Účet v oblacích

CO JSOU A JAK FUNGUJÍ ADULT DIALERY

VOJTĚCH BEDNÁŘ

Dávná, ale teprve nyní opravdu aktuální hrozba telefonického připojení k internetu děsí nejednoho uživatele. Nejste také vy obětí adult dialerů?

Dialery mohou přijít draho

Pan X je typický domácí uživatel internetu. Síť využívá k práci s e-mailovou schránkou, čte si noviny a odborné on-line zpravodajství, někdy, i když ne tak často, debatuje v diskusních skupinách. Připojuje se modemem, ze sítě Českého Telecomu, jeho typický měsíční účet za internet se pohybuje v řádu stovek korun.

Co je to dialer?

- Dialer je program nebo skript, který mění telefonické připojení sítě, nebo vytáčí číslo se speciální tarifikací za účelem zpřístupnění placeného obsahu
- Dialery využívají některé webové servery, zvláště s erotickým či ilegálním obsahem
- Podvodné dialery obcházejí uživatele. Instalují se bez jeho vědomí, mění nastavení telefonu a připojují počítač k draze tarifikovaným bodům

O to větší překvapení pro pana X je, když jednoho dne z Telecomu přijde vyúčtování zvící jednotek, nebo dokonce desítek tisíc korun, provolaných na linky se speciálním tarifem. Pan X přeci nikam nevolal, tak co se mohlo stát? Odpověď je jednoduchá. Náš uživatel se stal typickou obětí adult dialeru. Přese vše, co si o těchto pozoruhodných aplikacích a jejich možnostech zneužití i využití dále povíme, je chyba pouze a jedině na straně pana X a nikde jinde. On sám byl totiž zodpovědný za vstup vetřelce do svého počítače, za nainstalování dialeru a za vynechanou prevenci.

POZNEJ SVÉHO NEPŘÍTELE

Jedním z velkých a stále nevyřešených problémů webu a služeb na něm je způsob jejich placení. Zatímco u mnoha služeb se hledají kompromisy mezi platebními kartami, mikroplatebními systémy a elektronickým bankovnictvím, jistá část internetových služeb šla poněkud jinou cestou. Tam, kde z nějakého důvodu není možnost snadno průchodné a především průhledné cesty zpoplatnění obsahu, vymysleli provozovatelé alternativu. Touto alternativou je přimět uživatele, aby za využité služby platil svým vlastním telefonním účtem.

Vychází se z předpokladu, že většina zejména domácích uživatelů využívá k přístupu k síti dialup, tedy připojení pomocí komutované linky. Komutovaný uživatel platí svému poskytovateli telefonní linky, v našich podmínkách převážně Českému Telecomu, a v některých případech také poskytovateli služeb přístupu k internetu (ISP). U nás ale větší část domácností využívá „internetu zdarma“, kdy je část nákladů pro ISP obsažena přímo v telefonním účtu. Protože obě složky (nebo jen ta jedna viditelná) jsou přesně stanoveny, lze velmi efektivně sledovat celkové náklady za přístup k internetu za platební období, obvykle je to měsíc.

Co když ale dojde k překonfigurování telefonického připojení v počítači tak, že se místo k přístupovému bodu ISP připojuje pomocí komutované linky jinam? Někteří poskytovatelé obsahu této možnosti využili. Obvykle se jedná o společnosti nabízející řekněme okrajový obsah, obvykle pornografického charakteru, a také warez (ilegální kopie softwaru, cracky atd.). Pro takové subjekty je obtížné využívat klasických platebních kanálů buďto proto, že jejich činnost není právě v souladu se zákony, proto, že účtování a zpracování plateb by jinak bylo obtížné, nebo z jiných důvodů.

Prakticky to funguje takto: Část webu poskytovatele obsahu je přístupná klasickým způsobem z internetu. Pokud se chce uživatel dostat k tomu „zajímavějšímu“, je mu nabídnuto stažení aplikace, která to zajišťuje. Aplikace změní nastavení vytáčeného připojení, počítač odpojí od sítě a pak spojení znovu zavede, nyní již s pozměněnými parametry.

V některých případech má uživatel po vytvoření nového připojení přístup pouze k tomu obsahu, který mu má softwarový konfigurátor připojení – dialer poskytovat. Jindy se poskytovatel obsahu chová také jako regulérní ISP.

Kolik lze utratit?

- Pokud dialer volá na číslo v ČR, je cena obvykle 60 Kč za minutu připojení
- Volání do zahraničí může být ještě dražší, a zahraniční dialery jsou schopny z České republiky fungovat
- 1 hodina strávená na internetu s adult dialerem v rámci ČR stojí 3 600 Kč

Tehdy má uživatel přístup ke všem protokolům a službám, které jinak využívá bez viditelné změny. Nicméně není připojen ke svému ISP, ale k poskytovateli jednoho konkrétního obsahu. A protože jeho přístupový bod neakceptuje klasický tarif pro přístup k síti, ale jiný, speciální a mnohem vyšší, může telefonní účet vyrůst do nepříjemných výšin.

Dialery jsou legitimní součástí mechanismů plateb za internetový obsah. Mají svůj význam a jsou užitečné podobně, jako sama telefonní čísla se zvýšeným tarifem. Problém je v tom, že právě dialery mohou být snadno zneužity.

Standardním postupem je, že pokud nějaký web využívá dialeru, musí uživatele o této skutečnosti informovat a také mu říct, že pokud si program stáhne a spustí, dojde k jeho přepojení na telefonní číslo se zvýšeným tarifem, nebo do zahraničí. Uživatel by také měl mít možnost připojení standardním způsobem ovládat, odpojit a přejít na své původní a standardně placené. Protože svět počítačů připojených pomocí dialupu je poměrně homogenní a protože techniky v nich použité umožňují provádět rozsáhlé změny nastavení na dálku, lze snadno uživatelovu kontrolu obejít. Tak vznikl problém, který už desítky Čechů a tisíce uživatelů v jiných zemích stál mnoho peněz.

▲ **Na webové stránce Českého Telecomu www.telecom.cz/infocentrum/o_cem_se_mluvi/podvodna_volani_activex/ naleznete podrobné informace a prezentace k problematice podvodného přesměrování na linky se zvláštním tarifem**

TECHNIKA DIALERU

Adult dialer může mít několik forem. Buďto se jedná o aplikaci určenou pro obecný operační systém (jakákoliv Windows, ale také Mac OS), nebo o aktivní prvek ve formě komponenty ActiveX, nebo dokonce javového appletu. Aplikace může být vybavena digitálním podpisem. Ten je původně určen k tomu, aby bylo zajištěno, že program po svém vytvoření a podepsání nebyl změněn, ve skutečnosti ale plní trochu jiný účel. Standardně nastavená Windows se totiž k podepsaným programům chovají benevolentněji, a také je pravděpodobnější, že uživatel bude souhlasit se spuštěním něčeho, co se tváří „certifikovaně“.

K tomu, aby mohl dialer fungovat, potřebuje odpovídající prostředí. Pokud je dialerem aplikace, která kromě samotného spojení s přístupovým bodem poskytovatele obsahu zajišťuje také jeho prohlížení nebo jinou práci s ním, toho moc nepotřebuje. V zásadě postačí fungující operační systém a přístup k modemu. Lehčí verze dialerů se spoléhají na webový prohlížeč a samy zprostředkovávají pouze připojení. A ty technicky „nejlehčí“ pak pouze překonfigurují připojení v operačním systému. To znamená, že musí mít oprávnění něco takového udělat.

▲ **Na webovém sídle DigiWeb (www.digiweb.cz) se v rubrice TOP – Speciály dozvíte mnoho zajímavých informací o podvodných dialerech, a kromě toho se můžete zúčastnit diskuse**

Samotný prvek – dialer, je z technického hlediska malou a jednoduchou záležitostí. Všechny technologie, které využívá, jsou již obsaženy v operačním systému a on v sobě, v ideálním případě, potřebuje mít jen postup, jak jich využít a co všechno změnit.

DIALER JAKO BOMBA

Dialery jako takové se používají již poměrně dlouhou dobu. Jsou to někdy více, jindy méně korektně fungující prostředky obživy svých tvůrců. Před nedávnem se ale objevila jejich nová forma. Není přímo svázána se žádným obsahem, připojuje se k bodům chovajícím se jako běžný ISP, interakce s uživatelem při instalaci je redukována na minimum. Z klasického dialeru se tak stává podvodný. Lze k němu přijít snadno. Většinou na stránkách s pornografickým a jemu spřízněným obsahem, v místech, která slibují nebo i nabízejí „ilegální“ data. Stačí, když uživatel klepne na odkaz, a je mu nabídnuto stažení a spuštění většinou velmi malého programu. V některých případech, kdy má dialer formu komponenty, to dokonce ani není nutné. Nastavení sítě je změněno, následuje krátké odpojení od sítě a další provoz, tentokrát již za komerční tarif. Počet případů, kdy lidé na tento princip naletěli, se nedávno prudce zvýšil.

Jaká je prevence?

- Programy aktivně blokující změny telefonického připojení (www.optimaccess.cz)
- Pravidelná kontrola před spywarem
- Pozorně si všímat, co instalujeme
- Prohlížeč nastavený tak, aby se dotazoval před instalací součástí

Telefonní číslo se zvláštním tarifem, které je dialery využíváno, se může nacházet u nás i v zahraničí. Zejména ve druhém případě bývá velmi obtížné zjistit, komu patří, tedy kdo je zodpovědný za peníze převedené z kapes uživatelů dialupu v míře větší, než si tito uživatelé představovali. Protože samotné spojení funguje obvykle bezvadně, není chyba na straně provozovatele telekomunikačních služeb a ISP, který byl změnou konfigurace vyřazen ze hry, za útok pochopitelně také nemůže.

DIALER MINIMALISTA

Pro to, abychom mohli připojit počítač k síti pomocí telefonu, potřebujeme kromě modemu a jeho ovladače ještě několik údajů. Především se jedná o telefonní číslo, dále pak o nastavení DNS serveru, a o identifikační údaje, tedy jméno a heslo. Protože adresy DNS a některé další údaje se mohou měnit, existuje a obvykle je využívána možnost jejich automatické konfigurace při navázání spojení. Také přihlašovací údaje nejsou zcela nezbytné, připojení může fungovat i bez toho, aby někde na serveru existovaly pro ověření jejich protějšky. Takže pro změnu připojení stačí teoreticky změnit jen to poslední, tedy telefonní číslo.

To je v prostředí majoritního OS Windows poměrně jednoduché. Verze 9x a ME nejsou prakticky nijak chráněny proti tomu, aby jakékoliv nastavení nebylo upraveno uživatelem, ale procesem. V případě Windows založených na technologii NT (verze NT, 2000 a XP) lze různým úrovním administrace počítače přidělovat různé restrikce, a úplný přístup ke všemu má jen administrátor. I to má ovšem výrazný háček. Na mnoha domácích počítačích připojených k internetu se totiž pracuje jen z jednoho účtu, s administrátorskými právy a bez jakýchkoliv úprav v implicitním nastavení přístupů. Společně s Internet Explorerem pak tvoří velká část domácích počítačů ideální cíl dialerů. Webový prohlížeč je spoluviníkem jejich funkce také proto, že bývá nastaven na poměrně nízký stupeň ochrany a protože má všechny technologie nutné pro jejich funkci integrovány přímo v sobě. Samotnému dialeru pak stačí teoreticky jen změnit kritické telefonní číslo ve stávajícím připojení. Pokud se skutečně jedná o „bombu“, nemusí dále vyvíjet prakticky žádnou činnost, protože svou práci již jednou udělal.

Jaká je léčba?

- Odpojit počítač od internetu, v rámci možností vypnout modem, nenavazovat další spojení
- Program pro eliminaci spywaru s podporou odhalení dialerů
- Kontrola telefonních čísel v nastavení dialupu
- Kontrola paměti, kontrola, zda nemá dialer vlastní ikonku, odkaz v nabídce Start nebo odinstalátor

ČESKÁ SMRŠŤ

Existuje mnoho podvodných dialerů (adult dialery se jim říká právě pro jejich svázanost s erotickým obsahem), poměrně málo je jich aktivních u nás. Značnou popularitu si vysloužily erotické stránky *www.amaterky.com* zejména proto, že byly medializovány, faktem ovšem je, že do jisté míry nezaslouženě. Podobný dialer, který se velmi nenápadně vnucoval na tomto serveru, se vyskytuje na mnoha dalších, českých i zahraničních. Minuta volání na pozměněnou linku vyšla na šedesát korun, to ovšem nemohla být nejvyšší možná částka. Sdružení obrany spotřebitelů ČR *(www.900.spotrebitele.info)* na počátku dubna evidovalo více než devadesát poškozených, kteří s ním spolupracují a kteří kvůli dialerům přišli o 1 600 000 Kč. Skutečný počet lidí, jejichž telefonní účty se díky adult dialerům vyšplhaly do závratných výšin, je ovšem nejspíše o několik řádů větší. Český Telecom spekuloval o počtu přes 900, ani to ale nemusí být konečné číslo. Zahrnuje totiž pouze ty uživatele, u nichž došlo k prudkému výkyvu telefonního účtu v položce čísel se speciální tarifikací (900). V současnosti již byla podána trestní oznámení v souvislosti s činností dialerů fungujících bez vědomí uživatele. Dominantní telekomunikační operátor také provedl několik preventivních opatření snižujících riziko zneužití. Causa je ovšem stále otevřená a je škoda, že technologie, která sama o sobě má opodstatnění a právo žít na slunci světa IT, byla zneužita v neprospěch těch, pro něž byla určena.

▲ Ze stránek brněnské firmy Sodat (www.optim-access.cz) si můžete stáhnout freeware ochranného systému OptimAccess Dial verze 1.0

▲ Server Sdružení obrany spotřebitelů ČR (www.900.spotrebitele.info/) je zdrojem cenných informací co dělat v případě, že jste byli poškozeni

Jak se chránit před podvody způsobenými adult dialery

PREVENCE JE NEJLEPŠÍ OBRANOU

Operační systém bez zabezpečení, otevřený přístup ke konfiguraci telefonického připojení sítě a uživatel – ignorant. To je vše, co podvodné dialery potřebují pro umožnění co největšího a co nejtrvalejšího výdělku svým tvůrcům a pánům. Léčit následky jejich fungování je dlouhodobé, nejisté a náročné. Předcházet jejich činnosti ovšem můžete již dnes.

První fází je rozhodnutí, zda jste nebo nejste riskantní uživatel. Navštěvujete servery s pornografickou tematikou nebo jiným, již vyjmenovaným obsahem? Klikáte na odkazy v reklamních e-mailech, které vám přicházejí a které slibují zajímavá místa? I v případě, že jste na všechny tyto otázky odpověděli negativně, neznamená, že jste v bezpečí. Váš počítač může používat kdykoliv někdo jiný, kdo tyto zásady nerespektuje, nebo se můžete dostat na server snažící se vám vnutit dialer zcela náhodou.

Základním kamenem prevence před vysokým telefonním účtem je být pozorný, neustále pozorný. Pokud prohlížeč požádá o instalaci čehokoliv do počítače, byť by to bylo digitálně podepsáno, je dobré velmi dobře zkoumat, co se vlastně instaluje a co to bude dělat. Pokud stránky požadující instalaci nedostatečně popisují co se instaluje, popisují to laxně na způsob „a small plugin required to run this site“, anebo instalovaný prvek bagatelizují, je implicitní odpověď NE. I v případě, že je dokumentace k dispozici, je velmi dobré si ji přečíst a považovat nad možnými důsledky nainstalování dialeru, zejména ekonomickými. Jeho odstranění totiž může, ale také nemusí být jednoduché.

Pokud používáte Internet Explorer, máte možnost měnit úroveň zabezpečení, ve většině případů se nachází na kartě Zabezpečení v Možnostech sítě internet. Obáváte-li se o svou bezpečnost před dialery, nastavte prvky ActiveX a plug-iny tak, aby se systém vždy před jejich instalací dotazoval, a to bez ohledu na to, zda se jedná o podepsané či nepodepsané prvky. Vyspělejší uživatelé také mohou uvažovat o nastavení aktivního skriptování. Čím více restriktivnější nastavení zvolíte, tím více riskujete, že se omezí funkčnost některých standardně používaných aplikací, jako jsou například elektronická bankovnictví (zvláště to v podání Komerční banky je na změny nastavení aktivního skriptování poměrně náchylné), administrační webové aplikace a podobně. Na druhou stranu ovšem bezpečnost vašeho systému stoupne o něco více směrem nahoru.

Telefonické připojení sítě lze chránit jednoduchým a především bezplatným řešením české společnosti Sodat. Jmenuje se *OptimAccess Dial* a můžete si je stáhnout ze stránek *www.optimaccess.cz*. Jednoduchá aplikace zablokuje telefonické připojení proti možnosti změnit jeho konfiguraci neoprávněnému uživateli nebo procesu. Toto řešení je zajímavou a účinnou metodou, jak se vyhnout dialerům, které mění standardní systémová nastavení. Pokud ovšem fungují jako samostatné programy komunikující s modemem, nepomůže.

▲ Dialery nabízí na internetu spousta firem (např. www.tibsystems.com)

▲ Nástroje pro odstraňování spywaru, jako například Spybot – Search and Destroy, dokáží vyhledat a neutralizovat nainstalované dialery (security.kolla.de)

Nástroje pro odstraňování spywaru, jako například skvělý Spybot – Search and Destroy, o kterém jsme již psali, dokáží najít a neutralizovat nainstalované dialery. Problém je v tom, že když máme něco neutralizovat, musíme tím být již nakaženi. Spybot je vybaven také preventivní částí, dokáže aktivně blokovat škodlivé plug-iny včetně dialerů, ovšem pouze ty, které zná. Proto je riskantní se na něj zcela spolehnout a doufat, že nás skutečně zcela ochrání.

Určitou prevencí před dialery je použití alternativního webového prohlížeče, například Mozilly *(www.mozilla.org)* nebo Opery *(www.opera.com)*. Jednak jsou optimalizovány na to, aby fungovaly z prostředí Internet Exploreru, který je majoritní, existuje pro to ale ještě jeden důvod. Konkurenční prohlížeče nejsou tlačeny stavem, kdy výrobce softwaru co nejvíce napomáhá komerci na webu i za cenu jistého omezení možností uživatelů.

Významnou prevencí je nenavštěvovat místa, kde se dialery vyskytují. Některé erotické servery, nebo také stránky obsahující odkazy na cracky, jsou známy tím, že se uživatele intenzivně pokoušejí zmást. Otevírají mnoho dalších oken prohlížeče o různých rozměrech, s různým nastavením, s různým obsahem. Při zavírání těchto oken se otevírají další, a tak je velmi jednoduché splést se a odsouhlasit nainstalování něčeho, co nechceme. Pokud se již na takové stránky z jakéhokoliv důvodu chcete podívat, pokuste se s nimi pracovat opatrně a spíše pomaleji, je tak snadnější všimnout si podezřelých hlášení prohlížeče nebo dokonce operačního systému.

Obecnou prevencí u moderních Windows (NT,2000,XP) je pracovat z jiného než z administrátorského účtu. Vytvořte si jednoho relativně omezeného uživatele a po internetu surfujte z něj. Plné možnosti administrátora přeci nepotřebujete tak často.

CO S DIALEREM?

Pokud máte podezření, že došlo k nechtěné instalaci adult dialeru do vašeho počítače, pokuste se jednat klidně. Odpojte se od internetu a vypněte modem. Máte-li interní a objeví se vám okno pro připojení k síti, stornujte jej. Pomocí aplikace pro odstraňování spywaru proveďte testování na přítomnost škodlivých modulů. Většina dialerů, například od *www.directplugin.com,* by měla být šťastně nalezena a eliminována. Pokud tomu tak není, můžete vyzkoušet i kombinaci více odstraňovačů.

Nemáte-li program pro mazání spywaru, podívejte se, zda nainstalovaný dialer nezanechal stopy v ovládacím panelu *Přidat nebo odebrat software*. Některé, ty slušnější, tak lze odinstalovat snadno a pohodlně. Jiné typy si vytvářejí položky v startovacím menu, nebo dokonce otevírají rezidentní ikony v systémové oblasti. V nich bývá funkce pro odstranění nebo vypnutí. Pokud je dialer přítomen v paměti, lze zjistit jeho fyzické umístění a odtud jej vymazat.

Dalším krokem je zjištění, v jakém stavu se nachází telefonické připojení sítě. Je dobré mít svá nastavení zálohována v souborech. Pokud nějaká aplikace změní telefonní číslo nebo jiné parametry stávajícího spojení, stačí je vymazat a obnovit ze zálohy. Dialer ovšem může, pokud je rezidentní, nastavení připojení monitorovat a v případě navrácení do původního stavu je změnit zpět. Proto by měl být samozřejmě nejdříve odstraněn.

Jaké jsou možnosti obrany před podvodem?

- Telefonní účet se zřejmě zaplatit musí
- Sdružení na obranu spotřebitelů
- Policie, trestní oznámení na původce dialeru

CO S PENĚZI?

Měli jsme dialer, byl nalezen, až když přišel telefonní účet na nesmyslně vysokou částku. Dialer byl odstraněn, telefonní účet nám ale zůstal. Nemá smysl útočit na Telecom, protože ten za to nemůže. Pokud instalaci dialeru předcházelo licenční ujednání, nebo důsledné upozornění, nemůžete udělat nic, a účet stejně budete muset zaplatit. Přestože dnes již Telecom upozorňuje před použitím čísla se speciální tarifikací a dokonce varuje zákazníky; pokud dojde k podezřelé činnosti na jejich lince, absolutní ochrana neexistuje. Skutečně podvodné dialery monitoruje Sdružení obrany spotřebitelů. Bližší informace o něm i o jeho aktivitách lze najít na stránkách *www.900.spotrebitele.info/*. Po napadení podvodným dialerem lze podat trestní oznámení na neznámého pachatele. Telekomunikační společnosti totiž nerady dávají k dispozici kontakty na své zákazníky, kteří vlastní čísla 900xxx. To je pochopitelně další problém, nicméně se zdá, že i ony mají poslední dobou tendenci spolupracovat.

Obtížným je určit, co je a co není podvodný dialer. Nakolik musí jeho provozovatel informovat uživatele o činnosti instalovaného softwaru, aby nešlo o podvod. Tato hranice je poměrně tenká, vždy lze vymyslet mnoho fíglů, které umožní uživatele zároveň informovat, a současně jej přesvědčit o instalaci plug-inu. Podobné to je ostatně i s dialery, které se mohou šířit elektronickou poštou, respektive být stahovány díky odkazům v ní.

Na počátku a na konci každého problému je člověk. Veškerá technika je ve skutečnosti jen nástrojem, a i podvodné dialery jsou vlastně jen bitvou mezi vychytralým podnikatelem na jedné straně a ignorujícím uživatelem na straně druhé. Pokud nezanedbáte prevenci a budete si všímat, na co klikáte, nebezpečí vám nehrozí. V opačném případě platíte za vlastní hloupost. 3 0323/FEL ❑