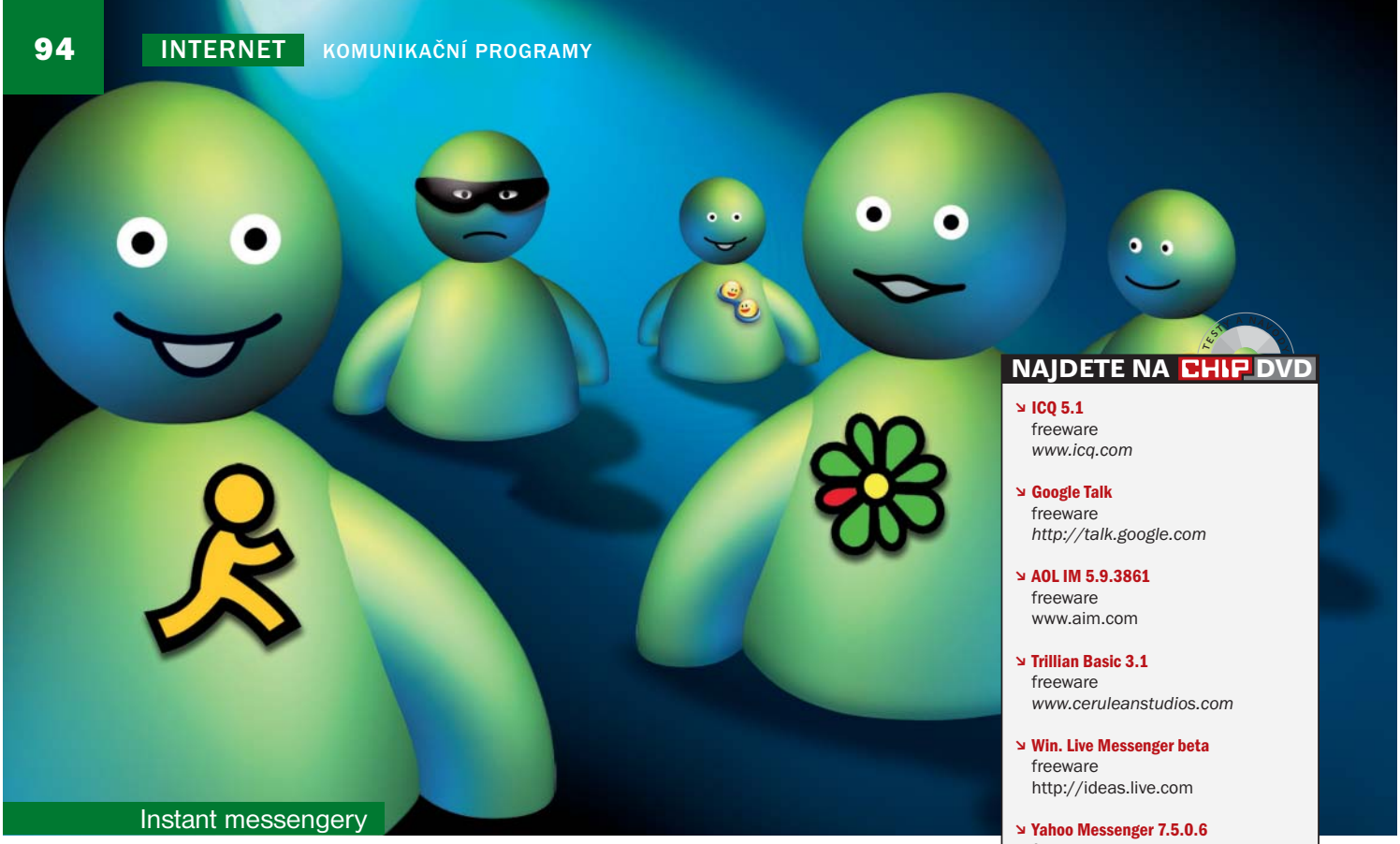


Instant messengery

NAJDETE NA CHIP DVD

- **ICQ 5.1**
  freeware
  www.icq.com
- **Google Talk**
  freeware
  http://talk.google.com
- **AOL IM 5.9.3861**
  freeware
  www.aim.com
- **Trillian Basic 3.1**
  freeware
  www.ceruleanstudios.com
- **Win. Live Messenger beta**
  freeware
  http://ideas.live.com
- **Yahoo Messenger 7.5.0.6**
  freeware
  www.yahoo.com

ICQ & spol.: Hrozba i pro Windows

„Chataři“ vedou nebezpečný život. Po elektronické poště a webových prohlížečích si teď hackeři vzali na mušku rychlé komunikační programy. Jak dokonale nás ICQ a spol. chrání před viry, krádežemi hesel a spywarem?

Text: Valentin Pletzer, *autor@chip.cz*

„Haha, našel jsem vaši fotku.“ Kdo se při obdržení této chatové zprávy neubrání zvědavosti a klikne na připojený odkaz, namísto údajného obrázku si do počítače stáhne červa „I-Worm.NewPic“. Ten pak jako klasická zadní vrátka (backdoor) otevře hackerům volný vstup do počítače, zaznamená osobní údaje oběti a pošle je na adresu útočníka.

Internetová mafie si teď jako novou cílovou skupinu vybrala „chatující“ uživatele a své záškodnické programy šíří prostřednictvím instant messengerů. Počet útoků na chatovací programy se podle studie FaceTime Security Labs během jednoho roku zvýšil na dvacetinásobek. Nejoblíbenějším cílem je toho času MSN Messenger od Microsoftu, ale pod palbu se postupně dostávají i AOL, ICQ a Yahoo. Fatální přitom je, že téměř 50 % všech „chatařů“ používá messengery i na firemním pracovišti, čímž „narušují“ firewall a maří tak i sebelepší ochranu.

Chip proto šest instant messengerů podrobil důkladnému bezpečnostnímu testu – včetně zbrusu nových beta verzí od Microsoftu a Yahoo. Naše testovací účty jsme bombardovali infikovanými odkazy, prolamovali jsme firewall a „napichovali“ probíhající konverzace. Výsledek byl naprosto tristní – v komunikačních programech její bezpečnostní mezery „jako vrata“. Zvláště alarmující je, že žádný z testovaných messengerů nemá vhodná bezpečnostní opatření pro děti.

Přečtěte si, jaké prostředky internetová mafie používá a jak se lze proti nejhorším nebezpečím bránit. ➔

V TOMTO ČLÁNKU NAJDETE

ZÁVĚRY Z TESTU

Málokdy dopadne tolik programů v jednom testu tak špatně. Dokonce i vítěz testu, Live Messenger od Microsoftu, v bezpečnostní zkoušce neuspěl ve dvou důležitých bodech. Jak test ukázal, chatovací nástroje v roli vstupní brány pro hackery přivedou každý firewall k zoufalství. Dokud se výrobci nepolepší, máme pro vás jediné doporučení: Tam, kde jde o zachování firemního tajemství, od instant messengerů ruce pryč! Soukromí uživatelé se musí ochránit sami a naučit se žít se „zbytkovým“ rizikem.

SLABÉ MÍSTO: ČLOVĚK

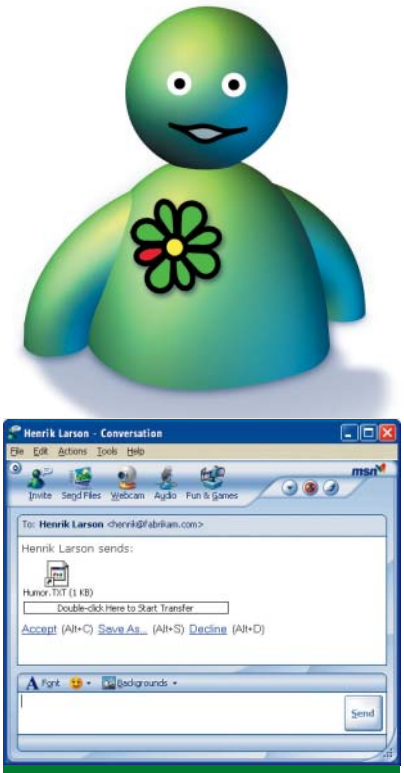
Phishing a spyware obléhají chatující uživatele

Hackeři zneužívají důvěřivosti „chatařů“ k šíření trojských koní nebo k vypátrání utajených hesel. Většina útoků spočívá v rozesílání krátkých zpráv obsahujících nějaký internetový odkaz. Zpráva předstírá, že „přilinkovaným“ souborem je nějaká fotografie nebo video. Pokud na něj adresát klikne, nenápadný program deaktivuje veškerý bezpečnostní software. Od té chvíle má hacker volný přístup do počítače a může si z něj stáhnout vše, co se mu zdá zajímavé. Poté jsou otevřena „zadní vrátka“ a napadený počítač začne být zneužíván jako základna pro další útoky.

Postup je v podstatě stejný jako u phishingových mailů, které lákají na podvrženou webovou stránku, na níž má pak oběť vyzradit informace týkající se jejího on-line bankovnictví. Že se phishing a spyware už dlouho neomezují jenom na elektronickou poštu, to nejnověji potvrdil červ „Maniccum“, který měl spadeno na uživatele AOL a MSN.

Nebezpečí: Tady nic nezmůže ani dobře míněná rada, že se nemají otevírat žádné soubory neznámého původu. Červi totiž především využívají seznamy kontaktů uložené v napadených počítačích – a tak výzva, abyste si prohlédli nějakou fotku, vám pak přijde od známého či kolegy. Nejnověji se objevují dokonce červi, kteří fingují účastníky chatu a dokáží i jednoduchými větami odpovídat na otázky.

Co pomáhá: Poněvadž žádný nástroj neposkytuje účinný spamový a phisihingový filtr, nejdůležitějším bezpečnostním pravidlem je neotvírat žádné odkazy, které dostanete v chatu. Pokud po příslušném souboru neodbytně toužíte, měli byste si alespoň zjistit, zda na druhém konci „drátu“ vůbec sedí živý člověk. Pošlete mu otázku formulovanou tak, aby ji pro tento účel naprogramovaný červ nemohl zodpovědět nějakou standardní floskulí. Většině českých uživatelů také při rozlišování potenciálního nebezpečí pomůže to, že většina „zákeřných zpráv“ je v angličtině. Základní ochranu poskytují také aktuální antivirové programy nebo internetové bezpečnostní balíky.



PHISHING: Odkazy a názvy souborů jako „Humor.txt“ mají důvěřivé uživatele přimět k nainstalování spywaru.

SOFTWAROVÉ NEDOSTATKY

Chyby v komunikačních programech otevírají hackerům dveře dokořán

Obecně platí, že každý program, který vytváří spojení „do internetu“, představuje bezpečnostní riziko. Že byly instant messengery až dosud napadány poměrně zřídka, není dáno jejich zvláštním zabezpečením, ale způsobem, jakým spolu komunikují: většina klientů nevytváří přímé vzájemné propojení. Mnohem častěji probíhají rozpravy přes poskytovatele chatu, kteří dokáží většinu útoků centrálně odfiltrovat.

Aby hacker mohl přes internet zaútočit, potřebuje znát bezpečnostní díru, ke které má přístup. V případě chatovacího programu je to rozhraní, jímž procházejí síťové pakety. Typický scénář zde využívá přetečení bufferu při zpracování těchto paketů: hacker vyšle paket, který napadený počítač špatně interpretuje a spustí například trojského koně.

Nebezpečí: Polovina testovaných messengerů nemá aktualizační funkci – a přitom vykazují závažné bezpečnostní mezery. Jak tyto problémy vypadají, to prozrazují četné webové stránky, na nichž hackeři nabízejí své „nádobíčko“. Jím často dokážou zhroutit nejen messenger, ale s ním i celá Windows. Pro „script kiddies“ jsou takové útoky většinou příliš náročné, zkušený hacker však nějakou cestu vždy najde.

PŘEHLEDNĚ: BEZPEČNOSTNÍ ZÁSADY

Pozor na odkazy a přílohy
Nikdy neotvírejte soubor od někoho, koho neznáte. A přijde-li zpráva od vašeho známého, přiložený soubor nebo odkaz otvírejte až po zpětném kontrolním dotazu.

Nahrávejte aktualizace
Ačkoliv se k vám spyware a trojské koně vtírají přes messenger, stále využívají známé bezpečnostní mezery v operačním systému. Udržujte proto v nejnovějším stavu nejen chatovacího klienta, ale i Windows.

Aktivujte firewall a virový skener
Bez aktivního firewallu nabízíte hackerům k využití pár bezpečnostních děr navíc. Váš počítač samozřejmě chrání také často aktualizované antivirové programy.

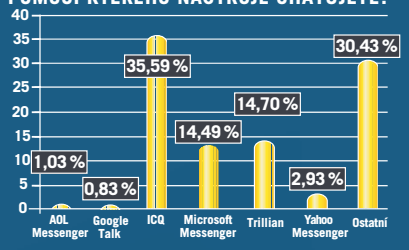
Nenechte se odposlouchávat
Každá rozprava, kterou vedete, může být zaznamenána. Proto byste své diskuse měli dobře zašifrovat – například nástrojem Simp Lite.

JAK JSME TESTOVALI MESENGERY

Kladné body jsme udělovali za phishingový filtr, dětskou ochranu, aktualizační a šifrovací funkci. Pozitivně také hodnotíme, je-li možné blokovat účastníky a rozumí-li si messenger s firewallem a virovým skenerem.

TRŽNÍ PODÍLY

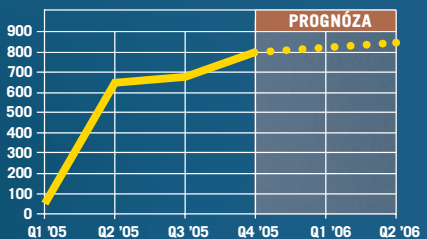
POMOCÍ KTERÉHO NÁSTROJE CHATUJETE?



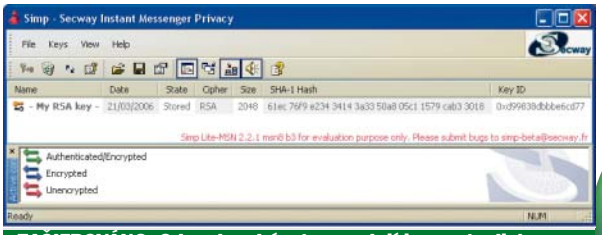
Čtenáři Chipu používají různé chatovací programy. Nejoblíbenější je ICQ.

PROGNÓZA OHROŽENÍ

ÚTOKY NA MESSENGERY



Od začátku roku 2005 napadení rapidně přibývá, tendence stoupající.



ZAŠIFROVÁNO: Odposlouchávat se nedají jenom ty diskuse, které jsou zašifrovány – například nástrojem Simp.

Co pomáhá: Svůj komunikační program stále udržujte v nejnovějším stavu. Některé programy naštěstí umožňují automatický update, a především tyto programy byste měli používat. Například „Live Messenger" od Microsoftu je pravidelně aktualizován společně s Windows. Jiné nástroje, jako AOL nebo Trillian, mají vlastní aktualizační funkci. Kdo chatuje prostřednictvím Yahoo, Googlu nebo ICQ, musí se čas od času postarat o novou verzi sám. Tyto programy aktualizaci neumožňují, což je u chatovacích nástrojů nepochybná slabina.

CHYBĚJÍCÍ KONTROLA

Dítě terčem v chatovací síti

„Postupují velice jemně a dokáží si získat důvěru dětí," tak popisuje chování pedofilů na internetu Jörg Pecanic z poradny pro dětskou pornografii při dolnosaském Zemském kriminálním úřadu (LKA). Vzdor opakovaným výzvám expertů neobsahují běžné chatovací programy žádné ochranné mechanismy, třeba nadřazené heslo pro nastavení v setupu. Například ICQ sice umožňuje blokovat neznámé kontakty a jejich navazování, ale pro dnešní děti odkojené počítačem není žádný problém příslušné zaškrtnutí zrušit. V otázce ochrany dětí však beznadějně propadly i ostatní instant messengery.

Nebezpečí: U žádného z testovaných programů se neobjevil ani náznak toho, že by se výrobce snažil o nějaké řešení. Mnohem více se poskytovatelé snaží uniknout z problému pomocí zvláštní klauzule: dětem mladším než 12, případně 13 roků je prakticky u všech providerů obecně zakázán přístup. A poskytovatelé si také vyhrazují právo přístup okamžitě zablokovat.

To ovšem neznamená, že by děti nemohly zakládat chatovací konta. Redakci je známo několik případů, že děti pod 12 let chatují bez jakéhokoliv omezení. A ani při našich zkouškách jsme žádné překážky neobjevili. Pokud není například zadáno datum narození, nemá poskytovatel žádnou šanci zjistit skutečný věk. Co zde naprosto chybí, jsou kontrolní rutiny, které by znemožnily zadává-

	1	2	3	4	5	6
Produkt	**Live Messenger**	**AIM**	**Trillian Basic**	**ICQ 5**	**Google Talk**	**Yahoo Messenger**
Dodavatel	Microsoft	AOL	Cerulean Studios	ICQ	Google	Yahoo
Freeware / financován z reklamy	adware	freeware (vlastní reklama)	freeware	adware	freeware (vlastní reklama)	adware
Internet	*http://ideas.live.com*	*www.aim.com*	*www.cerulean-studios.com*	*www.icq.com*	*http://talk.google.com*	*www.yahoo.com*
Bezpečnostní test						
Hodnocení zabezpečení	74 bodů ■■■□□	67 bodů ■■■□□	67 bodů ■■■□□	61 bodů ■■■□□	48 bodů ■■□□□	47 bodů ■■□□□
Phishingový filtr	• (jen filtr odkazů)	–	–	•	–	–
Blokování účastníků	•	• (varování a blokování)	•	•	•	–
Autorizace nových účastníků	•	•	•	•	•	• (ignorování)
Automatická aktualizace	• (přes Windows Update)	•	•	–	–	–
Ochrana dětí	–	–	–	–	–	–
Zašifrování chatu	–	–	–	–	–	–
Deaktivace záznamu (logu)	•	•	–	•	na serveru Google	–
Podpora firewallu	Socks/Proxy	Socks/Proxy	jen Proxy	Socks/Proxy	jen Proxy	Socks/Proxy
Jiné prostředky						
Podpora VoIP	jen USA u MCI	vlastní přímé spojení	vlastní přímé spojení	vlastní přímé spojení	vlastní přímé spojení	přes Yahoo Voice
Videochat	•	•	jen ve verzi Pro	•	–	•
Themes	jen pozadí a ikony	•	•	•	–	•
Konferenční chat	–	–	•	•	–	•
Rozesílání souborů	jedna složka na účastníka	společná složka, přímé rozesílání	společná složka, přímé rozesílání	společná složka, přímé rozesílání	–	přímé rozesílání
Podpora e-mailu	jen Live/Hotmail	AIM.com a POP3	jen ve verzi Pro	–	jen Google Mail	jen Yahoo Mail
SMS	•	–	–	•	–	–
Další speciality	služby jako hry, MTV	služby jako burzovní zprávy, mapy měst	jen ve verzi Pro	služby jako hry, seznamka	–	služby jako hry, aktuální zprávy

ní falešných osobních údajů – například kontrola průkazu.

Co pomůže: Rodiče by své děti měli poučit o nebezpečích při chatování a stanovit jim jasná pravidla. To nejdůležitější zní: Dítě se nikdy se známostí navázanou v chatu nesmí setkat osobně! Hlavně nezkušeným dětem či mladistvým se při chatování rovnou dívejte přes rameno – jen tak můžete v případě potřeby zasáhnout.

POSKYTOVATELÉ RIZIKA

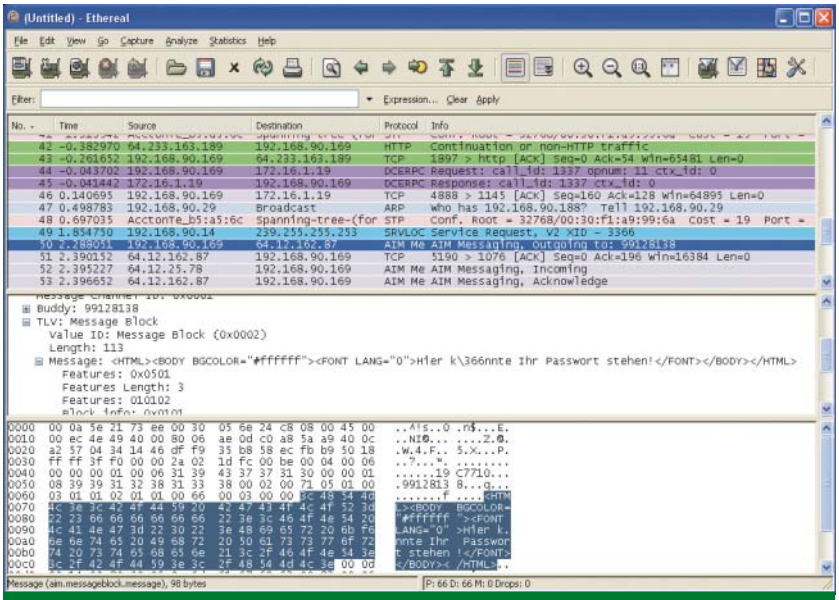
Cizí lidé znají vaše tajemství

Málokdo si uvědomuje, že technicky není pro messengerové poskytovatele žádný problém vaše konverzace odposlouchávat. V podmínkách pro používání ICQ je dokonce výslovně stanoveno, že pracovníci poskytovatele smějí chat souběžně číst. A navíc – každá informace posílaná po síti může být i zveřejněna. Přeloženo do češtiny to znamená, že „ICQ Inc. je oprávněna transportovaný materiál ... používat ..., včetně uveřejnění".

Nebezpečí: Ať používáte kterýkoli z chatovacích programů, přenos dat mezi účastníky není šifrován. A ke všemu je pak ještě vaše diskuse uložena – ve tvaru pro každého čitelném. Odposlech vaší komunikace je však snadný nejen pro provozovatele sítí, ale také pro hackery. Klasickými místy napadení jsou veřejné hotspoty, neboť k odposlechu rozhovoru je nutno splnit jeden předpoklad: útočník musí mít možnost vklínit se někde v síti mezi dva chatující účastníky. Útok „napříč" internetem není možný. Pokud se však hacker i jeho oběť nacházejí v téže síti, může útočník pomocí nástrojů jako „Ethereal" nebo „Cain&Abel" protokolovat všechna data a vybírat z nich zajímavé informace, například konverzaci, hesla nebo adresy.

Co pomůže: Jedinou obranou je zašifrovat chat a protokoly diskusí „vlastnoručně". Ale nejjednodušší cestou, jak uchránit log soubory před zvědavými pohledy, je vůbec je nezakládat. Vypnutí protokolování konverzace umožňují všechny programy zastoupené v našem testu.

V této souvislosti zaslouží pochvalu Microsoft, AOL a ICQ, u jejichž produktů je nutno protokolování nejprve zapnout. Dokud tak neučiníte, jsou vaše „chat-logy" v bezpečí. U ostatních messengerů musíte příslušné nastavení provést v setupu, jinak se založí nezašifrovaný protokol. Jinou překážku klade hackerům Google Talk. V něm jsou totiž, není-li definováno jinak, všechny rozpravy ukládány v Gmail účtu na serveru. Znamená to, že k chatovacím protokolům se hacker nedostane ani v případě, že se „naboural" do PC uživatele.



HACKER ÚTOČÍ: Programy jako Ethereal usnadňují hackerům odposlech konverzace na síti.

Chcete-li vzdor uvedeným bezpečnostním rizikům své diskuse ukládat, doporučujeme použít k tomuto účelu šifrovací nástroj (například opensourcový TrueCrypt). Ten umožňuje zřídit zašifrovanou „jednotku" a messenger nainstalovat na ni. Pak ovšem musíte pokaždé, když zapnete počítač a chcete chatovat, tuto jednotku otevřít pomocí hesla.

To ale ještě není všechno: Vaše konverzace je sice zabezpečena na lokálním počítači, ale cesta po internetu ještě bezpečná není. Chcete-li odstranit i tento problém, budete potřebovat přídavný modul nebo nějaký program, který zašifruje datový proud, například „Simp Lite". Po vytvoření silného kryptografického klíče jako v PGP běží vše bez vašeho dalšího přičinění. Běžné chatovací klienty překonfiguruje nástroj samočinně; messengery, které Simp Lite nezná, musíte nastavit sami.

SOFTWAROVÍ DIVERZANTI

Trojské koně maskované jako komunikační programy

Ze všech nejdříve to „potrefilo" blízkého příbuzného chatovacích programů – VoIP software Skype. Už dávno bezpečnostní experti varovali, že trojské koně a „boty" se mohou maskovat jako programy pro chatování nebo pro „Voice over IP". A na jejich slova došlo. Bot „MyTob" tuto myšlenku nakonec uskutečnil.

Nebezpečí: Záškodník po napadení počítače vytvoří spojení k hackerovi, přičemž předstírá, že datový proud v síti je chatovací diskuse. Firewall pak domněle neškodná data bez překážek propustí do internetu.

Co pomůže: Drastická rada bezpečnostních expertů je strohá: zakázat chatování. Pokud bude administrátor blokovat chatovací datový provoz skutečně jakéhokoliv druhu, bude síť samozřejmě v bezpečí. Takové opatření se však dá realizovat jenom ve firmách. Pokud se chatování nechcete vzdát, měli byste jeho datový proud alespoň nechat probíhat přes proxy nebo firewall zajištěný heslem. Pokud se ovšem „trojanovi" jednou podaří dostat se k datovému proudu, ani heslo nebude nic platné.

Nejlepší ochranu poskytují i zde bezpečnostní softwarové balíky s firewally a virovými skenery – ovšem jen tehdy, jsou-li tyto programy v nejnovějších verzích. Je-li trojský kůň příliš čerstvý a vychytralý, i tato ochrana selže. Symantec už ohlásil speciální „Security Suite" pro instant messengery. V Chipu jej samozřejmě co nejdříve otestujeme a i nadále vás o útocích na chatovací nástroje budeme průběžně informovat. ■ ■ ■