Útok viru! Co dělat?

Myslíte si, že máte svůj počítač dokonale chráněný? Žádný bezpečnostní program vám nezaručí stoprocentní ochranu před spywarem, červy, trojskými koni a nebezpečnými rootkity. Chip otestoval **DVACET ANTIVIROVÝCH NÁSTROJŮ** a může vám prozradit, které stojí za investování. Jako bonus jsme přidali i přímé srovnání s několika bezplatnými nástroji.

CLAUDIO MÜLLER

Sedíte u počítače a surfujete po internetu nebo píšete e-mail. Najednou se stane něco divného. Právě používaný program se zhroutí, spustí se Internet Explorer s neznámými WWW stránkami a počítač se několikrát za sebou restartuje. Zdá se, jako by váš počítač ovládal někdo jiný. A tak tomu i skutečně je: do vašeho počítače se vloudil malware a internetová mafie si z něj pomocí několika triků udělala zombie „na dálkové ovládání“. Nejhorší je, že náznaky napadení poznáte pouze tehdy, když hacker zanedbá maskovací techniky. Opravdu nebezpečné trojské koně a rootkity dokáží dokonale maskovat svou přítomnost – jedině tak mohou bez obtíží pracovat a mít neustálý přístup k vašim důležitým datům.

Myslíte si, že se vás výše uvedené problémy netýkají? Máte ve svém počítači antivirový nástroj a předpokládáte, že vám poskytne kvalitní ochranu před hrozbami z internetu? My vám prozradíme, zda tomu tak skutečně je...

Otestovali jsme téměř dvacet nejznámějších virových skenerů a vyzkoušeli jsme, zda dokáží odhalit jak neaktivní, tak nainstalované škůdce, a především zda je dokáží odstranit.

To, že situaci se nevyplácí podceňovat, napovídají i aktuální údaje: virové laboratoře každý měsíc odhalí více než milion nových škůdců. V této kritické době odborníci odhadují, že přibližně 40 procent antivirových skenerů nemá aktuální signatury.

Kromě toho, že jsme otestovali skupinu antivirů, jsme pro vás na DVD připravili také balík bezpečnostních nástrojů, které dokáží váš počítač zabezpečit.

Pokud chcete rychle zjistit, zda je váš počítač napaden, můžete využít internetové „on-line“ antiviry, případně speciální bezpečnostní nástroje, o kterých jsme se zmiňovali v minulém čísle Chipu. V krajním případě lze také použít specializované bezplatné nástroje z dílen antivirových firem, které dokáží odhalit určitou skupinu škůdců.

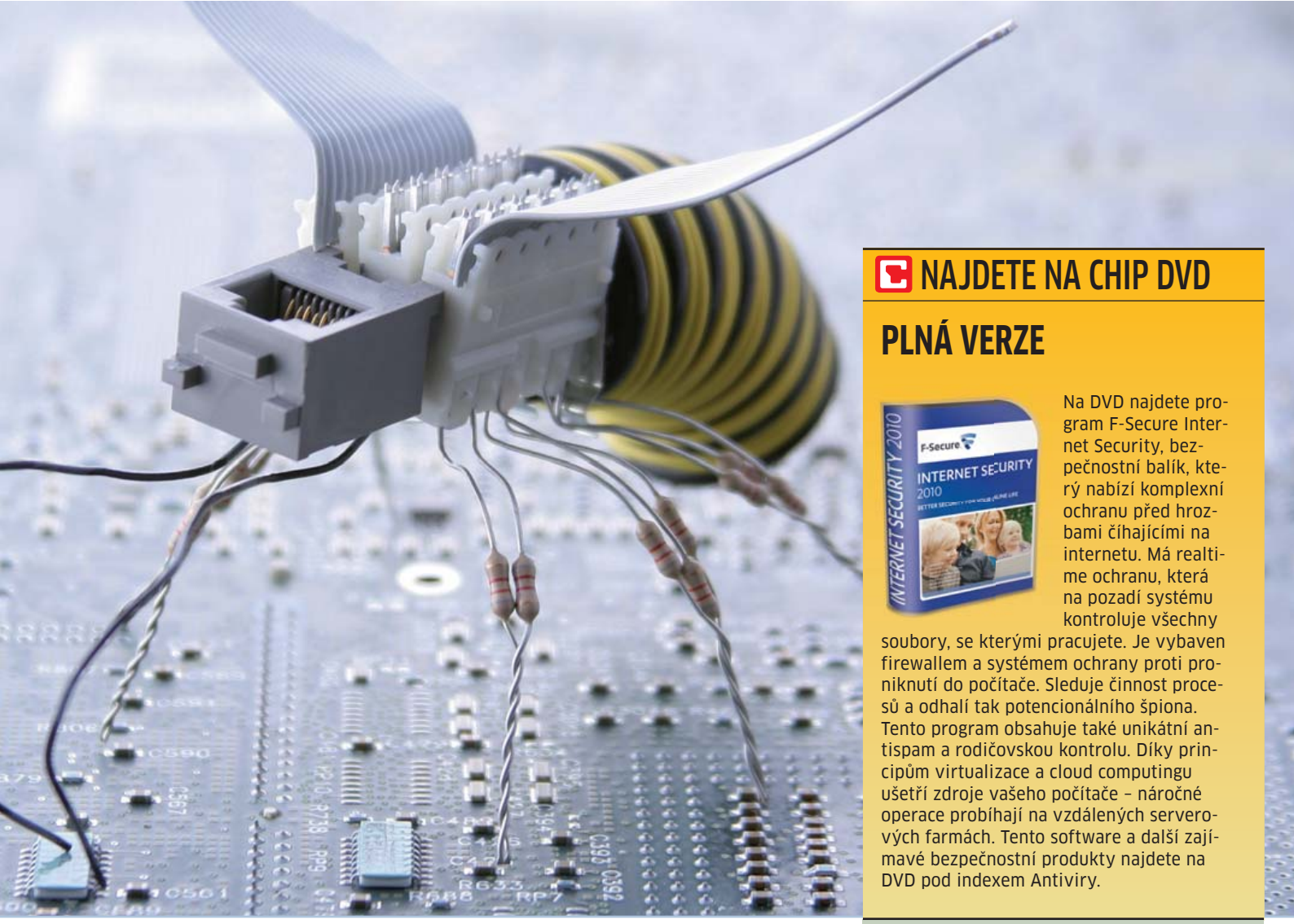
Pokud ale zjistíte, že je váš počítač napaden, doporučujeme co nejrychlejší akci k minimalizaci škod napáchaných malwarem. K jeho odstranění můžete například použít antiviry z našeho testu – stačí si jen vybrat ty nejlepší...

Bezpečnostní hlídka: Malware bez šance

Experti z laboratoře „AV-test“ nainstalovali na počítač deset virů, které reprezentují různé používané techniky: spyware krade hesla, trojské koně stahují malware z internetu, červi se šíří přes e-mail a rootkity se skrývají a zavrtávají se hluboko do systému. Dobrý antivirový nástroj si dokáže poradit se všemi zmiňovanými hrozbami. Musí nabídnout rychlou detekci a bezproblémové odstranění. A právě identifikace a eliminace jsou kritéria, která hrají v našem hodnocení rozhodující roli – tentokrát nebereme příliš ohled na spotřebu systémových zdrojů a uživatelskou přívětivost.

Opět vítěz: Stejně jako v předchozích testech potvrdil nástroj od Symantecu, že patří mezi absolutní špičku...

FOTO: ISTOCKPHOTO/LUCA DI FILIPPO



NAJDETE NA CHIP DVD

PLNÁ VERZE

Na DVD najdete program F-Secure Internet Security, bezpečnostní balík, který nabízí komplexní ochranu před hrozbami číhajícími na internetu. Má realtime ochranu, která na pozadí systému kontroluje všechny soubory, se kterými pracujete. Je vybaven firewallem a systémem ochrany proti proniknutí do počítače. Sleduje činnost procesů a odhalí tak potencionálního špiona. Tento program obsahuje také unikátní antispam a rodičovskou kontrolu. Díky principům virtualizace a cloud computingu ušetří zdroje vašeho počítače – náročné operace probíhají na vzdálených serverových farmách. Tento software a další zajímavé bezpečnostní produkty najdete na DVD pod indexem Antiviry.

INFO

Virové skenery na internetu

Nechcete na svůj disk instalovat žádný nástroj? Pak je pro vás nejrychlejším způsobem, jak zjistit, zda je váš počítač nakažen, použití internetového skeneru. Práce s ním je snadná a obvykle bezproblémová – jediným zádrhelem může být požadavek v podobě Internet Exploreru, ale nástroje od firem F-Secure nebo Eset fungují i v konkurenčním Firefoxu. Pokud potřebuje zkontrolovat samostatný soubor, nahrajte ho na server VirusTotal, kde ho zkontroluje 41 různých antivirových motorů.

http://housecall.trendmicro.com

http://security.symantec.com

www.bitdefender.com/scanner/online/free

www.f-secure.com/en_EMEA/security

www.kaspersky.com/virusscanner

www.pandasecurity.com/activescan

www.virustotal.com

V ideálním případě dokáže antivirový program identifikovat a „chytit“ malware dříve, než se nainstaluje do počítače. Z tohoto důvodu máme připravenu databázi s 3 194 nejrozšířenějšími škůdci, díky které můžeme otestovat schopnost detekce jak na základě signatur, tak i pomocí heuristické analýzy. Účastníci testu také museli nejprve detekovat neaktivní malware pomocí skeneru, podruhé se pokusit zabránit malwarovému útoku na počítač pomocí „strážce“ na pozadí. Většina programů se s naší „výzvou“ vypořádala výborně – více než polovina programů nenechala „projít“ ani jeden vir. Na druhou stranu nás ne zrovna příjemně překvapily obranné výkony nástroje firmy Ashampoo (jeho skener však pracuje bezchybně). Zdaleka nejhorší výkony předvedl bezplatný nástroj ClamWin: „nevšiml“ si více než 500 virů a jeho funkci lze za „ochrannou“ označit jen s velkou nadsázkou...

Komplexní sken: Hledání aktivních útočníků

Po této optimistické detekci jsme se dostali k druhé části testu, a s ní přišlo i trpké vystřízlivění: nástroje se měly pokusit počítač od škůdců vyčistit...

Rozhodující pro nás bylo to, zda antivir dokáže eliminovat všechny komponenty malwaru (například procesy nebo spustitelné soubory). To je důležité, protože například pokud zůstane na počítači „installer“ malwaru, může být vir znovu kdykoliv aktivován. Jediným řešením je tedy kompletní smazání všeho, co s malwarem souviselo – od „zbytků“ po instalaci až po položky v registrech.

Smutné je, že žádný z nástrojů nedokázal dosáhnout plného počtu bodů, nicméně alespoň trochu optimismu přidá skutečnost, že více než polovina testovaných produktů dokázala všechny připravené škůdce změnit na neškodný „odpad“. Norton Antivirus, eScan od firmy MicroWorld a Spyware Doctor dokonce dokázaly kompletně eliminovat čtyři z pěti virů. Největším překvapením to bylo v případě nástroje Spyware Doctor, jehož skenovací nástroj dosáhl v oblasti detekce nenainstalovaného malwaru druhého nejhoršího skóre (98,31 procenta). V případě bezplatných nástrojů dokázala jen Avira eliminovat všech pět virů, na počítači však po nich zůstalo ještě něco málo „odpadu“...

Avast a AVG si nedokázaly poradit se škůdcem označeným jako Rontokbro, což

Bezplatná ochrana: Antiviry dostupné zdarma neodstraní každý vir, přesto nabízejí přijatelný poměr ceny a výkonu...

je e-mailový červ, který blokuje systémové nástroje a pokouší se zabránit updatu antivirových signatur. Jako nejhorší se opět ukázal ClamWin – detekoval pouze tři škůdce, ale nedokázal s nimi nic udělat...

Jeho pozornosti zcela unikl například vir Banload, který rozhodně nelze označit za „drobnost" a jehož aktivace by měla dalekosáhlé následky. Ten totiž stahuje a instaluje do počítače další malware. Během chvíle dokáže udělat z počítače takové „smetiště", že jediným reálným dezinfekčním řešením je reinstalace systému.

Rootkity: Příliš tuhý oříšek...

Ve druhém kole našich testů měly antivirové nástroje za úkol najít a odstranit rootkity. Ty patří k nejnebezpečnějším škůdcům, na které můžete narazit. Dokáží totiž napadat a infikovat systémové procesy a v některých případek také proniknout i k jádru systému. Díky tomu se pak mohou maskovat skrýváním vlastních procesů...

Navíc je velmi obtížné je odstranit. V našem testu jsme použili rootkit označovaný jako NTRootkit, který většině účastníků testu připravil perné chvilky. Tento škůdce se skrývá v paměti RAM, kde čeká na příkazy přicházející nově vytvořenými zadními vrátky v systému. Při pokusu o jeho odstranění selhala přibližně polovina testovaných nástrojů. V tomto testu opět zcela zklamal Ashampoo Antivirus. Nástroj sice detekoval neaktivní „installery", ale poté, co se nainstalovaly, nenašel ani jeden z nich...

Někteří účastníci na tom ale byli podstatně lépe: nejen že detekovali i aktivní rootkity, ale také je dokázali ze systému odstranit. Během tohoto testu jsme zaznamenali i několik zajímavých situací: některé nástroje nebyly schopny při klasickém skenování neaktivní rootkit odhalit a detekovaly ho teprve až ve chvíli, kdy se stal aktivním – a to i přes maskovací techniky. Podobnou „akci" předvedl nástroj od firmy Panda, který si „nevšiml" installeru škůdce jménem Infostealer (špionážní program zaměřený na krádeže hesel), detekoval ho teprve až po aktivaci. Důvod: některé nástroje mají signatury pouze pro aktivní komponenty, případně nedokáží najít neaktivní rootkity pomocí heuristické analýzy.

VÝSLEDEK: Dobrou zprávou je, že téměř polovina testovaných antivirů nabídla excelentní výsledky. Bohužel ve všech případech jde o komerční nástroje – freewarové antiviry jsou o jednu úroveň níže.

Bez zaváhání lze doporučit produkty na prvních šesti místech. Excelovaly především nástroje Norton Antivirus a Trend Micro Internet Security: po testu po sobě „nechaly" jen drobný „nepořádek" v podobě několika neškodných zbytků. Mezi nejlepší patřil i F-Secure Antivirus, který najdete i v námi zdarma nabízeném balíku Internet Security (více informací naleznete v rámečku na předchozí stránce). Pokud nechcete za bezpečnostní produkty utrácet peníze, chybu neuděláte použitím libovolného nástroje z trojice Avira, AVG, Avast. V některých případech jsou i lepší než některé placené nástroje. Za zklamání lze označit především nástroje od firem Ashampoo nebo Dr. Web. Je tedy jen na vás, zda se pokusíte internetové mafii postavit a svůj počítač proměníte v nedobytnou pevnost, nebo zda necháte jeho brány otevřené dokořán...

AUTOR@CHIP.CZ

VÍTĚZ TESTU 11/2009

MÍSTO 1–10	1. MÍSTO	2. MÍSTO
Produkt	**Norton AntiVirus 2009**	**Trend Micro Internet Security 2009**
Verze	16.5.0.134	17.1.1250
Výrobce	www.symantec.com	www.trendmicro.com
Cena (přibližně)	920 Kč *	50 eur
Celkové hodnocení	98,6	97,2
Detekce nenainstalovaného malwaru (celkově 3 194 aktuálních vzorků malwaru)		
Skener	100,00 %	100,00 %
Rezidentní ochrana	100,00 %	100,00 %
Odstranění nainstalovaného malwaru (detekce/odstranění aktivních komponent/kompletní vyčištění)		
Win32/AutoIt	●/●/●	●/●/●
Win32/Autorun	●/●/●	●/●/–
Win32/Banload	●/●/●	●/●/●
Win32/Mytob	●/●/–	●/●/–
Win32/Rontokbro	●/●/●	●/●/●
Odstranění nainstalovaných rootkitů (detekce neaktivních rootkitů/detekce aktivních/odstranění aktivních rootkitů)		
Win32/Hupigon	●/●/●	●/●/●
Win32/Infostealer	●/●/●	●/●/●
Win32/NTRootkit	●/●/●	●/●/●
Win32/Pigeon	●/●/●	●/●/●
Win32/PolyCrypt	●/●/●	●/●/●

* Cena za verzi 2010.

CENOVÝ TIP 11/2009

MÍSTO 11–20	11. MÍSTO	12. MÍSTO
Produkt	**Panda Antivirus Pro 2009**	**Avira AntiVir Personal - Free Antivirus**
Verze	8.00.00	9.0.0.403
Výrobce	www.pandasecurity.com	www.free-av.com
Cena (přibližně)	1100 Kč	freeware
Celkové hodnocení	91,8	89,4
Detekce nenainstalovaného malwaru (celkově 3 194 aktuálních vzorků malwaru)		
Skener	100,00 %	100,00 %
Rezidentní ochrana	100,00 %	100,00 %
Odstranění nainstalovaného malwaru (detekce/odstranění aktivních komponent/kompletní vyčištění)		
Win32/AutoIt	●/●/–	●/●/–
Win32/Autorun	●/●/–	●/●/–
Win32/Banload	●/●/–	●/●/–
Win32/Mytob	●/●/–	●/●/●
Win32/Rontokbro	●/●/–	●/●/–
Odstranění nainstalovaných rootkitů (detekce neaktivních rootkitů/detekce aktivních/odstranění aktivních rootkitů)		
Win32/Hupigon	●/●/●	●/●/●
Win32/Infostealer	–/●/●	●/●/●
Win32/NTRootkit	●/●/●	●/–/–
Win32/Pigeon	●/●/●	●/●/●
Win32/PolyCrypt	●/●/●	●/●/●

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

	3. MÍSTO	4. MÍSTO	5. MÍSTO	6. MÍSTO	7. MÍSTO	8. MÍSTO	9. MÍSTO	10. MÍSTO
	BitDefender Antivirus 2009	BullGuard Internet Security	NOD32 Antivirus 4	F-Secure Anti-Virus 2010	eScan Anti-Virus Edition	Kaspersky Anti-Virus 2009	G DATA Anti-Virus 2010	VirusScan Plus 2009
	12.0.12.1	8.7.1.17	10.0.977.409	5.3.161	10.0.977.409	8.0.0.506 (a.b)	20.0.4.9	13.3 Build 127
	www.bitdefender.com	www.bullguard.com	www.eset.cz	www.f-secure.com	www.microworld.de	www.kaspersky.com	www.gdatasoftware.co.uk	www.mcafee.com
	630 Kč	45 £	30 eur	850 Kč	25 eur	800 Kč	25 eur	40 eur
	95,8	95,8	94,4	94,3	93,5	93,3	93	91,9
	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %
	100,00 %	100,00 %	100,00 %	99,97 %	99,97 %	100,00 %	100,00 %	100,00 %
	●/●/–	●/●/–	●/●/–	●/●/●	●/●/●	●/●/–	●/●/–	●/●/–
	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–
	●/●/–	●/●/–	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/–
	●/●/●	●/●/●	●/●/–	●/●/–	●/●/●	●/●/●	●/●/–	●/●/●
	●/●/●	●/●/●	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/–
	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●
	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●
	●/●/●	●/●/●	●/●/●	●/●/●	●/–/–	●/●/–	●/●/●	●/●/●
	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●
	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/–

	13. MÍSTO	14. MÍSTO	15. MÍSTO	16. MÍSTO	17. MÍSTO	18. MÍSTO	19. MÍSTO	20. MÍSTO
	avast! 4.8 Home Edition	AVG Anti-Virus Free 8.5	Spyware Doctor + Antivirus	VirusBuster Professional Home	VIPRE Antivirus + Anti-spyware	Dr.Web Anti-Virus	Ashampoo AntiVirus	ClamWin Free Antivirus
	4.8.1335.0	8.5.374	6.0.1.445	5.3.161	3.1.2775	5.0.1.06018	1.61	0.95.2
	www.avast.cz	www.avg.cz	www.pctools.com	www.virusbuster.hu/en	www.sunbeltsoftware.com	www.freedrweb.com	www.ashampoo.com	www.clamwin.com
	freeware	freeware	40 eur	25 eur	30 USD	20 eur	30 eur	freeware
	89,3	84,5	83,8	81,8	75,8	64,4	66,6	20,8
	99,97 %	100,00 %	98,31 %	100,00 %	99,12 %	98,50 %	100,00 %	83,50 %
	99,97 %	100,00 %	98,31 %	100,00 %	99,06 %	98,47 %	98,18 %	n/a
	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	–/–/–	●/●/–	●/–/–
	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	–/–/–	●/●/–	–/–/–
	●/●/–	●/●/–	●/●/●	●/●/–	●/●/–	●/●/–	●/–/–	–/–/–
	●/●/–	●/●/–	●/●/–	●/●/–	●/●/–	●/●/–	●/●/–	●/–/–
	●/–/–	●/–/–	●/●/●	●/●/–	●/●/–	●/●/–	●/●/–	●/–/–
	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/–/–	●/●/●
	●/●/●	●/●/●	●/●/●	●/–/–	●/●/–	●/●/●	●/–/–	●/●/●
	●/●/●	●/–/–	●/●/●	●/–/–	●/–/–	●/●/–	●/–/–	●/–/–
	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●	●/–/–	–/●/–
	●/●/●	●/●/●	–/●/●	–/●/●	●/●/–	●/●/●	●/–/–	●/●/–