James Bond ve vašich službách

V současném světě se informace cení. Jedni se snaží své informace ochránit, jiní se je naopak pokouší získat, a to nejrůznějšími způsoby. Jedním z nich je používání speciálních programů, tzv. klávesnicových špionů.

Zajímá vás, co se děje s vaším počítačem během vaší nepřítomnosti? Určitě ho používají vaši kolegové, příbuzní, známí a kamarádi. Ale vysledovat, kdo a čím se konkrétně zabývá, je pro vás téměř nemožné. Klávesnicoví špioni ale nejsou potřeba pouze proto, abyste mohli někoho sledovat. Zadáváte-li do počítače nějaké důležité textové informace a máte strach, aby nebyly porušeny, budete se cítit jistější, budete-li vědět, že se ukládají ještě někde a že v případě, kdy bude kvůli vaší nebo cizí neopatrnosti odstraněn důležitý soubor, nebude těžké obnovit jeho obsah.

Nad těmito problémy se zamýšleli mnozí programátoři po celém světě. Vytvořili "klávesnicové špiony" - speciální utility, které jsou schopné vést podrobnou statistiku práce počítače, to znamená ukládat sledy zmáčknutých kláves nebo dělat kopie obrazovky (screenshoty). Tyto programy si také mohou pamatovat všechny navštívené internetové servery, všechny aplikace spuštěné během práce na počítači a mnoho dalších údajů. Na internetu je možné najít mnoho podobných nástrojů, ale většina z nich nepracuje ve skrytém režimu, vytváří přehledy, ve kterých se velmi těžko orientuje atd. Po pečlivém výběru jsme se tedy rozhodli uvést pouze šest utilit. Všechny mají podobné možnosti a funkce, ale liší se různými doplňkovými zvláštnostmi a každý program má nějakou "třešničku na dortu".

Perfect Keylogger

Jako prvního zástupce této skupiny programů vám představujeme Perfect Keylogger. Je to výborný program pro monitorování práce na tu počítači, který sleduje prakticky veškerou činnost uživatele. Perfect Keylogger nabízí dva typy instalace: obyčejnou, při které se instalují všechny komponenty, nebo skrytou, při které se instaluje pouze špionský modul. Během instalace je také možné vybrat název procesu, který se bude objevovat v seznamu úloh (defaultně se nabízí bpk, ale je možné zvolit libovolné slovo podle přání). Program obsahuje úplnou sadu všech standardních funkcí. Je to záznam všech zmáčknutých kláves, kde se zároveň uvádí, ve kterých aplikacích byly použity, schopnost snímat kopii obrazovky v zadaném intervalu (na screenshotu je uvedeno jméno uživatele a systémový čas). Program je také schopen odesílat reporty e-mailem.

Nastavení Perfect Keyloggeru umožňují určit velikost logovacího souboru a také typ souboru reportu - v HTML nebo v zašifrovaném souboru .DAT, který může otevřít pouze prohlížeč Log Viewer, vestavěný do programu. Perfect Keylogger dokonce umožňuje přikládat k dopisu kopie obrazovky. Po odeslání e-mailem mohou být všechny reporty nevratně odstraněny. Utilita má ještě celou řadu užitečných možností: kontrolu nastavení pošty, možnost ukládání reportů na FTP server atd.

Co se týká nejzajímavějších voleb programu, můžeme se zmínit o vestavěném filtru umožňujícím vybrat aplikaci, kterou má Perfect Keylogger sledovat. To umožňuje značně zmenšit rozměr reportu a odfiltrovat nepotřebné smetí.

Ikonka programu na systémové liště je viditelná a schovává se pouze po zmáčknutí kombinace kláves "Ctrl+Alt+L". Přitom pro přístup k nastavením vyžaduje program heslo (samozřejmě pokud jste ho uvedli).

Perfect Keylogger je výborně vycvičený špion, který bedlivě pozoruje všechno, co se děje na vašem počítači. Pochopitelně plná verze programu je komerční, nicméně k dispozici je zcela zdarma Perfect Keylogger Lite, ve kterém sice chybí mnohé doplňkové funkce (například nelze schovat ikonku na liště), ovšem pro běžného uživatele zcela dostačuje.

Spytech SpyAgent

Jedná se nejspíše o nejlepší program ze všech, které jsou uvedeny v tomto přehledu, protože obsahuje prakticky všechny možnosti, které jen může klávesnicový špion mít. Design rozhraní je na nejvyšší úrovni, vše je jednoduché a pochopitelné. Průvodce nastavením pomůže i nováčkovi se během několika málo minut orientovat v programu. Povídání o všech funkcích tohoto programu by zcela jistě vydalo na celý článek, proto se zmíníme pouze o těch, které chybí v ostatních programech.

SpyAgent obsahuje výkonný systém filtrování, ve kterém je možné vybrat, kterého uživatele má sledovat a dobu, kdy má sledování probíhat. Obsahuje nejen filtraci podle aplikací, ale také podle prohlíženého obsahu WWW serverů. Umí také sledovat programy - instant messengery (ICQ, Yahoo

Messenger, MSN Messenger). Zapisují se všechna modemová spojení. Jako příjemný doplněk obsahuje SpyAgent utilitu pro kontrolu IP adres pomocí služby WHOIS.

V programu se také velmi pohodlně pracuje s reporty. SpyAgent umí ukládat a vytvářet reporty ve formátech TXT, HTML a XLS. Můžete si také zvolit, jaké reporty chcete dostávat e-mailem. Program umí i vyhledávat v archivech reportů.

Samozřejmě že kvůli velkému množství funkcí zabere nastavení určitý čas, ale vývojáři také umožnili uložení všech nastavení. To může ušetřit čas například při instalování programu na cizím počítači (po dobu nepřítomnosti uživatele tohoto počítače :-)).

PC Acme Pro

Výborná alternativa ke dvěma výše uvedeným utilitám. PC Acme Pro má vícejazyčné rozhraní, bohužel čeština chybí. Program samozřejmě neobsahuje tak velké množství funkcí (například chybí možnost snímání obsahu obrazovky), nicméně mezi jeho základní přednosti patří nejlépe organizovaná práce s reporty. Program vytváří úplný a velmi pohodlný HTML report, který obsahuje dokonce informace o kliknutích myší a o klíčích přidaných do systémových registrů různými aplikacemi. Do nejmenších detailů promyšlená filtrace také značně zmenšuje objem log souboru. Program je schopen analyzovat získané údaje ve třech režimech - ve zjednodušeném, standardním a v rozšířeném.

PC Acme Pro je schopen nejen odesílat reporty e-mailem, ale také je ukládat do přístupných zdrojů v lokální síti.

Jak jsme se již zmínili, program obsahuje vícejazyčné rozhraní, nápověda je pouze anglická.

IOpus STARR PC & InternetMonitor PRO

STARR PC obsahuje stejně jako ostatní představitelé daného přehledu standardní sadu funkcí, nicméně i zde jsou příjemné doplňkové možnosti. Program umí vytvářet reporty ve formátech HTML, TXT a XLS a dokáže také chránit soubor reportu heslem. Hotové reporty (mimochodem zapakované) mohou být také uloženy na lokální síti nebo odeslány e-mailem. Program při odesílání takové zprávy do pole Předmět pomocí speciálních funkcí vkládá název počítače, jméno uživatele a datum vytvoření reportu. Výborně to pomáhá při prohlížení velkého množství reportů, které přišly z různých počítačů. Program obsahuje pohodlný systém nastavení času odeslání a rozměrů souborů.

Při práci ve Windows 2000/XP se program spouští jako systémová služba a jeho název je možné v případě potřeby změnit.

Existuje také verze programu STARR PC & Internet Monitor Home, která neobsahuje možnost odesílání reportů elektronickou poštou a ukládání na lokální síti. Nicméně její cena je značně nižší než cena profesionální verze.

Windows Keylogger

Windows Keylogger je program se zvučným názvem, který se do našeho testu nedostal náhodou. Stejně jako všichni špioni se chrání heslem, obsahuje pohodlný plánovač úkolů, umí odesílat reporty e-mailem. Také má možnost kontrolovat nastavení pošty, dělat snímky obrazovky, ale jeho největší přednost spočívá v tom, že se může sám zničit. Tuto funkci neobsahuje žádný z výše uvedených klávesnicových špionů. Zřejmě kvůli tomu ho některé antivirové programy považují za trojského koně, i když žádné škodlivé následky jsme po jeho použití nezjistili.

Soubor reportu se ukládá pouze ve formátu TXT. Bohužel jakékoliv filtry pro sledování aplikací vývojáři neimplementovali a tím zkomplikovali úkol vyhledávání potřebných údajů v reportech.

Hook Dump

Program vytvořil ruský vývojář Ilja Osipov. Má poněkud asketické rozhraní a skromný soubor funkcí. Nicméně tento program je zcela zdarma. Základními prováděnými funkcemi jsou zápis všech zmáčknutých kláves a názvů oken, ve kterých došlo k aktivaci klávesy. Také se zaznamenávají všechna kliknutí levým a pravým tlačítkem myši.

Hook Dump může pracovat ve skrytém režimu a může se automaticky spouštět při startu systému. Nastavení programu se provádí editací konfiguračního souboru Hookdump.ini, který je umístěn v kořenovém adresáři programu.

Bohužel program Hook Dump je poněkud zastaralý a vývojář dávno neobnovoval a nepodporoval svůj výtvor (deklaruje jeho použití pouze pod Windows 3.1 a 95), nicméně Hook Dump se rozlezl po internetu a je k nalezení na mnohých souborových serverech po celém světě. Vesměs je to klasika tohoto žánru.

Bilance

Je těžké vybrat mezi uvedenými programy ten nejlepší. Všechny jsou svým způsobem dobré, každý si může najít svého uživatele. Nicméně podle množství funkcí je nejlepší SpyAgent, výbornou konkurencí je pro něj Perfect Keylogger. Právě tento program jsem si vyhlédl kvůli překrásné možnosti ukládání reportů na FTP. Vždyť po testovací instalaci během čtyřiadvaceti hodin všechny programy zcela naplnily poštovní schránku. K dobrým programům též patří PC Acme Pro, kvůli podrobným a pro čtení pohodlným reportům. A milovníkům softwaru zdarma mohu doporučit starý dobrý Hook Dump.

Maxim Naumenko

POPISOVANÉ PROGRAMY

PERFECT KEYLOGGER 1.4.7
Vývojář: Blazingtools Software
Server vývojáře: www.blazingtools.com
Podmínky šíření: shareware
Cena: 34,95 USD
Operační systém: Windows

SPYTECH SPYAGENT 4.32.02
Vývojář: Spytech Software and Design, Inc.
Server vývojáře: www.spytech-web.com
Podmínky šíření: shareware
Cena: 49,95 USD
Operační systém: Windows

PC ACME PRO 6.20
Vývojář: Raytown Corporation
Server vývojáře: www.keyloggers.com
Podmínky šíření: shareware
Cena: 189,95 USD
Operační systém: Windows

IOPUS STARR PC & INTERNET MONITOR PRO 3.27
Vývojář: Iopus Inc.
Server vývojáře: www.iopus.com
Podmínky šíření: shareware
Cena: 69,95 USD
Operační systém: Windows

WINDOWS KEYLOGGER 5.03
Vývojář: Christian Walter
Server vývojáře: www.littlesister.de
Podmínky šíření: shareware
Cena: 20 USD
Operační systém: Windows

HOOK DUMP 2.8
Vývojář: Ilja Osipov
Server vývojáře: www.ilya.nn.ru
Podmínky šíření: freeware
Operační systém: Windows

ANTI-KEYLOGGER
Vývojář: Raytown Corporation
Server vývojáře: www.anti-keyloggers.com
Podmínky šíření: shareware
Cena: 59,95 USD
Operační systém: Windows

KEYLOGGER KILLER V1.0
Vývojář: Tooto Technologies

Server vývojáře: www.tooto.com
Podmínky šíření: shareware
Cena: 29,95 USD
Operační systém: Windows

PROSTŘEDKY BOJE PROTI KLÁVESNICOVÝM ŠPIONŮM - KONTRAROZVĚDKA

Všichni dávno chápou, že tam, kde pracuje rozvědka, se vždy najde i kontrarozvědka. Dobrého špiona jen tak lehce neodhalíte, existují však protiopatření. Proto lidé, kteří předpokládají, že mají na svém počítači nainstalovaný program (klávesnicového špiona), jenž sleduje všechnu jejich činnost, mohou použít příslušný program pro jeho zjištění. Tyto programy pracují na obdobném principu jako antivirové programy pomocí heuristické analýzy. Kontrolují aktivní procesy v systému, a pokud zjistí, že některý z procesů kontroluje klávesnici, okamžitě to oznámí uživateli.

Povíme vám o dvou nejzajímavějších představitelích této třídy programů.

Anti-keylogger

Vývojáři tohoto programu, kteří mimochodem vytvořili i PC Acme Pro, tvrdí, že tento program pracuje pomocí vynalézavých matematických algoritmů a neobsahuje jakoukoliv databázi. Při prohledávání program nenašel pouze SpyAgent, PC Acme Pro a Perfect Keylogger. Ostatní špioni byli odhaleni okamžitě. Program má výborné a srozumitelné rozhraní. Má ale i své nedostatky: při spuštění programu se počítač, zvláště pak méně výkonný, začne hrozně loudat a mnohé aplikace začnou "zamrzat".

Keylogger Killer

Tento nevelký program zabírá všehovšudy 52 KB, ale se svým úkolem se dokáže vypořádat na výtečnou. Lehce odhalil všechny programy tohoto přehledu, kromě PC Acme Pro. Ale ani zde se to neobešlo bez kuriozit: mezi klávesnicové špiony byl zařazen i vcelku neškodný program - automatický přepínač různých rozložení klávesnic. I když to není těžké pochopit, protože pracuje na stejném principu - sleduje všechna stisknutí tlačítek.

Program obsahuje také funkce eliminování a obnovy špionských modulů, které se vyvolávají kliknutím pravým tlačítkem myši.