**Bezpečnostní hrozby z Internetu**

**Malware**

Malicious Software zahrnuje kromě samotných virů spoustu dalších typů programů, jejichž výskyt v počítači je nežádoucí. Dělíme je do několika typů:

***Spyware***

Spyware je program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele. Narozdíl od backdooru jsou odcizovány pouze „statistická“ data jako přehled navštívených stránek či nainstalovaných programů. Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie nemůže být zneužita. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí.

***Adware***

Obvykle jde o produkt, který znepříjemňuje práci s PC reklamou. Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování, společně s vnucováním stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem. Část Adware je doprovázena tzv. „EULA“ - End User License Agreement – licenčním ujednáním. Uživatel tak v řadě případů musí souhlasit s instalací. Adware může být součástí některých produktů. Ačkoliv nás reklama doprovází během celé činnosti s daným programem, odměnou je větší množství funkcí, které nejsou v klasické free verzi (bez reklamy) dostupné.

***Dialer***

Dialer je program, který změní způsob přístupu na Internet prostřednictvím modemu. Místo běžného telefonního čísla pro Internetové připojení přesměruje vytáčení na čísla se zvláštní tarifikací, např. 60 Kč / minutu (tzv. „žluté linky“). V některých případech se tak děje zcela nenápadně nebo dokonce automaticky, zvlášť když oběť používá špatně nastavený internetový prohlížeč. Dialer může být na PC vypuštěn návštěvou „nevhodné stránky“ (např. pornografické), například za využití technologie ActiveX, takže problémy mohou nastat především uživatelům Internet Exploreru. V jiném případě může jít o nenápadný spustitelný soubor (.EXE), který je nic netušícímu uživateli vnucován ke stažení klasickým dialogem.

**Spam**

Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging. E-mailové adresy do spamových databází jsou získávány mj. pomocí robotů, které procházejí webové stránky a sbírají e-mailové adresy na nich uvedené. Také registrací na některých serverech s uvedením vaší adresy je možné přidat se na seznam pro spam.

**Backdoor, Zombie, Botnets**

Některé viry (červy) často jako svojí další činnost instalují do PC tzv. Backdoor (zadní vrátka), které umožní k systému přístup útočníkovi. Z takto nakaženého PC může být vytvořena „zombie“ pod kontrolou autora viru. Sítě takových strojů se nazývají botnets a často jsou využívány k další nekalé činnosti jako je např. odesílání spamu nebo provádění DDoS (Distributed Denial of Service) útoků.

**Hoax**

Anglické slovo HOAX v překladu znamená: Falešnou zprávu, Mystifikaci, Novinářskou kachnu, Podvod, Poplašnou zprávu, Výmysl, Žert, kanadský žertík. V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem, ale i další fámy, petice, výstrahy, pyramidové hry, řetězové dopisy apod. Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to s největší pravděpodobností HOAX. Takové zprávy obtěžují příjemce, zbytečně zatěžují linky a vyzrazuje informace (e-mailové adresy), čehož se dá dále využít pro spam.

**Phishing**

Phishing je činnost, při které je rozesílán email uživatelům Internetu, který se tváři, že byl odeslán z legitimní organizace (většinou finanční, banky apod.). Předmětem takového emailu je získat osobni informace uživatele, zejména pak čísla platebních karet a jejich PIN a následně jejich zneužití. Phishing email obsahuje často odkaz na stránky s formulářem, který uživatel v dobré víře vyplní a odešle. Odeslaná data vsak nekonči u bankovního či finančního ústavu, ale v rukou tvůrce phishing emailu.

**Další**

Kromě těchto existují i další pojmy v oblasti. Rootkit je program maskující svoji přítomnost svojí co nejhlubší infiltrací do operačního systému, keylogger (nebo jiný logger) zase zaznamenává činnost na PC a k informacím umožní přístup útočníku. Čas od času se objevují další pojmy ukazující na jiný typ či podtyp podobných programů.

**Použitá literatura:**

HÁK, Igor. *Moderní počítačové viry* [online]. [cit. 2013-02-03]. Dostupné z: <http://www.cmsps.cz/~marlib/bezpecnost/viry/velka_kniha_o_virech.pdf>

*Počítačové viry* [online]. [cit. 2013-02-03]. Dostupné z: <http://www1.osu.cz/~klimesc/public/files/Pocitacove%20systemy/Prednasky/08_-_Pocitacove_viry.pdf>

*Počítačové viry, antivirová ochrana a bezpečnost na internetu* [online]. [cit. 2013-02-03]. Dostupné z: http://www.ped.muni.cz/wtech/old2012/u3v/iepp/05.pdf