Nebezpečný software

K infikování počítače potřebují škůdci **ZRANITELNÉ PROGRAMY**. Takových programů je bohužel v současné době více než dost. Chip vám ukáže desítku těch nejrizikovějších a také vám prozradí, jak se vyhnout útokům, které jsou na ně vedeny a zaměřeny.

MARKUS MANDAU

Potápění se ke žralokům zažívá boom. Stále více turistů vyhledává extrémní nebezpečí – například právě pohled z očí do očí s mořským agresorem. Pokud se na pobřeží Jižní Afriky zúčastníte takové akce, pak vše, co musíte udělat, je vlézt do kovové klece hned pod povrchem moře. Odtud si pak můžete snadno pořídit pár senzačních „úlovků" z dovolené – fotografií bílých žraloků, kteří jsou vábeni na kusy syrového masa.

Žádný účastník takové akce by ale ani ve snu nepomyslil na to, že by vlezl do moře, aniž by byl chráněn klecí. Mnozí internetoví surfaři se však chovají mnohem rizikověji: ignorují důležité bezpečnostní aktualizace a virtuálně tak lákají hackery, aby „navštívili" jejich počítač. Poskytovatel bezpečnostních služeb Trusteer zkontroloval software na 2,5 milionu počítačů. Výsledek? 80 procent všech uživatelů surfuje se zastaralými a nespolehlivými verzemi „flashe". V případě oblíbeného „pdf" nástroje Adobe Readeru dosahuje toto číslo dokonce až 84 procent. Přitom k tomu, aby se malware sám usadil na PC, stačí pouhá návštěva infikované webové stránky či otevření zmanipulovaného dokumentu.

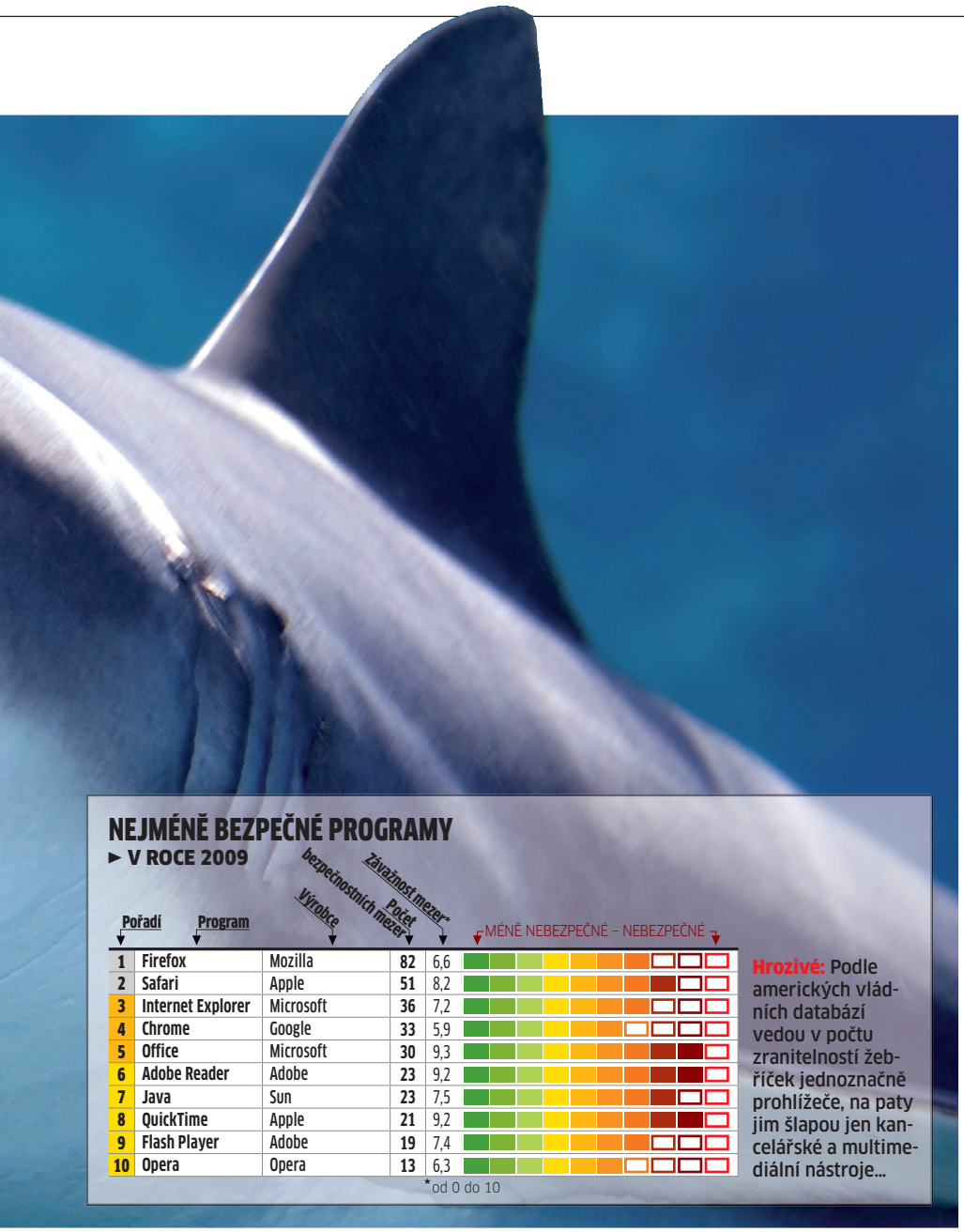
Protože s novými verzemi Windows je stále komplikovanější přímý útok na operační systém (viz rámeček na straně 54), hackeři se stále častěji pokoušejí dostat do cizích počítačů pomocí jiných aplikací. Jejich šance jsou poměrně vysoké: americká „The National Vulnerability Database", která je přidružená k vládnímu oddělení „Homeland Security", zaznamenává v softwarových produktech současnosti celkem 38 571 bezpečnostních mezer. Odhaduje se, že každý z nás denně narazí v průměru na 19 z nich.

Mnoho bezpečnostních mezer postihne software, se kterým běžný uživatel sotva přijde do styku – například operační systém Solaris od Sunu, vysoko v seznamu však najdete i známé programy (viz tabulka vpravo), které

PLNÁ VERZE NA DVD

UpdateStar 4.6 Premium Edition

Pravidelná aktualizace používaného softwaru je důležitá nejen kvůli novým funkcím a možnostem programů, ale rovněž i z hlediska bezpečnosti. Součástí aktualizací programů totiž zpravidla bývají i opravy bezpečnostních problémů. Plná verze programu UpdateStar vám pomůže sledovat aktuálnost verzí instalovaného softwaru po následujících 6 měsíců.



NEJMÉNĚ BEZPEČNÉ PROGRAMY
► V ROCE 2009

Pořadí	Program	Výrobce	Počet bezpečnostních mezer	Závažnost mezer*	MÉNĚ NEBEZPEČNÉ – NEBEZPEČNÉ
1	Firefox	Mozilla	82	6,6	
2	Safari	Apple	51	8,2	
3	Internet Explorer	Microsoft	36	7,2	
4	Chrome	Google	33	5,9	
5	Office	Microsoft	30	9,3	
6	Adobe Reader	Adobe	23	9,2	
7	Java	Sun	23	7,5	
8	QuickTime	Apple	21	9,2	
9	Flash Player	Adobe	19	7,4	
10	Opera	Opera	13	6,3	

*od 0 do 10

Hrozivé: Podle amerických vládních databází vedou v počtu zranitelností žebříček jednoznačně prohlížeče, na paty jim šlapou jen kancelářské a multimediální nástroje...

80 procent všech uživatelů je ohroženo

se nacházejí téměř na každém počítači. Proto je důležité udržovat tyto programy aktualizované pomocí aktualizačních nástrojů – nebo ještě lépe používat bezpečnější alternativy (viz nástroje na DVD).

Než však detailně popíšeme bezpečnostní mezery a navrhneme bezpečnější softwarové alternativy, pojďme se podívat na rozhraní Windows, které několik let způsobovalo obrovské problémy: pojďme prozkoumat hrozbu jménem ActiveX. Podle zprávy bezpečnostního oddělení IBM „X-Force“ začaly útoky přes rozhraní ActiveX dominovat letos – v současné době se drží na špici s podílem přibližně 60 procent. Při třech z pěti útoků na prohlížeč tedy bylo využito bezpečnostních mezer v modulu Windows.

ActiveX: Otevřená rána Windows

Rozhraní ActiveX bylo do Windows implementováno v roce 1996 – bylo určeno pro standardní programy, jako jsou Internet Explorer, Media Player a Outlook s cílem přidání nových funkcí – například doplňku ActiveX pro QuickTime. Problémem je však to, že technologie ActiveX byla vyvinuta v době, kdy byl internet ještě bezpečným místem, a tomu odpovídá i její zabezpečení – například plug-in ActiveX je považován za bezpečný i s pouhou signaturou.

Microsoft dokáže označit komponenty ActiveX, u kterých bylo prokázáno, že jsou nespolehlivé, pomocí tzv. kill bitu. Pomocí aktualizace položky v registrech je lze takto „deaktivovat“. Pokud se chcete sami podívat, které kill bity jsou nastaveny ve vašem systému, hledejte tuto informaci v registrech v sekci „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveXCompatibility“. Kill bit je označen symbolem „compatibility flags“ s hodnotou „0x00000400“.

Mezery ActiveX jsou velkou hrozbou především proto, že plug-iny mají stejná systémová práva jako programy, ve kterých pracují. Pokud například uživatel XP běžně surfuje jako administrátor s Internet Explorerem, pak mají jeho moduly s ActiveX kompletní přístup k systému; ve Vistě a Windows 7 nabízí operační systém alespoň základní ochranu v podobě kontroly uživatelských práv (User Account Control) – tedy za předpokladu, že je zapnuta.

Většina infikovaných webových stránek dokáže mezer v plug-inu ActiveX využívat. Stačí použít některý z „neošetřených“ triků a plug-in se spustí v prohlížeči. Pokud pro vás není používání služeb ActiveX nezbytné, doporučujeme ho v Internet Exploreru vypnout. Příslušné volby najdete v nabídce »Nástroje | Možnosti Internetu | Zabezpečení | Vlastní úroveň«

Od počátku roku do konce července letošního roku se problémy zdvojnásobily: celý systém ohrozily další dvě mezery v ATL (Active Template Library), které se používají k programování plug-inů ActiveX. Důsledek je hrozivý: zkontrolován (a v případě potřeby přeprogramován) musí být v podstatě každý plug-in, který byl kdy vytvořen. Jedna ATL mezera umožňuje přetečení bufferu, pomocí něhož dokáže infikovaný plug-in zapisovat do jiných oblastí paměti, které jsou například vyhrazeny pro služby Windows. Druhá mezera „uniká“ kill bitu v registru a umožňuje aktivaci dalších nebezpečných plug-inů, aniž by o tom uživa-

NA DVD

Bezpečnější programy

Automatic Update Client ► varuje před nebezpečnými nástroji

Flashblock ► blokuje Flash ve Firefoxu

IE7Pro ► vylepšení IE i z hlediska bezpečnosti

PDF Quick Reader ► alternativa k programu Adobe Reader

Personal Software Inspector ► kontroluje operační systém

Software UpToDate ► získává důležité aktualizace

SUMo ► nástroj upozorňující na aktualizace programu

UpdateStar ► vyhledávač nových verzí softwaru

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

tel věděl. Microsoft naštěstí mezitím uvolnil pro Outlook a Media Player odpovídající záplaty, které problém odstraňují, je však (jako obvykle) obrovské množství uživatelů, kteří pracují s neaktualizovanými aplikacemi.

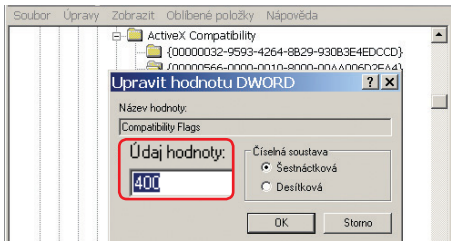
Existuje ale i jiné řešení: uživatelé mohou využít alternativní prohlížeč, který žádné plug--iny ActiveX nevyužívá. Experti předpokládají, že pro celkovou bezpečnost systému je nyní rozhodujícím faktorem výběr webového prohlížeče. Podle zprávy IBM lze polovinu všech kritických mezer (z hlediska bezpečnosti) najít v prohlížečích. Výrobci to ale uživatelům příliš neusnadňují: situace v oblasti prohlížečů je nyní o dost zamotanější než dříve. Například Internet Explorer byl roky považován za rizikový. To není nic překvapivého, protože Microsoft svůj prohlížeč (především ve verzi 6) dlouho ignoroval – až bylo příliš pozdě něco dělat. Z tohoto přístupu profitoval především Firefox, mnoho dalších uživatelů pak přešlo i na jiné alternativní prohlížeče, protože je považovali za bezpečnější než IE. A jak je tomu v současnosti?

Prohlížeč: Firefox je plný mezer

Dnes se věci mají trochu jinak: v roce 2009 bylo ve Firefoxu odhaleno více než 80 mezer. Stal se tak „nejděravějším“ browserem a potvrdil déletrvající nepříjemnou tendenci v oblasti zranitelností, a to dokonce i v porovnání s Internet Explorerem. Statistika je překvapivá: počet mezer ve Firefoxu je už dva roky nepřetržitě na vzestupu, naopak počet hrozeb v Internet Exploreru se pomalu snižuje. Statistická data přesto nemohou implicitně potvrdit, který z těchto dvou prohlížečů je bezpečnější. Přístup ke zjištěným zranitelnostem je totiž často rozdílný – zatímco Mozilla záplatuje relativně rychle a důkladně, Microsoft částečně ignoruje problémy, které ještě nebyly využity malwarem. Proto je pro výběr správného prohlížeče lepší, pokud se podíváte na detaily jednotlivých problémů: dnes je většina útoků prováděna přes XSS (Cross-Site-Scripting) a pomocí podobných metod. Klasický příklad: během nahrávání stránky je nebezpečný obsah nainstalován na jinak spolehlivý web – pouhou záměnou HTML prvku. Chyby prohlížeče, které jsou využity k XSS útoku, mohou být poměrně banální. Nejlepším příkladem tohoto tvrzení je nedávno objevená bezpečnostní mezera, pomocí níž může být „oklamána“ SSL certifikace. Stačí jen menší modifikace odkazu: v adrese je na první pohled vše, co potřebujete pro pocit bezpečí – odkaz na WWW stránku obsahující certifikát. Skutečnost je ale jiná: pouhé kliknutí na odkaz typu www.paypal.com/0.malware.org, stačí většině prohlížečů jako platný certifikát pro Paypal, protože si „0“ vyhodnotí jako „značku stop“. Skutečná doména však přichází pouze po „nule“ – a to je to, čeho pak využívá hacker. Firefox 3.5 nemůže být tímto způsobem oklamán, ale Internet Explorer ano. Na druhé straně mohou útočníci u Firefoxu zneužít pomocí SSL triku aktualizační funkci, aby na systém nainstalovali malware. V Internet Exploreru tento hackerský trik možný není, protože Microsoft nekontroluje platnost pouze pomocí SSL. Závěr je ale smutný pro oba prohlížeče: ani jeden z nich nedokáže své uživatele stoprocentně ochránit. Na první pohled je tedy nejlepším řešením použití alternativních browserů, jako jsou Safari od Applu či Google Chrome, ve kterých trik se SSL nefunguje.

Z hlediska bezpečnosti to ale nejlepší řešení není: oba zmiňované prohlížeče jsou totiž ve statistikách (z hlediska mezer) na nelichotivých předních pozicích. Za většinou zranitelností stojí Web Kit engine, který je u obou browserů zodpovědný za zpracování JavaScriptu. Například jen v tomto roce bylo v tomto enginu nalezeno už více než 30 mezer.

Ani SSL už není bezpečné



ActiveX: ActiveX doplňky mohou být deaktivovány pomocí tzv. kill bitů.

Jediným doporučeníhodným prohlížečem, tedy pokud jde o bezpečnost, tak zůstává Opera. Například v loňském roce u ní společnost Secunia konstatovala pouze dvě vážná bezpečnostní „doporučení“ (pro verzi 9), nejnovější Opera (s číslem 10) je prozatím bez ztráty „bodu“.

Multimédia: Katastrofa pro Apple a Adobe

I ten nejbezpečnější prohlížeč vám je k ničemu, pokud jsou snadno napadnutelné plug-iny důležité pro zobrazení obsahu webu. U hackerů jsou v současnosti oblíbené multimediální doplňky, jako například QuickTime či Flash Player, protože je lze nalézt v téměř všech systémech; a také proto, že pokrytí „trhu“ dosáhlo u Flash Playeru (podle Adobe) 99 procent. Pravděpodobnost úspěšného útoku je zde tudíž vyšší než v případě přímého útoku na prohlížeč, protože dokonce i Internet Explorer, který v oblasti prohlížečů kraluje, je používán „pouze“ přibližně 65 procenty uživatelů.

Multimediální plug-iny jsou často náchylné k útokům, které vyvolávají přetečení bufferu. Scénář je vlastně téměř vždy stejný: surfař je zlákán k otevření infikovaného video- či audiostreamu, který nutí QuickTime či flash doplněk, aby psal do oblasti vyhrazené paměti. Tímto způsobem může být spustitelný kód infiltrován do systému. Bezpečnostní mezery, které využívají přetečení bufferu, jsou tedy vždy klasifikovány jako kritické. Není divu, že QuickTime má extrémně vysokou průměrnou hodnotu (9,2 z 10), pokud jde o závažnost bezpečnostních mezer.

Problém bohužel nemůže být omezen pomocí zakázání vybraného formátu, protože spektrum problematických formátů zpracovávaných multimediálními doplňky je příliš široké. Kromě obvyklých souborů MOV byla v tomto roce zranitelnostmi zasažena i videa ve formátu AVI nebo například obrázky ve formátu PSD. Protože QuickTime nemůže být ničím nahrazen, mají uživatelé pouze dvě volby:

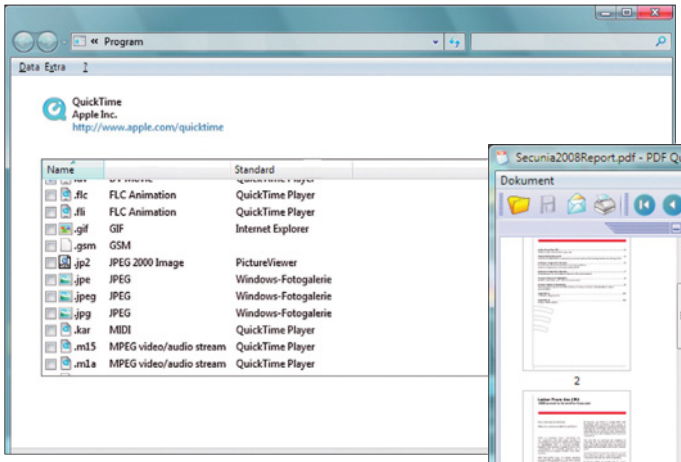
INFO

Zabezpečení Windows

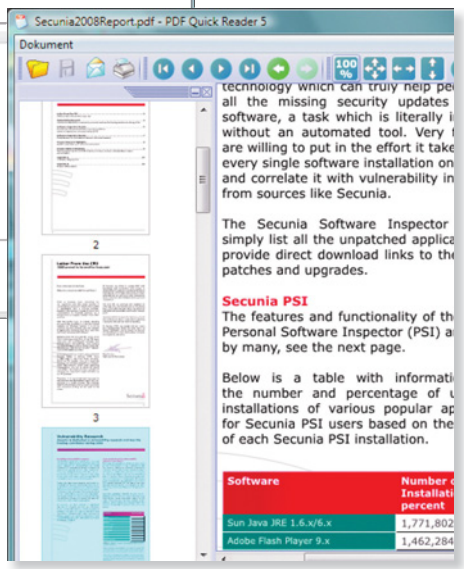
DEP: (Data Execution Prevention) neboli „Omezení spouštění dat“ je sada technologií, které provádějí dodatečné kontroly paměti, aby pomohly zabránit spuštění škodlivého kódu v systému. V praxi to funguje tak, že DEP rezervuje v paměti oblasti pro „nespustitelné“ kódy. Pokud se malware pokusí v této oblasti spustit kód (například pomocí přetečení bufferu), je tento pokus detekován a zastaven. DEP v současnosti podporuje již většina běžného softwaru.

Problém: Celá řada těchto programů funguje ve Windows XP bez této ochrany; pokud je v programu použit plug-in bez podpory DEP, je tato funkce jednoduše vypnuta. Podrobnější informace o této funkci (i s příklady pro Windows XP) najdete na adrese **http://support.microsoft.com/kb/875352**.

ASLR: (Address Space Layout Randomization) je metoda, jak útočníkům znemožnit (nebo alespoň ztížit) zjištění místa, kde se nachází důležitý systémový proces. Tato technologie přiděluje systémovým službám náhodně různé oblasti paměti, čímž ztěžuje jejich napadení. ASLR byla poprvé představena až ve Windows Vista, XP touto funkcí nedisponují…



QuickTime: Tento přehrávač byste měli využívat pouze pro přehrání multimediálních formátů od Applu…



PDF Quick Reader: Alternativa k rizikovému Adobe Readeru

odinstalování QuickTimu nebo jeho konfiguraci takovým způsobem, že doplněk přehrává pouze MOV streamy s tím, že pro přehrání všech ostatních formátů budou použity alternativní programy.

U doplňku od Adobe je situace ještě komplikovanější, protože Flash Player je obvykle standardním plug-inem určeným pro on-line sledování filmů a videí. Pokud surfujete pouze po populárních stránkách jako YouTube, pak jste celkem v bezpečí – horší situace je při pravidelných návštěvách rizikových videowebů. Poté vám zbývá jen možnost deaktivovat Flash v prohlížeči nebo použitím filtru blokovat obsah Flashe. Toho lze u Internet Exploreru dosáhnout například pomocí vylepšení prohlížeče s názvem „IE7pro“, ve Firefoxu pak například pomocí doplňku FlashBlock (oba najdete na DVD).

Mimochodem, Firefox ve své aktuální verzi kontroluje, zda není nainstalovaná zastaralá verze Flash Playeru, a doporučí aktualizaci.

Office: Nebezpečné PDF skripty

Po prohlížečích jsou podle X teamu IBM nejběžnějšími cíli hackerů kancelářské programy – a to s téměř 30 procenty útoků. Nejrozšířenější (a tedy nejvíce napadaný) je Adobe Reader, jednoduchá čtečka souborů ve formátu PDF. Důvodem je i to, že v něm najdete i již zmiňované Flash knihovny. Dalším nebezpečným prvkem je tzv. ActionScript, který řídí flashové animace. Chyby v tomto skriptovacím „jazyce“ tudíž ohrožují všechny produkty Adobe – od jednoduchých čteček až po platformy pro webové aplikace.

Nejnovějším příkladem útoku zneužívajícího ActionScript je Heap Spraying. Tato metoda se používá k naplnění RAM nesmyslnými kódy a jejím konečným cílem je přetečení bufferu. Heap Spraying zneužívající JavaScript je velice známý a pro Adobe Reader existuje jednoduché řešení.

Klikněte na nabídku »Edit | Preference« a v sekci „JavaScript“ odstraňte zatržítko u položky »Enable Adobe JavaScript«. Podobný postup pro ActionScript neexistuje, protože tato funkce nemůže být v Adobe Readeru deaktivována.

Chcete-li jako uživatel stát na té bezpečnější straně, doporučujeme nahradit Adobe Reader něčím bezpečnějším – jako je například nástroj PDF Quick Reader, který naleznete na Chip DVD (podobných programů však existuje celá řada). Výhodou těchto alternativních PDF čteček je také skutečnost, že nedokáží zobrazit Flash, a nejsou tedy ovlivněny zranitelnostmi tohoto formátu.

Zdá se vám to jako přehnaná opatrnost? Problémy s Adobe Readerem byly ještě nedávno tak velké, že F-Secure, výrobce bezpečnostních produktů, zrazoval před jeho používáním. Mezitím Adobe reagoval a pro Reader zavedl fixní „Patch-day“ (den, kdy jsou distribuovány opravy programu), podobně jako to dělá Microsoft. Problém týkající se Flash Playeru je ale stále nevyřešený…

Jak jsme zmiňovali již v úvodu, Microsoft Office už není prvořadým cílem pro malwarové útoky. To ale neznamená, že není bez bezpečnostních mezer.

Například v letošním roce bylo nalezeno několik bezpečnostních mezery a všechny byly klasifikovány jako závažné, protože infikované dokumenty obvykle způsobily přetečení bufferu. Postihly především dvě součásti balíku Office: Excel a PowerPoint. Výhodou je, že uživatelé mohou tento problém vyřešit poměrně snadno: stačí na internetu neotevírat dokumenty v těchto formátech.

Pro experty a uživatele, kteří chtějí vědět více, nabízí Microsoft nástroj OffVis (prozatím v beta verzi). OffVis otevírá dokumenty Office, ale zobrazuje je v „Hex kódu“ a ukazuje jejich vnitřní strukturu i s integrovanými prvky. Navíc OffVis také identifikuje škůdce, kteří využívají běžných bezpečnostních mezer.

Žádné opatření vám ale moc nepomůže, budou-li uživatelé ignorovat důležité bezpečnostní aktualizace. To má totiž za následek stále se zvyšující počet infikovaných powerpointových dokumentů, které jsou napadeny přes mezeru objevenou před třemi roky, jež slouží k propašování trojského koně do systému. Tohoto škůdce OffVis zná. A jak je na tom váš Office? AUTOR.@CHIP.CZ

INFO

Pět nejvíce využívaných mezer v prohlížeči

Dvě věci, které jsou společné pro všechny mezery v prohlížečích: z malwarové scény jsou vyhnány pomocí populární Exploit sady nástrojů a mohou být odstraněny pomocí aktualizace softwaru.

1. MICROSOFT MDAC ACTIVEX

Identifikace: CVE-2006-0003
Tato mezera v Microsoft Data Access Components se používá pro přístup do databází a ke zdrojům dat. Umožňuje také útočníkovi obejít nastavení zabezpečení IE.

2. MS SNAPSHOT VIEWER ACTIVEX

Identifikace: CVE-2008-2463
ActiveX plug-in do MS Office – Snapshot Viewer umožňuje vzdálený přístup k počítači a dokáže i nahrávat další škodlivé skripty.

3. ADOBE READER

Identifikace: CVE-2007-5659
Tato zranitelnost způsobí přetečení zásobníku v programu Adobe Reader a umožní propašování dalšího malwaru do počítače.

4. MICROSOFT INTERNET EXPLORER 7

Identifikace: CVE-2009-0075
Při navštívení speciálně upravené webové stránky lze do počítače propašovat prostřednictvím aplikace Internet Explorer 7 škodlivý kód.

5. REALPLAYER ACTIVEX

Identifikace: CVE-2007-5601
Chyba v databázi modulů Real Playeru umožní provedení „přetečení bufferu“.