Operace SWORDFISH 2

Vložil/a Mirek [1], 28 Červen, 2010 - 23:27

- Free Mind [2]
- Hacking [3]

Možný scénář útoku na uživatele internetového bankovnictví podle mistra na konspirativní teorie.

Před nedávnem vyšel na portálu soom.cz příspěvek na téma Internetové bankovnictví a nešifrované SMS [4]. Než budete číst dál, doporučuji si ho přečíst, stejně jako diskusi pod ním, neboť se v ní objevily docela zajímavé názory.

Za povšimnutí stojí především komentář uživatele DJVyn, který mě inspiroval k napsání tohoto příspěvku. Nemusíte být zrovna zaměstnancem velké čtyřky [5] nebo IDC [6], abyste dovedli predikovat, jak by útok na uživatele internetového bankovnictví mohl v blízké budoucnosti probíhat. Pokud vezmete v úvahu tempo, jakým se informační technologie vyvíjejí, počet a typ útoků, nejeví scénář takového útoku na uživatele internetového bankovnictví až tak nepravděpodobný, jak by se mohlo na první pohled zdát.

Volba platformy pro šíření škodlivého kódu

Můžeme předpokládat, že uživatel, který se chová nezodpovědně a stáhne si do svého počítače nějakého trojana, se bude pravděpodobně stejně nezodpovědně chovat i při používání svého smartphonu, a možná ještě víc. To, že dochází ke konvergenci mobilů a počítačů, na to upozorňují i přední konzultační společnosti. Lze tedy očekávat, že do několika let, pokud k tomu již nedošlo, klasické mobilní telefony prakticky vymizí z trhu a budoucnost zcela ovládnou smartphony. Takový telefon pak bude vzhledem k přítomnosti operačního systému, jehož funkce jsou dokumentovány a který je vzhledem k možnostem nahrávání dalších aplikací, stejně zranitelný jako klasické stolní počítače.

Vektor útoku

Platformu pro šíření škodlivého kódu tedy máme, nyní již zbývá jen vyřešit, jak ten škodlivý kód na tu spoustu počítačů a smartphonů dostat. Není to až tak těžké, stačí jen vhodně využít některých lidských vlastností a možností, které skýtá Web 2.0 [7]. Např. ukrýt škodlivý kód do aplikace, o které se dá předpokládat, že o ní je nebo bude velký zájem, případně za kterou se běžně musí platit. Může to být třeba nějaká jednoduchá ale přitom velice chytlavá hra, ta se pak začne neuvěřitelně rychle šířit, třeba přes Facebook. A lidé ji začnou na internetu sami vyhledávat a stahovat do svých počítačů a mobilních telefonů. Útočník dokonce nemusí za tímto účelem ani vyvíjet vlastní produkt, ale může využít již nějakého jiného, který na trhu již je a u kterého se dá penetrace očekávat nebo dokonce, který si již své postavení na trhu získal a jeho popularity využít. O jaký konkrétní produkt by se mohlo jednat, ponechám na vás.

Business model

Útočník však může být rafinovaný, a aby nevzbudil podezření, nebude svůj produkt nabízet zdarma, ale nechá si za svůj produkt nebo službu též zaplatit. Takový obchodní model by nebyl ničím novým, vždyť v podstatě totéž dělají autoři falešných antivirů a antispywarů. Nechají si za „antivir“, který žádné viry ani odhalit neumí, zaplatit a ještě pak inkasují provizi za pronájem botnetu, jehož součástí se nakažený počítač stane. A pokud nastaví vhodnou cenu, kterou bude drtivá většina zájemců

ochotna zaplatit, vydělají na tom v každém případě. Svému produktu nemusí dělat ani žádnou velkou reklamu. Stačí, když „cracknutou“ verzi svého vlastního produktu nabídnou ke stažení na nějaké komunitní síti, diskusním fóru apod. Bude jim v podstatě jedno, odkud si zájemce jejich produkt stáhne a zda za něj zaplatí či nikoliv. Nezapomínejte, že útočník sleduje přeci jen trochu jiné cíle. Jde mu o to, aby se jeho produkt masově rozšířil, a zároveň aby nevzbudil podezření. Slabinou popsaného útoku je hlavně masivnost této akce, neboť s počtem nakažených počítačů a mobilních telefonů poroste i riziko odhalení.

Najímáme vývojáře

Vzhledem k tomu, že v této oblasti se točí obrovské množství peněz a naprostou většinu útoků provádí vysoce organizované skupiny, nebude pro ně problém si najmout vývojáře, který pro ně daný produkt vyvine. Dokonce s ním může být uzavřena i klasická smlouva a za svou práci dostane zaplaceno. Mimochodem, kdo se o tuto problematiku zajímá, ví, že je to naprosto běžná praxe. Vývojář tak vůbec nebude tušit, pro koho vlastně pracuje a k čemu má jeho dílo posloužit. Vzhledem k tomu, že součástí takových organizovaných týmů jsou i ženy, může být vývojář získán i jiným způsobem. Pro takovou ženu není problém svést nadějného studenta informatiky, představit ho svému šéfovi, který mu nabídne práci hlavního vývojáře. (Není podstatné, zda se bude jednat o studenta MIT nebo ČVUT. V obou případech na nabídku kývne, neboť si užije a ještě si k tomu slušně vydělá. No, kdo z vás by to pánové nebral?) Dále si taková skupina může najmout nějakou firmu na propagaci svého produktu. Na trhu je spousta firem typu Býk&Bodlák, která tuto práci velice ráda odvede. Tím, že se bude tato organizovaná skupina chovat stejně jako jakýkoliv jiný seriózní obchodník a bude čelit i stejným problémům, nevzbudí žádné podezření.

Smrt přichází z cloudu

Nutno podotknout, že v prvopočátku nemusí být škodlivý kód v produktu vůbec přítomný. Škodlivý kód se může objevit až v některé další verzi, která bude distribuována jako (ne)oficiální upgrade, nebo si produkt bude sám stahovat aktuální verze z internetu. Dost možná, že se ale na nějakém serveru objeví (ne)oficiální rozšíření, které bude přidávat nějaké „úžasné“ vlastnosti, které oficiální verze neobsahuje. V tuto chvíli si oficiální autor produktu vytváří alibi. V původní verzi přeci žádný škodlivý kód nebyl, a že někdo vytvořil rozšíření a do něj začlenil škodlivý kód, za to on nemůže. V okamžiku, kdy počet stažení překročí určitou hodnotu, se kód aktivuje a začne přihlašovací údaje a zprávy, které na něj chodí posílat na server útočníka. Útočník bude muset nějakým způsobem vyřešit, kam data, která pro provedení útoku potřebuje, posílat. Především kam přeposílat ty SMS zprávy s OTP. Enormní počet odeslaných SMS zpráv na jedno telefonní číslo by mohl vzbudit podezření u operátora. Útočník se proto bude nejspíš snažit využít internetovou konektivitu a zprávu poslat touto cestou. Do budoucna lze počítač s tím, že smartphony budou do internetu připojeny neustále a pokud ne, tak si spojení v případě potřeby vytvoří. Mezitím kdesi v cloudu [8] nebo na pronajatém nebo hacknutém serveru jakéhosi obskurního poskytovatele, který s nikým nekomunikuje, a který slouží jako C&C server probíhá též párování credentials a OTP. Následně jsou jednotlivé transakce dokončovány a peníze převáděny mezi několika účty. Pak už je potřeba peníze jen někde vybrat, třeba ve Western Union.

Závěr: Uživatel by se měl chovat obezřetně a nést odpovědnost [9] za zabezpečení svého počítače, minimálně bezpečnostní produkty by měl stahovat pouze z důvěryhodných zdrojů, nejlépe přímo ze serveru daného výrobce, nenavštěvovat pochybné stránky a do svého počítače instalovat jen to, co opravdu potřebuje. Pokud má přesto potřebu zkoušet nejrůznější SW, tak např. v sandboxu a na servery jako je internetové bankovnictví přistupovat z virtuálního stroje [10] s důvěryhodným OS.

Vážně si myslíte, že se tohle nikdy nemůže stát?

URL článku: https://security-portal.cz/clanky/operace-swordfish-2

Odkazy:
[1] https://security-portal.cz/users/mirek
[2] https://security-portal.cz/category/tagy/free-mind
[3] https://security-portal.cz/category/tagy/hacking

[4] http://www.soom.cz/index.php?name=articles/show&aid=510
[5] http://cs.wikipedia.org/wiki/Velk%C3%A1_%C4%8Dty%C5%99ka_auditorsk%C3%BDch_firem
[6] http://www.idc.com/
[7] http://www.cleverandsmart.cz/web-20-mnoho-povyku-pro-nic/
[8] http://www.cleverandsmart.cz/cloud-computing/
[9] http://www.cleverandsmart.cz/preneste-odpovednost-na-klienta/
[10] http://www.cleverandsmart.cz/rizika-virtualizace/