Problém s boty je horší, než si většina lidí myslí

Vložil/a IDC CEMA [1], 29 Březen, 2010 - 14:03

- Hacking [2]
- Konference [3]
- Security [4]
- Tisková zpráva [5]

Rozhovor s Craigem Schillerem, bezpečnostním ředitelem Portlandské státní univerzity, keynote řečníkem na konferenci IDC IT Security Roadshow 2010.

Craig Schiller je diplomovaný bezpečnostní odborník informačních systémů se zaměřením na řízení bezpečnosti a bezpečnostní architekturu. V počítačovém průmyslu působí již 28 let, z toho 8 let jako odborník na informační bezpečnost.

Je ale také autorem knihy Botnets: The Killer Web App, která je první publikací zabývající se fenoménem botnetů. Zeptali jsme se ho na to, proč je tato oblast jiná, než běžné viry, a proč bychom se měli s botnety bojovat s vyšším nasazením.

Roman Smělý

Myslíte si, že jsou sítě botů, takzvané botnety, skutečně největší bezpečnostní hrozbou?

Řekl bych, že ano. A to především z toho důvodu, že všechny tyto hrozby jsou zaměřeny na finanční zisk. Jakmile se totiž dostanou na váš počítač, začnou hledat čísla kreditních karet, čísla bankovních účtů, hesla k těmto účtům nebo vaše čísla pojistek. Prostě vše, co umožní krádež identity.

A jakmile tyto informace mají, dopad na konkrétní osobu je devastující. Věšina firem, jakmile zjistí, že má podobné viry v síti, tak je vyčistí. Ale už neřeknou uživateli, aby kontaktoval svoji banku, zrušil svoji kreditní kartu, změnil si hesla. Takže tato osoba je pak ponechána ve své zranitelnosti týdny a týdny. A vůbec o těchto únicích neví.

Krádež identity je poměrně rozšířená záležitost ve Spojených státech. V Evropě existuje mnohem méně takových příkladů. Čím to je?

Řekl bych, že si toho lidé nejsou tolik vědomi. A přitom tomu jsou vystaveni stejně. Ve Spojených státech máme nově zákon, který říká, že pokud vaše osobní informace byly kompromitovány, tak firma, která je měla chránit, vám to musí říct.

Takže nastal obrovský nárůst oznámených krádeží identity. A to přitom neznamená, že se to najednou změnilo a je toho víc. Jenom je to vyžadováno zákonem. Takže si myslím, že podobné to bude i tady. Pokud by se změnil zákon, abyste museli tyto ztráty hlásit, tak byste viděli mnohem větší množství zneužitých kreditních karet a dalších informací.

Postoj ve Spojených státech, ještě před tím, než se zákon změnil, byl takový, že přece nechceme něco takového oznamovat. Mohlo by to mít vliv na náš tržní podíl, zákazníci by nás opustili. Je jasné, že například ztráta čísel kreditních karet by důvěru snížila. To se ale v Evropě děje také.

Proč lidé, i přestože určitě o sítích botů slyšeli, zatím na tyto hrozby nedbají?

Pokud lidé vyrůstají v prostředí běžných virů, které vám zpomalují počítač a průběžně vás akorát rozčilují, je to pochopitelné. Jenže problém s boty je mnohem větší, než jenom starost o jeden konkrétní počítač. Onen uživatel vidí „och, můj počítač je zase nakažen“, a tak jej vyčistí. Jenže už

nevidí tisíce dalších počítačů, které jsou také nakaženy. Nevidí data, která byla ukradena z těchto počítačů a zneužita za účelem kriminality.

Všechno, co uživatelé vidí je „aha, byl jsem infikován virem“. Vůbec netuší, že třeba právě jejich počítač už byl zneužit pro šíření dětské pornografie nebo spamu, který všichni nenávidí. Pokud by zjistili, že byli infikováni, a hlavně, co onen virus udělal, určitě by je to znepokojilo mnohem víc. Ale to teď nejsou, protože to nevidí. Hodně současných „záchranných“ akcí se zaměřuje na to, aby se počítač uvedl opět do provozuschopného stavu. Nedívají se na to, co počítač vlastně dělá.

Na Portlandské univerzitě tenhle přístup začínáme měnit. Jakmile máme infikovaný počítač, uděláme určitou forenzní analýzu, která nám řekne, co všechno počítač dělá a s kým ještě komunikuje. Snažíme se najít maximum vodítek, které by nám řekly, kdo je ještě infikován. Součástí je i to, o jaký byznys útočníkům vlastně jde.

Je možné odhadnout množství peněz, které se v byznysu se sítěmi botů pohybuje?

FBI nebo CSI dělají každý rok průzkumy na téma, o kolik podniky přicházejí prostředků v důsledku těchto útoků. Pravdou je ovšem to, že to nikdy nikdo neví přesně. Nevíme, kolik kreditních karet bylo ukradeno, kolik bylo za každou kreditní kartu zaplaceno. Jenom víme, že se to děje často.

Zažila vaše univerzita útok botů, a pokud ano, jak se s tím vyrovnala?

Ještě před tím, než jsem se dostal na pozici ředitele informační bezpečnosti, jsem se s takovým útokem setkal. První, co jsme zjišťovali, bylo, o jaký rozsah poškození se jedná. A zjistili jsme, že kromě jedné nákazy, kterou jsme našli, máme ještě další. Museli jsme od univerzitní sítě oddělit na 300 stanic. Byly to počítače, u kterých se boti snažili rozlousknout administrátorská hesla. Využívaly k tomu distribuovaný útok pro odhalení hesel.

Jakmile jsme posléze našli první nakažený počítač, který útok prováděl, prošli jsme jeho bezpečnostní logy, a zjistili, jaké další počítače jsou do útoku zapojeny. Získali jsme seznam asi 40 počítačů, u kterých jsme také procházeli bezpečnostní logy. Tyto počítače se snažily prolomit do oněch asi 300 stanic.

Druhá síť botů pak již prolomené počítače využívala pro nelegální distribuci intelektuálního vlastnictví, jako jsou například filmy či hudba.

To je zřejmě nejběžnější porušení…

Ano, útočníci odhadli, že tak zřejmě budou nejblíže k cílové skupině (smích). Nicméně z technického hlediska se jednalo o velmi sofistikovaný útok. Boti zřídili virtuální FTP server, který byl zařazen na seznam míst, ze kterých se dá nelegální obsah stáhnout. Každý z infikovaných počítačů měl složku, ve které byly údaje o jeho výkonu. Jak dlouho trvá dostat data na tuto stanici, jak rychle se stahují na různá místa planety a tak dále. Díky těmto datům si mohli uživatelé vybrat to správné místo pro stažení písničky nebo filmu.

Chytré hlavy!

Ano, velmi chytré. Fungovalo to tak léta a my jsme neměli tušení, že tomu tak je. Protože z provozu na síti, který sledujete, nezjistíte, že se právě přenášejí špatná data.

URL článku:
https://security-portal.cz/clanky/probl%C3%A9m-s-boty-je-hor%C5%A1%C3%AD-ne%C5%BE-si-v%C4%9Bt%C5%A1ina-lid%C3%AD-mysl%C3%AD

Odkazy:
[1] https://security-portal.cz/users/idc-cema
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/konference
[4] https://security-portal.cz/category/tagy/security
[5] https://security-portal.cz/category/tagy/tiskov%C3%A1-zpr%C3%A1va