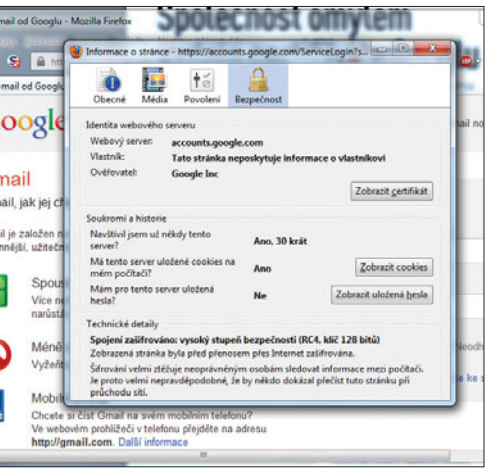
Omylem vydané certifikáty Googlu

Poskytovatel SSL certifikátů omylem vydal dvěma zákazníkům důležité certifikáty.

Turecký vydavatel certifikátů Türktrust vydal v srpnu 2011 SSL certifikáty, pomocí nichž je možné bez dalších kontrol vytvořit doménové certifikáty – tzv. Sub CA certifikáty. Certifikáty obdrželi dva zákazníci – turecké ministerstvo pro informační technologie a jedna turecká banka. K situaci prý došlo omylem, kvůli chybě při správě certifikátů, nicméně některé zdroje naznačují, že vzhledem k rozsahu domén v rozšíření Subject Alternative Name nemuselo jít o náhodu. Podrobnosti o celém případu najdete na webu KrebsonSecurity (**bit.ly/VydnG8**).



Zatím není známo, zda byly certifikáty zneužity, nicméně pokud by se dostaly do špatných rukou, škody by mohly být obrovské: hackeři by mohli vytvořit falešné webové stránky, které by se díky certifikátům tvářily jako pravé.

FALEŠNÉ CERTIFIKÁTY MOHOU OKLAMAT I ODBORNÍKY

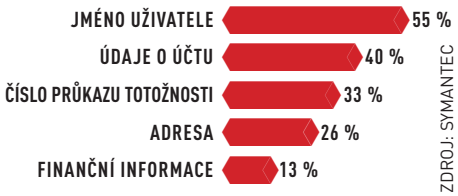
Smutné je, že k podobné události nedošlo poprvé. Už v roce 2011 byly v Íránu falešné certifikáty domény Googlu zneužity k útokům typu man-in-the-middle. O něco později vydal partner certifikační autority Comodo falešné certifikáty pro weby Mozilly, Googlu, Yahoo a Skypu. V nových verzích internetových prohlížečů jsou zmiňované certifikáty zakázány, aktualizace důvěryhodnosti certifikátů Türktrust proběhla na počátku letošního roku. Nebezpečí takovýchto kauz spočívá v tom, že falešné certifikáty nemusí rozpoznat ani odborníci. Zkušenější uživatelé to řeší například tak, že některé problematické certifikační autority (např. Comodo) nepovažují za důvěryhodné.

Pravý nebo falešný?

Rozpoznat pravý certifikát není úplně jednoduché.

KTERÁ DATA KRADOU HACKEŘI?

Při typické krádeži dat získají útočníci pravé jméno uživatele a informace o jeho účtu.



ZDROJ: SYMANTEC

Antiviry: 400% nárůst

Obchod Alza.cz zaznamenal nebývalý zájem o licence antivirových programů, který může souviset s DDoS útoky. Manažer nákupu Alza.cz Petr Hrabal k tomu dodává: *„Těší nás zodpovědnost a chování našich zákazníků, kteří nechtějí podcenit vzniklou situaci. Je vidět, že povědomí o nebezpečí virové nákazy počítače je už nyní velmi vysoké."*

Evropa proti internetovým podvodům: Vytvořeno centrum počítačové kriminality

11. ledna tohoto roku bylo oficiálně vytvořeno Evropské centrum pro boj proti počítačové trestné činnosti. Centrum, které má své sídlo v Europolu v Haagu, chce podle komisařky EU Cecilie Malmströmové operativně podporovat individuální počítačovou obranu států EU a rozšiřovat odborné znalosti.

Tým složený z třiceti osob se chce zaměřit na boj proti organizované trestné činnosti a na odhalování finanční trestné činnosti.

DATOVÉ ÚNIKY MĚSÍCE

UNISTER: ÚNIK DAT Z CESTOVNÍ KANCELÁŘE

Data přibližně 4 700 cestujících společnosti Ryanair mohl kvůli chybě cestovní kanceláře Urlaubstours získat kdokoliv. Volně k dispozici byla například jména a letové trasy, dokonce bylo možné provádět změny v rezervacích. Podle vedení mateřského koncernu Unister je už mezera uzavřena. Jméno firmy, provozující kromě cestovní kanceláře i celou řadu dalších webů, ale není našim čtenářům neznámé: v prosinci loňského roku jí unikly údaje o 400 000 kreditních kartách.

DAWANDA: PŘÍSTUP K UŽIVATELSKÝM ÚČTŮM

Nákupní portál DaWanda musel na začátku ledna bojovat se zásadním bezpečnostním problémem. Uživatelé získali po přihlášení přístup k informacím o účtech jiných uživatelů, a to i s jejich citlivými daty. Podle mluvčího portálu DaWanda mohl být příčinou i útok hackerů. Problém už prý byl ale odstraněn.

UBISOFT UPLAY: HACKEŘI UKRADLI ÚČTY

Celá řada uživatelů on-line herní platformy Uplay už nemá přístup ke svým hráčským účtům. Uživatelé obdrželi automatickou zprávu, že na jejich účtu došlo ke změně: útočníci nahradili původní e-mailovou adresu určitou ruskou adresou. Ubisoft útok potvrdil, má ale podezření, že uživatelé používají stejné heslo u více služeb a hackeři ukradli hesla z nich.

11 %

VŠECH UŽIVATELŮ SMARTPHONU SI UKLÁDÁ ČÍSLO SVÉ KREDITNÍ KARTY PŘÍMO DO PŘÍSTROJE.

FOTO: THINKSTOCK/HEMERA

Nadvláda INF/Autorun pokračuje i v roce 2013

Nevypadá to, že by škodlivý kód INF/Autorun měl v nejbližší době opustit post nejrozšířenější hrozby na světě. Žebříčku malwaru vévodil i v lednu 2013, s mírou infekce 3,27 %. Na druhé místo se celosvětově i v Evropě zařadila hrozba HTML/Iframe.B, na třetí pozici zůstal HTML/ScrInject.B.
V Evropě se na prvním místě žebříčku usadil malware Win32/Qhost, který zároveň dosáhl ve světě na čtvrtou pozici.

INF/Autorun představuje různé druhy malwaru využívající jako cestu k napadení počítače soubor autorun.inf. Tento soubor obsahuje příkaz k automatickému spuštění aplikace po připojení externího média (nejčastěji USB flash disku) k počítači s operačním systémem Windows. HTML/ScrInject.B je generická detekce webových HTML stránek obsahující falešný skript nebo iframe tag, který automaticky přesměruje uživatele ke stahování škodlivého kódu. HTML/Iframe.B označuje generické detekce škodlivých iframe tagů vložených do HTML stránek, které přesměrovávají prohlížeč na specifickou URL adresu obsahující škodlivý software. Win32/Qhost se před načtením systému sám zkopíruje do složky Windows %system32%. Poté komunikuje přes DNS se svým řídicím a kontrolním serverem. Tento malware se šíří přes e-mail, a jakmile infiltruje systém, umožňuje ho útočníkovi na dálku ovládat.

České uživatele internetu ještě nedávno ohrožovala hrozba, která podvodně ukradla přihlašovací údaje více než 16 tisícům uživatelů sociální sítě Facebook. Trojský kůň využíval ke krádežím přihlašovacích údajů do Facebooku jejich propojení se statistikami uživatele ve hře Texas Holdem Poker, pokud ji uživatel hrál. Texas Holdem Poker je oblíbená facebooková aplikace od společnosti Zynga Inc. Podle stránky AppData má měsíčně více než 35 milionů aktivních uživatelů. Pomocí tohoto malwaru získal útočník přihlašovací údaje uživatele, jeho skóre ve hře a také informaci o tom, kolik kreditních karet má uložených ve svém nastavení Facebooku, a může je tedy použít pro navýšení svého kreditu v pokeru.

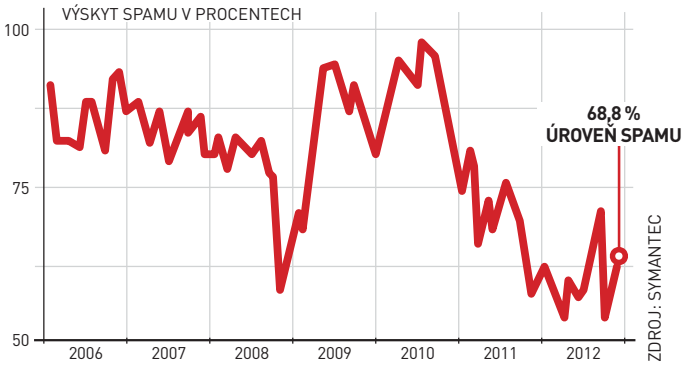
Hráč si totiž může žetony doplnit i výměnou reálných peněz zadáním údajů ke své kreditní kartě nebo PayPal účtu. Pokud šlo o hráče bez kreditní karty nebo s nízkým skóre, dostal nakažený počítač příkaz vložit na jeho facebookový profil odkaz na phishingovou stránku. Ta přímo nebo nepřímo lákala hráčovy přátele na web připomínající hlavní přihlašovací stránku Facebooku. Pokud do ní tito lidé vložili své přihlašovací údaje, ty pak skončily v rukou útočníka. Nutno podotknout, že podobným způsobem mohly být zneužity i jiné facebookové aplikace.

11 milionů počítačů bylo napadeno největším světovým botnetem Butterfly.

36 milionů eur bylo ukradeno pomocí mobilního trojského koně Zeus.

SPAM NA MINIMECH

Celosvětový výskyt spamu průběžně klesá: úspěšnost „obchodních" e-mailů i nadále klesá a díky tomu klesá i počet nevyžádané pošty v našich schránkách. Zatímco v srpnu 2010 tvořil spam téměř 91 % poštovního provozu, v současnosti je to už pouze 69 %.



ODKUD K NÁM SPAM PŘICHÁZÍ

INDIE	9,0 %	RUSKO	7,1 %
USA	7,6 %	KANADA	6,0 %
BRAZÍLIE	7,3 %	VIETNAM	4,2 %

Samsung: Vadné CPU nabízí root přístup

Chyba v zabezpečení, která byla zjištěna v prosinci 2012, usnadňuje na smartphonech spouštění programů s právy administrátora. Ovlivněna jsou zařízení s CPU Samsung Exynos 4210 a 4412, tedy například Galaxy S II a III a Galaxy Note 10.1. Ve Velké Británii je již k dispozici záplata, která by brzy měla být dostupná všude.

Java: Hackeři pilně využívají mezery

Bezpečnostní expert s pseudonymem Kafeine objevil kritickou mezeru v nejnovější verzi softwaru Java (verze 7, aktualizace 10). Dokonce na svém blogu nabízí ke stažení kód použitelný k provedení útoku. Malware lze spustit na počítači přes zranitelnost, kterou již hackeři aktivně využívají. Aktualizace Javy je již k dispozici ke stažení na internetu.

Jak malware vydělává peníze

Tým laboratoří FortiGuard Labs mapuje současný svět internetových hrozeb: bankovní malware, falešné antiviry i vyděračské programy.

Fortinet zveřejnil studii o vývoji kybernetických hrozeb ve čtvrtém čtvrtletí roku 2012. Analýza, kterou vypracoval tým odborníků laboratoří FortiGuard Labs, ukazuje čtyři typické metody, které internetoví podvodníci používají při okrádání svých obětí; každé z těchto metod odpovídají i konkrétní druhy malwaru. Studie také upozorňuje na rostoucí množství malwaru pro systém Android (zejména reklamní sady) a na aktivity hacktivistů, jako jsou například pokusy o skenování webových serverů a hledání jejich zranitelností.

Simda.B: Tento sofistikovaný malware předstírá, že se jedná o aktualizaci přehrávače Flash Player. Po instalaci krade malware uživatelská hesla, což útočníkovi umožní získat přístup k účtům oběti. E-mail a účty na sociálních sítích jsou poté zneužívány k šíření spamu a dalšího malwaru. Spravuje-li oběť nějaký web, podvodníci sem začnou umísťovat škodlivý obsah. Pokoušejí se rovněž zneužít účty v on-line platebních systémech.

FakeAlert.D: Jedná se o falešný antivirus (shareware, fake AV). Šíří se prostřednictvím pop-up oken, která tvrdí, že počítač je infikován. Malware předstírá, že po zaplacení odstraní z počítače oběti nalezené viry. FakeAlert.D se chová způsobem typickým pro většinu hrozeb z této kategorie malwaru.

Ransom.BE78: Jde o software vydírající uživatele (ransomware), který oběti brání v přístupu k datům na počítači. Po útoku malwaru mohou nastat problémy při spouštění počítače nebo malware zašifruje uživatelova data. Podvodník pak požaduje, aby uživatel zaplatil za opětovné zpřístupnění dat. Na rozdíl od falešného antiviru nedává ransomware uživateli volbu program nainstalovat, ale instaluje se automaticky sám.

Zbot.ANQ: Tento trojský kůň je programem z rodiny nechvalně známého malwaru Zeus. Funguje na straně klienta, zachytí přihlašovací údaje do on-line bankovnictví a pomocí sociálního inženýrství se pokouší o instalaci i do smarpthonu. Pak dokáže ovládnout celou bankovní transakci včetně kódu k potvrzení platby posílaného SMS zprávou a začne z bankovního účtu oběti převádět peníze na účty prostředníků (bílých koní).

ANDROID: NEVYŽÁDANÁ REKLAMA NA VZESTUPU

Výzkumníci FortiGuard Labs zaznamenali již ve třetím čtvrtletí roku 2012 reklamní sadu Android Plankton. Tento malware zobrazuje na infikovaném zařízení se systémem Android ve stavovém řádku nevyžádanou reklamu a provádí i další škodlivé aktivity. V posledních třech měsících sice samotná sada Plankton ustoupila, nicméně objevily se kity s podobnou funkčností, které se jí zřejmě přímo inspirovaly. Uživatelům lze pro ochranu doporučit, aby si při instalaci nové aplikace vždy všímali, jaká požaduje práva. Mobilní aplikace by se také měly stahovat ze spolehlivých zdrojů; je vhodné vybírat aplikace, které již vyzkoušeli a kladně hodnotili další uživatelé.

SKENOVÁNÍ WEBOVÝCH SERVERŮ

V posledním čtvrtletí roku 2012 byla zaznamenána vysoká aktivita nástroje ZmEu. Jedná se o sadu vyvinutou rumunskými hackery, která slouží k nacházení webových serverů, na nichž běží zranitelná verze nástroje phpMyAdmin (slouží pro administraci databáze MySQL). Útočníci, především z řad hacktivistů, mohou takový server ovládnout. Laboratoře FortiGuard Labs doporučují přejít na nejnovější verzi softwaru phpMyAdmin.

Antivirové řešení pro Android

Společnost TrustPort vydala antivirové řešení pro přístroje s mobilní platformou Android. „Aplikace TrustPort Mobile Security pro Android používá výkonnou technologii s vlastním skenovacím motorem. Naši vývojáři používají rozsáhlou databázi virových vzorků a nebezpečných webových stránek. Proto můžeme našim zákazníkům přinést kvalitní ochranu mobilních zařízení před malwarem a jinými typy útoků," říká Pavel Mrnuštík, ředitel firmy TrustPort. „Naši novou aplikaci ocení také rodiče, protože Mobile Security chrání jejich děti. V případě, že se ztratí dítě, které má na svém smartphonu nainstalovánu naši aplikaci, jeho rodiče ho vždy najdou díky integrované funkci geolokace," dodává.

Bezpečnostní řešení pro mobilní zařízení TrustPort Mobile Security kontroluje na vyžádání každou aplikaci, kterou si uživatel nainstaluje, a každý soubor, který si stáhne. Pokud si uživatel instaluje či aktualizuje již nahranou aplikaci, TrustPort Mobile Security tuto aplikaci automaticky ověří a v případě potřeby ji umožní odinstalovat. U produktu TrustPort Mobile Security jsou samozřejmostí funkce, jako je skenování telefonu na vyžádání či rezidentní ochrana proti malwaru, ale i řada dalších – webový štít, správce aplikací, filtr hovorů a SMS, šifrovaná záloha dat a geolokace.

Další díry u Adobe...

Aplikace od firmy Adobe jsou už dlouhou dobu známé jako obrovské potenciální riziko. Tuto teorii znovu potvrdily i dva nové nálezy: v Shockwave Playeru byly objeveny dvě zranitelnosti umožňující poškození paměti, respektive přetečení bufferu s následkem spuštění libovolného kódu. Zranitelnosti se týkají verzí pro Windows a Apple OS X. Ještě horší je situace u aplikace Flash Player, kde bylo nalezeno dalších šest zranitelností, přičemž pět z nich umožňuje spuštění libovolného kódu a jedna únik citlivých informací.

U Flash Playeru je nepříjemné, že kromě Windows a Apple OS X jsou zranitelností postiženy i verze pro Linux a mobilní platformu Android. Problémy aplikace Flash Player se navíc týkají i produktu Adobe AIR. Podrobnější informace o všech zranitelnostech najdete na webu firmy Adobe. Na všechny zmiňované zranitelnosti již byly vydány záplaty, proto doporučujeme uživatelům co nejdříve aplikace aktualizovat.

PLACENÁ INZERCE

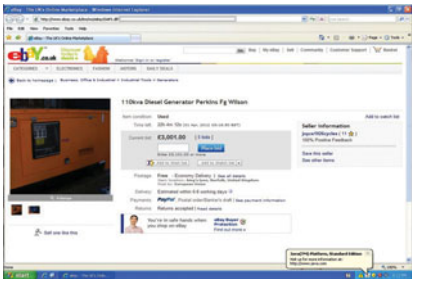
Už i dítě umí vytvořit internetový malware

Společnost AVG vydala zprávu o bezpečnosti na internetu za čvrté čtvrtletí roku 2012, ve které překvapí především informace o nových škodlivých kódech, včetně trojského koně, kterého vytvořilo jedenáctileté dítě.

Společnost AVG vydala zprávu o bezpečnosti na internetu za čvrté čtvrtletí, ve které překvapí především informace o nových škodlivých kódech, včetně trojského koně, kterého vytvořilo jedenáctileté dítě.

Děti jsou v oblasti informačních technologií v současné době velmi zdatné, a to v mnohem nižším věku, než tomu bylo u předchozích generací. Společnost AVG dokonce získala důkazy, že děti jsou schopné vytvořit malware, aby ukradly logovací data hráčů on-line her. Není podstatné, zda jde o jejich vrstevníky, nebo dospělé hráče. Na první pohled se může zdát, že odcizení přihlašovacích údajů do hry není až tak velkým problémem. On-line herní účty však bývají často napojeny na platební nebo kreditní karty, aby mohl uživatel během hry například nakupovat předměty či bonusy, případně existuje virtuální měna, jejíž hodnota se může vyšplhat k tisícům korun. Dochází bohužel i k situacím, že hráč pro přístup do svého herního účtu používá stejné přihlašovací údaje jako třeba do svých sociálních sítí, čímž se navíc vystavuje nebezpečí kyberšikany, krádeže identity a dalších nepříjemností.

„V poslední době jsme si všimli několika příkladů, kdy velmi mladí lidé vytvářeli malware, včetně jednoho jedenáctiletého Kanaďana," říká Yuval Ben-Itzhak, technický ředitel AVG Technologies. „Kód je obvykle postaven na základě jednoduchého trojského koně, napsaného za použití .NET Frameworku. Ten se



Výzkumníci AVG narazili na odkaz přesměrovávající na exploit kit Blackhole i na eBay.

zvládne naučit i začátečník, navíc ho lze snadno šířit pomocí linků v e-mailech nebo ho rozesílat po sociálních sítích. Věříme, že těmto dětským programátorům jde většinou jen o vzrušení z pocitu, že mohou nějak vyzrát na svoje vrstevníky, a nejde jim o finanční zisky. Přesto je to bezpochyby znepokojující a stále častěji se objevující skutečnost. Je logické, že někteří z nich budou v budoucnu v pokušení pustit se do závažnějších kyberzločinů."

MOBILNÍ HROZBY STÁLE NA VZESTUPU

Zpráva AVG Technologies rovněž zdůrazňuje dramatický a stálý nárůst mobilního malwaru. Jde hlavně o kódy cílící na Android, velmi populární operační systém Googlu. Během roku 2012 zaznamenaly AVG Threat Labs první rootkit pro Android, příklady útoků na mobilní internetové bankovnictví, škodlivé aplikace, které zasílají prémiové SMS, nebo trojským koněm infikované verze oblíbených her v neoficiálních obchodech s aplikacemi, včetně jedné z nejprodávanějších aplikací Angry Birds Space.

Mobilní hrozby se objevují i v predikcích na rok 2013, také ve formě zvýšeného výskytu tzv. MITMO (Man-In-The--Mobile) útoků, které cílí na aplikace pro počítačové a mobilní internetové bankovnictví.

SADY NÁSTROJŮ NEVYKLÍZEJÍ POLE

Vedle vzestupu mobilního malwaru si Threat Labs všímají také faktu, že sady nástrojů stále dominují oblasti on-line hrozeb. Skoro 60 % veškeré kyberzločinecké on-line aktivity bylo v roce 2012 prováděno prostřednictvím sad nástrojů (exploit toolkitů). Proč k tomu došlo? Zkušení kyberzločinci si uvědomili, že mohou vytvářet a na komerční bázi prodávat sady nástrojů technologicky méně zkušeným kolegům, kteří se snaží proniknout na kyberzločinecký trh. Jedním z příkladů nových exploit kitů, které se objevily v posledním čtvrtletí loňského roku a které se významně podobají Blackhole exploit kitům, je Cool Toolkit. Tento nový toolkit obsadil 16 % v top webových hrozbách v posledním čtvrtletí roku 2012, první místo obsadil se 40 % Blackhole. Další informace o bezpečnostních hrozbách najdete na webu AVG.

Gang počítačových podvodníků zničen

Během několika minulých měsíců pracovali odborníci ze společnosti Trend Micro na shromažďování důkazů v souvislosti s ransomwarem pojmenovaným Reveton, což je virus známý též jako „policejní trojský kůň". Policejní orgány ve Španělsku se jako první začaly tímto případem zabývat, a to v důsledku masivního rozsahu stížností obětí, které na základě falešné zprávy od policie platily finanční pokuty. Trend Micro a španělští kriminalisté na případu úzce spolupracovali, včetně sdílení tajných informací, vzorců chování a souvisejících technických detailů. Na základě výsledků jejich analýz byli kriminalisté schopni zmapovat podvodnou síťovou infrastrukturu, zejména přesměrování provozu a centrální uzly (command a control servery). Tyto informace také přímo přispěly k zatčení minimálně jedenácti osob. Jeden ze zatčených, 27letý muž, je považován za hlavního člena počítačového podvodnického gangu, který ransomware vytvořil. K zatčení tohoto počítačového zločince ruského původu došlo v Dubaji (UAE) a nyní se pracuje na jeho vydání do Španělska, kde bude postaven před soud. Podle odhadů policie „vyprala" jen tato skupina za jediný rok přes milion eur. Podrobnější informace najdete na internetovém blogu firmy TrendMicro (**http://bit.ly/ZaObci**).

Český internet v křížové palbě

Až do nedávné doby jsme se mohli tvářit, že Česko je na internetové mapě tak bezvýznamným hráčem, že se nás kybernetické šarvátky netýkají.

Naše země se však v několika dnech ocitla v kybernetické palbě a její důsledky pocítil každý z nás. V pondělí byly napadeny servery českých zpravodajských webů, v úterý stránky Seznamu a některých úřadů, ve středu pak servery internetového bankovnictví. Útok byl přitom proveden primitivní, ale účinnou, metodou DDoS. Situaci komentuje Vladimír Brož ze společnosti Fortinet.

CO JE DDOS ÚTOK?

Útok DDoS je realizován tak, že směrem k napadenému serveru je vysláno obrovské množství požadavků, např. na zobrazení webové stránky. K serveru, pokud přímo nezkolabuje, se pak nedostanou legitimní uživatelé. Útok DDoS je proveden z velkého množství míst, takže není možné útočníka snadno odříznout, a bohužel ani poznat: využívá anonymitu davu. O nebezpečnosti DDoS útoků se v dubnu 2007 přesvědčilo například i Estonsko. Poté, co byl z centra Tallinu odstraněn pomník rudoarmějce, stalo se cílem bezprecedentního ataku. V zemi na několik dní prakticky přestal fungovat internet. Nefungovala burza, stát neplnil své základní funkce, nepracovaly internetové obchody, platby se prakticky zastavily. Škody šly do desítek milionů dolarů.

KDO NA NÁS ÚTOČÍ?

Správci postižených serverů hlásí, že útoky přicházejí tu ze Švýcarska, tu z Ruska, tu z Polska a dalších zemí. To ale není vůbec podstatné a rozhodně to neznamená, že by nám Švýcarsko, Rusko, Polsko či kdokoliv jiný vyhlásil válku. Jednak je možné adresu původce poměrně snadno zfalšovat (a zamést tak stopy), jednak se k útokům využívají sítě unesených počítačů (zombie). To jsou počítače, do kterých útočníci pronikli a využívají je pro své nekalé rejdy. Jejich majitelé přitom zpravidla vůbec nic netuší.

Musíme se tedy smířit s tím, že útočníka takto přímo nevystopujeme. Podívejme se na to, oč mu jde. Tě() půjde o výpalné, kvůli kterému se podobné útoky často dějí. Na to je aktuální útok zaměřen na mnoho serverů a rychle mění cíle. Pak je tu varianta, že někdo chce na něco upozornit: kybernetické útoky jsou čím dál tím oblíbenějším nástrojem aktivistů, pomáhajícím jim ke zviditelňování se (viz aktivity skupiny Anonymous). K útokům se však nikdo bezprostředně nepřihlásil a chybí jim jakýkoliv podpis. K přihlášení samozřejmě může dojít i zpětně, protože útok byl evidentně dobře připraven a promyšlen. Možná šlo o demonstraci síly a schopnosti. Je tu ale samozřejmě i možnost, že útočníkovi je nějaká Česká republika úplně ukradená, že si nás, obrazně řečeno, napíchl špendlíkem na mapě a že si jen testuje své možnosti a schopnosti – řízení počítačů, koordinaci útoků, rychlé změny cílů, reakci na obranná opatření apod. Z toho by vyplývalo, že skutečný útok přijde později a jeho terčem bude někdo úplně jiný. V tom případě jsme jen „pískovištěm", na kterém si útočník hraje.