

Komentář

Brno 19.1. 2012

SpyEye – zvědavé oko vám ošálí zrak a vybílí účet

Zcizení identity, odepření služby, úniky osobních dat, průmyslová špionáž a sabotáž. I když se jedná o reálné problémy, tak se veřejnosti těžko popisují a ještě hůře se vysvětlují jejich dopady. Veřejnost tyto případy řadí do škatulky sci-fi románů a projevuje žádný nebo minimální zájem. Rozhodně se ale není čemu divit, protože málokdo na ovládání své automatické pračky používá SCADA systémy, a ještě méně lidí ve sklepě o víkendech obohacuje uran.

Pochopitelným příkladem toho, jak může běžný uživatel dojít k újmě na Internetu, je sada pro začínající elektronické kriminálníky („malware toolkit“, „crime kit“) - SpyEye. Poskytne modernímu zloději prostředky k vykrádání účtů neznámých lidí, aniž by byly kladeny vysoké nároky na jeho znalosti a zkušenosti. SpyEye kontrolní centrum je naprogramováno v php a jeho zprovoznění je jen o něco málo složitější než instalace vlastního blogu nebo diskusního fóra. Na rozdíl od open source php aplikací SpyEye není k dispozici zdarma, ale jeho vývojář(i) za něho inkasuje(i) peníze výměnou za další podporu a aktualizace. Často však celá sada unikne a začne se lavinovitě šířit po Internetu, takže si ji může stáhnout kdokoli.



Obrázek 1 Nalézt instalační sadu SpyEye pomocí Googlu je otázka několika vteřin. Na obrázku je jeden z mnoha zdrojů, tento konkrétní má 1404 stažení.

Jakmile je kontrolní centrum funkční, nekalý živel se zaměří na ovládnutí uživatelských počítačů. Důležité pro útočníka je nasměrovat uživatele (resp. jejich prohlížeče) na webové stránky, kde jsou již nachystány exploity na neaktualizovaný software, a to nejenom prohlížeče, ale i Javu, Flash a Adobe Reader. Exploity jsou samozřejmě také součástí celého balíku a čím jsou aktuálnější, tím větší je útočnickova šance na úspěch. Jak dlouho se potom na počítači trojský kůň udrží, záleží také na tom, jak často se dokáže měnit, aby unikl detekci antiviru. Kvůli aktualizacím exploitů a trojského koně jsou útočníci často ochotni za „licenci“ SpyEye platit a neaktuální verze SpyEye dostupné veřejně již neslibují tak velkou vidinu zisku.



Obrázek 2 Screenshot instalátoru SpyEye z "oficiálního" manuálu.



Obrázek 3 Mapa objevených kontrolních center SpyEye. Geografické umístění kontrolního centra ale nijak neomezuje jeho možnosti ovládat napadené stroje kdekoli jinde na světě. Zdroj: <https://spyeetracker.abuse.ch/> (leden 2012)

S ovládnutými počítači má útočník v podstatě neomezené možnosti a nejsilnější devizou SpyEye je automatické zachytávání informací o kreditních kartách a bankovních účtech, které jsou shromažďovány v kontrolních centrech plně k dispozici útočníkovi. **Novinka, kvůli které proběhla médii vlna zpráv o SpyEye, je skrývání převodů peněz před uživatelem.** Funkce vychází z úvahy, že čím déle si uživatel nevšimne podezřelých převodů peněz ze svého účtu, tím déle je možné mu krást peníze.



Obrázek 4 Submenu kontrolního centra SpyEye, které se věnuje nastavení krádeží nejrozumnějších údajů.

Skrývání podvodných převodů funguje velmi přímočaře, SpyEye je jednoduše v bankovním výpisu (prostřednictvím internetového bankovníctví) uživateli nezobrazí. Vše samozřejmě funguje jen na nakaženém počítači, kde může trojský kůň manipulovat s tím, co bude uživateli zobrazeno. Jakmile se uživatel připojí z jiného počítače, uvidí všechny peněžní transakce, včetně těch „nechtěných“.



Obrázek 5 Hlavní menu kontrolního centra SpyEye. Kromě toho, že trojský kůň na počítači sbírá data, může zprostředkovat útočníkovi i vybrané služby (např. RDP, Socks proxy, FTP).

SpyEye samozřejmě není zdaleka jediný nástroj svého typu, ale je jeden z nejčastěji probíraných a pozornosti upoutal poté, co v roce 2010 převzal kód podobného nástroje – Zeus. Za spolupráci na vývoji malware toolkitů bývají nabízeny poměrně lukrativní odměny, což ukazuje i na jistotu tvůrců návratností těchto investic. Na dalším obrázku je jeden z inzerátů na vývojáře a podporu. Z obrázku je i zřejmý původ celého projektu.



Obrázek 6 Zdroj: <https://krebsonsecurity.com/2011/06/criminal-classifieds-malware-writers-wanted/>.

Obrana proti SpyEye je teoreticky velmi jednoduchá. Je důležité udržovat aktualizované browsery a veškeré jejich addony a paginy, jako Flash a Java (rozhodně nestačí pouze aktualizovaný operační systém). Dále samozřejmě aktualizovaný antivirus, firewall a ideálně softwarová IPS, která zabrání zneužitím případných zranitelností. Na domácím počítači, pokud má uživatel motivaci se o něj trochu starat, je to relativně jednoduchý úkol. Mnohem větší

výzva je udržet takový stav napříč firemním prostředím, kde mají uživatelé výrazně menší motivaci chovat se obezřetně, hlásit podezřelé chování nebo nefunkční bezpečnostní software, který je vlastně „jen obtěžuje“. Správci na druhou stranu musí hlídat příliš mnoho oblastí zároveň. Řešením může být jedna centrální konzole (McAfee ePolicy Orchestrator) na správu a monitoring zmíněných oblastí – antivirový software, firewall, IPS a kontrola aktualizací software ve společnosti.

Zkoumáním principů použitých ve SpyEye a dalších crime kitech se zabývá mnoho společností i jednotlivců a zájemci mohou dohledat velké množství informací nebo zkoumat přímo samotný kód. Další zdroje:

- blogy McAfee: <https://blogs.mcafee.com/tag/spyeye>,
- blog Briana Krebse: <https://krebsonsecurity.com>,
- zpráva Ryana Sherstobitoffa k pozměňování bankovních výpisů pomocí SpyEye: <http://issa.org/images/upload/files/Sherstobitoff-The%20New%20Frontier%20for%20Zeus%20and%20SpyEye.pdf>,
- server sledující výskyt kontrolních center SpyEye: <https://spyeyetracker.abuse.ch>.

Komentář připravil Robert Šefr, IT Security Consultant, COMGUARD a.s.