ÚTOKY PŘÍMO z prohlížeče

Největší hrozbu pro počítačové uživatele už nepředstavují infikované e-maily nebo USB disky s malwarem, ale obyčejné surfování. My vám poradíme, jak rizika minimalizovat.

PETR KRATOCHVÍL

Prvořadým cílem naprosté většiny hackerů a počítačových podvodníků je zisk, čemuž se snaží přizpůsobit i vyvíjený malware. A ač jsou způsoby využití počítače různé, jednu činnost mají uživatelé společnou – surfování na internetu. Toho si pochopitelně všimli i hackeři.

Útoky na počítač

Způsobů, jak mohou autoři malwaru propašovat své výtvory na váš počítač, je celá řada. Stále oblíbenou klasikou jsou infikované USB disky, pomocí kterých se šíří nákaza jako za starých časů, a účinný může být také personalizovaný phishing. Při něm hacker uživatele přesvědčí, že by měl navštívit určitý web a z něj si něco stáhnout do počítače. V tomto případě je malware maskován jako užitečný program, kodek nebo přehrávač videa. Obě zmiňované metody ale mají celou řadu nevýhod. Velké množství uživatelů už má pro USB vypnutý autostart, případně cizí disky rovnou kontrolují antivirem. Účinný phishingový útok zase vyžaduje užší zaměření (nebo určení konkrétního cíle a využití spear phishingu), což zvyšuje náklady na útok a snižuje jeho efektivitu.

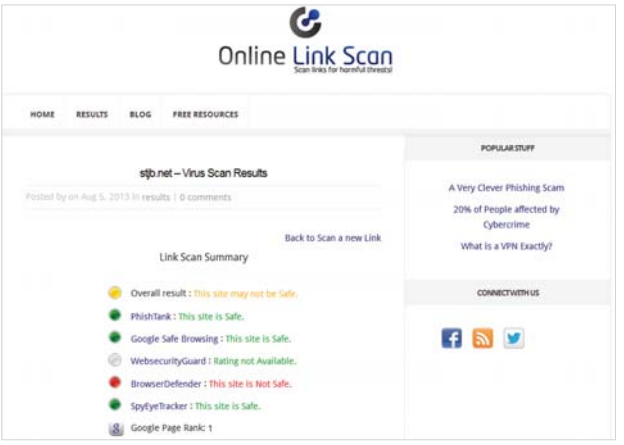
Autoři malwaru jsou si těchto slabin vědomi, a proto stále častěji využívají pro své útoky infikované webové stránky. Mechanismus takovéhoto útoku je relativně jednoduchý a umožňuje zasáhnout široké spektrum uživatelů: nejprve je hacknuta libovolná WWW stránka a do ní je propašován škodlivý kód. Jakmile uživatel tuto stránku navštíví, pomocí JavaScriptu je prověřen software v počítači (operační systém, prohlížeč, doplňky...) a zjištěny jeho zranitelnosti. V případě nalezené slabiny je použit potřebný exploit, který umožní snadný průnik do systému. Poté jsou deaktivovány bezpečnostní mechanismy a případně otevřeny další komunikační kanály (porty). Jakmile má hacker počítač pod kontrolou, je na něj nahrán malware podle potřeb hackera – například čtečka zaznamenávající stisknuté klávesy nebo řídicí prvek botnetu.

Problémem útoků tohoto typu je jejich automatizace – pro úspěšný průnik stačí jediná skulina v jinak dobře chráněném systému.

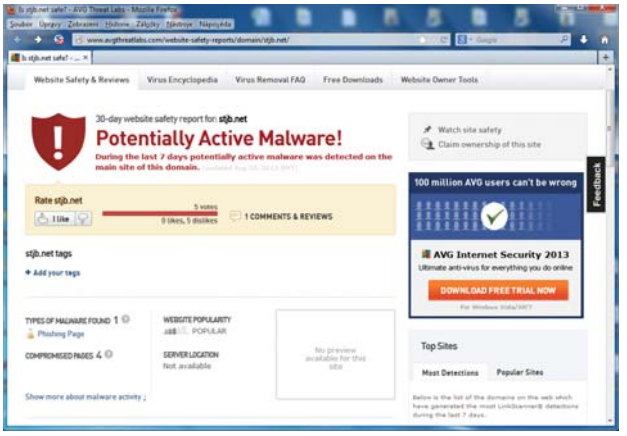
Jak se chránit

Méně zkušené uživatele určitě napadne, že stačí nenavštěvovat nebezpečné weby, a riziko infekce je minimální. Tento způsob ochrany ale bohužel nefunguje: cílem hackerů jsou často obyčejné weby (blogy, diskusní fóra, zpravodajské stránky), které za rizikové rozhodně označit nelze. Zajímavým paradoxem je, že mezi nejméně rizikové patří erotické stránky – jejich vlastníkům často přináší nemalé zisky, a tak je jejich ochrana na velmi dobré úrovni. Ochrana před tímto typem útoků ale není nemožná a surfaři mají teoreticky dvě možnosti, jak hackerům ztížit jejich práci.

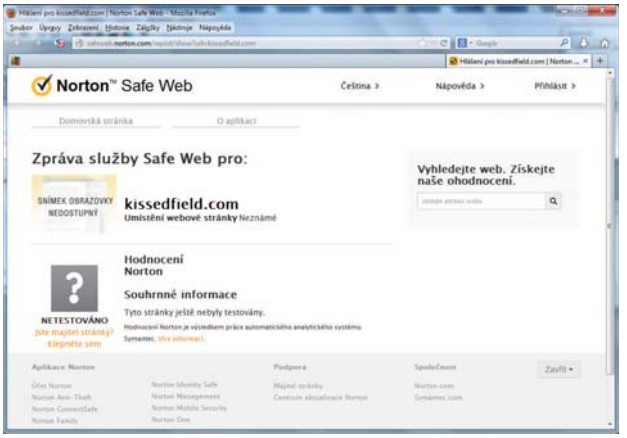
Nejefektivnější je minimalizace potenciálně zranitelných aplikací. To znamená nejen pravidelnou aktualizaci operačního systému a používaných programů, ale především vypnutí většiny doplňků pro prohlížeče. V ideálním případě by měl být vypnut JavaScript a zakázány všechny rizikové prvky – především Java, Flash, Quicktime a různorodé doplňky od Adobe (viz graf → str. 108). Nevýhodou této strategie ale je, že prudce poklesne komfort surfování – především vypnutý JavaScript na celé řadě webů znamená jejich omezenou funkčnost. Určitým kompromisem může být v případě Firefoxu použití doplňku NoScript, který umožní povolení konkrétních prvků pro zvolené



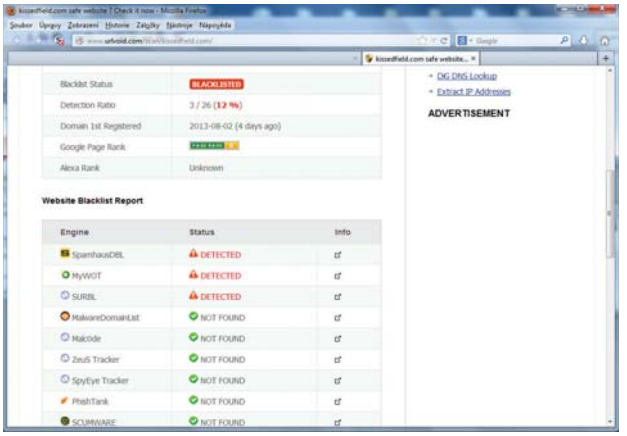
Vyberte si: Typickým problémem celé řady služeb je fakt, že místo pomoci vám rozhodování, zda je web bezpečný či nikoliv, spíše ztíží.



Přestože je služba pouze v angličtině, nemá ani začátečník problém se zjištěním typu hrozby.



Link skenery některé méně frekventované weby nemusí vůbec znát.



Využití agregátoru je v tomto případě výhodou – potvrzení hrozeb ze tří zdrojů už na lehkou váhu rozhodně brát nelze.

weby, ale ani tato taktika není dokonalá. Méně zkušený uživatel může například jen s obtížemi poznat, kdy může JavaScript povolit a kdy nikoliv.

Druhou možností je využití tzv. link skenerů, které by vám měly napovědět, zda je web, který se chystáte navštívit, bezpečný. Link skenery jsou v současnosti nedílnou součástí kvalitních bezpečnostních balíků, celá řada firem je ale také nabízí jako bezplatnou internetovou službu. Bohužel ani tyto na první pohled dokonalé nástroje vám stoprocentní ochranu nenabídnou.

Jak poznat bezpečné stránky?

Aby link skener zcela znemožnit útok ze stránek na počítač uživatele, musel by vždy před návštěvou vybraného webu provést jeho důkladnou kontrolu – prověřit všechny jeho prvky, případně i jeho podstránky. To ale v některých případech není technicky možné (například u reklamních bannerů), ale ani žádoucí. Stačilo by totiž, aby si o kontrolu webu zažádalo několik desítek uživatelů najednou, a zátěž webu by se zvedla jako při DOS útoku. Proto se pro kontrolu bezpečnosti navštěvovaných webů používají dvě méně drastické metody.

První z nich využívá většina známých link skenerů (obvykle i těch z placených bezpečnostních balíků). Spočívá v tom, že web není kontrolován při každé návštěvě, ale jen jednou za určité časové období – v řádu hodin či dnů. Pokud je navíc některý z uživatelů bezpečnostního balíku vystaven útoku z tohoto webu, jsou stránky označené za nebezpečné. Zde hrají důležitou roli především dva faktory: využití cloudové sítě firmy a počet uživatelů programu. Jinými slovy – čím větší firma s pokročilejšími cloudovými službami a čím větší počet uživatelů, tím větší šance na odhalení nebezpečného webu. Pokud tedy využíváte bezplatnou webovou variantu link skeneru, doporučujeme podezřelý web zkontrolovat pomocí více služeb.

Druhou metodou, jak zjistit potenciálně rizikový web, je použití služby, která využívá hodnocení reputace. Typickým představitelem této metody je služba WOT (Web of Trust), která kombinuje zkušenosti a hodnocení uživatelů s dalšími nezávislými zdroji. V databázi WOT je nyní více než 20 milionů stránek, které jsou uživateli hodnoceny z hlediska několika kritérií – důvěryhodnosti, ochrany osobních dat nebo bezpečnosti dětí. Pokud máte v prohlížeči nainstalován doplněk, který je k dispozici pro všechny hlavní prohlížeče, zobrazí se vám před navštívením již hodnocené stránky semafor: zelená znamená zcela bezpečné stránky, oranžová částečně bezpečné a červená nebezpečné.

Z výše uvedeného principu vyplývají i slabiny služby – subjektivní hodnocení spoléhá především na uživatele, kteří nemusí potenciální bezpečnostní hrozby odhalit, nebo naopak bezpečné stránky (které měly v minulosti problémy) mohou být označeny jako rizikové.

Jak je tedy zřejmé, zcela bezpečného surfování nelze teoreticky dosáhnout ani s jednou metodou – pojďme se ale podívat, jak to vypadá v praxi.

Spolehlivost nehledejte

Kontrolu bezpečnosti surfování většina z nás očekává právě na webech firem zabývajících se počítačovou bezpečností. A pravda je, že ji u většiny z nich najdete – obvykle je sice (z logických důvodů – viz Jak jsme testovali) poněkud skrytá, ale minimálně pomocí Googlu není těžké ji odhalit.

JAK JSME TESTOVALI

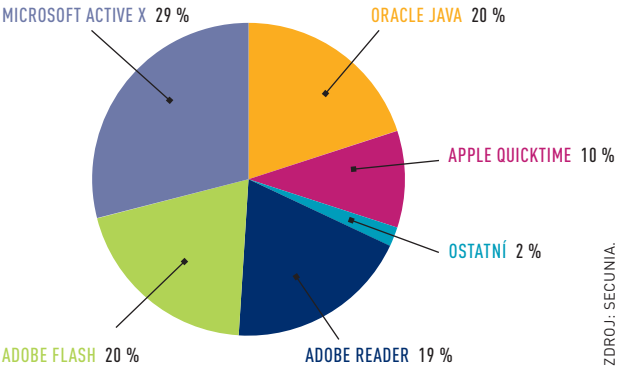
V rámci tohoto testu tentokrát vítěze nenajdete. Během prověřování jednotlivých služeb jsme se shodli na tom, že žádná z nich nesplňuje naše požadavky. Přesto si z testovaných parametrů můžete udělat obrázek o tom, jak na tom jednotlivé služby jsou.

Klíčovým ukazatelem kvality link skenerů by měla být detekce hrozeb na zvolených webech. Ani u jedné z testovaných služeb se nám ale nepodařilo najít web, u něhož by se i všechny ostatní služby shodly na jeho nebezpečnosti. Častokrát je tedy uživatel nucen řešit své dilema tak, že pokud je web alespoň jednou službou označen jako nebezpečný, není vhodné ho navštívit.

Dalším sledovaným údajem byla informace o času skenu – uživatel si tak může udělat obrázek o aktuálnosti údajů. Některé weby ale v této oblasti poněkud zaostávají, a tak tuto informaci tají. U celé řady webů nám také chyběla historie hrozeb – surfař si díky ní může udělat obrázek o kvalitě práce webmastera. A pokud byl již web v minulosti několikrát infikován, může být jeho návštěva rizikem. U některých služeb chyběla i informace, jaká hrozba byla na stránkách nalezena. Zpráva „Web je nebezpečný, dávejte si pozor" totiž příliš důvěry nedává. Jen okrajovou záležitostí byla rychlost testovaných služeb, která je (kromě Comodo Web Inspectoru) dostatečná.

SLABÁ MÍSTA BROWSERŮ

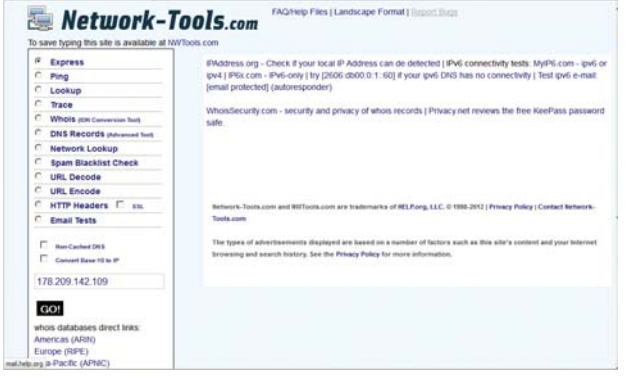
Hackeři využívají doplňky v internetových prohlížečích pro útok na počítač. Tyto rizikové prvky byste pro větší bezpečnost měli mít v ideálním případě deaktivované.



ZDROJ: SECUNIA.

PRO WEBOVÉ ČMUCHALY

Při prověřování jednotlivých internetových stránek vám doporučujeme navštívit web Network Tools (**network-tools.com**). Najdete na něm celou řadu praktických nástrojů, umožňujících například zjistit, komu patří konkrétní web nebo jestli není na blacklistu spammerů. Dvanáct šikovných služeb a celou řadu praktických odkazů využijí jak začátečníci, tak i zkušení surfaři.



Typickou ukázkou může být Symantec: jeho služba SafeWeb je sice v češtině, najít na ni ale odkaz z českého webu Symantecu je práce pro zkušeného detektiva. Celkově je však stránka přehledná a nechybí informace s popisem nalezené hrozby. Podstatně hůře je na tom McAfee a jeho SiteAdvisor. Na potenciální hrozbu sice upozorní, podrobnější informace ale chybí. Zpráva „Tento odkaz je podezřelý. Byl testován a byla zjištěna potenciální rizika zabezpečení. Buďte opatrní“ působí spíše trapným dojmem.

Pravým opakem je služba Website Safety Rating and Reports od AVG. K dispozici je sice jen v angličtině, za to na ní ale najdete informaci, kdy byl web testován a jaké konkrétní hrozby na něm byly nalezeny. Často zde také najdete komentáře k podezřelým webům, které vám umožní udělat si lepší obrázek. Zcela zklamal web Browsing Protection od F-Secure. Je sice v češtině, ale chybí jakékoliv podrobnosti o skenování či nalezených hrozbách. To důvěru surfařů rozhodně nezíská.

O něco lépe si vedl Web Inspector od Comodo. Je mnohem přehlednější a nechybí ani přesný čas skenování – naše výtka tak putuje jen k příliš krátké historii skenování: sedm dní je pro získání obrázku o spolehlivosti stránek příliš málo.

Na závěr našeho testování jsme ještě vyzkoušeli službu URL Void a byli jsme příjemně překvapeni. Tento agregátor link skenerů nabízí prověření webu u 26 služeb a databází, což z něj dělá našeho jednoznačného favorita. Není sice v češtině a chybí u něj i historie hrozeb, vše ale vynahrazuje svými schopnostmi. Nelze ho sice označit za dokonalý nástroj pro bezpečné surfování, z námi testovaných služeb má k němu ale nejblíže.

PETR.KRATOCHVIL@CHIP.CZ

SLUŽBY NA KONTROLU ODKAZŮ

VÝROBCE	SYMANTEC	AVG	MCAFEE	F-SECURE	COMODO	NOVIRUS-THANKS COMPANY
SLUŽBA	Safe Web	Website Safety Rating and Reports	SiteAdvisor	Browsing Protection	Web Inspector	URL Void
ADRESA	safeweb.norton.com	avgthreatlabs.com/website-safety-reports	siteadvisor.com	browsing-protection.f-secure.com/swp	siteinspector.comodo.com	urlvoid.com
ČEŠTINA	•	–	•	•	–	–
DATUM POSLEDNÍHO TESTU	–	•	–	–	•	•
HISTORIE HROZEB	–	•	–	–	•	–
POČET SKENŮ/DATABÁZÍ	1	1	1	1	1	26
POPIS HROZBY	•	•	–	–	•	•