění Visty zdrží o čtyři sekundy. Doby nabíhání po instalaci jiných účastníků testu se pohybovaly mezi 39 a 49 sekundami. Jediným výstřelkem je F-Secure AntiVirus – s ním Vista startovala neuvěřitelných 70 sekund.

Nástroj od F-Secure se příliš nevyznamenal ani ve využívání operační paměti: 160 MB vyhrazených jako „private bytes" – exkluzivně obsazené části paměti – je jednoznačně příliš mnoho!

Ergonomie: Některé bezpečnostní nástroje matou odborným slangem

Nechme ale stranou výkonnostní problémy: ať už je bezpečnostní nástroj jakkoli rychlý a štíhlý, teprve když s ním uživatel dokáže bez problémů zacházet, se ukáže, nakolik je skutečně platný. Až příliš často totiž vynervovaní uživatelé vystavují svůj počítač vážnému nebezpečí tím, že bezpečnostní program prostě vypnou.

Co do uživatelské přívětivosti totiž mají někteří výrobci ještě co dohánět. To se týká především varovných zpráv. Právě výsledky analýzy chování bohužel příliš často obsahují pro laiky bezcenné informace. V horších případech to může mít i efekt známý z osobních firewallů: uživatel je konfrontován s fakty, jimž nerozumí – a místo aby si ujasnil důsledky, odpovídá pak na každý dotaz automaticky „Ano – blokovat" nebo „Ne – pokračovat".

A co horšího: chce-li uživatel získat další informace, a klikne proto na tlačítko podrobnější nápovědy, téměř pokaždé skončí na nějaké anglickojazyčné webové stránce. To je problém i při dobré znalosti angličtiny – narazí tam na spoustu technických detailů, jimž by těžko rozuměl i v mateřštině.

To, že uživatelská přívětivost není pro výrobce virových skenerů cizím slovem, dokazují ovládací plochy a nabídky všech testovaných produktů – přinejmenším dokud není aktivován režim pro odborníky. Pak už jsou pro smysluplná nastavení zapotřebí jisté předběžné znalosti. Naštěstí jsou přednastavené parametry vesměs zvoleny docela dobře. Zbývá už jen doufat, že se všem výrobcům podaří zabudovat do svých bezpečnostních souprav tak dobrá řešení, jako je AntiBot.

AUTOR@CHIP.CZ

	7. MÍSTO	8. MÍSTO
	Norton Antivirus 2008	Panda Antivirus + Firewall 2008
	950 Kč	1 500 Kč
	symantec.com	pandasecurity.com
	1	3
	68	58
	■■■□□	■■□□□
	10 %	45 %
	20 %	0 %
	50 %	0 %
	80 %	45 %
	35 %	15 %
	20 %	0 %
	0 % / 0 %	20 % / 0 %
	42 sekund	49 sekund
	60 MB	80MB
	8MB	101MB
	velmi dobrá	velmi dobrá
	detailní informace jen anglicky	detailní informace jen anglicky
	několik expertních voleb	mnoho expertních voleb
	mj. firewall, ochrana browseru	mj. firewall, ochrana browseru

SOUHRN_ROZPOZNÁVÁNÍ MALWARU

RADY PRO NÁKUP

KOMBINOVAT

Pokud už používáte nějaký virový skener nebo bezpečnostní soupravu, nemusíte tyto prostředky odinstalovat. Raději svůj ochranný software zkombinujte s nástrojem, jakým je například vítěz našeho testu.

UPGRADOVAT

Bezpečnostní software vždy zatěžuje systém počítače. Vyhrazuje si pro sebe operační paměť a odčerpává drahocenný výkon procesoru. Zejména uživatelé, kteří právě přestoupili na Vistu, by měli tyto skutečnosti uvážit a pokud možno posílit své hardwarové vybavení.

PŘEDEM VYZKOUŠET

Mnohé produkty poskytují velmi detailní informace, jiné se zase zaměřují spíše na začátečníky. Zda vám bude nějaký nástroj vyhovovat, to poznáte vyzkoušením demoverze.

VÍTĚZ

NORTON ANTIBOT

Nejvyšší počet rozpoznaných škůdců a žádné falešné poplachy: to v našem testu dokázal jen Norton AntiBot. Zatímco jeho konkurence je nastavena příliš ostře nebo pracuje příliš nepřesně, tento software se žádných chyb nedopustil. V současnosti je Norton AntiBot samostatný program. Znamená to, že jej do předem nainstalovaných bezpečnostních produktů Symantecu nelze integrovat „beze švů". Jeho výhodou však je, že se dá takřka libovolně kombinovat s programy jiných výrobců.

CENA: 30 eur

JAK CHIP TESTUJE

Ve spolupráci s virovou testovací laboratoří AV-Test (www.av-test.org) jsme zkoušené skenery podrobili tvrdému testu. Tentokrát jsme se chtěli dozvědět jenom to, jak dobré je rozpoznávání malwaru na základě jeho chování – výkonnost ani ergonomii jsme do bodového hodnocení nezahrnuli.

ZABEZPEČENÍ: Programy musely poznat 20 aktivních škodlivých programů, zablokovat je a odstranit, a kromě toho deset normálních aplikací nechat bez povšimnutí. Poněvadž u skenerů často není možné vypínat jejich jednotlivé komponenty, v testovacím protokolu bylo vždy poznamenáno, jakou technikou (signatury nebo rozpoznávání podle chování) byl malware odhalen. Pouze výsledky testu analýzy chování určily výsledné pořadí.

VÝKONNOST: Nakolik virové skenery zdržují náběh Windows? Kolik operační paměti si nárokují? Ani ten nejlepší bezpečnostní software není nic platný, jestliže jej uživatel kvůli zrychlení práce vypne.

ERGONOMIE: Poněvadž ani profesionálové nedokázali vysvětlit mnohá varovná hlášení, zajímala nás i srozumitelnost zpráv. Kromě toho jsme sledovali, jak přehledné a podrobné jsou u skenerů nabídky funkcí a volby nastavení.