6. část

Počítačová „válka Roseových“

Slova stalking a spyware nejsme zvyklí vídat pospolu příliš často. Nový případ našeho vyšetřovacího týmu počítačové kriminality však oba pojmy svedl dohromady. *Valentin Pletzer, autor@chip.cz*

Je to takové, jako kdyby stále ještě měl klíč od mého bytu a chodil si tam číst mé maily,“ běduje Daniela R. Přibližně před měsícem se rozešla se svým tehdejším přítelem, 34letým počítačovým specialistou. Ten ji však brzy poté začal všemožně pronásledovat: neustále se ozývá a vyčítá jí vše, co udělala nebo řekla, a dokonce se i nečekaně objevuje při jejích schůzkách s kamarádkami. O těch by přitom vůbec neměl vědět, neboť termíny setkání si jejich účastnice domlouvají jenom e-mailem. Postupně tak vzplálo nepřátelství, ne nepodobné tomu ve filmu Válka Roseových, a Daniela R. se ocitla na pokraji duševních sil. Mladá žena už několikrát změnila všechna hesla ve svém PC, koupila si poslední verze antivirových a antispywarových programů, ale „stalkerský“ teror pokračuje.

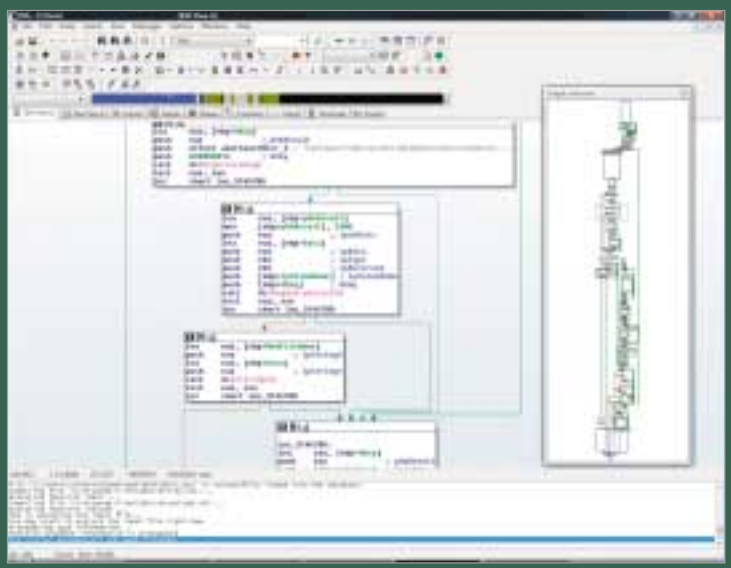
Když se obrátila na náš detektivní tým, dali jsme se ihned do práce. Nejprve kontrolujeme její počítač. Typický PC: operační systém Windows XP, programy Outlook Express, Internet Explorer a pro rychlou komunikaci instant messenger. K tomu příležitostně využívaný Word 2003, na pozadí běží virový skener. Aktualizace probíhají automaticky z internetu, takže se počítač zdá proti spywaru, trojským koňům a virům zabezpečen dostatečně. Zkoumáme proto nejprve síť – směrovač je však v pořádku a v konfiguraci žádné anomálie nevykazuje. A poněvadž je router s PC spojen kabelem, nepřipadá v úvahu ani odposlech přes WLAN. Výtky Daniely R. vůči jejímu expříteli se tak prozatím jeví spíše jako neodůvodněné.

Snímáme „otisky prstů“

Znovu se věnujeme počítači. Zde si v prvé řadě bereme pod lupu probíhající procesy. Zachytit všechny aktivní procesy nám pomáhá jednoduchý nástroj Process Explorer od firmy Sysinternals. Můžeme tak zjistit kontrolní součty každého aktivního programu a porovnat je s rozsáhlou databankou. V ní jsou tyto údaje obsaženy pro všechny známé soubory a programy – poněvadž přitom jde o jedinečné hodnoty, představují cosi jako „otisky prstů“. Počínaje systémovými soubory až po aplikace jako Nero nebo software od IBM. Procesy, jejichž kontrolní součty databanka neobsahuje, přijdou na separátní seznam. To nastane například tehdy, je-li program úplně neznámý nebo byl-li známý soubor modifikován.

Normálně by nás nyní čekala velmi únavná práce. Až dosud totiž bylo nutné analyzovat podezřelé procesy ručně. My však máme k dispozici prototyp nového analytického nástroje, v němž pracuje podobná heuristika jako ve virových skenerech. Činnost programů zde analyzují speciální algoritmy, které dokážou odhalit příbuznost se známými nástroji i v případech, že se ji hacker snaží zastřít. A profesionálové v řadách internetové mafie také samozřejmě dělají všechno možné, aby antivirové programy přelstili. Je tak poměrně běžné, že hackeři své útočné programy mění a modifikují tak dlouho, až je virový skener není schopen rozpoznat. Mohou to být

Rozpitvaný trojský kůň



SPECIÁLNÍ NÁSTROJE Programy jako disasembler IDA pomáhají vyšetřovatelům při analýze trojského koně a jeho obsahu.

Nový seriál Chipu

V americkém kriminálním seriálu o CSI objasňují vyšetřovatelé zločiny pomocí vědeckých metod. Chip si vzal „Kriminálku Las Vegas" za vzor pro novou řadu článků, která ukáže, jak profesionální vyšetřovatelé a specialisté bojují proti strmě narůstající počítačové kriminalitě.

menší změny programového kódu, ale také třeba komprimace souborů nějakým neznámým algoritmem. Základní způsob práce programu, pořadí jednotlivých funkcí atd. ovšem zůstávají stejné jako v původním špionážním nástroji – a právě to umí odhalit náš speciální program.

A opravdu, analytický program zabral. Oznamuje nám, že údajný plug-in pro instant messenger je něco úplně jiného, než za co se vydává. Vykazuje totiž zřetelnou podobnost s jistým „stavebnicovým" trojským koněm, jehož zdrojový kód je každému přístupný na internetu. Musíme tedy vycházet z toho, že zmíněný „pseudoplug-in" někdo vědomě do počítače nainstaloval. A je-li domněnka Daniely R. správná, pak to udělal její bývalý přítel krátce předtím, než jejich vztah definitivně ztroskotal. Poněvadž se komunikační program samočinně spouští při každém zapnutí počítače, mohl také maskovaný trojský kůň stále běžet, aniž by vzbudil pozornost.

Právě odhaleného trojského koně tedy začínáme podrobně zkoumat. Pomocí profesionálního disasembleru IDA od DataRescue převádíme strojový program do jazyka asembleru. V této podobě je kód trojského koně pro zkušeného profesionála čitelný téměř tak snadno jako originální zdrojový text programu. Díky tomu jsme schopni způsob činnosti vetřelce velmi přesně identifikovat. Jakkoli je náš poznatek překvapivý, samotný trojský kůň příliš inovativní není. Rozpoznáváme typické prvky, mezi nimi například keylogger, sejmutí obrazovky a další spywarové funkce. Autor tedy mnoho vynalézavosti neprojevil, pouze se bohatě „obsloužil" z nabídky existujících stavebních prvků.

Špionovi na stopě

A pak nacházíme rozhodující stopu: v textu programu objevujeme název domény! Největší část dálkově řízených trojských koňů a „botů" je zpravidla kontrolována prostřednictvím nějakého IRC serveru. Ty se k němu přihlašují jako chatovací programy a hacker tam zadává své příkazy. IRC příkazy ovšem mohou být identifikovány heuristickými metodami současných antivirových programů. Tomu, jak se zdá, chtěl náš hacker pokud možno zabránit. Jenomže to, že si jako svůj „velín" vybral právě webový server s doménou „cz", byla jeho kardinální chyba. Stačí totiž jednoduchý dotaz „whois", a už víme, kdo je útočníkem: skutečně je jím bývalý přítel naší zákaznice. Odstraňujeme trojského koně z počítače a Daniele R. doporučujeme, aby se se zjištěnými skutečnostmi obrátila na policii. K tomu jí dáváme do rukou naši kompletní dokumentaci. S těmito důkazy by mělo být snadné pohnat „stalkera" k právní odpovědnosti.

Obrana před novými útoky

Zatímco balíme své „nádobíčko", ptá se nás Daniela R., jak se má proti podobným napadením bránit v budoucnu. Můžeme jí však poradit jediné: s neznámými soubory a e-maily zacházet opatrně a pravidelně si stahovat aktualizace – vždyť přímý přístup k danému počítači už její „bývalý" nemá. Každá jiná možnost by laikovi práci na PC silně zkomplikovala. „Dokonalá ochrana neexistuje," řekl nám ostatně i antivirový expert Eugene Kaspersky, když jsme se ho zeptali na jeho názor. „Trend směřuje ke stále cílenějším útokům. A čím lépe je útočník připraven, tím vyšší má šanci na úspěch. Je to problém, který se však týká především firem."

Valentin Pletzer

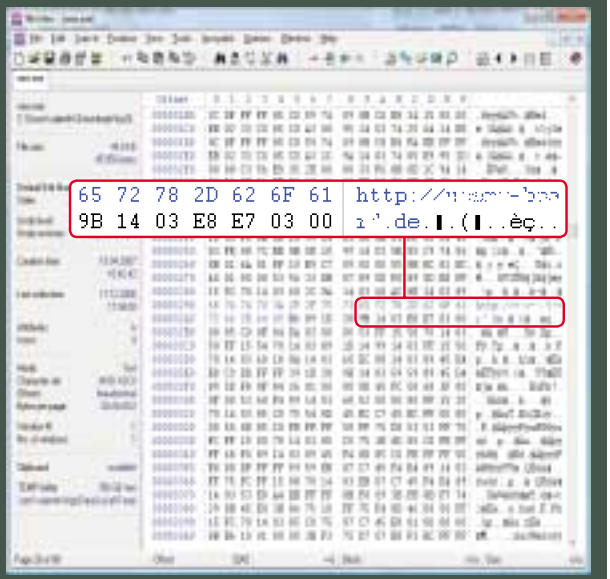
VÍCE INFORMACÍ

www.viruslist.com/weblog: Expertní blog firmy Kaspersky vypráví o zcela všedním malwarovém běsnění.

EXPERT

Eugene Kaspersky (41) je antivirový specialista a zakladatel firmy Kaspersky Labs. Stále častěji zaznamenává cílené útoky na jednotlivé osoby i firmy.

Důkaz



PŘÍMÁ STOPA **Jedno místo v kódu trojského koně navedlo tým CSI na přímou cestu k útočníkovi.**