Trojské koně pro Apple

Vložil/a el tenedor del ... [1], 16 Září, 2005 - 16:19

- Apple [2]
- Cracking [3]
- Hacking [4]
- Mac OS [5]

Navzdory tomu, že zejména státní správa a školství v naší republice nesmyslně protlačuje technologie úzce vázané na proprietární software společnosti Microsoft, v některých oblastech si svoje postavení drží i jiné platformy. Některé jsou u nás známé nebo používané méně než ve světě (RiscOS, IRIX, ...), jiné se u nás v poslední době prosazují více. A k těm patří i stroje firmy Apple. Ať už svého Maca máte nebo ne, ať už je máte rádi nebo ne, dávám vám teď možnost dozvědět se něco o trojských koních, o jejichž existenci vím a dají se sehnat.

V době, kdy typický domácí počítač měl několik tlačítek a sedmisegmentovku nebo řadu LEDek, přišel Apple s jednodeskovým počítačem, který komunikoval s uživatelem pomocí klávesnice a obrazovky, jak bylo tehdy zvykem na "velkých" počítačích. O rok později vznikl počítač se zvukem a barevnou grafikou, jehož architekturu ne zrovna zdařile okopírovalo IBM do svého PC. Tato firma v počítači Lisa jako první použila grafické uživatelské prostředí, převzaté ze sázecích strojů Xeroxu. Úspěch Macintoshe nemá cenu zdůrazňovat, snad jen v souvislosti se zavedením 3,5" mechanik a dalších technologií. O tom, že dnes v srdci těchto strojů bije UNiX, se nemá smysl rozepisovat, to udělali jiní (třeba článek na Rootu - Mac OS X je taky UNiX, root.cz [6]). V dobách starších systémů (OS 7-9) využívala PowerMacintoshe jako servery pro jejich praktickou nehacknutelnost americká armáda a i dnes používá servery od Applu, i když často ve spojení s jinými operačními systémy (OS X je koncipován především pro workstation).

Pochopitelně i na Macu žije malá hackerská komunita - malá proto, že většina těchto strojů je v držení profesionálů v oblasti grafiky a multimédií. To, plus ještě fakt, že tyto počítače dosud nepoužívají nepodařené procesory od Intelu, nýbrž kódově nekompatibilní PPC, je zatím dělá viruprostými - je jen málo lidí, kteří umí virus napsat a zároveň mají důvod či potřebu to opravdu udělat, a viry pracující s procesory x86 nejsou na Applu spustitelné (pokud nejde o interpretované skripty).

Hlavní předností těchto strojů, vedle jejich antivirově výhodné nekompatibility, je jejich kompatibilita, hlavně v datových formátech - kromě výhod UNiXu mají i většinu výhod Windows. MS Office pro Mac jsou lepší než na Windows, Windows Media Player, real Player a podobné sračky pro Mac taky existují, i když na druhou stranu zrovna Office, WMP a Real jsou vedle nového software od Adobe jedny z nejhorších programů na této platformě.

Ať už svého Maca máte nebo ne, ať už je máte rádi nebo ne, dávám vám teď možnost dozvědět se něco o trojských koních, o jejichž existenci vím a dají se sehnat. Chápu, že jde o informaci, která může zvýšit potenciální ohrožení, ale na druhou stranu může pomoci majitelům Maců i nemaců v obraně proti případné infekci, kterou často antivirové a antispywarové programy nejsou schopné odhalit. To má svůj důvod - některé z těchto programů jsou utility pro vzdálenou správu počítače a není žádoucí, aby antiviry bránily jejich instalaci. Pokud jsou ale instalovány proti vůli majitele, je dobré, aby měl možnost se o existenci těchto danajských darů a potenciálním ohrožení dozvědět, například z tohoto článku.

Rozdělme si trojské koně do několika kategorií

Podle systému - spustitelný kód klienta je určen buď pro starý systém (OS 7-9) bez UNiXového

jádra, nebo OS X s UNiXovým jádrem, u některých programů dokonce pro oba.

Dále podle crossplatfomnosti

1) existuje macovský klient k serveru, který běží na jiné platformě (ať už je specifický, takže k němu neexistuje neexistuje na hostitelské platformě klient, nebo jde jen o port klienta rozšířeného na cizí platformě pro Mac).
2) klient i server existují pouze pro Apple
3) server je určený pro Mac, klienty jsou dostupné nejen pro něj, ale i na jiných platformách
4) pro Mac existuje port nejen klienta, ale i serveru z jiné platformy
Podle funce - ve svém archivu si trojany rozděluju podle hlavního určení - na keyloggery a na takeover utility.

Pokud je mi známo, existují všechny tyto kombinace.
Takže do toho, začneme s keyloggery. Pro jistotu budu uvádět u programů verze, ve které se ke mně dostaly (některé existují i ve více verzích).

Na starém systému je oblíbený Oasis, KeyNabber 3.9, MacLife Insurance 2.0, Peeping Tom 1.4, SuperSave 1.1.2 a TextTrap. Na systémech s Carbonem funguje i KeyTrack určený pro OS X.

Pro OS X je určen KeyTrack, Carbon Keys 1.2 a Keystroke Recorder X 3.3.1.
Ne všechny keyloggery mají klasickou strukturu klient/server, některé prostě ukládají záznam do souboru a přístup si k němu zjednejte, jak chcete - což není problém, pokud chcete monitorovat aktivitu ostatních uživatelů, kteří mají přístup k vašemu počítači, na vzdálený počítač je dobré zajistit si přístup k logům nasdílením nebo pomocí dalšího trojana.

InvisibleOasis

je standardní "neviditelný" keylogger pro staré systémy, který je ke stažení přímo v podobě instalátoru. Výstup ukládá do souborů označených datem. Nemá samostatného klienta.
KeyNabber 3.9 je funkčně obdobný, rovněž pro staré systémy, jeho kód je odvozen z MacLife Insurance. Výstup ukládá do neviditelného souboru, což znesnadní jeho detekci, ale komplikuje to trochu přístup k němu..

MacLife Insurance 2.0

je celý balík zajímavých utilit, které mají zpříjemnit práci s počítačem - obsahuje FileSaver, který v pravidelných intervalech ukládá soubory i v aplikacích, které tuto funkci standardně neobsahují, čímž chrání data pro případ pádu systému. EyeSaver místo dat chrání samotného uživatele - monitoruje jeho aktivitu a doporučuje mu nejvhodnější dobu na přestávku v práci. MouseSaver mapuje "myšoidní" akce, jako je vysypání koše, zapnutí a vypnutí sdílení, a podobně, včetně těch, které si sami přidáte, na klávesovou zkratku. A pochopitelně je součástí balíku i KeySaver, který má rovněž bránit ztrátám napsaných dat. Pracuje jako ostatní keyloggery, navíc umožňuje nastavit, v kterých aplikacích se stištěné klávesy mají nebo nemají zaznamenávat.

Peeping Tom 1.4

kromě záznamu stištěných kláves, v němž umí vynechávat klávesové zkratky a dokonce i vymazávat smazané znaky, ukládá informace o spouštěných procesech - jak dlouho byl proces spuštěn, kolik žral procesorového času, dokonce si údaje o době spuštění porovnává se systémovým časem, aby zjistil, zda ho některý uživatel nevypíná.

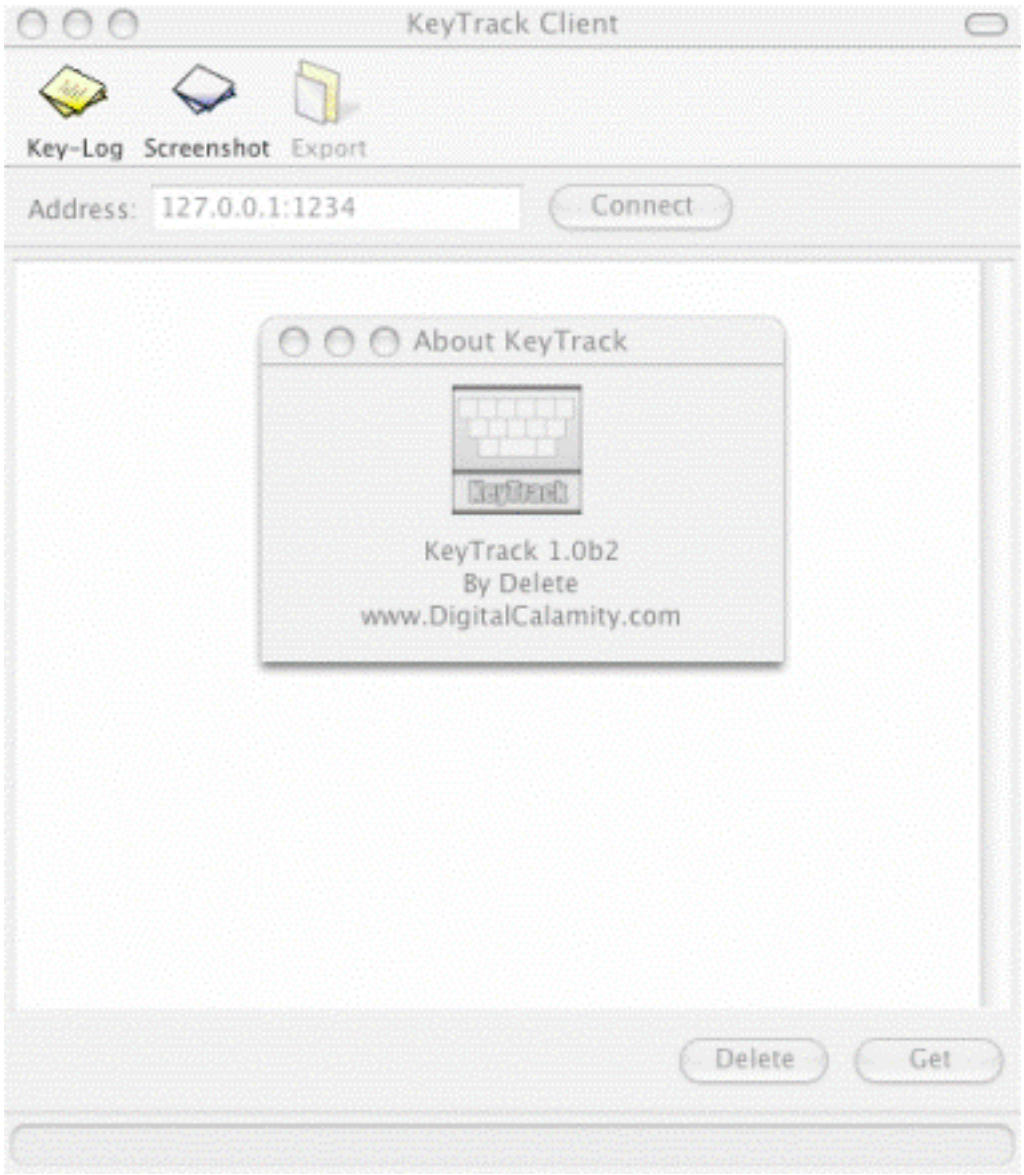
TextTrap

naopak není keylogger, zaznamenává výstupy na obrazovku, je možné zvolit si ze čtyř systémových funkcí pro výstup textu. Tímto způsobem můžete získat kompletní ICQ rozhovory nebo textové obsahy souborů, se kterými uživatel pracoval.

Podle mne nejsou právě popsané programy příliš zajímavé a navíc jsou podobné miliónům dalších. Podíváme se tedy na ty o něco zajímavější, se vzdáleným síťovým přístupem.

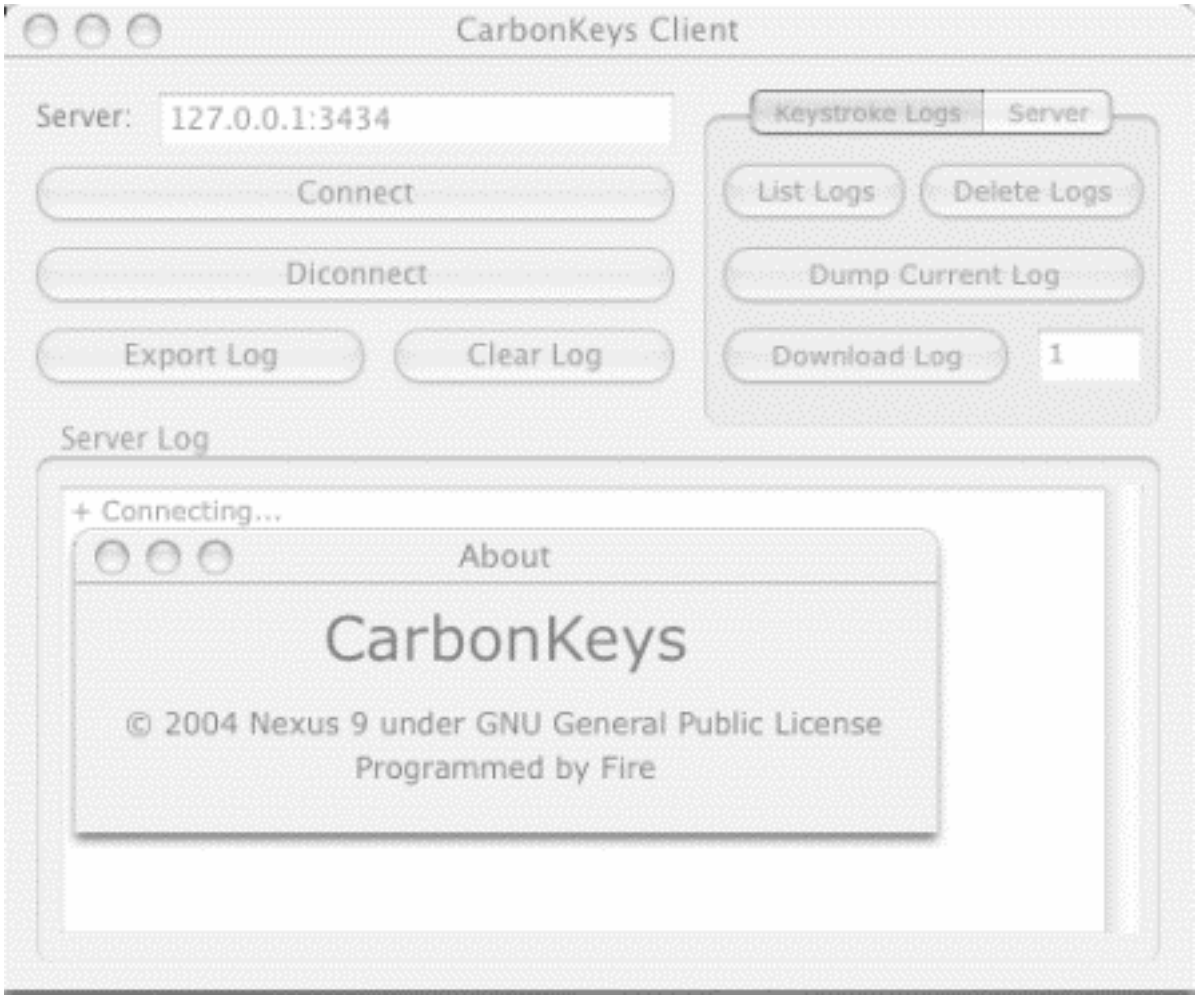
KeyTrack

je primárně určen pro OS X, je ale spustitelný i na starších systémech s knihovnou pro Carbon. Je rozdělen na server a klient, přičemž klient obsahuje i server editor. Kromě logu o stištěných klávesách vám umožňuje získat z počítače oběti i screenshot. Navíc si můžete nastavit posílání logů či screenshotů na svůj e-mail. To se hodí hlavně v případě, že počítač oběti nemá veřejnou IP nebo se účinně chrání firewallem.



CarbonKeys 1.2

je ještě hackerštější a zajímavější, protože je u něj přiložen i zdroják (RB) a popis protokolu - není tedy problém napsat si klienta i pro jinou platformu, nebo naopak vytvořit jinoplatformní server. I on obsahuje v klientu i server editor, který ovšem pracuje vzdálené.



Keystroke Recorder X 3.3.1

je sice komerční (29 $), ale docela vydařený produkt. Je takřka neviditelný - samozřejmě se neobjevuje v doku, ale ani ve ForceQuit menu a není snadno vysledovatelný ani z UNiXové řádky příkazem PS. Má oddělený server a editor. Logy kromě ukládání do souboru umí posílat e-mailem, takže nepotřebuje klienta, ve verzi 3.3.1 umí posílat logy v zakryptované podobě a posílat i screenshoty (případně je pakovat gzipem), takže máte přehled, co uživatel typicky dělá a občas si přečetete i zajímavé texty.

takeover trojany

.
Vynechal bych **VNC**, i když i to se dá použít pro snadné vzdálené ovládání nebo sledování činnosti oběti, ta si totiž zejména ve Windows často vůbec nevšimne, že se VNC spustilo a antiviry jsou zticha, na Macu je ovšem spuštěný VNC server mnohem více nápadný. (v této souvislosti si dovoluji upozornit na ScriptDaemon pro staré systémy bez příkazové řádky, který umožní přes telnet ovládat počítač pomocí příkazů AppleScriptu, a běží skrytě na pozadí).
Nevýhodou VNC je posílání bitmap, výhodou naopak crossplatformnost, je jedno, jste-li připojeni k widlím, UNiXu, nebo někam jinam.

Mnohem lepší a uniíverzálnější je

Timbuktu

, umožňující například i sdílení souborů, přenos grafické informace má mnohem rychlejší, než VNC,

existuje ovšem jen pro Windows a Maca, na jiné platformy vytvářeno není, a navíc jde o komerční produkt. Je ovšem psané velmi čistě, alespoň na Macu, nedělá problémy a pro vzdálené ovládání se opravdu hodí.

Apple Remote Desktop

taky vlastně není trojan. Serverovou část ARD má každý počítač s MacOS X už zabudovanou, klientská část ARD se prodává, dostupná je i jako součást Mac OS X Server. Ačkoliv je totiž Mac OS X UNiX, a umí spouštět programy používající X11, už jeho předchůdce NeXT Step používal jinou technologii. X11 rozkládá informace o GUI do formy, vhodné pro síťovou komunikaci, a pak je zase skládá dohromady, což je v síti výhoda, ale na workstationu je to zbytečné. NeXT Step proto pro popis obrazu používal PostScript, kromě jiného tím bylo dosaženo plného WYSIWYGu (ten samý PostScript se posílal na obrazovku i na tiskárnu). Rozhraní X11 a NeXT Stepu s vektorovým popisem patří mezi GUI 2. generace, zatímco bitmapová Windows se až do verze xp pohybují v první generaci GUI. OS X je opět o krok dál, 3. generace GUI používá pro popis obrazové informace technologii založenou na PDF s popisy ploch, stínů a přechodů. Vzdálenou práci s touto plochou potom právě Apple Remote Desktop umožňuje.
Pokud si říkáte, že něco podobného existuje i pro Windows - ano, je to microsoftí Remote Desktop Connection. Klient pro OS X existuje a dokonce je ke stažení ze stránek Microsoftu zadarmo. Tím máte umožněno vzdálené ovládání počítačů s Windows, která RDC podporují.

Remote Mouse&Keys

taky není přímo trojan, ale ovládací panel pro stroje se starými systémy, který umožní ovládat jednoho Macintoshe z jiného, který má instalovaný ten samý ovládací panel (slouží jak jako klient, tak jako server). Ovládaný stroj ale musí mít povolené sdílení programů, tedy Remote Apple Events, což není příliš bezpečné, i když ho lze povolit jen pro vybraného uživatele a zaheslovat. Navíc neposkytuje žádný obrazový feedback. Přišel mi ale docela zábavný, tak ho uvádím.

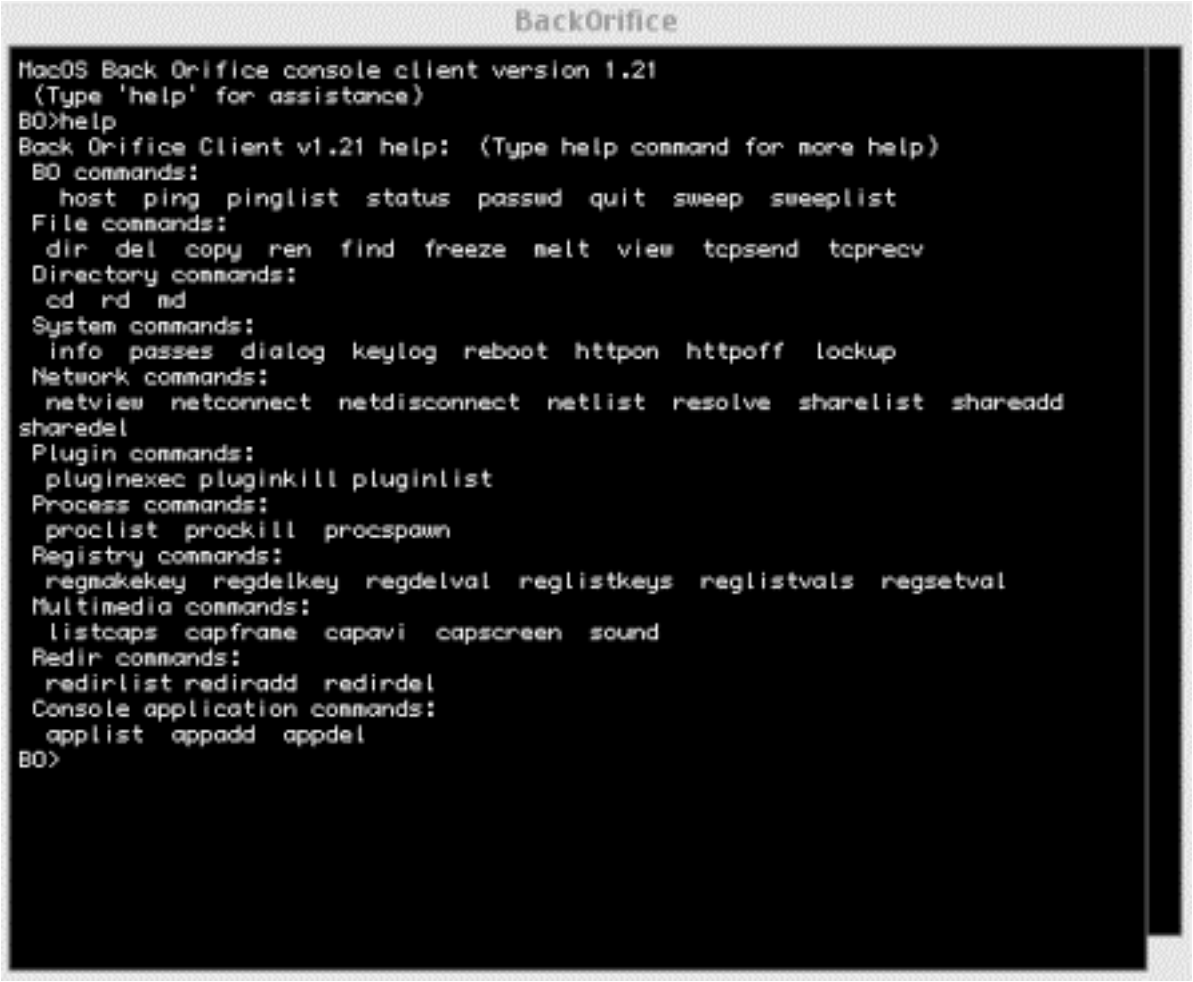
Takže ke skutečnějším trojanům, pro starší systémy jsou určeny MacBackOrificePPC, Mac NetBus 1.0 a 1.7, Sub7serverME a Sub7, pro OS X potom Sub7, WinJack, Xover 1.0 a 1.1, HellRaiser 2.5b a Termite.

Nejprve ty pro starší systémy:

MacBackOrificePPC

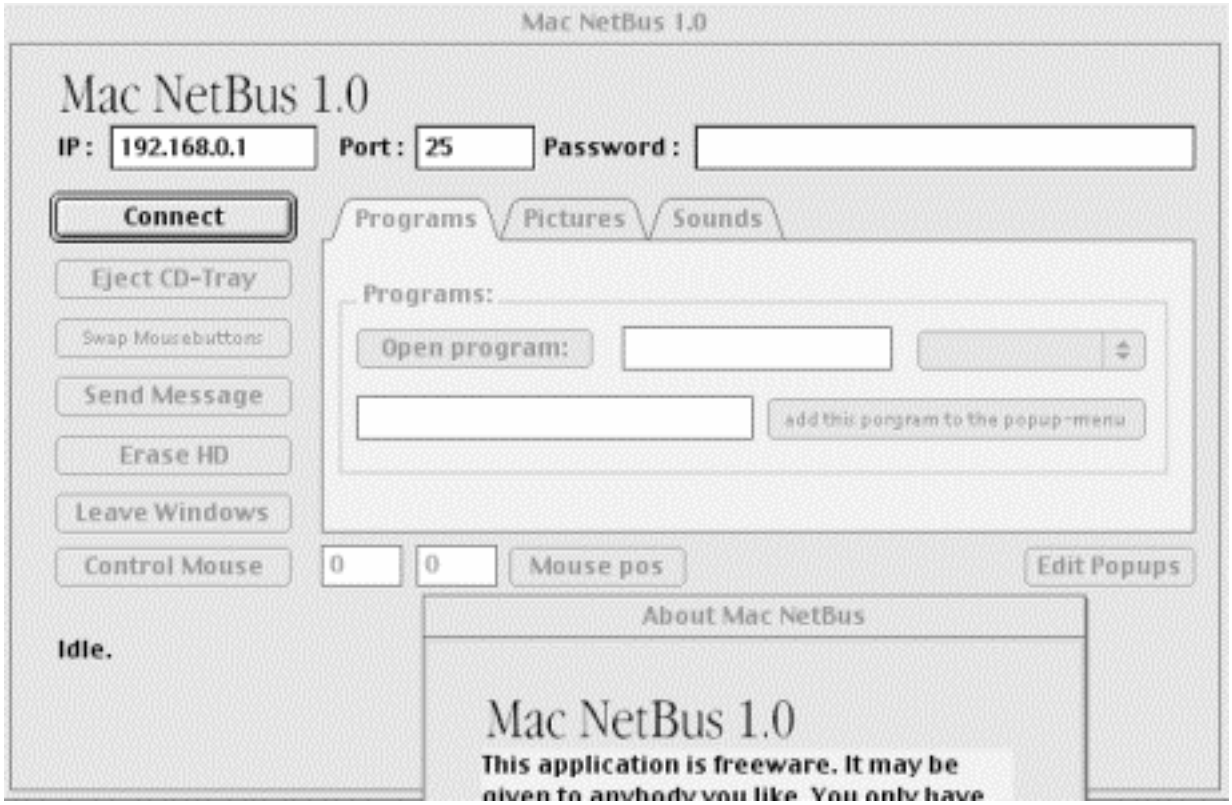
- název hovoří za vše. Jde o jednoduchého klienta ke klasickému windowsovému trojanu Back Orifice. Tento klient ale nemá GUI, ovládá se pomocí command line. Není to zrovna pohodlný způsob, ale pro vyzkoušení nebo skalním nadšencům vystačí. Podporuje všechny funkce serveru.

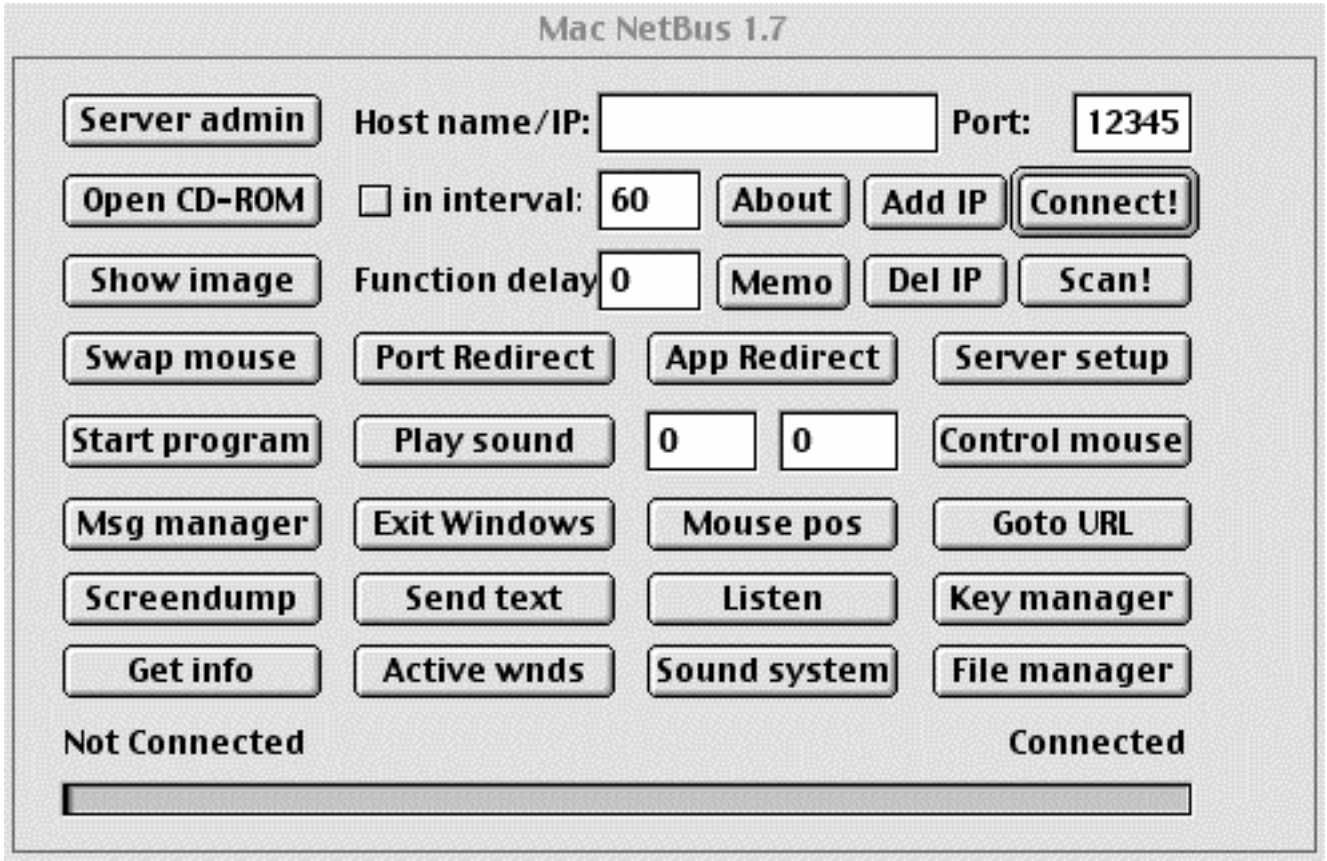
CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn



Mac NetBus

je opět klient ke známému windowsovému trojanu. Dostupný je ve verzích 1.0, která nemá zabudovány všechny funkce, a v kompletní verzi 1.7. Ovládá se mnohem příjemněji než MacBackOrificePPC.





Sub7

je ještě zajímavější, existuje k němu totiž klient jak pro starý systém, tak pro OS X (a systémy s knihovnou Carbon). A aby toho nebylo málo, pro starý systém (ne ale pro OS X) byl přeportován i server, podporující většinu funkcí obsažených ve verzi trojanu pro Windows (není podporována například informace o volném místu na disku, chat je jen jednosměrný, do Matrixu není možné psát

vlastní texty a chybí keylogger). Pro nastavení parametrů serveru je přiložen i Server Editor, při nastavování ale musí být jak editor, tak editovaný server na ploše. Navíc, jak BackOrifice a NetBus, tak i Sub7 jsou stařičké a profláklé programy, při zkoušení Sub7serverME se ozval i jindy mlčenlivý Virex a laskavě mne upozorňoval na infekci Sub7serverem - zatím jediná hláška, kterou jsem na stroji Apple zažil.

A teď k těm novějším: Sub7 client, který jsem už jmenoval, existuje i pro OS X.

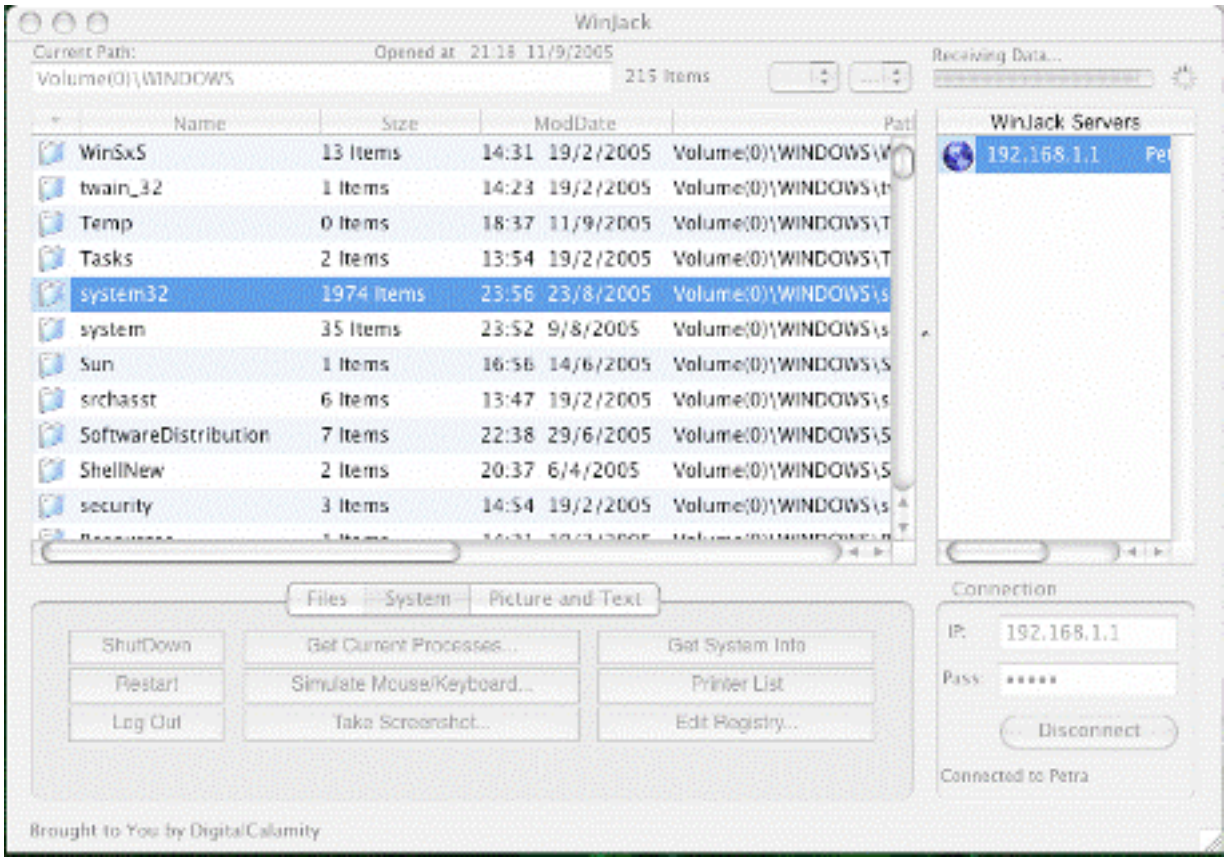


Můj oblíbenec se jmenuje

WinJack

. Klient je určen pro OS X, server pro Windows. Jde o program trochu staršího data, takže nejlépe chodí s Windows s DOS jádrem (95, 98, ...), ale s jistými omezeními ho uchodíte i na Windows s NT jádrem (2000, xp). O jaká omezení jde? Pod xp nefunguje spolehlivě installer, který má do serverové části zapsat údaje o jménu uživatele a heslu. Protože se údaje ukládají do neviditelného textového souboru, přihlašovací jméno můžete vepsat ručně, ale hashované heslo se vám tak snadno vepsat nepodaří. Většina funkcí jde normálně, potíž dělá jen ovládání myši (NT Windows mají potíž s údaji o souřadnicích) a některé destruktivní funkce - pokus o násilné vypnutí počítače "pouze" odhlásí uživatele, pokus o pouhé odhlášení neprovede nic. Výhodou tohoto trojana jsou nejenom klasické možnosti získat screenshot (v různých rozlišeních) nebo spouštět a ovládat programy, ale má i docela pěkné sdílení souborů, prochází i výměnné disky, potíže mi dělal jen při kopírování

šestisetmegového filmu. Velkou výhodou tohoto programu je to, že se vám klient může ohlašovat na vaši pevnou IP, takže pokud má dynamickou IP, máte přehled o aktuálním stavu, navíc nabízí správu více serverů, víte tak, kdy je která z vašich obětí aktivní, a umožňuje i proscanování určitého rozsahu IP adres s vyhledáním instalovaných serverů. Za jeho velkou výhodu považuju fakt, že jej antiviry a spyware removery nechávají na pokoji - díky tomuto odpornému ksindlu, který se na Windows (z pochopitelných důvodů) čím dál tím víc rozmáhá, jsem nemohl ani experimentovat se staršími trojany (BackOrifice, NetBus, Sub7), VirusScan prostě nebyl ochoten je nechat na pokoji.

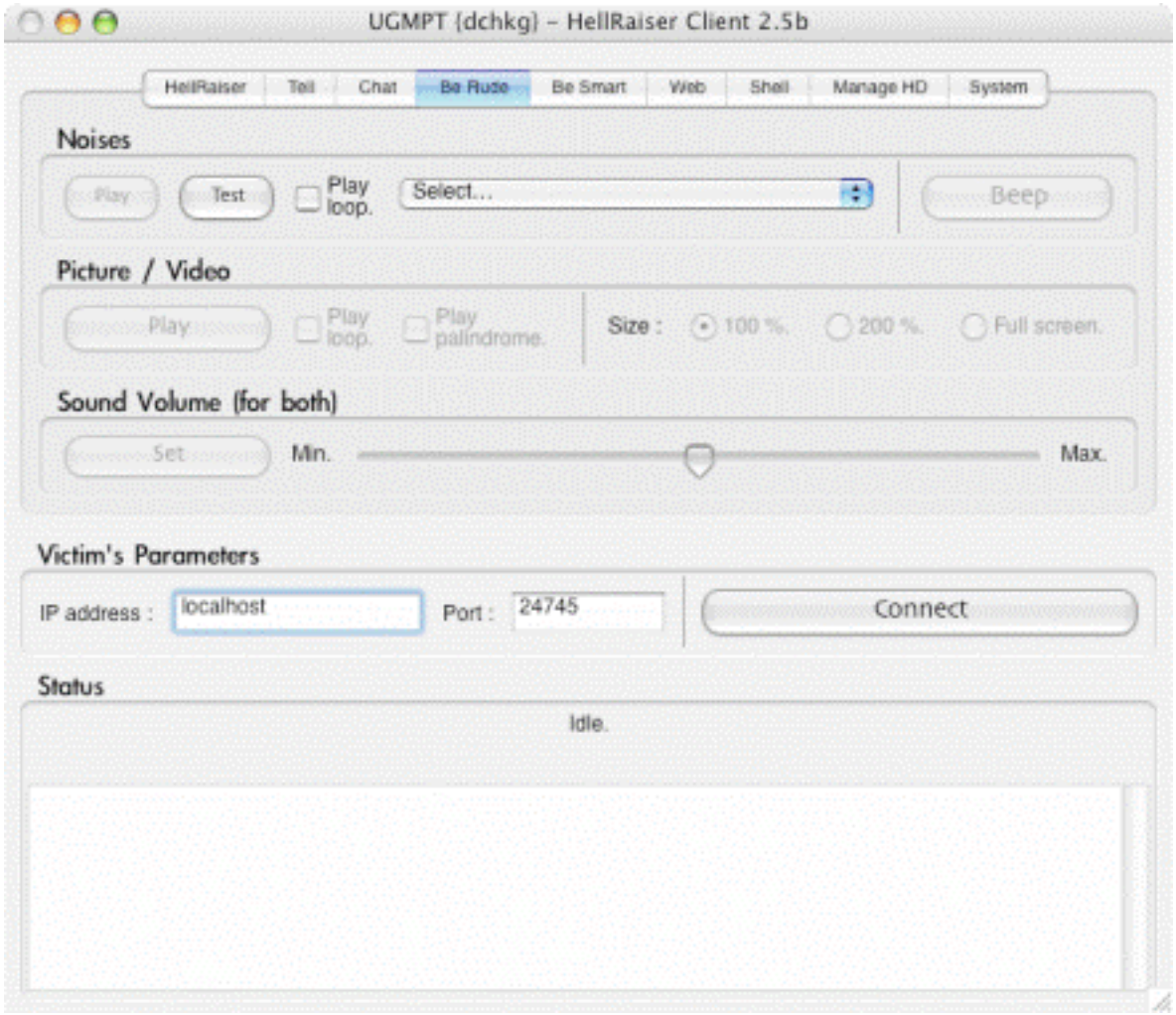


Xover

je trojan, jehož klient i server existují pouze pro OS X. Ve verzi 1.0 se mi nepodařilo ho spustit, zřejmě chodí jen pod určitou starší verzí OS X (nejspíš 10.1 nebo 10.2). Není to ale příliš velká škoda, moc toho neumí, jen vypínat, restartovat či uspávat počítač a stahovat screenshot. Verze 1.1 sice funguje i na novějších systémech, ale těžko ji označit za trojan, když na sebe dost okatě upozorňuje - nejen, že se zobrazuje normálně v doku, ale dokonce zobrazuje okno se stavem serveru, které lze sice skrýt, ale po novém startu se opět zobrazuje.

HellRaiser 2.5b

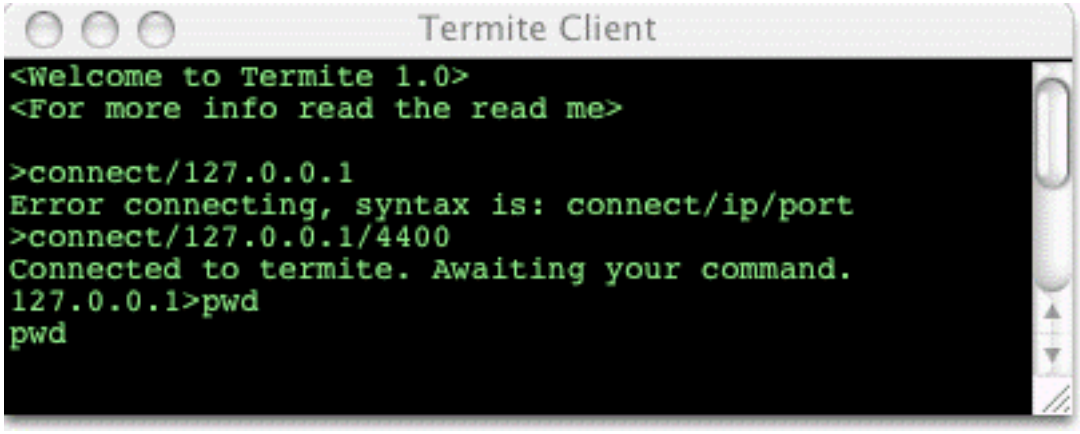
je trochu méně vážný - sice se dá použít k relativně solidní práci se soubory, aplikacemi, obrazovkou, shellem, ale jeho hlavní těžiště spočívá v opravdové jízdě do pekla - můžete počítač oběti donutit zobrazovat nebo říkat (Macy mají zabudované kvalitní reproduktory a SpeechManager je součástí systému už přes deset let) nejrůznější texty, vyluzovat strašidelné zvuky nebo přehrávat mnohohlasou polyfonii, k dispozici je i chat, kde si oběť může se svým satanem promluvit. Na týrání slabších jedinců jako dělané. Program se skládá z klienta, serveru a editoru, v němž si můžete, pokud má oběť dynamickou IP adresu, nastavit posílání její aktuální IP na e-mail. Server se nikam neinstaluje, jenom se skrytě spouští, užitečné je umístit ho do Startup Items. Je docela šikovný, to, že já ho nepoužívám, je dáno spíš tím, že ho nepotřebu - počítačů s Windows, které lze ovládat, se nabízí mnohem víc, než Maců, které navíc mají mnohem důslednější ochranu.



Z hlediska opravdových hackerů, tedy těch, co si nehrají s utilitkami typu "click me to hack", bude mnohem zajímavější

Termite

. Název je odvozen od terminálu, tedy okna, v němž se obvykle objevuje UNiXový shell. Termite totiž poskytuje vzdálené ovládání shellu, podobně jako SSH nebo telnet. Ovládá se, podobně jako MacBackOrificePPC, spartánsky pomocí command line. Skládá se ze serveru (pro OS X), server editoru a klienta (pro OS X, starší Mac OS a Windows). Sám o sobě tooho vlastně moc neumí, takže jako bonus má zabudovaný port scanner, na rozdíl od SSH a podobných ale umožňuje přístup shellu s právy uživatele, který má server spuštěný, bez znalosti jeho loginu a hesla. Představte si tedy, že se podaří spustit Termite administrátorovi nebo že poběží s rootovskými právy. Obyčejní lidé to nejspíš nedokážou zúročit, ale milovník UNiXového shellu to jistě ocení.



To by mohlo zatím stačit, doufám, že jste po přečtení článku opět o něco moudřejší a že jako moudří lidé víte, že dělat někomu naschvály se prostě nedělá - programy, které jsem vyjmenoval, najdou často i velmi užitečné uplatnění a ačkoliv se u mnoha z nich uvádí, že nejsou vhodné pro vzdálenou administraci, už mockrát se mi v této velmi seriózní úloze osvědčily.

URL článku: https://security-portal.cz/clanky/trojsk%C3%A9-kon%C4%9B-pro-apple

Odkazy:
[1] https://security-portal.cz/users/el-tenedor-del-diablo
[2] https://security-portal.cz/category/tagy/apple
[3] https://security-portal.cz/category/tagy/cracking
[4] https://security-portal.cz/category/tagy/hacking
[5] https://security-portal.cz/category/tagy/mac-os
[6] http://www.root.cz/serialy/mac-os-x-je-taky-unix/?SID=7EFDD01420B4DFEA329DA8994F0C18B1

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn