CSI: Internet

2. část

Špion jako dárek

Tentokrát jsou vyšetřovatelé Chipu na stopě útočníkovi, který ke své záškodnické činnosti nepotřeboval bezpečnostní mezeru v softwaru. Hacker oběť obelstil úplně jinak. *Valentin Pletzer, autor@chip.cz*

Když virový skener vyhlásil poplach, bylo už pozdě. Časové razítko označeného trojského koně dokazuje, že škůdce „páchal" v počítači svou činnost už déle než dva týdny. Jak se do počítače dostal a proč virový strážce ohlásil přítomnost vetřelce až nyní, to si majetkový poradce Richard B. nedokáže vysvětlit. „Můj bezpečnostní software je v nejnovějším stavu," říká. „A tak naivní, abych otevíral každou e-mailovou přílohu, také nejsem." Výše škod není známa. Především proto, že virový skener neposkytl žádné přesnější údaje o druhu škodlivého softwaru. Proto se pan B. obrátil na „vyšetřovatelský tým" Chipu, aby se věci pokusil přijít na kloub. Po vzoru detektivů z oddělení CSI („Crime Scene Investigation") v televizním seriálu Kriminálka Las Vegas nejdříve pátráme na místě činu – v kanceláři finančního poradce.

Zajištění stop

Hned na začátku nás čeká těžká rána – s postiženým notebookem se stále ještě pracuje. Za těchto okolností je velmi pravděpodobné, že už zmizely důležité stopy; průkazné protokoly činností a dočasné soubory mezitím mohl hacker odstranit. Abychom zabránili dalším změnám, ze všeho nejdříve si pořizujeme image pevného disku. Pak analyzujeme inkriminovaného trojského koně, kterého pan B. naštěstí nevymazal, ale nechal ho virovým skenerem přesunout do „karantény".

Starý známý...

Brzy zjišťujeme, že škůdcem je modifikovaná verze „BackOrifice 2000". Tedy „starý známý", který se objevil už v roce 1998, ale dodnes nic neztratil na své atraktivitě pro hackery. Tento malware dokáží internetoví gangsteři přizpůsobit svým potřebám prostřednictvím zdrojového kódu, stavebnicového principu a pluginů jako Remote Desktop a Password Extractor. V našem případě hacker zredukoval nástroj jen na to nejnutnější – a dokonce i částečně přepsal zdrojový kód. Tím se změnila signatura malwaru, který se díky tomu dokázal celé dva týdny vyhýbat odhalení virovým skenerem. Za to, že antivirový nástroj přece jen zasáhl, vděčí pan B. jenom náhodě: jiná varianta trojského koně, která byla mezitím objevena, se původnímu vetřelci natolik podobá, že signatura souhlasila.

Abychom poznali, na co měl hacker spadeno, musíme vypátrat, jaké funkce trojský kůň provádí. Nakonec zjišťujeme, že nástroj přijímá jeden jediný povel – ale ten opravdu stojí za to. Po jeho obdržení posílá trojský kůň hackerovi všechny dokumenty, které se v napadeném počítači vyskytují. To je ovšem pro Richarda B. scénář přímo hororový, neboť má v počítači uloženy také citlivé údaje svých klientů. Které soubory (a zda vůbec) byly skutečně odcizeny, to se už vzhledem ke smazaným stopám nedá dohledat. Pan B. tedy musí vycházet z toho, že postiženi jsou všichni jeho zákazníci.

Maskovaný a klamající

Poněvadž chceme získat další informace o hackerových motivech, pátráme po zdroji trojského koně. Nejprve si bereme pod lupu internetový prohlížeč. Poněvadž skoro každý útok je veden přes webové stránky nebo e-mail, hodně si od této cesty slibujeme. Bohužel se však jedná o slepou uličku: bezpečnostní nástroj jako

Důkaz 1

NEBEZPEČNÝ HARDWARE: Flash paměť v hezkém balení dá zapomenout na veškerou opatrnost. V tomto případě však v domnělém reklamním dárku čekal na svou příležitost zákeřný spyware.

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.

naschvál při zavírání automaticky vymazává cache, průběh i cookies browseru. Obracíme proto pozornost k softwaru, který má pan B. v počítači. On sám je přesvědčen, že do něj nikdy neinstaloval nic nebezpečného. „Nedávno jsem si dokonce nainstaloval nový antispywarový software, abych zabránil vstupu škůdců," říká – a celý náš tým okamžitě zbystřuje pozornost. Ani název produktu, ani jméno jeho výrobce nám totiž nejsou nijak povědomé! A tak se pouštíme do podrobného zkoumání programu. Brzy máme jasno: ačkoliv se zdánlivě jedná o docela obyčejný bezpečnostní software, pan B. se stal obětí tzv. „rogue antispywaru". Jde o mimořádně drzý podvod – spyware, který je maskován jako svůj pravý opak a vydává se za nástroj k odstraňování škůdců.

Strach jako zbraň

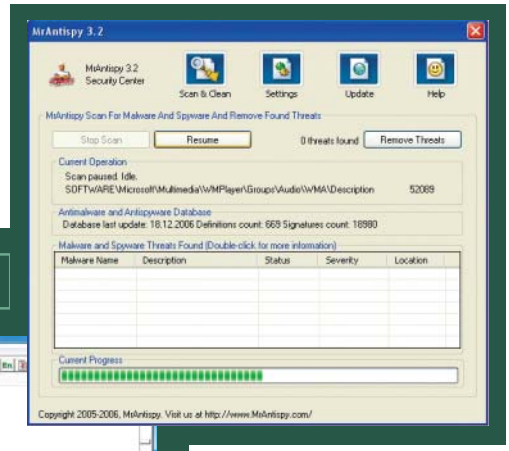
Byl to právě strach ze spywaru, který pana B. vehnal přímo do hackerovy pasti – stejně jako mnoho jiných uživatelů. Domnělému bezpečnostnímu softwaru oběť samozřejmě bez obav poskytne administrátorská práva, tedy právě to, co hacker potřebuje. Trojský kůň tak získá neomezený přístup do systému.

Zbývá ještě otázka, jak se malware do počítače vůbec dostal. K našemu překvapení vytahuje pan B. ze zásuvky jakousi USB paměť. „V ní to bylo. Reklamní dárek, který mi poslala bezpečnostní firma." To však ještě není všechno, neboť dodává: „Předtím jsem dokonce s někým telefonoval."

Teď už celá věc nabývá na výbušnosti. Pan B. se totiž nestal obětí nějakého nazdařbůh šířeného útoku na náhodné uživatele internetu. Byl napaden cíleně! A náš tým chce pochopitelně zjistit, kým. Zkoušíme štěstí a nástroj z „flešky" instalujeme na testovací počítač. Ihned po spuštění začíná program z internetu stahovat „update" – jako kdyby chtěl naistalovat aktualizace signatur pro hledání spywaru. Avšak namísto toho zavádí do počítače trojského koně.

Trik s USB pamětí

Hackerův trik není nijak nový. Už před nějakou dobou demonstroval newyorský bezpečnostní specialista Steve Stasiukonis z firmy „Secure Network Technologies", že největší slabinou v bezpečnostních systémech je člověk a jeho zvědavost. Jistá banka tehdy jeho firmu pověřila, aby v ní provedla důkladnou bezpečnostní kontrolu a nevynechala ani „social engineering". To pro bezpečnostní experty obvykle znamená začít flirtovat se sekretářkou nebo tlachat v kuřárně a pokoušet se tak objevit nějakou slabinu systému nebo vyzvědět heslo.



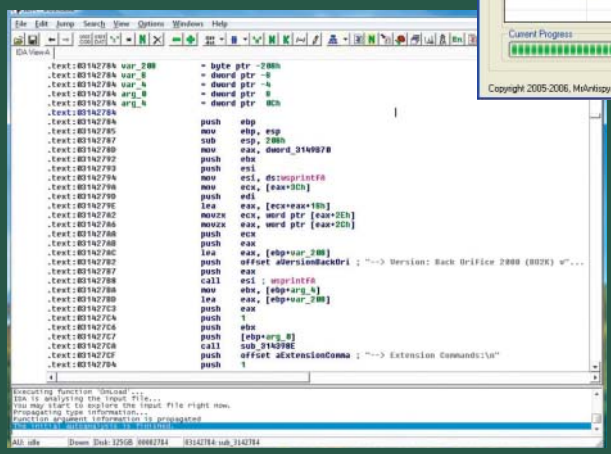
Mnohem lépe však funguje jednoduchý trik: Steve Stasiukonis nechal v prostorách firmy roztrousit flash paměti, které obsahovaly speciálně pro tento účel naprogramovaného trojského koně. Nacházeli je zaměstnanci – a hned je zvědavě připojovali k firemním počítačům. Z dvaceti nastražených návnad se „ujalo" celých patnáct. Stasiukonis tak získal přihlašovací jména a hesla i všechny další informace o jednotlivých napadených počítačích.

Krádež dat bez důkazů

Jakkoli byl vlastní útok jednoduchý, odhalit v případě pana B., kdo jej vlastně poškodil, je velmi složité. Poněvadž virový skener trojského koně deaktivoval, byl tak hacker varován a mohl po sobě zahladit stopy. Pravděpodobně má teď k dispozici kopie všech důvěrných dokumentů své oběti. Jelikož se zde nejspíš jedná o objednanou špionáž, je to pro pana B. nepříjemnost dvojnásobná. Pachatele se tedy našemu týmu bohužel odhalit nepodařilo – a panu B. tak zůstane jen poučení, že reklamním dárkům se nemá důvěřovat.

Valentin Pletzer

Důkaz 2



STARÝ ZNÁMÝ: **Analytický nástroj disassembler IDA odhalil v malwaru starého známého. Trojský kůň ještě dokonce obsahuje originální text „Back Orifice 2000".**