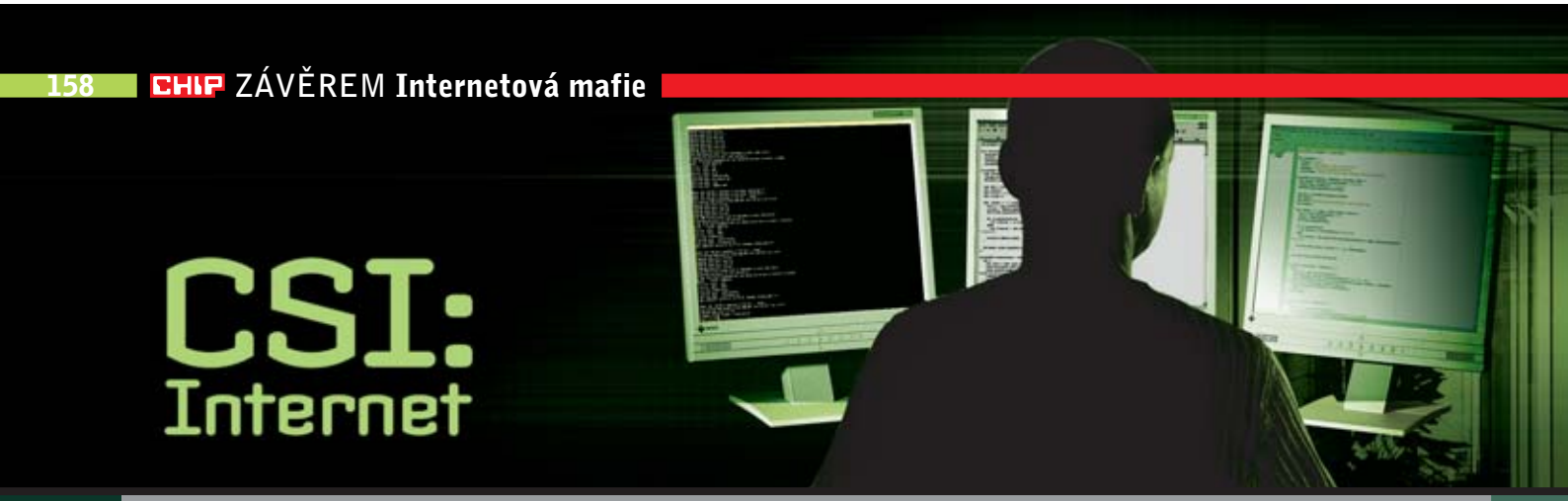


3. část

Otrávené pakety

Prolomené uživatelské účty u Amazonu a eBay nejsou nic neobvyklého. Náš dnešní případ je však poněkud záhadný: tým specialistů Chipu vyšetřuje kauzu „balíkového" teroru. *Valentin Pletzer, autor@chip.cz*

Tak vám zase vezu balík od Amazonu," diví se doručovatel. Dokonce i on už ví, že adresát, pan S., si po internetu vůbec nic neobjednal. Renému S. však začíná docházet trpělivost, a obrací se proto na Chip: „Trvá to už čtyři týdny. Přichází mi zboží z Amazonu a eBay, ačkoliv jsem si nikdy nic neobjednal. Musíte mi pomoci."

Na vině spyware?

Nejdříve nás napadá, že jde o další případ hackingu účtů, a to zcela klasicky pomocí spywaru. Takto se dají zjistit hesla, v horším případě dokonce čísla kreditních karet. Účty u eBay zneužívá hacker obvykle tímto způsobem: pod falešným jménem nabídne k prodeji drahé zboží a pak předběžnou platbou inkasuje peníze – samozřejmě aniž by cokoli dodal. Na případu pana S. je však něco podivného: jak se zdá, příslušnému hackerovi nejde o peníze. Vždyť René S. dosud žádnou finanční škodu neutrpěl: doručené balíky prostě hned posílal zpět.

Tedy žádný běžný špionážní útok! To naši speciální pátrací jednotku zaujalo a se svolením pana S. ihned začala zajišťovat stopy, neboť stejně jako v televizním seriálu o CSI je nezbytné shromažďovat důkazy přísně podle plánu. Pokud se v počítači něco změní, nebude už později před soudem použitelný jako důkazní prostředek – obviněný by pak mohl tvrdit, že jsme tam důkazy podstrčili později. Nejprve proto vyjímáme pevný disk z počítače a pořizujeme si jeho klon. S kopií teď můžeme bez nebezpečí zkoušet veškerý software.

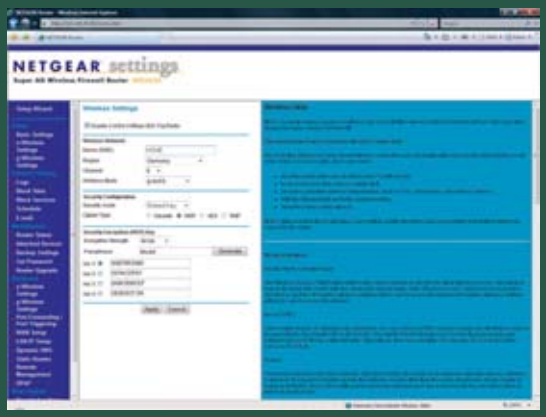
Forenzní analýza pevného disku

Pan S. nemá v počítači žádnou internetovou „security suite" a také jeho antivirový program už dávno není v aktuálním stavu. „Není divu, že se tam mohl nepozorovaně usadit spyware," říká jeden z vyšetřovatelů. Avšak při rutinní kontrole nenalézáme na pevném disku ani spyware, ani rootkity. To ale může také znamenat, že škůdce po splnění úkolu sám sebe vymazal, aby zahladil stopy. V dalším kroku proto zkoušíme pomocí nejrůznějších obnovovacích nástrojů zrekonstruovat odstraněná data. Ani pak však nejsme moudřejší; nejspíš už byla inkriminovaná oblast opět přepsána, a původní data jsou tedy nenávratně ztracena. S nadějí na digitální stopy v počítači se proto musíme rozloučit. Ale tak rychle se vzdát nechceme.

Poštovní doručovatel

NEVYŽÁDANÁ POŠTA: **Kdo od internetových zasilatelství dostává neobjednané zásilky, má ve své domácí síti pravděpodobně bezpečnostní problém – například se spywarem nebo rootkity.**

První stopa



SNADNÁ KOŘIST: **Bezdrátové sítě se slabým šifrováním WEP jsou snadno napadnutelné. Daleko bezpečnější jsou standardy WPA a WPA2.**

Nový seriál Chipu

V americkém kriminálním seriálu o CSI objasňují vyšetřovatelé zločiny pomocí vědeckých metod. Chip si vzal „Kriminálku Las Vegas" za vzor pro novou řadu článků, která ukáže, jak profesionální vyšetřovatelé a specialisté bojují proti strmě narůstající počítačové kriminalitě.

Nebezpečná periferie

Rozšiřujeme pátrání. Cílem hackerů nemusí být pokaždé jenom PC – v úvahu připadají i jiné přístroje zapojené v síti, například tiskárna. Jakmile se síťová tiskárna jednou ocitne pod hackerovou kontrolou, je to skoro stejně nebezpečné jako spyware v počítači. Pak má totiž hacker možnost číst všechny tiskové úlohy. A v nich se právě citlivé údaje, jako jsou přihlašovací data nebo čísla účtů, vyskytují dostatečně často.

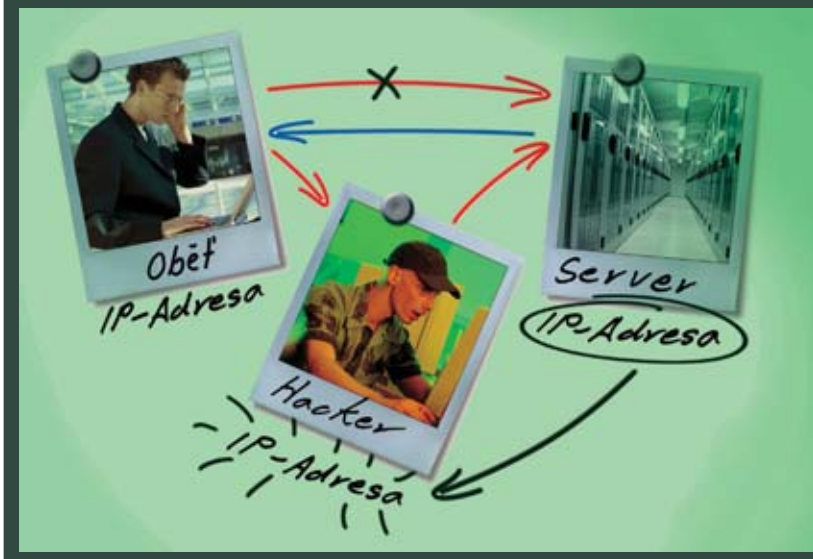
Zaměřujeme se tedy na hardware v síti, ta však až na jedno internetové rádio a jeden WLAN směrovač nic jiného neobsahuje. To hackerův výběr dosti omezuje. Nejprve si bereme pod lupu rádio. Znovu slepá ulička: přístroj neumožňuje prakticky žádné manipulace a je nakonfigurován úplně normálně. Zbývá router – a tady nás čeká důležité odhalení týkající se konfigurace WLAN: namísto bezpečného šifrovacího standardu WPA či WPA2 zajistil René S. svou rádiovou komunikaci pouze pomocí WEP. Vzhledem k tomu, že tuto ochranu dokáže s nástroji jako WEPCrack nebo AirSnort prolomit v několika minutách i začátečník, zkoumáme znovu počítač pana S. Tentokrát máme spadeno na bezpečnostní mezery a síťová nastavení, která by vetřelci mohla umožnit přístup k datům. Avšak operační systém je v nejnovějším stavu a ani jinak žádné vstupy do sítě nezjišťujeme.

Past na hackera

Protože v případě pana S. nebyl napaden ani hardware, ani software, mnoho možností – jde-li skutečně o akci hackera – už nezbývá. Máme jisté podezření a soustřeďujeme se na starý, ale velmi účinný hackerský trik: útok typu „man in the middle". Při tomto napadení se útočník vklíní do sítě a celý datový proud odvede k sobě, čímž získá nad daty plnou kontrolu. Než data vrátí na původní místo určení, může ukrást hesla a manipulovat obsahy souborů.

Teorii tedy máme – chybí už jen důkaz. Rozhodujeme se proto nastražit hackerovi návnadu. Nejdříve musí pan S. nově nastavit všechna svá hesla, heslo pro WLAN, e-mailový účet a hesla pro Amazon a eBay. Tak chceme hackera vylákat z jeho úkrytu. Jakmile se pokusí ukrást hesla znovu, past by měla sklapnout. Pro sledování provozu na síti instalujeme dva „pozorovací" počítače. Jeden je vybaven nástrojem „Netstumbler" a monitoruje všechny bezdrátové sítě v okolí. Na druhém počítači běží protokolovací program „Wireshark", který zaznamenává veškerá data pohybující se v naší síti. Teď už zbývá jen čekat.

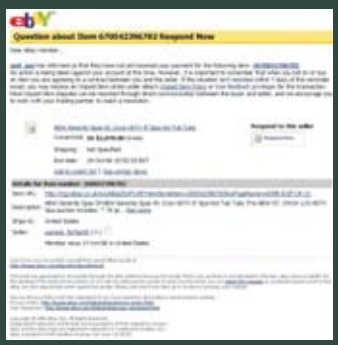
Podezření



TAJNÝ ODPOSLECH: **Při útoku typu „man in the middle" odvádí hacker proud dat k sobě. Oběti přitom předstírá, že IP adresa jeho počítače je adresou serveru.**

Spadla klec...

Po týdnu se věci dávají do pohybu. Naše „pozorovatelna" WLAN vyhlašuje poplach. Hacker je zpět! Jak jsme doufali, změněnými hesly se ho podařilo vylákat z úkrytu. Přímo pozorujeme, jak narušuje síťové spojení u donucuje tak počítač pana S. aby se nově přihlásil ke směrovači. Trik je známý, a jsme proto před hackerem o krok napřed. Ten nyní vysílá do směrovače právě ty signály, které zaznamenal, když se PC směrovači nově hlásil. Standard WEP má totiž jednu slabinu: mnohé WLAN pakety prozrazují při přenosu část hesla, ovšem jen malou. Útočník proto na jeho kompletní odhalení potřebuje velmi mnoho paketů – asi 70 000 až 100 000. Pokud síťový provoz jenom prostě odposlouchává, může trvat hodiny nebo i dny, než nashromáždí kritický objem – pokud pan S. náhodou dlouho nesurfuje a vytváří hodně paketů. Náš protihráč tak trpělivý není a spouští tzv. „replay atak": nástrojem jako AirReply si vynucuje vysílá-



OBVYKLE: **Pod falešným jménem hacker nabídne k prodeji drahé zboží a pak předběžnou platbou inkasuje peníze.**

ní mnoha paketů. To je ovšem pro nás ideální příležitost, jak útočníka přistihnout při činu.

Vyzbrojeni třemi měřicími přístroji, které zjišťují intenzitu elektromagnetického pole rádiových sítí, se vydáváme na lov. Ze tří stran se přibližujeme k signálu, který stále sílí. Je přitom nutná nejvyšší opatrnost, aby nás hacker nespatřil a signál nepřerušil. Vše probíhá podle plánu – a už ho máme: hacker sedí ve vedlejším domě! Zůstáváme potichu a jen pozorujeme, jak si pan soused počíná dále. A v klidu shromažďujeme důkazy.

Náhle se „replay atak" přerušuje. Zřejmě už má útočník vše, co potřebuje k prolomení hesla WEP. Pro nás to znamená znovu čekat. Čím rychlejší je PC, tím rychleji lze WEP heslo zjistit. Náš hacker k tomu potřebuje zhruba hodinu. S vyčenichaným heslem se ihned přihlašuje do WLAN pana S. A začíná s další fází svého útoku: je jí „ARP poisening".

Neviditelný třetí

Alarmuje nás tentokrát druhá pozorovatelna – a teorie o útoku „man in the middle" se potvrzuje. Při tzv. „ARP poisening" záškodník zaplavuje síť zfalšovanými ARP pakety, tedy takovými, které MAC adrese přiřazují IP adresu. V tomto případě ovšem hacker rozesílá zprávu, že IP adresa routeru je spojena s jeho vlastní MAC adresou. Výsledkem je, že všechny síťové požadavky původně určené routeru nejprve dorazí k útočníkovi. Aby se spojení v síti pana S. nepřerušilo, podařený soused samozřejmě odvedené pakety zase posílá zpět na správnou MAC adresu – tedy do směrovače.

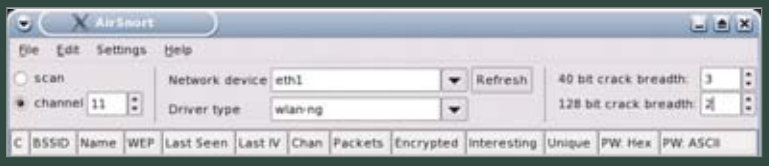
Které informace si útočník z datového proudu vytahuje, to se můžeme jen domnívat – pravděpodobně to budou všechna hesla, která se po síti přenášejí. Týká se to například všech HTTP stránek vyžadujících „login", stejně jako POP3 e-mailových účtů. HTTP stránky sice teoreticky chráněny jsou, dají se však přesto načíst pomocí následujícího triku. Otevře-li surfař HTTP stránku, dochází k výměně klíčů a SSL certifikátu, který odesílatel autentizuje. Pouze je-li certifikát platný, jsou akceptovány i klíče. Jinak obdrží návštěvník stránky chybovou zprávu o neplatnosti certifikátu. Na přání návštěvníka však přesto může být klíč akceptován. A právě tuto okolnost zneužívají hackeři: úplně normálně spustí svůj útok „man in the middle" a pak oběti podstrčí vlastní SSL certifikát. To sice vyvolá chybovou zprávu, ale tu většina uživatelů zpravidla ignoruje – mezi nimi i René S.: „Nevěděl jsem, co si mám se zprávou počít. A poněvadž se jinak na webové stránky nedostanu, zprávu jsem prostě ignoroval." Osudná chyba, neboť právě pak hacker udeřil.

Konfrontace s hackerem

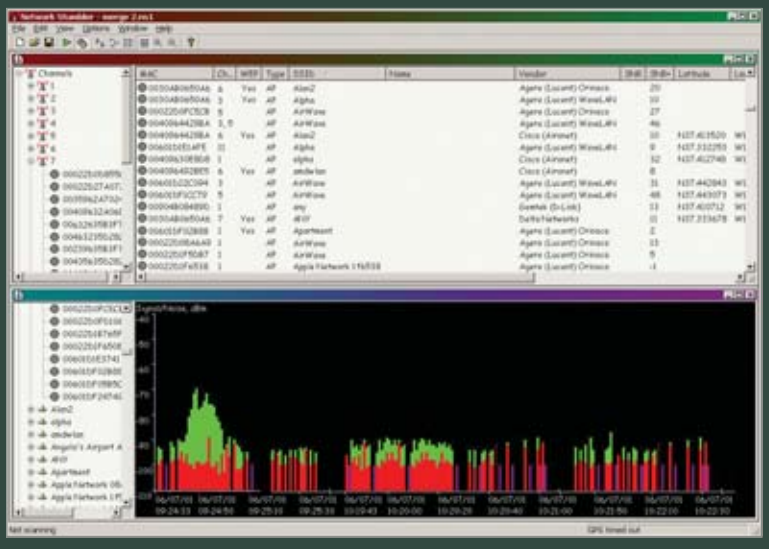
Spolu s panem S. oslovujeme hackerského souseda. Ten vše popírá a nechce s námi mluvit. Co ho přimělo k tomu, aby pana S. touto cestou šikanoval, tedy asi objasní až soud. Právní stránka případu je však každopádně jednoznačná...

Ale ať už soud rozhodne jakkoli, René S. je především rád, že balíkovému teroru už je konec. A to co se týče jak balíků z pošty, tak i „otrávených" paketů v síti. Napříště už samozřejmě chce svou domácí síť lépe zajistit a veřejným hotspotům se úplně vyhnout. Ještě mu stačíme vtisknout do ruky naši kompletní dokumentaci – a už přijímáme další telefonát. Ale o tom až v dalším pokračování našeho seriálu „CSI: internet". Budeme se zabývat tvrdou průmyslovou špionáží - odcizením utajované konstrukční dokumentace. *Valentin Pletzer*

Hackerské nástroje



JEDNODUCHÝ ÚTOK: **S nástroji, jako je AirSnort, dokáže napadnout bezdrátovou síť i hackerský začátečník. Stačí zadat vyhlédnutou oběť a kliknout na „Start"...**



NA ČÍHANÉ: **Nástrojem „Netstumbler" lze monitorovat všechny bezdrátové sítě v okolí.**

VÍCE INFORMACÍ

www.oxid.it/cain.html Hackerská souprava nástrojů, která umí překontrolovat sítě z hlediska útoků typu „man in the middle.