On-line skenery: Bezpečí z webu

On-line antivirové skenery byly původně jen jednoduché a nijak výkonné pomůcky pro případ nouze. S rostoucím významem internetu však stále více rostla i jejich důležitost, až dosáhly současné podoby: staly se z nich výkladní skříně bezpečnostních firem, bezplatné ukázky kvalitních technologií.

PETR KRATOCHVÍL

On-line antivirům se věnujeme v Chipu již několik let a hned v úvodu je nutné říci, že na změny k lepšímu narážíme až v poslední době. Ano, základní skener nabízely téměř všechny firmy už od nepaměti, jeho používání však bylo pro většinu uživatelů peklem. Nutnost použití pouze Internet Exploreru, nestabilita, komplikované ovládání – to vše sráželo jakkoliv kvalitní nástroj do kolen a nutilo uživatele přecházet od jedné firmy ke druhé. O průlom se postarala v loňském roce firma Eset, která nabídla rychlý, snadno ovladatelný a výkonný nástroj, který v testu porazil konkurenci rozdílem třídy. Tentokrát ale konkurentů přibylo, takže boj snadný nebude...

BitDefender

WEB: www.bitdefender.com/scan8/ie.html

Rychlé spuštění, nejmenší objem stahované databáze, minimalistické nastavení a přijatelná rychlost. I tak lze ve stručnosti charakterizovat nástroj od firmy BitDefender. Na první pohled se sice zdá, že chybí rozsáhlejší možnosti nastavení, po podrobnějším prozkoumání sekce „Scanning options“ si však všimnete malého odkazu „click here“, pod kterým najdete vše důležité. Nám se například líbila možnost nastavení toho, co bude nástroj dělat s nalezenými škůdci (smazat, zeptat se uživatele, jen nahlásit...), nebo možnost zkontrolovat soubory jen s určitou příponou. Jako jeden z mála skenerů nabízí tento nástroj také možnost pozastavení skenování.

Ve finále mu tak lze vytknout pouze nepřehledné ovládání, které může méně zkušeným uživatelům dělat problémy.

Eset On-line scanner

WEB: www.eset.cz/eos/eset-online-scanner

Jak si povede loňský vítěz – to byla jedna z nejdůležitějších otázek celého testu. A hned v úvodu vás můžeme ujistit, že ani tentokrát firmě Eset ostudu neudělal. Důležité je už v úvodu poznamenat, že verze, kterou jsme testovali, je předfinální – tzv. Release Candidate (RC). Finální verze by se měla objevit v létě tohoto roku.

Ve srovnání s loňským rokem Eset na skeneru opět zapracoval a nabídl několik novinek – kromě podpory alternativních prohlížečů je to například identifikace nainstalovaného antiviru, detekce rootkitů nebo hledání potenciálně nežádoucích aplikací.

Za vynikající lze označit rychlost, ovládání by nemělo dělat problémy ani začá-

KROK ZA KROKEM

Ačkoliv většina uživatelů preferuje nainstalované antiviry, i jejich on-line verze jsou užitečnými pomocníky – především díky stále aktuálním signaturám. A jak vám tedy mohou pomoci při odstraňování nežádoucích počítačových návštěvníků?

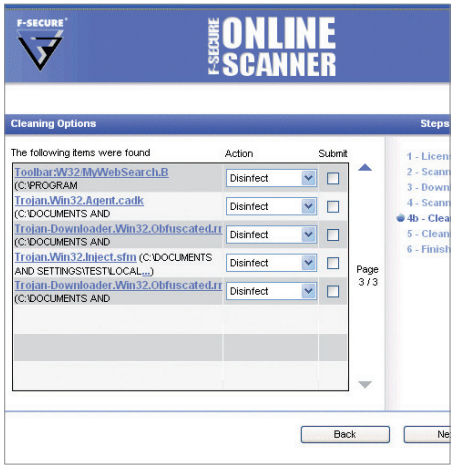
1) Prvním krokem by měla být co nejlepší detekce. V ideálním případě doporučujeme použití alespoň tří nástrojů, které zaručí skutečně důkladné prozkoumání napadeného systému. Pokud dokáží nástroje škůdce alespoň zčásti odstranit, jedině dobře.
2) Důležitý je ale finální export výsledků vyhledávání. Ten vám totiž v druhém kroku napoví, které specializované nástroje pro odstranění škůdců stáhnout.
3) Pokud si nejste jisti, zda je nalezený soubor skutečně malware (což se často stává u souborů typu „svchost.exe“), odešlete soubor na detailní analýzu – například na známý „File scanner“ Jotti (**http://virusscan.jotti.org**).
4) Po odstranění všech škůdců počítač restartujte a znovu systém zkontrolujte několika skenery. Teprve poté si můžete být jisti, že jste opravdu vyhráli...

tečníkům. Avšak ani tento nástroj není bez chyb. Vadila nám absence pozastavení skenu (k dispozici je jen ukončení), vážným nedostatkem je chybějící export výsledků. I přes tyto výtky však zůstává on-line skener od Esetu dobrou volbou, a to nejen v případě, že spěcháte…

F-Secure

WEB: http://support.f-secure.com/enu/home/ols.shtml

Jeden z nejrozporuplnějších nástrojů nám nabídla firma F-Secure. Její nástroj byl přehledný, přijatelně rychlý i praktický, ale



F-Secure Online scanner: Největší balík stahovaných dat nakonec překročil hranici 100 MB.

narazili jsme i na dva nepříjemné problémy. Prvním z nich bylo množství stažených dat. „Oficiální" ukazatele množství stažených dat sice nejprve ukázaly nutnost stažení relativně přijatelným 50 MB, poté se začaly stahovat tři megabajty, poté čtyři… a ve finále jsme na disku objevili přes 100 MB dat. To na pomalejších linkách nemusí být zrovna ideální. Samotná práce se skenerem byla rychlá a praktická, potěšila nás možnost individuální volby při odstraňování nalezených škůdců. Naše kladné dojmy ale ve finále totálně pohřbila absence automatického „odinstalování" nástroje (tedy spíše smazání). Na webu sice najdete návod na jeho odstranění, podle našeho názoru však jde o zbytečně komplikovanou nepříjemnost. Pokud ale máte dostatečně rychlý internet a velký disk, hoďte naše výtky za hlavu a nástroj alespoň vyzkoušejte…

Kaspersky

WEB: www.kaspersky.com/virusscanner

Nástroj od firmy Kaspersky si měl teoreticky poradit se všemi třemi nejrozšířenějšími browsery, v praxi se nám ale podařil pouze sken s použitím IE. Ve Firefoxu a Opeře tomuto nástroji „chyběla" Java (kterou ale v IE bez problémů našel). Další postup už byl bez komplikací: spuštění ná-

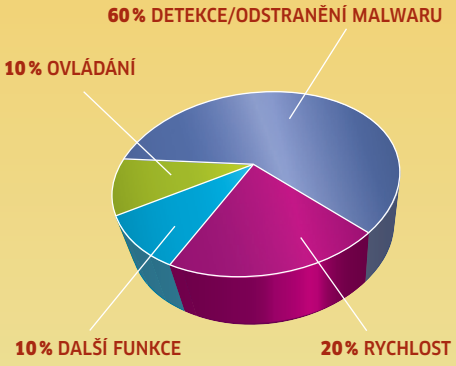
SOUHRN ON-LINE SKENERY

JAK CHIP TESTUJE

Nejdůležitějším kritériem našeho testu byly pochopitelně detekční schopnosti. Testovací počítač jsme zaplnili škůdci všeho druhu a poté jsme postupně nechali jednotlivé nástroje předvést, co umí. Hodnotili jsme počet detekovaných a odstraněných škůdců, spolu s důkladností provedení této operace (pokud se po restartu objevil škůdce znovu, na hodnocení se to výrazně projevilo). Ocenili jsme i možnost exportu výsledků, která je podle našeho názoru v boji proti škůdcům klíčová. Na druhém, nezavirovaném testovacím počítači, který byl starší a na disku měl velké množství souborů, jsme sledovali rychlost prohledání celého PC při maximálním využití schopností on-line skeneru.

Další „kladné body" jsme přidávali za přehledné ovládání, přijatelné množství stažených dat a pochopitelně za rychlost. Hodnotili jsme možnosti nastavení, podporu prohlížečů a také rozsah vyhledávaných hrozeb. K příjemným překvapením patřil i fakt, že velké procento nástrojů obsahovalo i detekci rootkitů – vzhledem k charakteru nástroje sice nepůjde o žádný zázrak, na základní kontrolu ale postačí.

Do našeho testu se nedostal produkt od Symantecu (najdete ho na adrese **http://security.symantec.com/sscv6/WelcomePage.asp**), který se svým principem mírně liší, především se nám ho však na testovacím počítači nepodařilo zprovoznit…



ZÁVĚR

Nástroj od firmy F-Secure nabídl druhý nejrychlejší sken, našel nejvíce škůdců a výsledky hledání dokáže exportovat do souboru ve formátu „html". Co víc si přát? Snad jen menší zabrané místo na disku a podporu alternativních prohlížečů. A minulý vítěz? Pro rychlou kontrolu počítače bychom stále doporučili nástroj od firmy Eset, k důkladnější kontrole je ale lepší počkat o chvíli déle a použít konkurenční nástroje.

POŘADÍ	1. MÍSTO	2. MÍSTO	3. MÍSTO	4. MÍSTO
Firma	F-Secure	Eset	Kaspersky	Panda
Produkt	Online scanner	Online scanner	Online Virus Scanner	ActiveScan
Web	http://support.f-secure.com/enu/home/ols.shtml	www.eset.cz/eos/eset-online-scanner	www.kaspersky.com/virusscanner	www.pandasecurity.com/homeusers/solutions/activescan/
Celkové hodnocení	67 bodů	56 bodů	48 bodů	44 bodů
Detekce/odstranění malwaru (60 %)	70	40	50	60
Rychlost (20 %)	80	90	10	10
Ovládání (10 %)	40	80	80	40
Další funkce (10 %)	50	60	80	20
Funkce a vlastnosti				
Podpora browserů: Firefox/Opera/IE	–/–/●	●/●/●	–/–/●	●/–/●
Detekce virů/malwaru/rootkitů/potenciálně nežádoucích programů	●/●/●/–	●/●/●/●	●/●/●/●	●/●/●/–
Odstranění hrozeb	●	●	–	●*
Uložení výsledku skenu (formát)	● (htm)	–	● (htm, txt)	●*
Naměřená data				
Počet kontrolovaných souborů	26 997	48 463	49 750	324 890
Doba kontroly (m:s)	32:51	**26:43**	59:55	**72:52**
Zabrané místo na disku (MB)	**130**	76	67	102
Počet nalezených/odstraněných škůdců	**12/8**	4/3	7/-	7/4

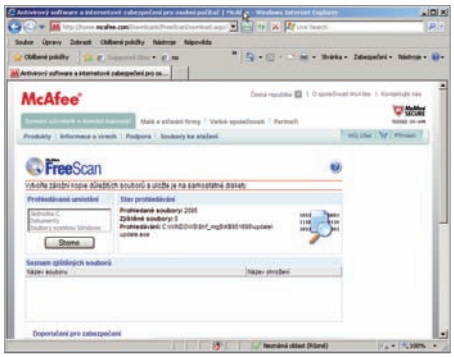
stroje, nahrání updatů, kontrola disku – jednoduché a přehledné jako v klasickém antivirovém nástroji. Pochválit musíme i možnost kontroly archivu mailového klienta, vybrané složky, nebo dokonce individuálního souboru. Jedinou výtkou, kterou jsme měli k praktickému použití skeneru, byla jeho rychlost – patřil k nejpomalejším v testu, což ho s nemožností odstranit nalezené hrozby a s chybějícím pozastavením skenu odsouvá mimo oblast našich doporučení...

Microsoft

WEB: http://onecare.live.com/site/en-US/center/howsafe.htm

Vzhledem k tomu, že se Microsoft pustil do experimentů v oblasti bezpečnostních nástrojů, nemohl v testu chybět ani jeho pokus v oblasti on-line skenerů.

Ano, i přes rozsáhlé zkušenosti Microsoftu v jiných oblastech lze tento nástroj považovat za spíše nepovedený pokus. Hned v úvodu uživatele otráví nutnost proklikat se spoustou oken a několikrát potvrzovat instalaci doplňku. O to překvapivější je poté automatické spuštění skenování. Nástroj se ve finále ani nezeptá, co chcete skenovat – automaticky kontroluje celý počítač, otevřené porty a „informace o počítači". Chybí možnost pozastavení skenu a exportu výsledků kontroly. Zkrátka – nástroj od Microsoftu je v tomto testu prozatím jen „do počtu"...



McAfee FreeScan: Starší nástroj se staršími radami. Kde ale vzít diskety?

Panda ActiveScan

WEB: www.pandasecurity.com/homeusers/solutions/activescan/

Další firmou, která na svém nástroji podstatně zapracovala, je Panda Security. Její nástroj zvládá detekci zranitelností, rootkitů, malwaru – zkrátka příjemně široký záběr. Jako jediná však nutí tato služba zájemce k registraci. Sken je sice možný i bez ní, ale teprve registrovaní uživatelé mohou vybírat nastavení kontrolovaných oblastí a především odstranit viry, červy a trojské koně. Kompletní odstranění malwaru nabízí až placená verze...

Nástroji také chybí možnost pozastavení skenu, k dispozici je pouze tlačítko pro zrušení kontroly. Musíme poznamenat i to, že jako jediný měl tento skener problémy s IE8 – nestabilita se pravidelně opakovala.

Nelíbilo se nám, že Panda hraje starou hru na „strašení uživatelů" – nejprve oznámí nalezené infikované soubory, pak oznámí detekci cookies a ve finále nabídne uživatelům nákup skvělého antivirového produktu. Podobné praktiky už konkurence dávno nepoužívá...

TrendMicro HouseCall

WEB: http://housecall.trendmicro.com/

Nástroj od firmy TrendMicro nelze označit jinak než jako příjemné překvapení. V minulých testech jsme byli otráveni komplikovaným ovládáním, rychlostí a především nestabilitou nástroje, což HouseCall odsunulo do kolonky „Zdaleka se vyhněte". Tentokrát to ale dopadlo úplně jinak. To, že firma na nástroji zapracovala, poznáte už na úvodní stránce – výčet schopností je skutečně impozantní. Kromě detekce malwaru a spywaru vás nástroj dokáže informovat o zranitelnostech nainstalovaných programů nebo potenciálně problematických síťových službách. Navíc je multiplatformní (Windows, Linux, Solaris), funguje jak ve Firefoxu, tak v IE, a problémy se stabilitou neměl ani při testech v RC IE8.

Na druhé straně také musíme poznamenat, že skener v IE vyžadoval zdaleka nejvíce zásuvných modulů a během skenování chybí jak možnost pozastavení, tak i zastavení kontroly. Před spuštěním máte možnost zvolit pouze mezi kontrolou celého počítače a vybraných složek, nepotěšila nás ani absence exportu výsledků. Dá se tedy říci, že i přesto, že firma TrendMicro na svém nástroji očividně zapracovala, stále mu ve srovnání s konkurencí ještě pár drobností chybí.

	5. MÍSTO	6. MÍSTO	7. MÍSTO	8. MÍSTO
	McAfee	TrendMicro	BitDefender	Microsoft
	FreeScan	Housecall	Online scanner	OneCare
	http://home.mcafee.com/Downloads/FreeScan.aspx	http://housecall.trendmicro.com/	www.bitdefender.com/scan8/ie.html	http://onecare.live.com/site/en-US/center/howsafe.htm
	43 bodů	34 bodů	31 bodů	11 bodů
	50 20 60 30	20 70 50 30	10 60 60 70	10 10 20 10
	–/–/●	●/–/●	–/–/●	–/–/●
	●/●/–/–	●/●/●/●	●/●/–/●	●/●/–/●
	–	●	●	●
	–	–	● (htm)	–
	47 698	n/a	277 865	n/a
	52:22	37:52	42:33	56:02
	71	28	38	70
	6/2	*/*	*/*	*/*

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

McAfee

WEB: http://home.mcafee.com/Downloads/FreeScan.aspx

Také nástroj od firmy McAfee podporuje jen Internet Explorer. Samotný skener je jednoduchý (na jeho nainstalování stačí jeden doplněk), možná až příliš. Nabízí jen tři volby – kontrolu celého disku, kontrolu systémových souborů a kontrolu složky Dokumenty. Nástroj působí dojmem pozdně devadesátých let – kopírování i skenování probíhá bez jakýchkoliv časových ukazatelů, jen s pohybující se ikonou složky nebo točící se lupou (pamětníci Windows 3.11 dojetím zamáčknou nejednu slzu). Nástroji sice chybí možnost pozastavení kontroly, má však v zásobě přibližně patnáct „moudrých rad" typu „Vždy používejte komplexní, aktuální antivirový program", kterými vás během skenování zásobuje. To, že chybí export výsledků, už asi nikoho nepřekvapí.

Perlička: Odhad stáří programu pravděpodobně nebude daleko od pravdy, protože jedna z moudrých rad zní: „Vytvořte záložní kopie důležitých dokumentů a uložte je na samostatné diskety."

PETR.KRATOCHVIL@CHIP.CZ

INFO

V boji proti malwaru

Hned v úvodu je nutné říci, že letos jsme pro on-line nástroje nachystali mimořádně těžké podmínky: kromě „běžných" virů jsme jim připravili i jednu klasiku v podobě záškodníka CoolWebSearch a jednoho odolného trojského koně. Je také nutné si uvědomit, že výsledky jednotlivých skenerů se mohou u jednotlivých typů „nákaz" lišit. S méně zavirovaným počítačem si všechny nástroje poradily bez problémů.

Prvním zklamáním v našem testu byl produkt od Microsoftu, kde zkolabovala už instalace nástroje. O něco dále se dostal pomocník od BitDefenderu, který skončil při pokusu o stažení virových definic. Z řad poražených se nejdále dostal HouseCall od firmy TrendMicro, který našel „jakýchsi" 22 hrozeb, ale zhroutil se při pokusu o jejich odstranění (aniž bychom mohli zjistit, co vlastně našel).

Mírné zklamání nás čekalo i u loňského vítěze – jeho rychlost a ovládání byly stále hodnoceny jako nejlepší, v detekčních schopnostech však za ostatními zaostal.

Zatímco z hlediska „hledání hrozeb" byly nástroje od McAfee, Pandy a firmy Kaspersky na přibližně stejné úrovni, v ostatních sledovaných kritériích jsme narazili na podstatné rozdíly. Nástroj od McAfee v nás vyvolával vzpomínky na minulé století, Kaspersky odmítal hrozby odstranit a Panda strašila pomocí „cookies" a sken jí trval světelný rok…

A příjemné překvapení? Na ovládání a uživatelské přívětivosti by sice u F-Secure ještě měli zapracovat, ve válce s malwarem ale tentokrát jejich nástroj nabídl nejlepší výsledky…