# Zadní vrátka od NSA: Šifrování nemusí být bezpečné

Použití backdooru v kódu programu umožňuje americké tajné službě získat data například z HTTPS.

Zdá se, že oddělení americké tajné služby NSA (National Security Agency), známé pod označením TAO (Tailored Access Operation), má zčásti přístup ke svatému grálu na internetu: k šifrování.

Podle nedávno zveřejněných dokumentů totiž NSA zabudovala zadní vrátka do šifrovacího standardu Dual EC DRBG, který slouží ke generování náhodných čísel. Ten je využíván například k tvorbě kryptografických klíčů a tím pádem umožňuje například odposlech HTTPS spojení zabezpečených nástrojem RSA BSafe. Už sama společnost RSA (zabývající se kryptografií) své zákazníky varovala před využíváním implicitně nastaveného generátoru náhodných čísel. Na problém už v roce 2007 upozorňovali dva výzkumní pracovníci společnosti Microsoft (Niels Ferguson a Dan Shumow), kteří si všimli nesrovnalostí v normě. Trvalo ale pět let, než se informace o celém rozsahu potenciálního rizika stala veřejně známou. Důvodem bylo i to, že tento standard, oficiálně vyvinutý Národním institutem pro normalizaci a technologie (NIST), také později ratifikovala Mezinárodní organizace pro normalizaci (ISO).


## ŠIFROVÁNÍ JE STÁLE UŽITEČNÉ

„Šifrování je stále náš přítel," říká bezpečnostní expert Bruce Schneider. Ten doporučuje používání kryptografických nástrojů jako TrueCrypt a také využívaní protokolu HTTPS. I když ho teoreticky mohou tajné služby prolomit, může pomoci proti zločineckým gangům, kterým jde, podobně jako NSA, o data uživatelů. Někteří bezpečnostní experti navíc podotýkají, že není jasné, zda šifrovací odborníci zpravodajských služeb prolomili také robustnější šifrovací algoritmy. Experti proto doporučují otevřené standardy jako například Open SSL, jejichž kód je veřejně dostupný, a proto je do něj mnohem obtížnější ukrýt zadní vrátka.

### Bezpečné:

**Použití šifrovacího nástroje TrueCrypt je bezpečné, pokud nastavíte dobré heslo.**

### PŘÍČINY ÚNIKŮ DAT

Není překvapením, že za ztrátu dat jsou zodpovědní především hackeři.


ZDROJ: SYMANTEC

# DATOVÉ ÚNIKY MĚSÍCE

### TWITTER: ZVEŘEJNĚNO 15 000 PŘÍSTUPOVÝCH ÚDAJŮ

Hacker označovaný jako Mauritania zveřejnil na internetu přibližně 15 000 přístupových klíčů k účtům na Twitteru. Nešlo o konkrétní hesla, ale o tzv. OAuth tokeny pro Twitter, tj. přístupové certifikáty pro konkrétní účty. Uživatelům se doporučuje resetovat všechna povolení pro aplikace využívající přístup k účtu na Twitteru, aby byly eliminovány staré OAuth tokeny.

### VODAFONE: ODCIZENY DVA MILIONY ZÁKAZNICKÝCH ÚDAJŮ

Informační specialista B. Burkhard údajně odcizil z německých serverů Vodafonu více než dva miliony datových záznamů zákazníků – včetně jména, adresy a údaje o účtu. Vodafone o tomto problému příslušné zákazníky informoval dopisem. Pachatel podezřelý z krádeže pracoval pro předchůdce Vodafonu, firmu Mannesmann, jako specialista na zpracování dat a později pracoval externě i pro Vodafone.

### SANTANDER BANK: PŘÍSTUP K BANKOVNÍM POČÍTAČŮM

Neuvěřitelnou drzost předvedli podvodníci, kteří chtěli získat přístupové údaje pro vzdálený přístup ke zmiňované bance ve Velké Británii. Pronikli do budovy, vydávali se za zaměstnance banky z IT oddělení a na vybrané počítače instalovali hardwarové klíče sloužící jako keyloggery. Podvodníci ale byli policií zatčeni dříve, než mohli způsobit jakoukoliv škodu.

## Riskantní osobní průkaz


Ačkoliv Češi patří se svými vládními IT průšvihy (IZIP, sKarta, INDOŠ) mezi evropskou špičku, problémy se nevyhýbají ani našim sousedům. Bezpečnostní experti v Německu zjistili, nové průkazy totožnosti (NPA) nemusí být zcela bezpečné: objevili totiž možnost, jak lze pomocí keyloggeru získat PIN. Nepomůže dokonce ani virtuální klávesnice: jakmile je program nainstalován, pošle pomocí screenshotu zadaný PIN hackerovi. Ministerstvo ale i přesto tvrdí, že nové průkazy jsou bezpečné.

## Stará chyba dělá nové mobily zranitelnými

Stará bezpečnostní mezera v softwaru Polaris Viewer ve smartphonech Samsung umožňuje útočníkovi spustit škodlivý kód v zařízení. Tento program je ale předinstalován i v modelech Galaxy S3 a S4 a dosud neexistuje žádná oprava tohoto problému. Uživatelé by proto měli ve správci programů Polaris Viewer deaktivovat.

# 75 %

**VŠECH PHISHINGOVÝCH E-MAILŮ JE PODLE STUDIE FIRMY KASPERSKY VYTVOŘENO ZA ÚČELEM KRÁDEŽE PENĚZ.**

## Odstranění cizích fotografií na Facebooku

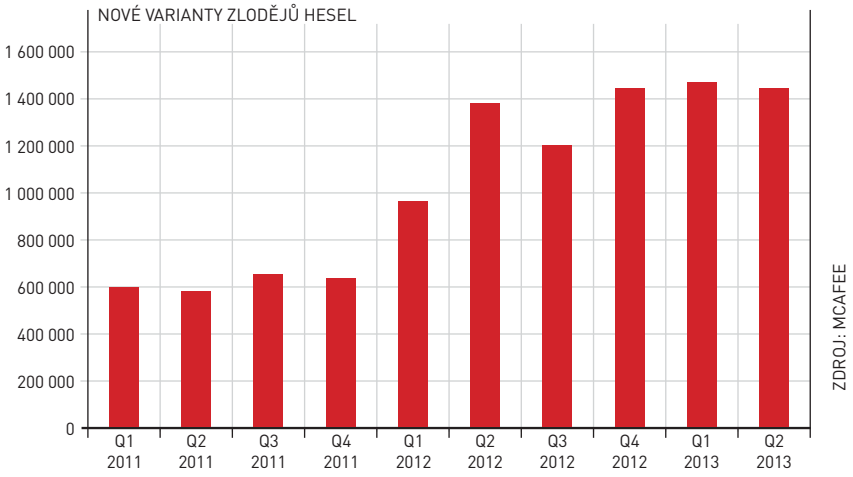
Ind Arul Kumar našel na Facebooku mezeru, která umožňuje smazat všechny fotografie patřící jinému uživateli. Chyba se vyskytla ve funkci, která je určena pro zasílání oficiálních žádostí o smazání fotografií. Kumar chybu okamžitě oznámil Facebooku a získal odměnu ve výši 12 500 dolarů.

## Windows 8: (Ne)bezpečná přihlašovací gesta?

U tabletů se systémem Windows 8 je možné odemknout počítač i pomocí gest prsty na obrazovce. Výzkumníci z univerzity v Delaware nyní objevili, že většina uživatelů si tato gesta nevybírá náhodně. V závislosti na tapetě prý existují různé body, které obvykle slouží jako začátek nebo konec gesta, například okolí očí. Díky tomu by prý vědci mohli odhalit celé gesto a odemknout počítač. Nicméně při testování v praxi byla míra úspěšnosti 13 procent, což není příliš mnoho.

## VŠICHNI CHTĚJÍ ZNÁT VAŠE HESLO

Ve srovnání s rokem 2011 se počet zlodějů hesel více než zdvojnásobil. Každý den se navíc objevuje 230 nových malwarů. Získaná data poté internetoví zločinci prodávají.




PHISHING V ČR:

# Bankovní trojské koně

Společnost ALWIL Trade připravila souhrn informací o phishingových útocích v České republice.

Letos v srpnu začali podvodníci rozesílat hromadné e-maily, které se vydávaly za zprávu České pošty a obsahovaly odkaz na web ceskaposta.net. Sama o sobě by byla tato záležitost banální, nicméně útok už je přímo navržen tak, aby reálně poškodil zákazníky bank v ČR. Obsahem podvodného e-mailu je informace o nedoručení zásilky, hrozba sankcemi a odkaz na web, kde má být možné zobrazit informace o zásilce. Namísto toho se však obětem do počítače stáhne škodlivý kód – malware. Útočníci používají zejména spustitelný soubor, maskovaný za dokument ve formátu PDF (soubor.pdf.exe).

Postup zvolený podvodníky distribuuje vůbec nejnebezpečnější druh malwaru: trojského koně, který se zaměřuje na e-banking. Tento malware představuje obdobu známějších a velmi sofistikovaných škodlivých kódů, jako je Zeus/Citadel či SpyEey. Snaží se získat přihlašovací údaje k internetovému bankovnictví. Program mj. funguje i jako keylogger, tedy zaznamenává použitá hesla (stisky kláves) a odesílá je podvodníkům. Vytváří také snímky obrazovky, takže přístupové údaje dokáže odcizit i při použití virtuální klávesnice. Po krádeži potřebných informací provádí finanční převody bez vědomí uživatele.

Na rozdíl od předchozích pokusů tohoto typu cílí tato kampaň na všechny uživatele největších českých bank. I když i zde došlo k pravopisným chybám a podivným formulacím v průvodním e-mailu, na zdokonalení takovýchto podvodů útočníci stále pracují. Nejprve využívali doménu ceskaposta.net, poté začali používat i adresu ceska-posta.org. Množství počítačů infikovaných tímto útokem, který probíhal od září, se v ČR zatím odhaduje na desítky, ale je otázkou, zda se již vlna útoků zastavila. České banky vydaly prostřednictvím asociace před touto vlnou útoků oficiální varování, bohužel oběti těchto útoků jen těžko získají ukradené peníze nazpět. Pro banky a další instituce se samozřejmě jedná o nepříjemnou záležitost, protože jsou vystaveny riziku soudních sporů s poškozenými uživateli. Pro uživatele není poučení z probíhajících útoků nijak překvapující – lze zopakovat doporučení používat bezpečnostní software (antivirus, firewall) a mít u všech aplikací i OS nastavené automatické aktualizace.

Ochranu výrazně posílí, pokud uživatel používá pro komunikaci se systémem elektronického bankovnictví více na sobě nezávislých kanálů, typicky rozhraní z počítače a autorizaci prostřednictvím SMS zprávy. Při použití bankovní aplikace ve smartphonu ale tato možnost odpadá. Malware pro smartphony dokáže odchytávat příchozí SMS zprávy a různě s nimi manipulovat. Při ovládání elektronického bankovnictví z mobilního telefonu se proto rozhodně vyplatí zabezpečit i toto zařízení.

## Projekt pro biometrické bezpečnostní systémy

V uplynulých letech se software pro rozpoznávání obličeje, hlasu a otisků prstů přesunul z vědecko-fantastických filmů do běžně dostupných zařízení, jako jsou například chytré telefony a tablety. Konsorcium TABULA RASA, sdružující dvanáct různých organizací ze sedmi zemí, získalo podporu z fondu Evropské unie pro výzkum a inovace. Nyní zkoumá účinnost tohoto softwaru a jeho odolnost proti stále častějším útokům na jeho zabezpečení s cílem vyvinout fungující protiopatření pro novou generaci bezpečnějších biometrických systémů.

Evropská unie investovala do projektu TABULA RASA 4,4 milionu eur. Společně s investicí 1,6 milionu eur ze strany samotného konsorcia byly tyto finance využity k rozsáhlému výzkumu a následnému testování.

V průběhu výzkumu uspořádalo konsorcium TABULA RASA soutěž s názvem „Spoofing Challenge", které se zúčastnili vědci z celého světa s jediným cílem – najít takové řešení, které dokáže oklamat různé biometrické systémy. Účastníci dokázali, že existuje mnoho inovativních a kreativních způsobů, jak přelstít systém. Při nejkreativnějším útoku, který se během soutěže objevil, využil jeho autor make-up k oklamání 2D systému na rozeznávání tváře a úspěšně se vydával za oprávněnou osobu. Další soutěžící k oklamání systémů úspěšně využili dobře známé strategie, jako jsou fotografie, masky nebo falešné otisky prstů („gumové prsty").

## Gopas HackerFest 2013

Po světovém setkání v americké Atlantě a evropském mítinku na Islandu se špičky etického hackingu sešly v Praze na HackerFestu 2013. Konference Počítačové školy Gopas přitáhla největší kapacity oboru, které se shodly na tom, že prioritním tématem je dnes obrana proti hackingu populárních mobilních zařízení a cenných firemních dat. Hlavní hvězdou byl Wayne Burke, špičkový profesionál se zkušenostmi z práce pro FBI, NATO i špičky světového byznysu, který nabídl svou nejnovější hackerskou prezentaci s názvem „Nabít a zabít – mobil jako současná zbraň hromadného ničení". Mezi další přednášející patřila například bezpečnostní specialistka Paula Januszkiewiczová, která má za sebou stovky IT bezpečnostních auditů a penetračních testů, nebo přední domácí odborníci na počítačovou bezpečnost Ondřej Ševeček, Michal Altair Valášek a William Ischanoe.