Hackeři nalézají zajímavější cíle

Dokáží paralyzovat nukleární jaderné elektrárny, zmanipulovat volby nebo jízdenky MHD – a jednou ročně se scházejí, aby to spolu prodiskutovali. Chip se zúčastnil jedné **KONFERENCE SUPERHACKERŮ** a získal tak možnost tajně poznat některé jejich nebezpečné útoky.

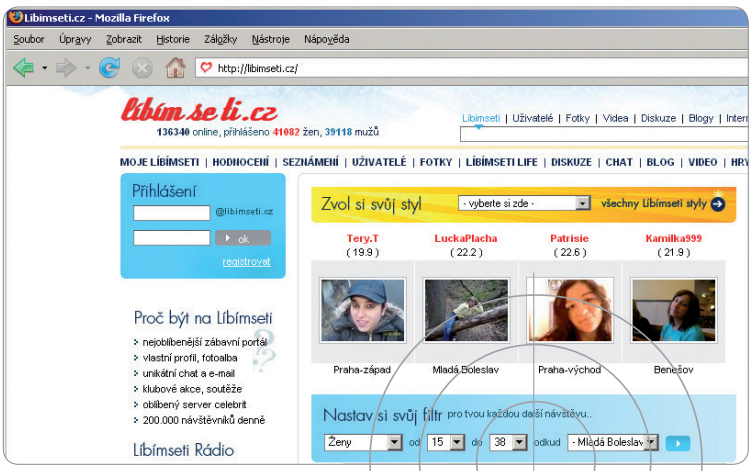
FABIAN VON KEUDELL

„Vládci internetu" to rádi krvavé – maso, které se položí na barbecue gril hackera, by mělo být opravdu šťavnaté. Kingpin, Eagle a GoodSpeed usrkávají pivo, dívají se do ohně a vypráví, jak dokážou manipulovat americkými volbami, převzít kontrolu nad jadernými elektrárnami a změnit všechna PC po celém světě v dálkově ovládaná zombie.

Pro spoustu internetových zločinců je tento „barbecue sraz" nejvýznamnější událostí Defconu, je to setkání superhackerů v americké metropoli Las Vegas. Hackeři, kteří zde předvedou své nejnovější techniky útoků, jsou považováni za hvězdy setkání.

I když místo svých pravých jmen používají pseudonymy, tady v Las Vegas jsou hackeři „otevření" jako nikdy předtím. Chip byl u toho – a to nejen během oficiálního setkání, ale také během barbecue, kdy se hackeři rozpovídali...

„Je tu mezi námi někdo od policie?" – tato úvodní otázka se stala běžným žertem konference. I proto, že je jasné, že FBI a jiné zpravodajské služby mezi posluchači byly. A bylo to právě barbecue a pár piv, co nakonec odhalilo následující: mnoho z těchto superhackerů, kteří se zde prezentují jako „špatní, zlí a hříšní", pracuje ve funkcích poradců pro veřejné úřady či bezpečnostní společnosti. A to je pravděpodobně důvod, proč dokonce ani zákon nemůže nic dělat, jen sedět a dívat se. Možná má ale především patřičný respekt a nechce riskovat, že hackeři své prostředky opravdu použijí ke špatným účelům.



SOCIÁLNÍ SÍTĚ

Sociální sítě jsou pro hackery lákadlem. Jak pro možnost vytváření falešných identit, tak i pro získávání citlivých dat...

Zfalšované volby: Hlas hackera je na počítači sčítán opakovaně

Zatímco maso prská na grilu, hovor se stáčí na nejopakovanější téma – americké prezidentské volby. Hacker zvaný Mouse měl před volbami v některých věcech jasno: Obama vyhraje. Alespoň pokud by Mouse udělal to, co by pro něj bylo dětskou hračkou: hacknul oficiální hlasovací počítač. „To je velmi jednoduché," uvedl Mouse. Začíná to otevřením zámku zakrývajícího samotný počítač. Jeho autoři zřejmě předpokládají, že je to „riskantní" a nikdo to dělat nebude – důsledkem je fakt, že ho často můžete otevřít jednoduchým klíčem na poštovní schránky. „Dokonce i prodejní automaty jsou lépe zabezpečené," říká Mouse. Pomocí datového portu pak Mouse připojil svůj počítač a software nazvaný „Everest" – a využil chyby v šifrovacím algoritmu zařízení.

Výsledek: Může volit svého preferovaného kandidáta, jak často chce, alespoň na tomto jednom stroji. Ale to, zda by opravdu mohl tímto způsobem ovlivnit volební výsledek, je diskutabilní.

„Prezidentské volby jsou stejně jen strojem na vydělávání peněz pro kriminálníky," říká Oliver Friedrichs, jeden z nejdůležitějších bezpečnostních expertů v nadnárodní bezpečnostní firmě. Zločinci k tomuto účelu používají tzv. typosquatting, což je typ zneu-

VOLEBNÍ POČÍTAČ

Hacker zvaný Mouse hacknul oficiální hlasovací počítač. Dokonce i prodejní automaty jsou prý lépe zabezpečené...

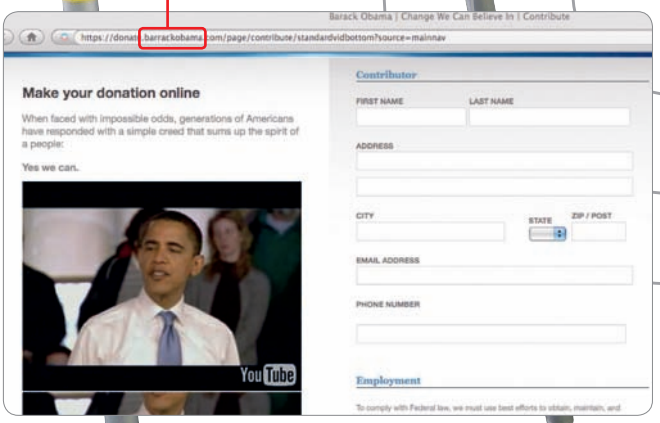
ATOMOVÁ ELEKTRÁRNA

Když Scott Lunsford americké vládě oznámil, že dokáže hacknout jadernou elektrárnu, všichni si z něho dělali jen legraci. O několik dnů později už ne...

TYPOSQUATTING

Prezidentské volby jsou prý stejně jen strojem na vydělávání peněz pro kriminálníky.

.barrackobama.



METRO

Studenti zmanipulovali RFID čipy, které najdete v jízdenkách na MHD v Chicagu, Londýně (a také Praze).

žití chyby v URL. Zaregistrují webovou stránku s URL, která je téměř identická se známou stránkou prezidentských kandidátů – například **www.barackobama.com**, ale třeba se dvěma „r". Takovéto „spellingové chyby" dělá spousta uživatelů. Svou chybu si ale v tomto případě nikdy neuvědomí, protože útočníci jednoduše zkopírovali originální stránku na stránku falešnou. Bohužel jakmile někdo použije na takové webové stránce informace týkající se vlastní kreditní karty, protože chce určitou částkou dotovat svého kandidáta, ve skutečnosti prozrazuje informace o své kartě zločincům. Proti těmto podvodům neexistuje žádná efektivní ochrana.

WI-FI SÍTĚ

Indiánský hacker tvrdí že dokáže, aby se extrémně dobře chráněné Wi-Fi sítě (AES šifrování, filtrování, firewall) zhroutily pouhými dvěma kliknutími myši.

Cracknuto: Nejbezpečnější zámek na světě zkolabuje za pouhých 30 sekund

„Nalezení bran do domácích počítačů je obvyklou zábavou i pro amatérské hackery – ale o tom to je," říká The Alffan s plnou pusou a odporně se zachechtá. „Ve starých školách neexistují dveře, které nelze otevřít," dodává. A to je pravda. Tento chlapík, který zrovna převaluje v puse kus hovězí svíčkové, totiž dokáže cracknout nejbezpečnější zámek na světě za 30 sekund. A ten není zabezpečený pouze klasickým bezpečnostním zámkem, ale má i elektronickou ochranu. Alffan také dokáže velice snadno odemknout jednoduché dveře pomocí vlastnoručně vyrobeného „univerzálního" klíče, který dokáže otevřít 80 % domovních zámků.

Dokonce i moderní alarmové systémy přestávají být dobrou ochranou, protože se přestávají deaktivovat pomocí kódu. Nyní se obvykle deaktivují pomocí čipové karty, kterou má majitel domu vždy v tašce. Když se blíží k domu, systém detekuje kartu a vypne alarmové senzory. Perfektní vstup pro hackera – ten získá přístup k domu pomocí zmanipulované čipové karty, aniž by spustil alarm. Podobně funguje také zabezpečení u aut. Hacker nám sám nabídne důkaz a na hotelovém parkovišti bezdrátově otevře BMW.

Russell, Zack a Alessandro používají velice podobnou technologii. Tito tři studenti žijí v Chicagu a nemají dost peněz na veřejnou dopravu – tedy alespoň to tvrdí. „Metro je příliš drahé," říká Russell. „Něco se s tím musí udělat," dodává Alessandro. A to je důvod, proč právě tito tři teď cestují zdarma. Cestovní jízdenky v Chicagu jsou opatřeny RFID čipy, které tito studenti zmanipulovali. Když nyní vloží svůj hackerský lístek do turniketu, ten se ochotně otevře. Tito tři „šikulové" pro tento účel využívají slabého místa v šifrovacím algoritmu – klíč má délku pouhých 48 bitů (a zakódovaný klíč může být pomocí softwaru KwickBreak přečten během mrknutí oka). K této akci je sice nutný hardware (seženete ho přibližně za 700 eur), na oplátku však mohou tihle tři cestovat zcela zdarma i o prázdninách, protože spousta dalších operátorů po celém světě používá stejný RFID systém jako v Chicagu. Naši studenti tak už úspěšně otestovali jedenáct takových systémů, včetně toho v londýnském metru.

Poznámka: Federální soud vznesl žádost o zabránění v přednášce třem zmiňovaným studentům. Soudce se domníval, že zveřejněním těchto informací dojde k ohrožení RFID systémů, což může být hrozbou pro veřejné zájmy a bezpečnost (Orwellův Velký bratr by jen závistivě zíral). Zmiňovanou přednášku najdete na adrese **http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf**...

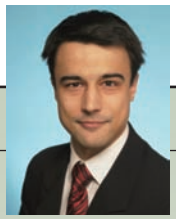
Smutná poznámka: V Praze se začíná zavádět „opencard", podle úředníků chytrá čipová karta, která vám usnadní život v hlavním městě **(opencard.praha.eu)**. Tato karta však obsahuje čip MIFARE, který najdete i ve výše zmiňovaných systémech v Chicagu...

Nukleární krize: Hacker převzal kontrolu nad jadernou elektrárnou

V ohrožení může být dokonce i bezpečnost nejdůležitějšího zabezpečovacího systému. Neexistuje zkrátka už nic zcela bezpečného – to je zřejmě jediná věc, na které se shodnou všichni účastníci tohoto „grilovacího večera". Účastníci Defconu rádi vyprávějí příběh jejich kolegy Scotta Lunsforda, bezpečnostního poradce v IBM. Když americké vládě oznámil, že dokáže hacknout jadernou elektrárnu, všichni si z něho dělali jen legraci. Jen o několik dnů později to byl on, kdo se smál naposledy. Lunsford se dostal do kontrolního systému jaderné elektrárny skrz slabinu v softwaru SCADA (Supervisity Control and Data Acquisition Software).

Zápletka příběhu: SCADA software je společným vývojovým projektem firem Siemens, ABB a Rockwell Automation. Tento software používá mnoho jaderných elektráren na celém světě, včetně celé řady evropských organizací. Ano, chyba v softwaru byla mezitím opravena, ale strach z děr a opravdového útoku hackera přetrvává.

Dobrou věcí je, že hackeři z Defconu jsou obvykle na světlé straně síly. Jejich „hackerské pokusy" jsou většinou kombinovány s hledáním řešení oprav, případně přímo s vytvořením záplaty. „Tato řešení ale nejsou



INFO

Hackeři a české právo

Vzhledem k celé řadě dotazů vztahujících se k podobně zaměřenému článku v jednom z předešlých Chipů jsme se rozhodli oslovit právní specialisty a prozradit vám, jak je to s legálností podobných aktivit a jaká je případně „cena“.

Na otázky tedy odpovídají Mgr. Martin Strnad a Mgr. Ivan Rámeš z advokátní kanceláře Havel & Holásek, s. r. o.

1) Je skenování portů ilegální?
Samo o sobě ne. V některých případech jde dokonce o odůvodněnou a žádoucí techniku, která se využívá například pro otestování kvality zabezpečení vlastní sítě. Skenování portů je zakázané jen tehdy, pokud by tím byla způsobena škoda třetí osobě (§ 420 a násl. občanského zákoníku) anebo by tím byl ohrožen provoz příslušného serveru (§§ 182, 184 trestního zákona). Obvyklé následné kroky (průnik do skenovaného systému, získání dat, jejich změna atd.) obvykle už ovšem nelegální jsou.

2) Pokud si někdo nechá otevřenou WLAN (nechrání ji pomocí WEP nebo WPA), je ilegální ji použít?
Ano. K užívání příslušného hardwaru a konektivity internetu je třeba svolení jejího provozovatele a pouhé nekvalitní zabezpečení tak rozhodně vyložit nelze. Pokud na takové svolení nelze usuzovat z dalších znaků (např. oznámení v restauraci o „Free Wi-Fi“), majiteli přísluší náhrada škody, případně ušlého zisku.

[Poznámka HH – originální text zákona pracuje s jiným pojetím – nejde o klasické české „připojení se přes volnou Wi-Fi“, ale o získání dat třetích osob z takové sítě]

3) Jsou hackerské nástroje legální (například při použití na inspekci sítě)?
Ano, žádný právní předpis platný v České republice samotné držení nebo tvorbu takových nástrojů nezakazuje. Není ovšem možné je například shromažďovat za účelem přípravy k jakékoli trestné činnosti, nebo je tak dokonce použít.

4) Pokud zapomenu heslo na vlastním PC, je legální si ho „hacknout“ (porušit ochranu systému)?
Je nutno rozlišovat pouhý průnik do systému (např. získání účtu na daném stroji, zjištění hesla apod.), který samozřejmě není v případě vlastního stroje zakázaný, a úpravu nebo odstranění ochrany práv k softwaru (např. „crack“ nutnosti aktivace atd.), které zakázané je coby zásah do práva autorského.

5) Celá řada firem ve svém SW v licenčních podmínkách zakazuje dekompilaci kódu. Je to legální?
Smluvně lze dekompilaci kódu zakázat, nicméně nelze vyloučit zákonná omezení plynoucí z autorského zákona, a to především v případech, kdy je nutno opravit chyby v programu či program pozměnit, aby byl v souladu s jeho určením, a dále v situaci, kdy je třeba zajistit kompatibilitu programu s jinými nezávislými počítačovými programy (tzv. interoperabilita).

vždy jednoduchá,“ vysvětluje Michael Smith (jméno je změněno) a pije další pivo. Specializuje se na společenské komunity. Jeho oblíbeným cílem je „Linked In“, americká profesionální komunitní databáze. Vypráví nám o fiktivních identitách, falešných seznamech přátel a zmanipulovaných profilech.

Jen o pár minut později jsme seděli v Cadillacu Escalade se zabarvenými skly a přihlašovali se do systému Linked In přes WLAN-Hotspot. „Společenské komunity mají dva hlavní problémy,“ vysvětluje Michael. „Jedním z nich je ‚defektní programování‘, druhým pak důvěřiví členové.“ Svá slova nám dokládá jen několik sekund poté. Ukazuje nám konto profesora univerzity MIT (Massachusetts Institute of Technology). Profesor neví, že je členem Linked In, protože jméno, foto a profil pochází od Michaela. „Patnáct přátel je tím kouzelným limitem,“ říká. „Pokud jich máte tolik, potom jich většina z nich věří, že je profil pravý. “

„Alarmové systémy přestávají být dobrou ochranou...“

Běžná skutečnost: „Přátelé“ v profilu jsou jednoduše členové, kteří akceptují jakoukoliv nabídku přátelství, která je jim nabídnuta.

Myslíte si, že se to u nás nemůže stát? Chip si to ověřil pomocí profilu v nejmenovaném komunitním webu. Naší návnadou byla dívka z Prahy. Bez fota, ale s přesvědčivým profilem. Výsledkem bylo asi 30 žádostí o přátelství během prvních 48 hodin.

Další test ukázal, jak jednoduše lze získat osobní data. Zámožný muž každý měsíc organizuje fotografickou soutěž – v tomto případě o nejlepší fotografii spoře oděné ženy. Ženské představitelky prý budou oceněny. Hlavní cenou má být víkend ve vile milionáře. Věřili byste této informaci? Děsivé je, že existuje spousta žen, které o sobě nemají valné mínění, posílají fotografie a také ochotně sdělují adresy a telefonní čísla.

Zpátky k Michaelovi, on-line hackerovi, který nám dále poodhaluje tajemství. „Poslední pochyby o on-line profilu jsou vyjasněny, jakmile se známí či prokazatelně existující lidé stanou přáteli předpokládaného člena,“ říká Michael. Jednoduše tedy takové lidi přiměje, aby se stali jeho přáteli. Michael k tomu ale nevyužívá sex-appeal, ale slabiny v HTML kódu na stránce komunitního webu. Použitím Cross-Site-Scripting mezery v tagu IMG propašuje kódy, pomocí nichž si může přidat každého člena jako přítele. Ostatní s tím nic nezmůžou. Zaměstnanci MIT mu pravidelně sednou na vějičku, a údajnému profesorovi dokonce i poslali své práce označené jako „důvěrné“.

Společenské komunity: Každý pomáhá hackerovi – ať chce nebo nechce

Michael mi ukazuje profil jednoho ze svých přátel. „Vždy se navzájem zlobíme upravováním profilu toho druhého,“ říká s úšklebkem. Nepotřebuje k tomu heslo; stačí malý skript. Poté, co v hacknutém profilu změnil údaj o sexuální orientaci, přidá další typ záznamové ochrany: když se oběť chce nalogovat, aby si změnila data zpátky, systém ji automaticky odmítne. Pak je jediným řešením kompletní vymazání profilu. Podle Michaela to také jde u celé řady jiných sítí (např. Xingu). O zabezpečení českých komunitních webů si po aféře „Líbimseti.cz“ také nikdo iluze nedělá. „Cena za bezpečné programování komunitních webů je příliš vysoká,“ říká Michael. „Musí se reformátovat celkový systém a to stojí peníze.“

Zpátky na místo barbecue... Indiánský hacker Ahmad vypráví, jak dokáže, aby se extrémně dobře chráněné WLAN sítě (AES šifrování, filtrování, firewall) zhroutily pouhými dvěma kliknutími myši. Další „chyba v zabezpečení“ nám později umožní odposlechnout důvěrnou satelitní telefonní konferenci dvou firemních lídrů. Ještě později večer nám Graham-Minor odhalí, jak dokáže pomocí iPhonu paralyzovat systém nejmenované zásilkové služby. S vírou, že všichni účastníci Defconu v zásadě chtějí, aby se stávaly pouze dobré věci, se zakousneme do steaku...

AUTOR@CHIP.CZ