

9 Malware a antimalware

Obsah hodiny



Obsahem této hodiny je seznámení se s různými typy malware a s ochranou proti nim.

Cíl hodiny



Po prostudování budete schopni:

- vyjmenovat a charakterizovat různé typy malware
- objasnit možnosti ochrany proti malware
- orientovat se v antimalware
- objasnit fungování antivirových programů

Klíčová slova



Počítačový virus, Worm, Trojský kůň, Spyware a AdwareBackdoor, Exploit, Rootkit , Hoax

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. Tyto skupiny se často překrývají.

9.1 Virus

Je nejstarším typem 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).

Termín počítačový virus byl poprvé použit v roce 1972, ve vědecko-fantastickém románu spisovatele Davida Herolda „When Harley Was One“. V tom smyslu v jakém ho známe dnes, byl poprvé definován Fredem Cohenem v roce 1983. První virus na počítačích třídy IBM PC s operačním systémem MS-DOS se objevil v lednu 1986 - pákistánský virus Brain.

Viry se dělí podle různých kritérií. Jedním ze základních je rozdělení virů podle toho, co napadají:

- **Boot viry** – napadají boot sektor, MBR a tím si zajistí své spuštění hned při startu počítače
- **Souborové viry** – jejich hostitelem jsou soubory, podle způsobu infekce se dělí
 - na přepisující,
 - parazitické
 - doprovodné
- **Multipartitní viry** - napadají boot sektor i soubory
- **Makroviry** – šíří se v prostředí aplikací podporují, které podporují makra (MS Word, MS Excel)

9.2 Červ (worm)

Je samostatný program, který ke svému šíření využívá bezpečnostní chyby nebo důvěřivé uživatele (červi v přílohách emailů). Po prvotním spuštění modifikuje systém tak, aby byl spouštěn při každém startu systému.

Šíří se ve formě síťových paketů od úspěšně infikovaného systému na další systémy v síti internet. Pokud takový paket dorazí k systému se specifickou bezpečností dírou, může dojít k jeho infekci a následně i k produkci dalších „červích“ paketů.

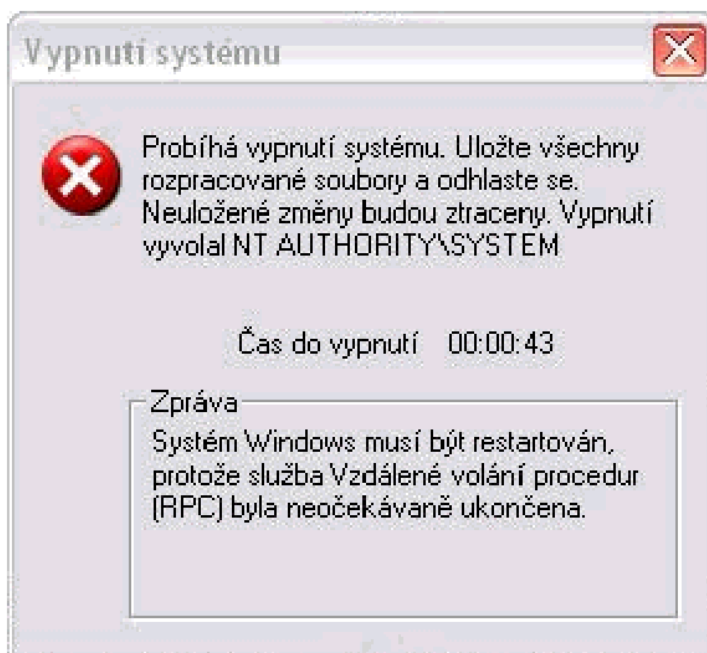
SQL Slammer (2003)

Zneužíval bezpečnostní díru v aplikaci Microsoft SQL server. Neprováděl žádnou destruktivní činnost, jedinou viditelnou nepříjemností byla schopnost 100% zahltit celou síť díky obrovské produkci UDP paketů.

Za 12 hodin bylo jedno infikované PC s dostatečně dobrým připojením schopno proskenovat všechny veřejné IP adresy celého internetu.

Lovsan / Blaster

Známý červ, který se objevil 11. 8. 2003 jako anomálie v podobě restartujících se Windows s minutovým odpočtem. Ještě více by se proslavil, kdyby mu vyšel úmysl s hromadným DDoS útokem na server windowsupdate.com.



Obrázek 9-1: MS Windows XP bez příslušné bezpečnostní záplaty po napadení červem Lovsan / Blaster.

Všechny červem infikované stanice měly 16. 8. 2003 zahájit společné "bombardování" serveru obrovským množstvím síťových paketů.

Microsoft celou situaci velmi elegantně vyřešil tak, že odstranil server windowsupdate.com z DNS záznamů a stanice tak nedokázaly cíl lokalizovat.

Denial of Service (DoS) jsou síťové útoky, které brání přístupu ke službám:

- zaplavováním spojení,
- zhroucením serverů nebo programů běžících na serverech,
- vyčerpáváním zdrojů na serveru ...

Záplavový útok: zdroje na serveru nebo na síti jsou narušeny nebo vyčerpány záplavou paketů. Distributed DoS (DDoS) útok, je nástroj pro mnoho záplavových útoků.

9.3 Trojský kůň (trojan horse)

Je program, který se vydává za legitimní software nebo je jeho součástí. Nereplikuje sám sebe a neinfikuje soubory. Šíří se pomocí kopírování takového software, nebo často pomocí jiných druhů malware (*dropper*).¹

¹ **Dropper** – „vypouštěč“ nese ve svém těle jiný škodlivý kód (například virus), který je vypuštěn po aktivaci trojanu do systému.



Obrázek 9-2: Trojský kůň

Nejčastěji vystupuje pod spustitelným souborem typu exe, který obsahuje jen samotné „tělo“ trojského koně.

Odstraníme ho odmazáním dotyčného souboru.

9.4 Programy shromažďující data

Existuje řada malware, který je zaměřen na sběr informací. Liší se tím, jaká data a za jakým účelem je shromažďují. Jedná se často o následující data:

- části registru systému (uživatelé často pracují pod účtem administrátora),
- IP adresu uživatele, někdy i MAC (fyzickou) adresu,
- historii prohlížených stránek,
- informace o software a multimediálních souborech, které jsou na počítači,
- seznam otevíraných souborů,
- celé dokumenty,
- uživatelova hesla.

Spyware a adware

Spyware je program, který shromažďuje informace o uživateli a odesílá je bez jeho vědomí útočníkovi (mnohdy se jedná např. o reklamní společnost, která takto získává informace pro cílenou reklamu). Spyware se často šíří jako trojský kůň – nejčastěji jako součást shareware.

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

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 bankovníctví, atd.).

Antivirem bývá považován za virus.

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.

K odstranění slouží některé antivirové programy nebo programy pro detekci a odstraňování spyware.

Ochrana

Existují programy, které umějí najít adware, spyware a další podobný malware, odstranit ho z počítače nebo uložit ho do tzv. karantény.

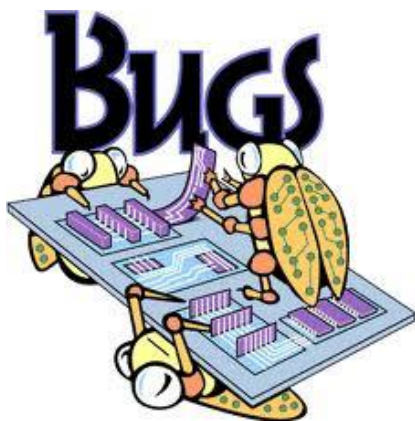
- Ad-Aware (Lavasoft),
- CounterSpy (Sunbelt Software),
- Spybot Search & Destroy (Patrick Koll),
- SpySweeper (Webroot),
- Spyware Doctor (PCTools),
- AVG Anti-Spyware (Grisoft),
- Trend Micro Anti-Spyware (Intermute),
- ...

Takovéto programy obsahují určitou databázi spywaru a adwaru a fungují tak, že prohledávají pevný disk, registry i paměť a detekují a identifikují malware právě podle databáze spywaru a adwaru,

Pozor, nejedná se o antivirový program !!!

9.5 Exploit

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



Obrázek 9-3: Chyby v programu ... bugs

Existují programy (např. Secunia Personal Software Inspector), které prohlédnou pevný disk PC a hledají aplikace, které mají zavedené ve své databázi jako "děravé".

Upozorní na ně uživatele a nabídnou instalační soubor či odkaz na záplatu, která daný problém řeší.

Je důležité sledovat vydávání záplat a instalovat je. I OS je sw, který obsahuje chyby. Prostřednictvím aktualizací (instalací záplaty) jsou odstraňovány.

9.6 Backdoor

Program umožňující vzdálenou kontrolu počítače útočníkem.

- Zadní vrátka jsou součástí softwaru a mohou být využívána k seriózním účelům (např. pro servisní přístup)
- nebo se může jednat o zapomenutou pomůcku pro ladění programu.
- Často jsou zneužívána (crackerem jako exploit), takže jsou klasifikována jako bezpečnostní riziko.

Může se šířit se jako trojský kůň nebo jako červ. Některé backdoory modifikují systém tak, že počítač začne rozesílat nevyžádanou poštu (*spam*).

9.7 Rootkit

Poněkud komplexnější software nahrávaný útočníkem na dobytí systém. Obsahuje různé nástroje pro ovládání systému a případné další útoky.

Maskuje přítomnost malware tak, aby nebyl běžně dostupnými systémovými prostředky odhalitelný. Za tím účelem obsahuje různé nástroje pro ovládání systému. Např. nástroje umožňující skrývat běžící procesy, soubory a systémové údaje.

Existují aplikace, které si kladou za cíl rootkit odhalit a zneškodnit ještě před vstupem do počítače.

V případě, že se rootkit již do počítače dostal, používají se specializované anti-rootkit balíčky určené pro odstranění konkrétního rootkitu.

Aplikace RootkitRevealer (Sysinternals)

Produkt pro obecné výhledávání skrývajících se aplikací (tedy i rootkitů). Vyžaduje určité znalosti uživatele, ten rozhoduje, zda jde o rootkit

Program provede průzkum PC (souborů, registru...) na co nejnížší úrovni operačního systému. K souborům přistupuje na úrovni diskového ovladače a k registrům pak jako k datovému souboru na disku.

Následně porovnává informace získané z těchto dvou úrovní a vyhodnocuje zjištěné rozdíly, které mohou být mimo jiné výsledkem působení rootkitu.

9.8 Hoax

Slovem hoax označujeme poplašnou zprávu, která obvykle varuje před neexistujícím nebezpečným virem.

Šíření poplašné zprávy je zcela závislé na uživatelích, kteří takovou zprávu e-mailem obdrží přepošlou ji dál.

9.9 Botnet

Program, je tajně nainstalován na uživatelském počítači, obsahuje komunikační a řídicí modul a umožňuje neautorizovanému uživateli

- měnit svoji funkčnost přidáním nového kódu nebo změnou stávajícího
- vzdáleně počítač ovládat a využít pro plnění různých příkazů.

Termín bot je odvozen od slova českého původu „robot“ a stejně jako robot je využíván pro různé „práce“. Pro počítač infikovaný botem se někdy používá termín „zombie“ (živá mrtvola) – stroj ovládaný útočníkem bez vědomí uživatele. Dle odhadů ovládají útočníci sedm procent z celkového počtu počítačů na celém světě, tj. cca 47 milionů strojů.

Počítače (mnoha různých uživatelů!) infikované stejným botem jsou sdružovány do sítě bot networks – botnet, někdy označovanou jako armáda zombie, kterou lze automatizovaně řídit prostřednictvím nástrojů vzdálené správy pro spuštění koordinovaného útoku.

Programů typů bot se vyskytuje celá řada. Podle odhadů antivirových společností se počet botů blíží k tisíci v rozmezí od velmi jednoduchých až po velmi složité.

Trendem dnešní doby je stírání hranic mezi jednotlivými typy malwaru. Některé boty mohou mít formu trojských koňů, jiné vykazují vlastnosti virů a jsou schopny se samy o sobě šířit; může se jednat i o kombinovanou hrozbu, např. spojení červa s botem.

Přes veškerou podobnost se však boty liší od virů, tak i od rootkitů. Klasický vir byl jednou naprogramován a má neměnnou funkčnost. Od rootkitů se boty liší masovým způsobem ovládnutí – jedním příkazem se komunikuje s řadou počítačů; u rootkitů tomu tak obvykle nebývá.

Aby bot mohl plnit požadované příkazy, musí komunikovat se svým řídicím orgánem, nejčastěji s autorem–hackerem. Boty mohou být ovládány několika různými způsoby, např. přes P2P (Peer to Peer) síť či diskusní skupiny, avšak nejběžněji přes chatovací kanály IRC (Internet Relay Chat). Jakmile je bot aktivován, připojí se na předem dohodnutý IRC server a čeká na příkazy, které hacker zapisuje do chatovacího kanálu.

Sítě botů se podílejí na útocích

- Denial of Service (DoS, odepření služby).
- Šíření spamu (dle skupiny Gartner Group je 70 procent spamu rozesíláno právě z botnetů). Pro spamemry je výhodnější a bezpečnější rozesílat spam z obrovské distribuované sítě.
- Phishing
- Sniffing.- bot modul změny napadený počítač v odposlouchávací stanici, jejímž prostřednictvím monitoruje síťový provoz a získaná data posílá hackerovi.
- Keylogger“.

Sítě botů se stále častěji uplatňují při šíření nového malwaru, jak červů, tak virů. Pro hackera je důležité, aby se nový kód rozšířil co nejrychleji. Proto je nutné jej na počátku epidemie začít rozesílat z co největšího počtu míst.

9.10 Antivirové program

Základním nástrojem pro vyhledání a vymazání malware v počítači jsou antivirové programy (AV).

AV rozeznává malware od regulérního software na základě určitých rysů (databáze vzorků a zkoumání chování atd.), které jsou přidávány AV společnostmi formou updatů. Pozor! 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). Z uvedených důvodů je proto velmi důležité AV pravidelně aktualizovat. Pokud je počítač připojen k Internetu, lze provádět aktualizace automaticky.

Antivirový program umí kombinovat několik druhů ochrany. Patří mezi ně:

- **antivirový monitor**, který umí na pozadí (on-line) kontrolovat otevírané soubory;
- **integrity checker (kontrolní součet)**, který umí zaznamenat modifikace souborů a adresářů, jež mohou indikovat napadení virem;
- **heuristická analýza**, jež vyhledává viry ne pomocí typické sekvence kódu, ale pomocí jejich chování a projevů.

Obvykle se kombinuje více metod, záleží na uživateli, jak si antivirový program nakonfiguruje:

- Rezidentní sledování je obvykle neustále spuštěno na pozadí
- V pravidelných intervalech podle nastavení uživatele se provádí kompletní kontrola souborů na pevných discích.
- Provádí se kontrola integrity všech souborů.
- Časově náročné heuristické analýzy se provádí pouze u změněných souborů.

Antivirový monitor: **porovnání s databází virů (skenování, scan)**

AV program využívá vlastní databázi známých virů. Testuje prohledávané soubory na výskyt určité posloupnosti bytů, která identifikuje vir z databáze. Jedná se o nejstarší a stále pravděpodobně nejrozšířenější způsob detekce napadení virem. Tato metoda umožňuje nalezení pouze těch virů, které jsou již zaneseny v databázi známých virů.

Databáze musí být proto pravidelně aktualizována, aby bylo skenování skutečně účinné.

Kontrola integrity

Při prvním spuštění si AV vytvoří databázi souborů a při dalších spuštěních srovnává aktuální stav souborů s příslušnými položkami ve své databázi a zjišťuje, zda se od posledního průchodu nezměnily. Uložením viru do některého souboru totiž dojde ke změně souboru.

Výhodou kontroly integrity je možnost nalezení dosud neznámého viru.

Nevýhodou je, že antivirový program nedokáže sdělit, že našel vir, ale pouze že došlo ke změně v souboru.

Záleží na uživatelově úsudku, zda se jedná o virový útok.

Heuristická analýza

AV program umí analyzovat kód souboru a jeho význam. Hledá v něm postupy, které jsou typické pro viry a které se v normálních programech nevyskytují.

Výhodou této metody je možnost nalezení virů, které ještě nebyly analyzovány a zaneseny do databáze virů.

Nevýhodou je možnost omylu a "nalezení" viru v souboru, který není virem napaden.

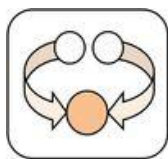
Rezidentní štít

Hlídá všechny aktivní procesy a přístupy k souborům, čímž dokáže detekovat známý malware ještě před jeho spuštěním (resp. zanesením do počítače). Když chce uživatel spustit některý program, antivirový program nejprve zkontroluje, zda neobsahuje virus.

V systému je neustále spuštěn proces, který kontroluje prováděné operace. Mohou být sledovány podezřelé operace se soubory a systémovými oblastmi disku.

Například při pokusu o zápis do boot sektoru je operace přerušena a uživatel dotázán, zda zápis povolí. Díky tomu již není nutné plánovat test celého počítače na každé ráno, ale spíše po každém důležitějším updatu.

Shrnutí kapitoly



Malware je všeobecné označení pro záměrně škodlivý kód, nejstarším je počítačový virus.

Počítačový virus je program, který vkládá sám sebe do jiných programů: spustitelných souborů (exe, com). „datových“ souborů (např. v dokumentech MS Office).

Základní rozdělení virů:

- Boot viry
- Souborové viry
- Multipartitní viry
- Makroviry

Další druhy malware:

- Červ
- Trojský kůň
- Backdoor
- Exploit
- Rootkit
- Hoax
- Spyware
- Adware
- Keylogger
- Dialer
- Botnet

Ochranou proti malware je antimalware. Jedná se o SW, který slouží k identifikaci, odstraňování a eliminaci malware, zejména počítačových virů.

Komplexním nástrojem pro ochranu počítače jsou antivirové systémy. Disponují řadou nástrojů pro detekci a identifikaci malware (nejen virů). Uživatel by je měl znát a měl by být schopen je správně nakonfigurovat.

Pro detekci malware používá řadu různých technik:

- porovnání s databází virů (skenování, scan),
- heuristická analýza,
- sledování změn (kontrola integrity),
- rezidentní sledování,
- detekce podezřelé aktivity nějakého počítačového programu.

Je velmi důležité AV pravidelně aktualizovat.

Kontrolní otázky a úkoly



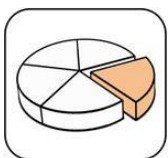
- 1) Co je to malware?
- 2) Charakterizujte viry.
- 3) Co je to spyware a adware, jak se proti nim chráníme?
- 4) Co je to Keylogger?
- 5) Co je to Backdoor?
- 6) Co je to Botnet?
- 7) V čem spočívá nebezpečí rootkitů?
- 8) Jaké techniky používají antivirové systémy

Otázky k zamyšlení



- 1) DoS (DDoS) útoky

Použitá literatura a jiné zdroje:



- [1] NYKODÝMOVÁ, Helena. Botnety: nová internetová hrozba. *Lupa.cz* [online]. 31. 5. 2006 [cit. 2012-03-22]. Dostupné z: <http://www.lupa.cz/clanky/botnety-internetova-hrozba/>
- [2] HÁK, Igor. *Moderní počítačové viry*. třetí vydání. Hradec Králové: Fakulta informatiky a managementu – Katedra informatiky a kvantitativních metod, 2005. Dostupné z: <http://www.viry.cz/download/kniha.pdf>