## Na DVD tentokrát ne...

K většině článků, které v Chipu najdete, vám obvykle nabízíme i servis v podobě programů na DVD. I když několik programů z tohoto textu na našem DVD najdete (např. browsery nebo Spybot S&D), většinu z nich si musíte stáhnout z internetu. Důvod je prostý – v oblasti bezpečnosti je jedním z nejdůležitějších kritérií aktuálnost. Někteří autoři své programy aktualizují i několikrát za týden, a tak instalace staré verze z DVD by byla ztráta času. Doporučujeme stahovat programy pouze z uvedených webů, které jsou ve většině případů domovskými stránkami autorů programu. Na stahovacích serverech často najdete starší verze, na jiných stránkách zase mohou být soubory infikované.

# Akce bez rizika

Bezpečně surfovat po známých webech dokáže i začátečník. Vrátit se z hlubin internetové džungle dokáže jen ostřílený profesionál. *Petr Kratochvíl, petr.kratochvil@chip.cz*

## V tomto článku najdete



Zapnou počítač, po nastartování Windows spustí Internet Explorer a navštíví všechny tři své oblíbené stránky, poté si přečtou poštu na freemailu a nakonec počítač vypnou s pocitem příjemně strávené půlhodinky. Diví se zprávám o počítačových virech a kroutí hlavou nad zprávami o nebezpečí z internetu. Ano, i takoví jsou mezi námi a pro ně je čtení tohoto článku ztráta času. Existuje však i další skupina – ti, kdo se každý den pohybují v temných částech internetových vod, ti, kdo každý den přemýšlí, jak přelstít internetovou mafii. A právě pro ně jsou určeny následující řádky.

## Instruktáž

Ať už si na internetu prohlížíte lechtivé fotografie celebrit, titulky ke svým oblíbeným filmům, nebo prostě jen hledáte zajímavé informace, každý pohyb na webu je pro vás malou bitvou, v níž vyhrává ten lepší. Každá vyspělejší země má své elitní bojové jednotky, které zvládnou to co ostatní nikoli. Ať už jde o jednotky SAS, GIGN nebo SEALs, jejich strategie při akcích na cizím území je vždy podobná:

1. výsadek,
2. zajištění základny,
3. bleskový průzkum,
4. rychlý útok,
5. bezpečný návrat.

Stejná pravidla platí i pro akce v temných částech internetu.

### Výsadek a vybavení

**Lepší výbava a více zbraní ve správných rukou dokážou divy.**

*[plukovník J. Matrix, Komando]*

Řekněme si to na rovinu – Internet Explorer 7 je poměrně kvalitní program, který v řadě oblastí dohnal svou konkurenci. Na tuto „akci" s ním však může jít

## S čím do akce?

**Mozzila Firefox**
Rychlý a spolehlivý nástroj bez výraznějších bezpečnostních slabin. Oblíbený u většiny profesionálů.
**Info:** www.czilla.cz

**NoScript** Účinný nástroj na blokování mnoha útoků. Proti razantnějším útokům je však zcela bezmocný.
**Info:** http://noscript.net/


**Spybot Search&Destroy**
Účinný prostředek proti většině běžných „zranění". V rukou profesionála dokáže zablokovat i nebezpečné „průstřely".
**Info:** www.safer-networking.org

**Process Explorer**
High-tech hračka sloužící ke sledování situace před akcí i během ní. Rozpozná potenciální infiltraci.
**Info:** www.microsoft.com/technet/sysinternals/utilities/processexplorer.mspx

**User Agent Switcher**
Maskovací nástroj pro oklamání nepřítele. Profesionály jím zcela neošálíte, běžní protivníci vás však budou hledat marně.
**Info:** https://addons.mozilla.org/cs/firefox/addon/59?id=59&vid=617

jen naprostý začátečník. Jeho podpora pro ActiveX a pro DLL toolbary je při této akci vhodná stejně jako fén na záškodnickou akci jednotky SAS. Zkušení mazáci sahají po lehce upraveném Firefoxu, případně po vyzkoušené Opeře. Nedoporučují se exotické výstřelky, neboť ty jsou obvykle vytvářeny na jádrech výše uvedených programů.

Nepodceňte ani přípravu další výbavy. Pokud máte nainstalovánu bezpečnostní soupravu, kterou jste kvůli zpomalení počítače vypnuli, opět ji aktivujte – lepší je počítač pomalý a bezpečný než rychlý a zavirovaný. Pokud se k nákupu výbavy teprve chystáte, doporučujeme nainstalovat balík Norton Internet Security, který v oblasti boje s malwarem exceloval i v našem testu. V žádném případě nedoporučujeme spoléhat se na Windows Defender od společnosti Microsoft, který už byl několikrát přímo napaden (pamětníci si určitě vzpomenou na trojského koně BankAsh-A). Před akcí se také vyplatí zkontrolovat systémové procesy – usnadní to pozdější kontrolu a hodnocení akce. Nejjednodušší je použít program Process Explorer, zobrazit seznam procesů a v nabídce *File* zvolit *Save As*. Poslední, z hlediska bezpečnosti však jednou z nejdůležitějších činností je „změna" účtu. Pokud na počítači pracujete s oprávněním administrátora, je více než vhodné před „akcí" snížit svá práva na úroveň obyčejného uživatele.

### Zajištění základny

**Vyrážet do akce ze základny, kterou ovládl zrádce, se nevyplácí.**

*[J. Rambo, Rambo 2]*

Jakékoliv obranné mechanismy jsou zbytečné, pokud je váš počítač již pod kontrolou rootkitu. Bohužel platí, že dobrý rootkit téměř nelze odhalit, přesto nezbývá než se o to pokusit.

Nejspolehlivějším nástrojem proti tomuto zákeřnému škůdci je nabootování z jiného média a porovnání se „standardním" stavem. Pokud se po nabootování objeví v systému pět nových složek, které ve Windows nevidíte, lze s vysokou pravděpodobností předpokládat, že v systému je rootkit. Dalším řešením je sken po síti – i zde lze odhalit přítomnost rootkitu. Pokud ve vašem případě nelze použít ani jedno z předchozích řešení, nezbývá vám než se spolehnout na momentálně nejrozšířenější řešení – na nástroj proti rootkitům. Takových nástrojů je k dispozici celá řada – obvykle je najdete v balících nabízejících komplexní ochranu (Internet Security), zároveň je však většina firem nabízí i zdarma. V tomto případě jde obvykle o malé jednoúčelové aplikace, které →

## Nástroje proti rootkitům

Boj s rootkity je jednou z oblastí, kde více, znamená lépe. Čím více nástrojů použijete, tím větší je pravděpodobnost, že potencionální rootkit najdete.

**RootkitRevealer**
www.microsoft.com/technet/sysinternals/Utilities/RootkitRevealer.mspx

**Blacklight**
www.f-secure.com/blacklight/

**Rootkit Detective**
http://vil.nai.com/vil/stinger/rkstinger.aspx

**Sophos Anti-rootkit**
www.sophos.com/products/free-tools/sophos-anti-rootkit.html

**McAfee Antirootkit**
http://news.bitdefender.com/NW253-en--BitDefender-Releases-Antirootkit-Beta.html

**AVG antirootkit**
www.antirootkit.com/software/AVG-Antirootkit.htm

→ dokážou (nebo se o to alespoň snaží) odhalit rootkit.

Dalším krokem by měla být instalace programu hlídajícího změnu bezpečnostních nastavení. Zde lze doporučit například TeaTimer, který je k dispozici jako součást programu „Spybot – Search & Destroy". Tento bojovník proti malwaru sice nepatří ke špičce, jeho síla totiž spočívá v jiné oblasti. Kromě toho, že dokáže zjistit problémy v registrech nebo odhalit všechny programy a DLL spouštějící se při startu systému, nabízí i hlídač systémových nastavení. Ten vás při změně systémových nastavení vždy upozorní, že se děje něco nekalého.

Ještě než se vydáte za dobrodružstvím, stojí za to vyzkoušet účinnost „základny". Jako zkouška může posloužit například známá služba „Shields UP!". Ta zkontroluje nejen přístupové cesty do vašeho počítače, ale také ukáže, co na sebe při brouzdání prozrazujete. Na podobném principu funguje i česká alternativa Test bezpečnosti **(http://test.bezpecnosti.cz/)**.

### Průzkum

**Budete neviditelní, ale uvidíte vše...**

*[J. Amstrong, Americký ninja]*

S dobrým vybavením a trochou zkušeností se obvykle není čeho bát, ale přesto se najdou chvíle, kdy se nevyplatí riskovat. Našli jste na fóru odkaz na stránky, které slibují lákavý obsah? Přišel vám přes ICQ od kamaráda podezřelý link na web, který byste měli určitě navštívit? Proč si tedy neudělat malý průzkum?

První, poněkud hrubou metodou je využití Googlu. Pokud si jeho pomocí vyhledáte zkoumané stránky, u některých nebezpečných stránek se může objevit zpráva „Tyto stránky mohou poškodit váš počítač". Důležité je slovo „může", protože při rychlosti práce internetové mafie mohou být ty stránky, které jsou dnes bezpečné, zítra zdrojem malwaru nejhoršího ražení. Druhým extrémem můžou být i ne zcela korektní poplachy (viz například web Země pohádek).

Dalším řešením je použití tzv. link skeneru, který dokáže zkontrolovat stránku se zadanou URL, zda neobsahuje nebezpečné prvky. Skener najdete na adrese **http://linkscanner.explabs.com/linkscanner/default.asp**. Jako perličku lze uvést, že firmu, která skener vyvinula, nedávno koupil Grisoft a že tento prvek bude součástí další generace bezpečnostních nástrojů s nálepkou AVG.

Poslední záchranou by měl být Malware Domain List **(www.malwaredomainlist.com/mdl.php)** neboli seznam nebezpečných webů, které obsahují (nebo obsahovaly) trojské koně, exploity či jiný malware.

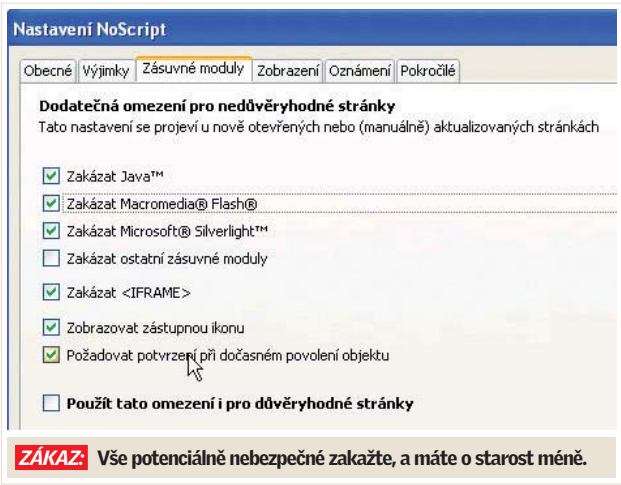
### Rychlý útok

**Pouze bleskurychlý útok je zárukou úspěchu.**

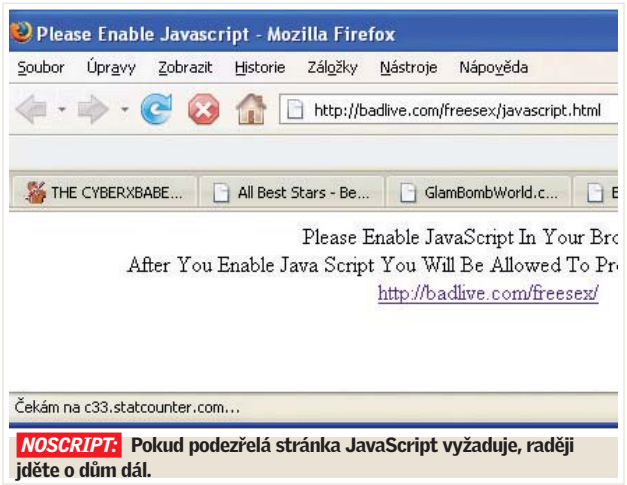
*[B. Lee, Karate Tiger 1]*

Těsně předtím, než se vydáte do hlubin internetu, je nutné učinit několik „předstartovních" příprav. Spusťte program Process Explorer a v nabídce View označte položku New process. Pokud by došlo k infekci počítače a ke spuštění nového procesu, program ho ihned zobrazí zelenou barvou. Druhým důležitým krokem


**LINK SCANNER:** Obzvláště nebezpečné stránky je lepší prozkoumat z bezpečné vzdálenosti. Často se tak vyhnete nepříjemným překvapením.




**ZÁKAZ:** Vše potenciálně nebezpečné zakažte, a máte o starost méně.




**NOSCRIPT:** Pokud podezřelá stránka JavaScript vyžaduje, raději jděte o dům dál.

je instalace rozšíření „No skript“. Jeho pomocí lze zabránit většině útoků, které Firefoxu hrozí. Dokáže totiž v browseru zakázat JavaScript, Javu i Macromedia Flash. Především JavaScript pak povolujte pouze na důvěryhodných webech. Pokud podezřelý web vyžaduje pro „svou plnou funkčnost“ JavaScript, raději „jděte o dům dál“.

Dalším trikem snižujícím riziko nákazy je maskování. Autoři nebezpečných stránek si svoji „záškodnickou práci“ usnadňují tím, že při vstupu na web detekují prohlížeč a teprve na jeho základě se pouštějí do útoku. A právě identifikaci by jim měl ztížit User Agent Switcher, který umožňuje měnit identifikaci browseru – prohlížeč se poté vydává za někoho jiného. Můžete být download manažerem GetRightu, prohledávacím botem na portálu Yahoo nebo spamovým robotem japonského podsvětí – fantazie se zkrátka meze nekladou. Obzvláště hravé uživatele potěší seznam na adrese www.user-agents.org, kde lze najít stovky identit.

### Během akce je třeba dodržovat několik důležitých zásad:

**1.** Na nic bezduše neklikat. Časům, kdy se dealer bezelstně ptal, jestli si ho opravdu chcete nainstalovat, už sice dávno odzvonilo, přesto lze z hlášení systému občas poznat náznaky nebezpečí. Pokud se vám na stránce s obrázky objeví dialogové okno s otázkou, zda chcete doplněk spustit, nebude asi něco v pořádku…

**2.** Nic není zcela zadarmo. Většina z nás sice pamatuje socialismus, na webu však stále platí, že nic zajímavého není zadarmo. V lepším případě „zaplatíte“ sledováním reklamy, v horším instalací trojského koně. Pokud vám někdo nabízí něco zdarma a přitom (jedinou) podmínkou je stažení „stahovacího programu“ nebo lišty, utíkejte pryč, až se vám bude prášit od myši.

### Návrat na základnu

**Doma je doma...**

*[Kevin M.; Sám doma]*

Po návratu z nebezpečných vod lze doporučit okamžitou kontrolu procesů (uložení současného stavu a porovnání se souborem uloženým před akcí) a kompletní sken celého počítače. Pokud na svém počítači nemáte kvalitní antivirový produkt, lze využít i některý z on-line skenerů nabízených známými bezpečnostními firmami. K dispozici je jich mnoho, jmenujme alespoň tři:

- Panda Active Scan **(www.pandasecurity.com/homeusers/solutions/activescan/?)**,
- Kaspersky Online Scanner **(www.kaspersky.com/virusscanner)**,
- F-Secure Online Virus Scanner **(http://support.f-secure.com/enu/home/ols.shtml)**.

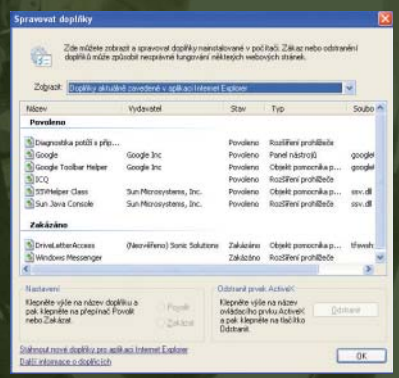
Po dokončení skenování smažte dočasné soubory ve složce Temporary Internet Files, a úklid je hotov. Váš počítač je opět v kondici a připraven na další nebezpečnou akci.

*Petr Kratochvíl*

## Pro případ nouze

Jak jsme uvedli už na počátku, návštěva nebezpečnějších oblastí internetu s microsoftským Internet Explorerem 7 (nebo ještě hůře s verzí 6) je na hranici mezi nebezpečným hazardem a cílenou sebevraždou. Přesto se vám může stát, že se tam s tímto browserem budete muset vydat, byť jen na chvíli. Než se kamkoliv vydáte, doporučujeme provést následující nouzové úpravy. Klikněte v Internet Exploreru na nabídku *Nástroje / Nastavení Internetu* a v následujícím okně na kartu *Zabezpečení*. Poté zvolte „Internet“ a v dolní části okna klikněte na tlačítko *Vlastní úroveň*. Zde deaktivujte vše v sekci ActiveX, zakažte také aktivní skriptování a skriptování appletů v jazyce Java. Doporučujeme také v sekci IFRAME zakázat spouštění programů a souborů.

Poslední důležitou sekcí, kterou je nutné mít neustále na očích, jsou doplňky. Klikněte na nabídku *Nástroje / Spravovat doplňky* a zvolte příkaz *Povolit nebo zakázat doplňky*. Zde najdete seznam všech nainstalovaných nebo aktuálně zavedených doplňků pro IE. Pokud se prohlížeč začne chovat podezřele nebo nestandardně, měla by první kontrola proběhnout právě sem...




**DOPLŇKY:** Komponenty ActiveX bývají spíše přítěží než výhodou...