Úvod do problematiky Malware

Tento dokument se pokouší shrnout základní informace o bezpečnostní problematice sítí z pohledu
běžného uživatele internetu, tak aby byl schopen zabezpečit svůj počítač a svoji práci.

Malware a jeho dělení – aneb virus není červ

Malware (malicious software – škodlivý software) je jakýkoliv software, který byl vyvinut za účelem poškozování počítačových systémů. Malware dále dělíme do skupin podle toho jak se spouští, jak se šíří a co dělá. Toto dělení není přesné, skupiny se překrývají a některé často zaměňují
či pohlcují v rámci zjednodušení věci.

1. Virus – nejstarší typ malware; stejně jako organický virus, není počítačový virus schopen samostatné existence a potřebuje ke svému „životu“ hostitele. Nejčastějším typem hostitele jsou spustitelné soubory, dnes už ale viry můžeme potkat i v některých „datových“ souborech (např. makroviry v dokumentech MS Office).

2. Červ (worm) – je již samostatný program, který ke svému šíření využívá bezpečnostní chyby nebo důvěřivé uživatele (červy v přílohách emailů). Po prvotním spuštění modifikuje systém tak, aby byl spouštěn při každém startu systému.

3. Trojský kůň (trojan horse) – je program, který se vydává za legitimní software nebo je jeho součástí. Šíří se pomocí kopírování takového software, nebo často pomocí jiných druhů malware (*dropper*).

4. Backdoor – je program umožňující vzdálenou kontrolu napadeného počítače útočníkem. Šíří se
jako trojský kůň nebo jako červ. Některé backdoory modifikují systém tak, že počítač začne rozesílat nevyžádanou počtu (*spam*) – takový počítač se pak nazývá *zombie*.

5. Spyware – je program, který shromažďuje informace o uživateli a odesílá je bez jeho vědomí útočníkovi (zde se většinou nejedná o osobu útočící na systém, ale např. o reklamní společnost, která takto získává informace pro cílenou reklamu). Spyware se často šíří jako trojský kůň – nejčastěji jako součást shareware.

6. Adware – je program znepříjemňující práci zobrazováním reklamy (otevírání pop-up oken, nastavováním domovské stránky v prohlížeči, atd.). Adware může být součástí legitimního software, za který tímto zobrazováním reklamy platíme.

7. Exploit – je software zneužívající určitou bezpečnostní díru (chybu). Často je vyvinut pro demonstrační účely bezpečnostními experty, může pak být však jednoduše použit pro konstrukci červa.

8. Rootkit – komplexnější software nahrávaný útočníkem na dobytý systém. Obsahuje různé nástroje pro ovládání systému a případné další útoky.

9. Keylogger – program zapisující uživatelem stisknuté klávesy. Získané informace odesílá útočníkovi. Často je tento program nastaven tak, aby zapisoval jen v citlivých situacích (přihlášení
do systému, internetové bankovnictví, atd.).

10. Dialer – program přepisující telefonní číslo modemového připojení většinou na linky s vyšším
tarifem („žluté linky“). Dialer může být i naprosto legální program zajišťující připojení k placeným
službám.

Prevence – aneb věnujte se malware dřív než se bude on věnovat Vám

Dobrou prevencí se lze vyvarovat téměř veškerého rizika spojeného s útokem malware. Mnohem obtížnější je prevence proti přímému útoku útočníkem (často nepřesně nazývaným *hacker*), nicméně
takové útoky nejsou pro svoji složitost (nejenom časovou) vedeny na uživatelské stanice, ale na vytipované servery.

Aktualizace operačního systému – to by měl být jeden ze základních návyků každého uživatele. Platí, že software je vždy bezpečný jen do té doby, než v něm někdo nalezne díru (chybu). A dále platí, že neexistuje software bez chyby. Společnost Microsoft vydává kritické záplaty na svůj operační systém několikrát do měsíce. Většinou všechny opravují bezpečnostní díry umožňující napadení systému nějakým typem malware.

Antivirový program (zkráceně AV) – základní vybavení pro udržení malware vně vašeho pc. Moderní antiviry již dávno nebojují jen proti virům (název přetrval z dřívějších dob), ale proti celé
řadě ostatních typů malware. Jejich záběr je dnes už tak velký, že se z antivirů stává úctyhodný balík
sofistikovaného software.
Jedna z nejdůležitějších částí moderních antivirů je rezidentní štít, spouštěný s každým startem pc a
monitorující na pozadí veškerou aktivitu. Tak je možno detekovat malware okamžitě při jeho pokusu o spuštění. Pozor ale – *čím více tím lépe* – zde neplatí, a i při vysokém stupni paranoii je pro
správný chod AV nutné, aby byl spuštěn vždy jen jeden rezidentní štít (jen jednoho AV).

Aktualizace antivirového programu – v dnešní době se může nový malware dostat do vašeho pc
přes internet během několika hodin od svého vzniku. Proto je vysoce doporučeníhodné aktualizovat
často (alespoň 1x denně nebo při každém připojení). Některé antiviry disponují velmi kvalitní heuristickou analýzou, která dokáže detekovat ještě neznámý virus (nicméně musí být alespoň

částečně podobný svým chováním nějakému známému), ale je vždy lepší mít co možná nejaktuálnější informace pro vyhodnocení.

Alternativní prohlížeč – většina malware využívá bezpečnostní díry nejpoužívanějšího software –
Microsoft (zkráceně MS) Windows s prohlížečem Internet Explorer (zkráceně IE). Používáním jiného prohlížeče lze velmi výrazně omezit nebezpečí plynoucí z prohlížení stránek. To je částečně
ale vykoupeno nedokonalou podporou některých MS technologií, které se používají ve specializovaných aplikacích (firemní aplikace, internetové bankovnictví). Je ale nutno přiznat, že většina těchto technologií sama není dostatečně zabezpečená a nehodí se pro nasazení mimo firemní
síť. Protože IE není možné jednoduše odinstalovat z Windows a alternativní prohlížeče jsou malé a
jednoduché, nabízí se možnost vhodně využívat oba (IE na firemní sítě a internetové bankovnictví a
alternativní prohlížeč na běžné prohlížení).

Alternativní mailový klient – většina malware chodící mailem využívá bezpečnostní díry nejpoužívanějšího poštovního klienta – MS Outlook Express (zkráceně OE). Riziko při jeho používání je ještě větší než při používání IE, protože nemůžete nijak kontrolovat, jaký mail vám přijde (nemůžete tedy spoléhat na to, že vám budou chodit jen bezpečné maily).
V dnešní době sice existuje mnoho alternativních poštovních klientů, nicméně většinou postrádají některé „firemní“ funkce, takže jejich nasazení je limitováno skoro jen pro domácí použití.

Osobní firewall (personal firewall, fw) – představuje pokročilejší obranu proti většině typů malware. Jeho funkce spočívá ve filtrování síťového provozu (např. požadavek z prohlížeče na webserver a jeho odpověď – zpět poslaná stránka, kterou prohlížeč zobrazí) mezi vaším počítačem
(Windows, vaše aplikace a data) a sítí (tedy vším, k čemu jste sítí připojeni) na základě daných pravidel.
Většina moderních osobních fw je vybavena přednastavenými pravidly pro bezproblémové sdílení
pracovních složek v síti, síťovým tiskem a občas ani není potřeba nastavovat pravidla pro všeobecně
známé a používané aplikace jako je IE či ICQ. Nicméně pochopení funkce pravidel a tím jejich správné nastavení je jedinou zárukou správné funkce fw (Fw, který na základě špatného pravidla pouští veškerou komunikaci jistě neplní svoji funkci).
Naopak správně nakonfigurovaný fw je vysokou zárukou zabezpečení i po relativně dlouhou dobu
bez nutnosti zásahu či updatu.

Konzervativnost, zdravý rozum a podezíravost – jsou pak nejdůležitějším doplňkem všech těchto
doporučení. I na velmi kvalitně zabezpečeném počítači je možné spuštění malware a dát tak zelenou
jeho nekalé činnosti, pokud ignorujete hlášení a na všechny otázky odpovídáte *Ano*, *Ok*, *Příště již*

nezobrazovat, *Přijmout*, *Povolit*, *Spustit* a další.

Detekce a eliminace – aneb už je to tady..

Čím více budete podceňovat prevenci, tím častěji se budete nalézat v této fázi (v tom lepším případě
– tedy když přítomnost malware zjistíte). Nejčastěji získáte podezření na přítomnost malware při změně chování aplikací (zpomalení, vyskakování oken, neustálé pracování počítače i když „nic neděláte“, nenačítání správných stránek, atd atd..). Pak přichází chvíle hledání příčiny.

Antivirový program – asi nikoho nepřekvapí, že základním nástrojem pro vyhledání a vymazání malware v počítači je právě AV. Jeho rezidentní štít hlídá všechny aktivní procesy a přístupy k souborům, čímž dokáže detekovat **známý** malware ještě před jeho spuštěním (resp. zanesením do počítače). Díky tomu již není nutné plánovat test celého počítače na každé ráno, ale spíše po každém důležitějším updatu.
Je důležité vědět, že AV rozeznává malware od regulérního software na základě určitých rysů (databáze vzorků a zkoumání chování atd.), které jsou přidávány AV společností formou updatů. Tzn. AV většinou není schopen rozpoznat malware, pokud ho nemá ve své databázi. Dále potřebuje
informace jak nalezený malware vyléčit (to se týká vlastně jen virů; nejčastější dnešní forma malware je samostatný soubor, tj. léčení odpovídá smazání). To z AV dělá dobrý samostatný a jednoduše použitelný nástroj, není však na místě podléhat nějakému falešnému pocitu nenapadnutelnosti.

Další detekční prográmky (AntiSpy, ...) – díky velkému rozkvětu a různorodosti malware (už to
nejsou jen viry) se objevily další programy (většinou menší, jednodušší než AV a tím i levnější či zdarma), specializované jednak na některé časté druhy malware, ale také na odstraňování jejich řádění (přenastavená výchozí stránka v prohlížeči, nastavení důvěryhodných zón, přesměrování DNS pomocí souboru hosts, a další), čímž se např. AV skoro vůbec nezabývají.
Rozmach těchto menších pomocníků (zvláště těch zadarmo) je na internetu tak velký, že se již objevily nedůvěryhodné až škodlivé exempláře. Je vhodné se proto držet osvědčených „značek“ a příliš neriskovat.

Osobní firewall – ačkoliv eliminace malware není primárním úkolem fw, tak jeho detekční a blokovací schopnosti přijdou v nouzi právě vhod.
Největší výhodou osobního fw (oproti např. firemnímu fw mezi firemní sítí a internetem) je možnost získání informace, který proces (spuštěný program) se snaží na síti komunikovat. Standardní gateway fw (fw oddělující sítě) tuto informaci získat nemůžou a tak jsou odkázáni pouze
na informace obsažené v posílaných datech (packetech; hlavičky odkud a kam, jaký protokol, jaké
porty). Bohužel normální komunikace (např. prohlížení stránek) vypadá mnohdy úplně stejně jako
nekalá komunikace malware.

Osobní fw však pozná rozdíl jestli komunikuje IE, ICQ klient nebo nějaký druh malware. Správně
nakonfigurovaný osobní fw tak téměř úplně znemožňuje síťovou práci malware a mnohdy vede k jeho snadné detekci. Důležité je si uvědomit, že k této detekci nepotřebuje žádné aktuální updaty, nicméně taky je důležité si uvědomit, že rozhodnutí, zda-li je detekovaná komunikace součástí nekalé práce malware, je jen na vás (zda-li tento program znáte, či vám přijde krajně podezřelý). Bohužel tyto rozhodnutí nejsou zvláště ze začátku příliš snadná a vyžadují nějaký čas strávený vyhledáváním informací či monitorováním podezřelých procesů.

Konkrétní programy

V tomto textu se zabývám pouze obecnou charakteristikou skupin programů a jejich možným použitím. Informace o konkrétních programech a odkazech na ně získáte např. na serveru Viry.cz, v
tamním fóru (http://www.viry.cz/forum/) v sekci Důležité informace.