
# ŠPION ve vašem bytě

Hackeři vás mohou pozorovat prostřednictvím webové kamery v počítači, televizoru nebo mobilním telefonu. Ukážeme vám, co všechno útočníci dokážou a jak se proti jejich trikům bránit.

CHRISTOPH SCHMIDT, PETR KRATOCHVÍL

Vaše televize vás sleduje, když vy sledujete televizi. Váš notebook vás pozoruje, když surfujete na internetu. Váš telefon tajně kontroluje každý detail vašeho bytu. A všechny takto získané fotografie směřují do rukou počítačových hackerů. Tato noční můra jen naznačuje, jaké hrozby lze čekat od zařízení, která nejsou dobře chráněna a která jsou vybavena kamerou. A že nejde o vymyšlenou hrozbu, to nedávno ukázala i aféra v USA, když bylo zjištěno, že půjčovna notebooků tajně sledovala své zákazníky – učitele a studenty. Existuje celá řada věcí, které mohou specializované programy pro sledování dělat, a nepříjemné je, že většina z nich je spojena s malwarem. Když na obrazovce vidíte vlastní fotografii z webkamery, je ransomwarová (vyděračský software) výhružka účinnější – máte tak bohužel jistotu, že váš počítač ovládli zločinci.

## Trojrozměrný plán vašeho bytu

Pokud se hackerům podaří získat přístup ke kameře mobilního telefonu, mohou být důsledky ještě závažnější. Vzhledem k tomu, že se mobilní telefony používají na různých místech a jsou často v pohybu, mohou specializované trojské koně vytvářet detailní, trojrozměrný a zoomovatelný snímek bytu či kanceláře. Díky tomu by si zločinci klidně mohli přečíst například poznámky v kalendářích, na tabulích nebo papírech položených na stole. Jakkoliv se to zdá neuvěřitelné, fakt je, že vědci již podobný zkušební „proof-of-concept“ software vyvinuli. Kromě počítačů a smartphonů jsou rizikové i televizory s integrovanou webkamerou – pokud je takový přístroj připojen k internetu, může být bez problémů napaden hackery. My vám ukážeme, jaké nebezpečí vám u těchto přístrojů skutečně hrozí a jak svá zařízení můžete chránit.

# PC A NOTEBOOKY: Cizí oči

Webkamery už patří u klasických počítačů a především notebooků ke standardní výbavě. Jen málokdo si ale uvědomuje, jaká rizika mohou tyto kamery přinášet.

Již na počátku devadesátých let se u počítačů začaly používat webové kamery – především pro videochatování nebo jednoduché sledování vybraného místa. V současnosti je už většina notebooků a „all-in-one" počítačů vybavena integrovanou kamerou s objektivem o velikosti průměru tužky, umístěnou v horní části displeje. Tuto kameru může zapnout každý software nainstalovaný na počítači a fotky či videa mohou být odeslány kamkoliv na internet.

Některé americké firmy, které nabízely počítače na splátky, této schopnosti až do září 2012 využívaly. Do jejich počítačů a notebooků byl nainstalován bezpečnostní software společnosti DesignerWare, který umožňoval lokalizaci a zablokování počítačů, za něž nebyly splátky zaplaceny. Zaměstnanci sedmi firem v tomto oboru používali tento software nelegálně pro přístup k veškerým možným informacím o uživatelích: od soukromých e-mailů a přihlašovacích údajů ke službám přes navštěvované webové stránky až po bankovní údaje. Také si ukládali fotografie dětí a dospělých pořízené webkamerou, občas i v situacích, kdy byli uživatelé počítačů nazí nebo se zabývali intimními činnostmi. Jaké důsledky může mít podobné špehování přes webkameru, to ukázal nedávný případ z New Jersey. Student tamní školy Tyler Clementi spáchal sebevraždu poté, co ho jeho spolubydlící tajně natáčel v kompromitujících situacích a videa zveřejňoval na internetu.

## Jak si můžete chránit své soukromí?

Externí USB webkamery nabízejí maximální možnost kontroly: můžete ji zakrýt, když ji nepoužíváte, otočit ji stranou nebo, což je nejbezpečnější způsob, ji odpojit z USB portu.

U notebooků jsou kroky k zabezpečení mnohem obtížnější – většina z nich sice disponuje klávesovou zkratkou pro vypínání webkamery, není ale problém ji opětovně zapnout pomocí softwaru. Bohužel, indikátorem natáčení nemusí být ani červená dioda. Na nedávné tiskové konferenci nejmenované bezpečnostní firmy byl představen produkt pro ochranu notebooků, který v případě odcizení dokáže zaznamenat pachatele pomocí aktivní webkamery. Podle diskuse s bezpečnostními experty je softwarové odpojení diody (indikující nahrávání kamery) dětskou hračkou.

Bezpečnějším řešením je zakázání webkamery přímo v BIOS, to lze ale doporučit pouze v případě, že webkameru používáte jen minimálně.

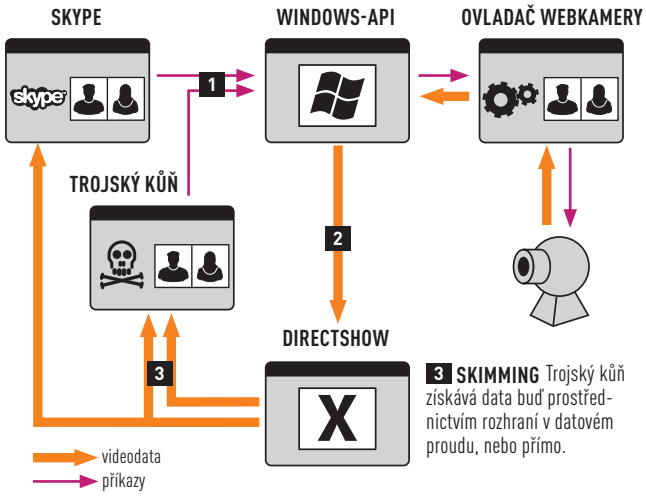
Nejefektivnější je tedy použití softwarových nástrojů na odhalení potenciálních hrozeb, které by vaši kameru mohly zneužít. Pro tento účel lze doporučit například program Spybot Search & Destroy (najdete ho na Chip DVD pod indexem Nepřítel).

### JAK MALWARE INFIKUJE VÁŠ POČÍTAČ?

Trojský kůň může pro své potřeby využívat i legální software v počítači. Díky tomu může být například pomocí potřebných API obrázek tajně předán legálnímu programu, který ho odešle na vybrané místo na internetu.

**1 SPOUŠTĚNÍ ÚLOHY** Legální a nelegální software mohou být zaměněny prostřednictvím volání ovladačů webové kamery.

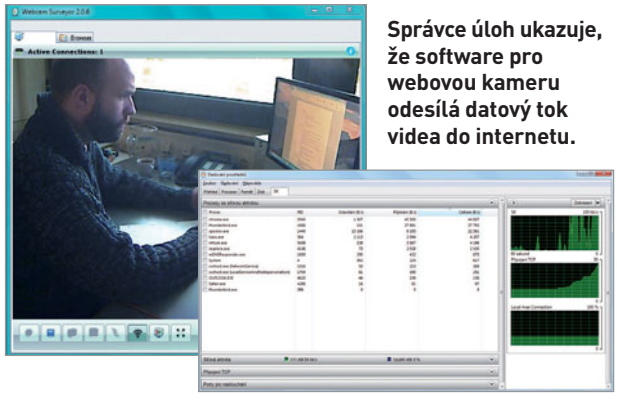
**2 ZPRACOVÁNÍ** Cíle je dosaženo prostřednictvím Windows API a DirectShow filtrů v softwaru.




**3 SKIMMING** Trojský kůň získává data buď prostřednictvím rozhraní v datovém proudu, nebo přímo.

### JAK LZE ODHALIT NECHTĚNÉ AKTIVNÍ WEBKAMERY

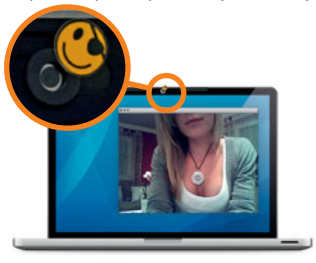
Aktivní kameru neprozradí ani svítící dioda – celá řada programů (například Webcam Surveyor) dokáže natáčet ve skrytém režimu bez jakékoliv indikace. Přesto existuje způsob, jak natáčení a přenos dat odhalit. Pokud spustíte správce úloh, prozradí natáčení aktivní proces videoprogramu a přenos videa na internet odhalíte aktivitou v záložce »Sítě«.



**Správce úloh ukazuje, že software pro webovou kameru odesílá datový tok videa do internetu.**

### MECHANICKÁ OCHRANA: JEDNODUCHÁ, ALE ÚČINNÁ

Pokud se chcete zabezpečit a nechcete, aby vás někdo mohl špehovat, pak kameru vypněte, když ji nepoužíváte, nebo ji alespoň otočte někam, kde není nic k vidění. U notebooků tento trik možný není, stále ale existuje jednoduché a účinné řešení například v podobě jednoduchých ochranných krytů.

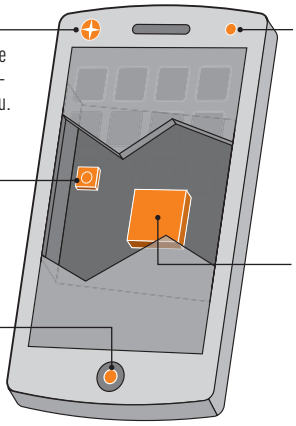


**Speciální kryty pro deaktivaci webkamery nemusí kazit vzhled přístroje.**


**Pokud obrátíte webkameru směrem ke zdi nebo stropu, bude pro hackera nepoužitelná.**

### SMARTPHONY: ZAJÍMAVÝ CÍL PRO HACKERY

Hackeři zjišťují, že smartphony mohou být velmi zajímavým cílem, protože obsahují velké množství dat, která mohou být odcizena. Zajímavé je také například to, že z tajně pořízených snímků lze získat i informace o tom, kde přesně byla fotografie pořízena.



**KOMPAS/GPS:** Přesné informace o poloze mohou být použity při plánování vniknutí do objektu.

**KAMERA:** Smartphone může zaznamenávat video, které hackeři nahrávají.

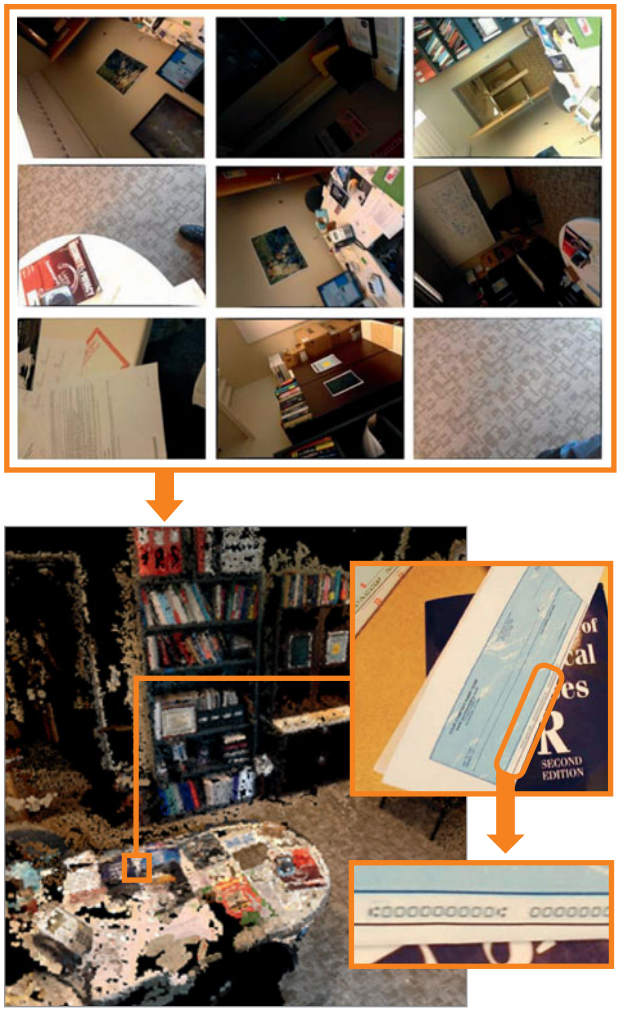
**SNÍMAČE:** Senzor rychlosti detekuje údery na klávesnici.

**UMTS:** Hackeři mohou díky 3G připojení určit, k jaké buňce je smartphone připojen.

**MIKROFON:** Konverzace může být zaznamenána bez povšimnutí.

### TROJSKÉ KONĚ MOHOU NATOČIT CELÝ BYT

Vědci vyvinuli trojského koně pro smartphony (Place Raider), který pravidelně tajně zaznamenává fotografie a ukládá je na serveru. To hackerovi umožňuje, aby si vyšel na virtuální procházku a rozhlédl se po pokojích, kde se smartphone používá.



**Server z chaotických fotografií v panoramatickém režimu vytvoří model, ve kterém si hackeři mohou přiblížit téměř libovolné místo.**

# SMARTPHONY: Vždy na stráži

Smartphone umožňuje rozsáhlé pohledy do soukromí svého majitele, a to nejen díky kameře, ale také celé řadě dalších senzorů.

S neustálým připojením k síti, jednou, nebo dokonce dvěma kamerami a celou řadou dalších senzorů se smartphone ukazuje jako mimořádně lákavý cíl nejen pro zvědavé hackery. Na rozdíl od klasických počítačů dokáže nejen zaznamenat některé kompromitující scény, ale také poskytnout celou řadu informací, které s obrazovým materiálem souvisí. Typickou ukázkou mohou být přesné informace, kde byla fotografie pořízena. Vědci již dokázali zmanipulovat smartphone tak, že se jim z řady tajně přijatých fotografií podařilo vytvořit rozsáhlé a zoomovatelné „panoráma" místnosti. V rámci něj bylo například možné hledat potřebné důležité informace, které by na první pohled mohly uniknout.

O široké spektrum informací, které smartphony nabízí, se začínají zajímat nejen hackeři, ale i výrobci smartphonů a jejich obchodní partneři, kteří chytré telefony dodávají na trh. Typickou ukázkou je například Ad-Tracking, který Apple představil s iOS 6. Ten funguje tak, že unikátní číslo jednoznačně spojuje uživatele s konkrétním zařízením se systémem iOS. Při návštěvě webové stránky a při použití aplikací je tato informace spolu s číslem předána reklamním serverům, jejichž provozovatelé získají přesný obraz o tom, co děláte a co vás zajímá. Návod, jak tuto špionáž můžete vypnout, najdete na → **str. 105**.

## Špionáž prostřednictvím mikrofonů a senzorů mobilních telefonů

Pokud si myslíte, že váš smartphone a jeho webová kamera jsou chráněny bezpečnostním konceptem platformy Android, uvažujete bohužel chybně. Bezpečnost tohoto operačního systému je založena na dvou základních kamenech. Za prvé: uživatel musí každé aplikaci udělit povolení činnosti. Za druhé: Android striktně odděluje jednotlivé aplikace od sebe.

Díky tomuto principu může malware nahrát na internet ukradené informace pouze v případě, že má od uživatele oprávnění k přístupu k síti. Bohužel to, že ani tento princip vám nezaručí bezpečí, ukazuje koncept supermalwaru Soundcomber. Ten totiž pro svou činnost potřebuje pouze povolení pro záznam zvuku, což lze zamaskovat například u neškodné aplikace na hlasové poznámky.

Poté dokáže Soundcomber tajně odposlouchávat telefonní hovory a získávat čísla zadaná přes klávesnici nebo přímo hlasem do telefonu. Tyto záznamy je poté možné odeslat na internet vyvoláním Android prohlížeče s konkrétní URL, která nevyžaduje povolení. Také je možné, aby součástí URL byla zaznamenaná (volaná) čísla, která lze takto uložit na webovém serveru.

Alternativně také může Soundcomber propašovat tato data prostřednictvím předáním typu mrtvá schránka další nainstalované malwarové aplikaci. Pro tento účel lze například vytvořit aplikaci pracující s fotografiemi, u které nebude podezřelá

práce s daty v telefonu a která bude mít od uživatele povolen přenos dat na internet (například na různá fotoúložiště). Kromě kamery a mikrofonu mohou uživatele smartphonu špehovat také senzory pohybu.

To je i cílem výzkumného projektu (sp)iPhone, který využívá senzory akcelerace iPhonu k určení, co se píše na klávesnici počítače, která je položena vedle telefonu na stole. Ač se to zdá neuvěřitelné, smartphone registruje vibrace a díky nim dokáže zrekonstruovat zadávaný text. Při využití slovníkové databáze vztahující se k tématu dosáhli vědci úspěšnosti přibližně 80 procent.

## Procházka vaším bytem

Ještě děsivější je to, co předvádí aplikace s názvem Place Raider, vyvíjená americkým Surface Naval Warfare Center. Ta běží na pozadí a ve chvíli, kdy uživatel svůj smartphone nevyužívá, v pravidelných intervalech snímá své okolí. Poté eliminuje s využitím výpočetního výkonu smartphonu nepoužitelná data – odstraněny jsou přesvícené, rozmazané nebo duplicitní snímky.

Nakonec aplikace nahraje vybrané fotografie na server, který z nich vytvoří 3D panoramatický model. Ten je ve finále vytvořen z tak velkého množství fotografií, že je možné při použití speciálního softwaru přečíst i dokumenty psané malým písmem (uložené v bytě). Tento software tak může v budoucnu sloužit k počítačové špionáži, ale také například zlodějům při plánování vloupání.

Vědci si jsou vědomi nebezpečnosti těchto hrozeb a zároveň sami navrhli ochranu před podobnými aplikacemi – základem by mohlo být pouze mechanické ovládání pořízení fotografií (či videa) a jakákoliv aktivace záznamu by měla být indikována zvukovým signálem.

## Jak chránit smartphone před špehováním

Přestože zde zmiňované špionážní aplikace jsou zatím používány pouze ve výzkumných projektech, je jen otázkou času, kdy je v chytrých telefonech začnou v praxi využívat hackeři. Zatímco uživatelé Apple iOS určitý druh ochrany mají (viz níže), uživatelé platformy Android musejí být opravdu opatrní.

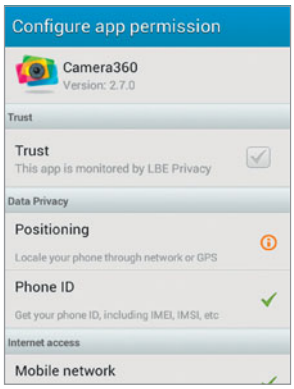
Základním kamenem ochrany na této platformě jsou kombinace povolení, pomocí kterých uživatel vybrané aplikaci sdělí, co smí a co nesmí dělat. Jakmile například aplikaci jednou povolíte přístup k fotoaparátu a na internet, může pak kdykoliv využít přístupu k fotoaparátu a získané fotografie a videa nahrát na internet. A to je důvod, proč by uživatelé měli instalovat jen aplikace od důvěryhodných výrobců a z důvěryhodných zdrojů, a i přesto vždy zkontrolovat požadované povolení.

V zájmu ochrany před trojskými koni (a malwarem obecně) byste měli povolení k přístupu ke kameře a internetu udělovat jen velmi obezřetně, v ideálním případě používat aplikaci, která tato oprávnění dokáže měnit i později po nainstalování.

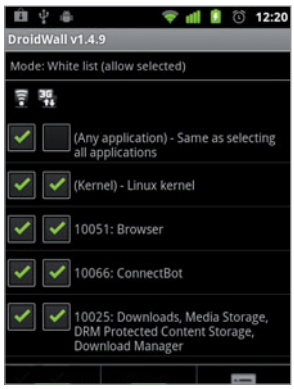
Uživatelé platformy iOS práva aplikací tak precizně regulovat nemohou, ale v podstatě to ani nemají zapotřebí – především díky přísné vstupní kontrole v App Storu. Do aplikace pro iOS je podle Omara Aboua Deifa, hlavního vývojáře aplikací společnosti vukee, obecně velmi těžké umístit trojského koně. Na rozdíl od Androidu musí mít v iOS aplikace velmi dobrý důvod, proč zůstat aktivní na pozadí. A pro Apple je snadné tyto důvody kontrolovat. Nicméně i zde doporučují experti dodržovat obecné pravidlo a odinstalovat z telefonu vše, co nepoužíváte. Jakmile je jednou aplikace odstraněna, již nepředstavuje potenciální hrozbu.

### VĚTŠÍ BEZPEČNOST: OMEZENÍ APLIKACÍ

Bezpečnostní nástroje dokážou omezit přístup aplikací i později po instalaci. LBE Privacy Guard pro tento účel vyžaduje root práva. Aplikace DroidWall přispívá k bezpečnosti jiným způsobem – dokáže deaktivovat přístup k internetu pro podezřelé aplikace. Díky tomu máte jistotu, že vaše soukromá data nezmizí kamsi na internet.

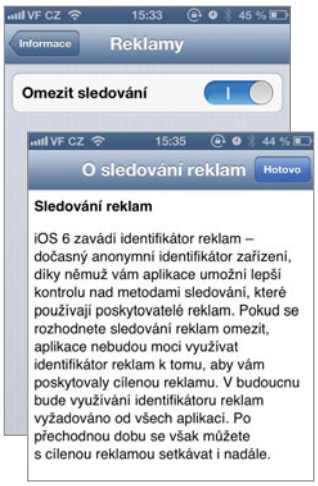



**LBE PRIVACY GUARD:** Pracuje na pozadí a kontroluje aplikace, které žádají o oprávnění. Díky tomu můžete každý požadavek podezřelé aplikace snadno schválit nebo zamítnout.




**DROIDWALL:** Klíčovou funkcí je povolení (či zákaz) přístupu aplikace k 3G nebo Wi-Fi. Lze tak i omezit přenos dat a prodloužit výdrž na baterii.


**RECONBOT (PRO IOS):** Promění každý iPhone v tajnou webkameru, která natáčí video, jež lze sledovat na dálku z webového prohlížeče.




**AD-TRACKING:** Sledování lze v iOS upravit v rámci nabídky »Nastavení | Obecné | Informace | Reklamy«.

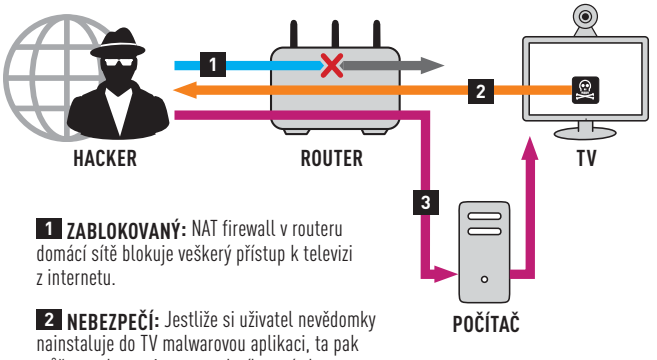
### ODBLOKOVÁNÍ IPHONU – VÍCE MOŽNOSTÍ A RIZIKA

Telefony Applu jsou relativně bezpečné. Tedy pouze do chvíle, kdy se jejich uživatel rozhodne si telefon hacknout pomocí tzv. jailbreaku. Problém je především to, že většina uživatelů tomuto zásahu nerozumí a pouze ho provedou krok za krokem podle návodu z internetu. Pokud ale návod není bezchybný a například uživatele neupozorní, že by si měli změnit implicitní heslo k SSH přístupu, může z toho být velký bezpečnostní problém.

**IPHONE** je relativně bezpečný telefon, pokud ale nepoužijete jailbreak.

### TELEVIZNÍ KAMERY: PŘÍMÉ A NEPŘÍMÉ ÚTOKY

Pokud chce hacker prozkoumat váš gauč v obývacím pokoji, musí do televizoru nebo na připojený počítač, který aktivuje TV kameru a přenos obrazu, propašovat malware. Ochrana: Vždy nainstalovat pouze důvěryhodný software a chránit počítač bezpečnostními nástroji.




**1 ZABLOKOVANÝ:** NAT firewall v routeru domácí sítě blokuje veškerý přístup k televizi z internetu.

**2 NEBEZPEČÍ:** Jestliže si uživatel nevědomky nainstaluje do TV malwarovou aplikaci, ta pak může snadno na internet odesílat snímky z webkamery.

**3 OBJÍŽĎKA:** Pokud se malware dostane v domácí síti na počítač, může zaútočit i na televizi a z ní nahrávat data na internet.

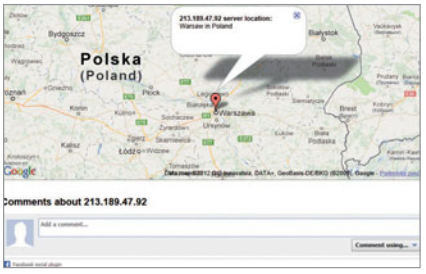
### MECHANICKÉ ODDĚLENÍ KAMERY

Pokud si myslíte, že jste sledováni, prvním krokem by mělo být odpojení kamery od PC nebo Smart TV.

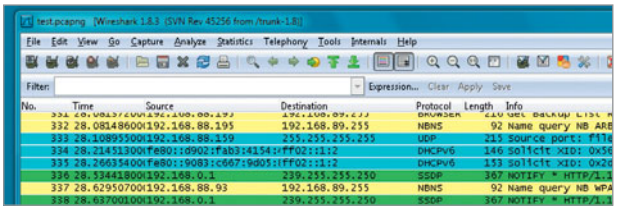
**Webkamery u Smart TV Samsung lze otočit kolmo, takže se objektiv skryje pod krytem.**

### PROVĚŘENÍ INTERNETOVÝCH WEBŮ

Pokud si nejste jisti kam se z vaší televize odesílají data, můžete pro tento účel využít specializované webové aplikace. Ty zjistí, kdo se za IP adresou skrývá. Tyto služby najdete například na **whatismyipaddress.com/ip-lookup** nebo **www.ip-adress.com/ip_tracer**.




**Díky této službě jasně poznáte kam se odesílají vaše data.**




**Pomocí nástroje Wireshark můžete získat a analyzovat údaje o síťovém provozu a zjistit, kam jsou zasílána data.**

# CHYTRÉ TV: Nejen pohled na gauč

Doopravdy dokážete odpočívat, i když je možné, že vás nahrává webkamera televizoru? Je tato hrozba reálná?

Nejnovější nejvyšší třída televizorů firmy Samsung přichází na trh s integrovanou webkamerou. Ta není integrována jen pro pohodlný videochat s přáteli, ale může spolupracovat i s dalšími vymožeností, jako je ovládání gesty nebo detekce obličeje. Vzhledem k tomu, že televizím nechybí ani připojení k internetu, mohou tyto nové funkce také zjednodušit přihlašování k webovým službám. Základním problémem z hlediska ochrany soukromí ale zůstává skutečnost, že jakmile má televize kameru a je připojena k internetu, mohou z ní být obrázky tajně odesílány na internet.

Pravda ale je, že chytré televizory prozatím představují pro hackery hodně tvrdý oříšek, a to nejen proto, že v této oblasti existuje pouze minimum komerčních aktivit. „Televizory obsahují proprietární systémy, a k internetu jsou navíc obvykle připojeny přes domácí router, což podstatně ztěžuje jejich napadení," tvrdí Stefan Ortloff, virový analytik u bezpečnostní firmy Kaspersky Labs.

Teoretickou možností, jak napadnout chytrý televizor, je naprogramování specializované aplikace, která musí být umístěna do „app storu" výrobce televizoru, odkud si ji musí zákazník stáhnout a nainstalovat. Další možností je napadení televize z webové stránky, kterou si uživatel zobrazí v prohlížeči integrovaném v televizoru. To je ale poněkud obtížné, protože jak systém, tak prohlížeč televizoru jsou zcela odlišné například od klasických Windows s prohlížečem. O tom, že to ale není nemožné, nás může přesvědčit například exšéf CIA David Petraeus, který se nedávno zmínil, že agentura tyto metody použila pro sledování podezřelých lidí.

## Jak se bránit špehování ve vlastním obývacím pokoji

Základem ochrany soukromí je v tomto případě router, přes který chytrý televizor komunikuje se světem. Dříve než se ale pustíte do ochrany televizoru, měli byste zkontrolovat samotný router – vyzkoušejte, zda neobsahuje potenciální zranitelnost, nebo zda dokonce není na webu výrobce k dispozici novější firmware.

Po aktualizaci otevřete konfigurační dialog routeru a přepněte se na sledování komunikace v síti. Některé routery obsahují funkci „capture", která v určitém intervalu sbírá kompletní informace o datovém provozu. Poté zapněte televizor, zkuste využít několik chytrých funkcí, včetně přístupu do „app storu", a na routeru sledujte, s jakými adresami televizor komunikuje. Poté si poznamenejte, na které IP adresy aplikace data odesílají, a tyto weby prověřte. Pokud si nejste stoprocentně jisti, že jde o důvěryhodný web, v konfigurační nabídce routeru ho přidejte na blacklist a poté v televizoru vyzkoušejte, zda má zákaz vliv na funkčnost. I u televizoru ale platí, že stahovat a instalovat aplikace byste měli pouze na důvěryhodných webech – v tomto případě pouze na stránkách výrobce.