TEST boot antivirů

Mezi nejnebezpečnější počítačové hrozby patří jednoznačně rootkity a malware. I proti nim ale existuje efektivní nástroj.

PETR KRATOCHVÍL

Již více než deset let testuje bezpečností software i hardware. Během této doby zjisitil, že pomocí šikovných nástrojů lze přestít i ten nejdokonalejší malware.

Na první pohled se zdá, že mít dobře zabezpečený počítač nikdy nebylo jednodušší. Mnoho bezpečnostních firem nabízí zdarma jednodušší verzi svého antiviru, k dispozici je spousta specializovaných bezpečnostních nástrojů a na internetu najdete celou řadu bezplatných bezpečnostních skenerů. V praxi se ale stále častěji setkáváme se zavirovanými počítači, vyděračským malwarem a phishingovými e-maily. Jak je to možné?

Rostoucí počet hrozeb

Důvody, proč se celková bezpečnostní situace nelepší, jsou dva. Pravděpodobně tím nejdůležitějším je obrovský tlak na výrobce softwaru (i hardwaru), kteří se snaží dostat své produkty na trh dříve než konkurence. Výsledkem jsou programy plné chyb, které se firmy snaží záplatovat za pochodu. Typickým příkladem je situace u prohlížečů, kde probíhá nemilosrdný boj o uživatele a nové verze prohlížečů (kromě Microsoftu) se objevují v rozmezí několika málo měsíců. Při tomto tempu není žádným překvapením, že jsou prohlížeče plné chyb. Například ve srovnání s rokem 2010 bylo loni v prohlížečích objeveno téměř dvakrát tolik zranitelností. Zajímavé také je, jak jednotlivé

firmy tento problém řeší. Za poněkud bizarní lze označit přístup Firefoxu a Googlu, kteří chyby opravují chrlením nových a nových verzí. Například Firefox 20 opravoval jedenáct chyb předchozí verze, přičemž čtyři z nich byly velmi nebezpečné, a tři dokonce extrémně nebezpečné. Nové verze tedy většinu bezpečnostních problémů vyřeší, ale tento přístup také vyžaduje neustálou pozornost uživatele: jakmile zapomene produkt aktualizovat, má problém. U Googlu ale musíme pochválit snahu podporovat nahlašování nalezených chyb – za jejich ohlášení sice zaplatí méně (500 až 1 000 dolarů) než například internetová mafie (minimálně 10 000 dolarů), i tak jde ale o pozitivní motivaci.

Druhým důvodem rostoucího počtu bezpečnostních problémů je profesionalizace internetové mafie. Tento trend je vidět na všech typech útoků – od stále dokonalejších malwarů až po propracovanější phishingové e-maily. Určitě si všichni vzpomenou, jak vypadaly první e-maily klientům České spořitelny – „Drahoušek zákazník“ uživatele spíše pobavil, než ohrozil. A nyní? Zprávy na první pohled nerozeznatelné od oficiálních, psané dobrou češtinou – podvod často rozpozná jen odborník.

Hrozby se zárukou

Mnohem nebezpečnější důsledky má ale tento trend u stále propracovanějších virů a malwaru. Profesionální hackeři nabízí i začínajícím počítačovým podvodníkům kreativní sady, umožňující vytvoření malwaru doslova na míru. Lze například zvolit způsob a účinnost maskování nebo vybrat, které bezpečnostní nástroje nedokážou hrozbu detekovat. A pochopitelně platí, že čím dražší nástroj, tím rozsáhlejší nabídka schopností. Experti odhalili, že některé hackerské gangy nabízí pro své produkty nejen kvalitní podporu, ale často také záruku, že malware nebude antiviry po určitou dobu detekovatelný.

Na základě těchto skutečností vás asi nepřekvapí, že bezplatné nástroje pracující jen s detekcí pomocí signatur mají jen malou šanci pokročilejší malware odhalit. Ještě hůře jsou na tom on-line antiviry, které se často spouští v prohlížeči a s minimálními právy ani nemohou maskovaný malware detekovat. Tyto bezpečnostní nástroje ale mají jiný účel: pokud na nějakou hrozbu narazí, máte jistotu, že ve vašem počítači není něco v pořádku.

Řešením tohoto bezpečnostního problému je kvalitní bezpečnostní balík, který kombinuje více ochranných mechanismů a umožňuje rozpoznat malware i podle jiných příznaků, než jsou signatury. Ne každý uživatel ale bude chtít do takovéto ochrany investovat stovky korun.

Kvalitní detekce zdarma s riziky

Přestože jste na kvalitní ochranu rezignovali a na svém počítači nemáte nic, co by hackerům stálo za ukradení, měli byste alespoň čas od času počítač důkladně zkontrolovat. Řádění malwaru vás totiž může stát i hardwarové zdroje a škodlivý software může být příčinou, proč váš počítač pracuje stále pomaleji. Jak ale důkladnou kontrolu provést, když nechcete utratit ani korunu?

Řešením jsou bootovací antivirové balíky. Ty mohou sloužit i jako nástroj poslední záchrany a najít malware využívající rootkitů, se kterým si běžný antivir neporadí. Jak tyto nástroje fungují?

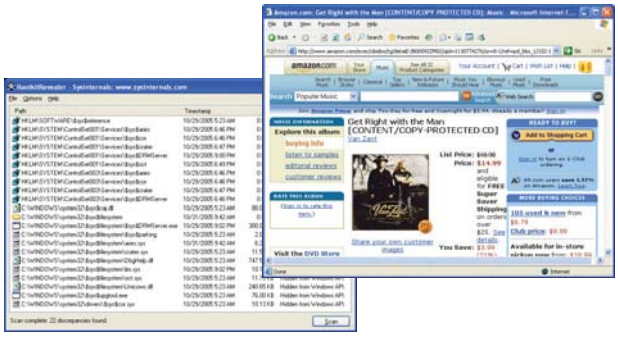
Základem je ve většině případů Linux, do kterého je přidáno skenovací jádro a aktualizační rutina. Nepříjemnou skuteč-

HISTORIE ROOTKITŮ

První zmínky o rootkitech pochází z operačního systému Unix, kde šlo o sadu programů sloužících k získání práv „roota“ (správce), zamaskování vstupu hackera a odstranění stop po útoku. Stejně jako operační systémy procházely i rootkity evolucí, se kterou se správci sítí poprvé důkladně seznámili v roce 1996. V tomto roce se začaly masivně objevovat rootkity pro SunOS 4.x a Linux Slackware, které dokázaly na tehdejší dobu neuvěřitelné věci – uměly odchytávat přihlašovací údaje, otevřít zadní vrátka k systému a pochopitelně také maskovat svou přítomnost.

Většina uživatelů Windows se ale o rootkitech dozvěděla až v roce 2006, kdy se provalila aktivita firmy Sony. Ta ve snaze zabránit kopírování svých CD nasadila speciální software, který se do počítače nakopíroval při odsouhlasení licenčních podmínek EULA. Tato na zakázku vytvořená DRM ochrana XCP od firmy First 4 Internet ale nebránila jen samotnému kopírování, ale také skrývala klíče v registru a soubory na disku (začínající na řetězec sys). Toho pochopitelně využila celá řada hackerů, kteří použili tento rootkit ke skrývání svého malwaru.

V současnosti už používá technologii rootkitu každý pokročilejší malware. Obvyklým postupem je, že na míru vytvořený malware využívá knihovny z rootkitu pro své maskování (například z Hacker Defenderu nebo z rootkitu FU). O oblíbenosti této technologie mezi hackery svědčí i skutečnost, že byl rootkit nalezen i v červu označovaném jako Bagle, trojském koni Goldun nebo nástroji na tvorbu sítě botů Rustock.



První komerční rootkit na hudebních discích od Sony odhalil Mark Russinovich pomocí vlastního nástroje RootkitRevealer.

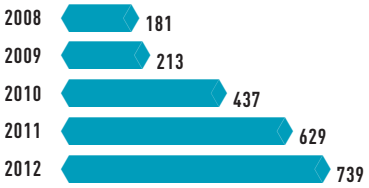
NEBEZPEČNÝ TREND

Vzrůstající počet zranitelností v programech ztěžuje práci klasickým antivirům a nahrává hackerům. Průměrně byly v každém programu objeveny čtyři zranitelnosti!

ZDROJ: SECUNIA

NEBEZPEČNÉ PROHLÍŽEČE

Prohlížeče patří mezi nejpoužívanější software, avšak jejich bezpečnost tomu neodpovídá. I u nich je znát strmě rostoucí počet zranitelností.



ZDROJ: SECUNIA

ností, bezpochyby vyplývající z nulové ceny, je ale to, že až na výjimky tyto nástroje nepatří mezi nejpropracovanější software. Většina zkušenějších uživatelů by bootovacím antivirům odpustila primitivní rozhraní, neodpustitelné jsou ale omezené skenovací schopnosti. Některé nástroje neumožňují kontrolu vybraných složek, hledání v archivech nebo pouze prověření boot sektoru. Pokud se je rozhodnete použít, rozhodně také doporučujeme zálohovat si důležitá data – při testování se nám několikrát stalo, že antivir bez ptaní odstranil důležitou komponentu systému a počítač se vzpamatoval až po obnově ze zálohy. I přes tato rizika lze bootovací antiviry označit za výkonné nástroje, které v rukou zkušených uživatelů dokážou vyčistit systém od všech škůdců. Pojďme se podívat, jak jsou na tom programy jednotlivých bezpečnostních firem.

Rozdíly více než podstatné

Jednou ze slabin bootovacích antivirů, která by mohla méně zkušené uživatele odradit, je rozhraní. Některé nástroje totiž jako by vypadly z historického filmu. Například F-Secure Rescue CD by zastarale působil i v minulém století. Navíc jeho ovládání využívající tabulátoru, šipek a stisknutých kláves může uživatelům zvyklým na myš pořádně zamotat hlavu. O něco lépe je na tom nástroj od AVG, který sice také funguje v textovém režimu, ovládat ho ale není takový očistec. Zbývající bootovací antiviry již fungují ve více či méně povedeném grafickém režimu. Bitdefender nebo Avira mají lehce retrovzhled, nástroje od firem Comodo a Kaspersky se od moderních (placených) antivirů příliš neliší.

Podstatné rozdíly také najdete ve schopnostech jednotlivých skenovacích nástrojů. Odstrašujícím případem může být opět F-Secure Rescue CD, který nenabídne téměř nic, o chloupek lépe jsou na tom Comodo, Bidefender nebo Kaspersky. Požadavky i těch nejnáročnějších uživatelů by měly uspokojit nástroje od AVG, nebo ještě lépe Aviry. Posledně jmenovaný nabízí možnost nastavit téměř vše – od volby cíle přes volbu skenovací metody až po možnost zakázat mazání nalezených hrozeb.

Poslední sledovanou kategorií byly dodatečné nástroje. V této kategorii exceloval AVG rescue CD, který kromě nezbytného správce souborů nabídl i utility pro práci s šifrovanými daty, pro obnovu souborů nebo na S.M.A.R.T. kontrolu disku. Za zmínku stojí také výbava bootovacích antivirů od firem Comodo a Kaspersky, které nabídly správce souborů a také jednoduchý prohlížeč. Ostatní nástroje zde zklamaly a náročnější uživatelé budou spíše zklamáni. Zcela zde zklamala většina nástrojů.

Nepříjemné detaily

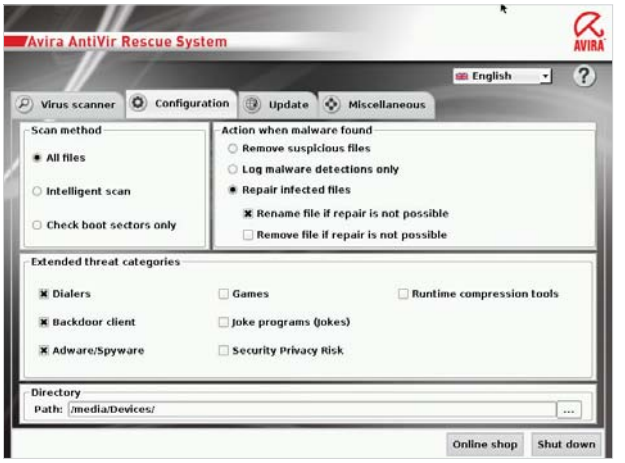
V rámci testu nám neunikly ani nepříjemné detaily, které podstatně znepříjemňují práci s bootovacím antivirem. Například nástroj od F-Secure po spuštění bootovacího disku teprve začne rozbalovat Linux a stahovat neúměrné (vzhledem ke kvalitě výsledného produktu) množství dat. Pokud tedy kontrolu provádíte v místě s pomalejším internetem, volte pomocníka od konkurence. Podobným neduhem trpěl i antivir od Bitdefenderu, u něj byla ale doba stahování kratší a výsledek (grafické rozhraní) odpovídalo době čekání.

Méně zkušení uživatelé by také měli zvážit, zda sáhnou po nástroji pracujícím v textovém režimu. Především u nástroje od F-Secure jsme v praxi vyzkoušeli, že ne každý zná příslušné triky pro pohyb kurzoru a volbu v nabídkách.

PETR.KRATOCHVIL@CHIP.CZ

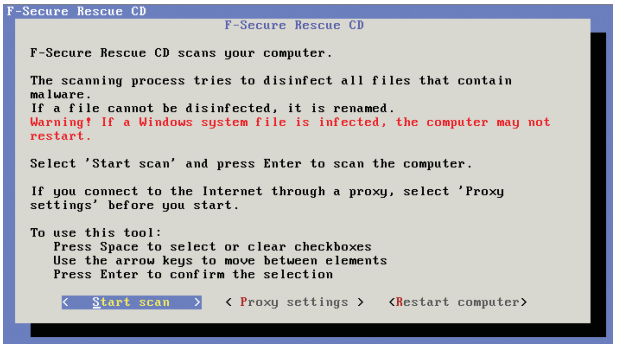
COMODO RESCUE DISC

Příjemné grafické rozhraní potěší, zamrzí pouze omezené možnosti skenovacího nástroje.



AVIRA ANTIVIR RESCUE SYSTÉM

Grafické rozhraní v lehce zastaralém hávu nevadí, experti ocení množství nastavení skenu.



F-SECURE RESCUE CD

Pro experty retro, pro většinu uživatelů noční můra. Ovládání kombinací šipek, písmen a mezerníku může být pro někoho skutečnou výzvou.

AVG RESCUE CD

Ani tento nástroj přílišnou ergonomií nevyniká, vše ale vynahrazuje rozsáhlými možnostmi skenování a bohatou výbavou dodatečných funkcí.

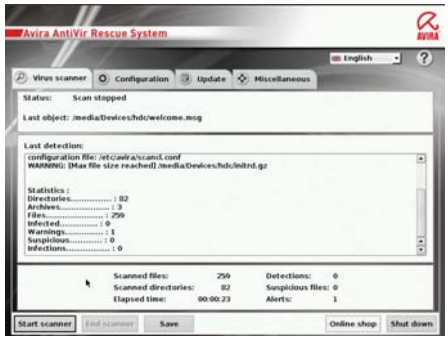
Jak Chip testuje

Bootovací antiviry jsme hodnotili podle několika kritérií. Nejdůležitějším byly schopnosti jednotlivých skenovacích nástrojů, které umožňují rychlou a bezproblémovou kontrolu zavirovaného počítače. Dalším ostře sledovaným parametrem byla ergonomie. Ne každý uživatel je IT expert a práce s těmito nástroji by měla být dostupná i těm méně zkušeným. Poslední věcí, na kterou jsme se zaměřili, byly dodatečné nástroje. Praktický je například internetový prohlížeč umožňující rychle získat tipy na řešení objeveného problému. Pro zkušenější uživatele se hodí například i možnost obnovy souborů nebo práce se zašifrovanými disky.

Schopnosti (50 %) Základem hodnocení byl rozsah funkcí antiviru a možnosti nastavení skenování. Kladné body dostávaly nástroje například za možnost skenu vybrané složky, kontrolu boot sektoru nebo možnost volby, co s nalezeným malwarem dělat.

Ergonomie (30 %) U ergonomie bylo rozhodující, zda nástroj nabídne uživateli grafické rozhraní, kladně jsme však hodnotili i snadné a logické ovládání.

Výbava (20 %) U tohoto kritéria jsme hodnotili dodatečnou výbavu bootovacích nástrojů. Kladné body zde nástroje dostávaly například za integrovaný prohlížeč, souborový manažer nebo možnost obnovy smazaných souborů. U některých nástrojů nás potěšila i možnost kontroly stavu hardwaru (disku a pamětí), případně nabídka úpravy registru Windows.

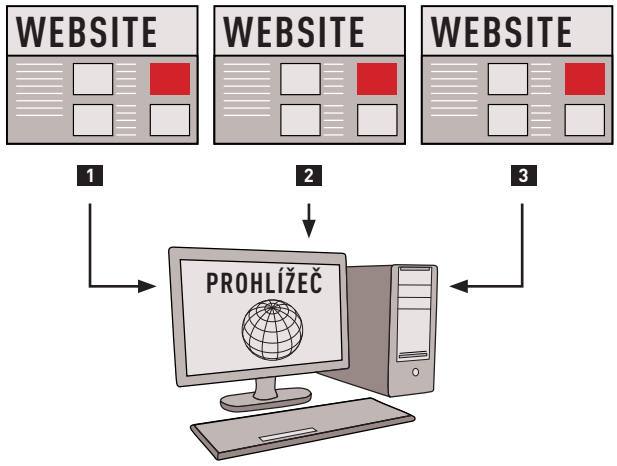


Vítěz našeho testu sice nenabízí žádné dodatečné nástroje, svou práci při hledání hrozeb ale odvádí velmi dobře.

VÍTĚZ TESTU

Žádný z testovaných programů nelze označit za jednoznačného vítěze – v pelotonu dominovala první trojka a každý z ní má uživateli co nabídnout. Bodově první Avira nabídne nejlogičtější ovládání s poměrně rozsáhlými možnostmi konfigurace skenu, chybí jí ale dodatečná výbava. Naopak AVG Rescue CD lze s jeho textovým rozhraním doporučit spíše zkušenějším uživatelům. Těm se ale odvděčí rozsáhlými možnostmi konfigurace skenu a také bohatou nabídkou dodatečných utilit. Například pokud se počítač chová „divně" a vy máte podezření na malware, pomocí AVG můžete prověřit, zda nejsou na vině poškozené paměti nebo odcházející pevný disk. Kompromisem mezi oběma zmiňovanými produkty je nástroj od firmy Kaspersky, který lze bez výhrad doporučit i surfařům začátečníkům.

Méně zkušení uživatelé by se naopak měli zdaleka vyhnout nástroji F-Secure Rescue CD, který je kombinací spartánské výbavy a textového rozhraní. Profesionálové se s těmito překážkami určitě poperou, začátečníci by měli raději zvolit kterékoliv konkurenční řešení. Vlastníci pomalejších datových linek by také měli zvážit nasazení produktu od BitDefenderu, který (podobně jako nástroj od F-Secure) stahuje příliš velký balík aktualizačních dat.



JAK FUNGUJÍ NEJNEBEZPEČNĚJŠÍ HROZBY
Do vašeho počítače pomocí zranitelnosti pronikne malware. **1** Pomoci downloaderu stáhne rootkit, který získá kontrolu nad počítačem a deaktivuje bezpečnostní nástroje. **2** Do systému se podle požadavků hackera stáhne další malware, který je maskován rootkitem. **3**

SROVNÁNÍ BOOTOVACÍCH ANTIVIRŮ

	ANTIVIR RESCUE SYSTEM	RESCUE DISK 10	RESCUE CD	CLEANING ESSENTIALS	RESCUE CD	RESCUE CD
VÝROBCE	AVIRA	KASPERSKY	AVG	COMODO	BITDEFENDER	F-SECURE
ADRESA (WWW.)	avira.com	kaspersky.com	avg.cz	freedrweb.com/livecd/	bitdefender.com	f-secure.com
CELKOVÉ HODNOCENÍ	64	60,5	58,5	45	43,5	14
SCHOPNOSTI (50 %)	90	55	70	30	40	20
ERGONOMIE (30 %)	60	70	25	60	55	10
VÝBAVA (20 %)	5	60	80	60	35	5
FUNKCE						
GUI (PŘÍK. ŘÁDEK / GRAFICKÉ)	•/•	•/•	•/–	•/•	•/•	•/–
AKTUALIZACE PŘES WEB	•	•	•	•	•	•
MOŽNOSTI SKENOVÁNÍ	velmi rozsáhlé	rozsáhlé	velmi rozsáhlé	rozsáhlé	standardní	omezené
VÝBAVA						
PROHLÍŽEČ	–	•	–	•	–	–
E-MAILOVÝ KLIENT	–	–	–	–	–	–
SPRÁVCE SOUBORŮ	–	•	•	•	–	–
DALŠÍ NÁSTROJE	–	–	obnova souborů, práce s šifr. disky editor registru	–	obnova souborů	–