Viry

+ antivirové programy

Historie virů – r. 1986

První virus pro IBM PC - virus Brain

Pákistánští bratři Basít a Amjád zjistili, že se dá změnit obsah boot sektoru diskety, který je vykonán vždy při spuštění OS z diskety (tzv. bootování). Tento nový kód se může naistalovat jako rezidentní program do paměti a pak sám sebe kopírovat na každou disketu přistupovanou přes mechaniku.

Tento kód nazvali **virus**.

První skutečný virus – Charlie nebo Vienna – v počítačovém programu Charlie byl kód, který s pravděpodobností 1:8 po spuštění napadeného souboru rebootoval PC.

Počítačový virus

Malware =Malign Software = škodlivý software.

Počítačový program, který se šíří, aniž by o tom uživatel věděl.

Viry umí jen to, co jakékoliv ostatní programy. Jsou jen vytvořeny pro škození.

Není pravda, že viry dokáží ničit monitory, pevné disky, procesory.

Je pravda, že dokáží simulovat poruchu těchto zařízení.

Definice viru

- program → má vždy autora
- šíření - záznamová média, síť
- činnost - bez vědomí a přání uživatele - ničení dat, pozměnění dat (nejhorší), blokování
- schopen se samostatně šířit → množit se - zapisuje svojí funkční část do jiných programů nebo do určitých míst na paměťových médiích
- dnes - zapisování do dokumentů - makroviry

Počítačový virus je spustitelný program, který je schopen sám sebe připojovat k jiným programům a dále se z nich (bez vědomí uživatele) šířit.

Projevy virů

- obtěžující chování – zpomaluje práci PC – pro své šíření, aktivaci a další "práci" potřebuje část systémových prostředků
- blokování místa v paměti
- grafické a zvukové projevy
- "žertovné" – nápisy na monitoru, padající písmena, záměna písmen, chod hodin pozpátku
- nestabilita systému – časté padání některé aplikace nebo zamrzáním celého systému
- poškození OS nebo dat - triviální vir přepíše bez varování obsah celého disku – pomůže záloha, zákeřnější pomalu a nenápadně mění data – záloha může obsahovat již také poškozené soubory

dnes – počítačové sítě

- krádež dat
- šifrování dat – vydírání – smazání viru znamená ztrátu dat

Části počítačového viru

- reprodukční část – zajišťuje šíření – základní a nejdůležitější část

ostatní části nejsou povinné :

- analytická část – zkoumá PC a zjišťuje potřebné parametry :
  - přítomnost antivirového programu, aby se jej pokusil vypnout nebo se mu vyhnout
  - nechráněná síť pro další šíření
- akční část – destrukce dat …
- spouštěcí mechanismus – "start" pro virus – virus čeká na konkrétní hodinu, datum, x-sté otevření souboru s virem - vir CIH (Černobyl) vždy 26.4.
- maskovací část – nenápadnost – snaží se měnit podobu, šifrovat se, vyskytovat se na neobvyklých místech (nápověda, HTML dokumenty)

Výroba virů

Na začátku – hluboké programátorské znalosti

Dnes - generátory virů – speciální programy na Internetu – na základě předdefinovaných údajů vytvoří virus

Rozdělení virů - dle napadených objektů

- Bootviry – napadají pouze systémové oblasti (Partition tabulka, boot sektor HDD nebo FDD)
- Souborové viry – napadají pouze soubory (obvykle soubory s příponou EXE, COM, SYS …)
- Multipartitní viry – napadají soubory i systémové oblasti
- Makroviry – napadají soubory, které mohou obsahovat makra (texty ve Wordu, Excelu) – nejnovější z r. 1995 – nejnebezpečnější virový problém

Rozdělení virů - dle manipulace s objekty

- přepisující virus – část těla oběti přepíše vlastním kódem – programy jsou nenávratně zničeny a jsou schopny pouze dalšího šíření viru
- link virus – připojí se k tělu oběti (před, za, doprostřed) a může tak zachovat původní funkce programu
- doprovodný virus – nezapisuje svůj kód přímo do napadeného EXE souboru, ale vytváří soubor stejného jména s příponou COM (využívají, že MS DOS dává přednost COM souborům před EXE)

Rozdělení virů –speciální vlastnosti

- virus přímé akce – vykoná vše a skončí (přepisující virus)
- rezidentní virus – je přítomen v paměti a může ovlivňovat neustále činnost PC, virus si nemusí hledat sám programy k napadení, sleduje soubory s nimiž uživatel pracuje a útočí na ně
- Stealth (tajný) virus – schovávají se a kódují - svojí činnost maskuje (modifikuje datum)
- fast infektor – rezidentní virus, který napadá soubory při jejich spouštění i při jakékoliv manipulaci s nimi
- slow infektor – šíří se co nejobezřetněji – napadají pouze nově vytvářené soubory

Další "viry"

E-mailoví či internetoví červi (worms) – v podstatě virus, který pro své šíření využívá služeb elektronické pošty nebo přímo Internetu - škodlivé skripty, download infikovaných souborů

Trojský kůň – programy, které vykonávají činnost, kterou uživatel očekává, a zároveň činnost o níž nemá tušení – př. sledujete video a zároveň tentýž program odesílá data z vašeho PC nebo je kóduje

Zadní dvířka (backdoor) – aplikace, které otevírají útočníkům PC – data nebo PC jako prostředek k dalším útokům

Antivirové techniky - I

- ***metoda scanovací = vyhledávací*** - hledá se charakteristický kód - pouze pro známé viry - podle databáze virů
- ***Test integrity*** – sleduje stav systému a vyhodnocuje změny souborů, systémových oblastí a obsahu adresářů a sdělí uživateli „zjištěna změna“– nevýhoda virus se zachytí až při šíření v systému
- ***heuristická analýza*** - místo kontroly sekvence znaků se sleduje spuštěný program a podle toho, co dělá, se usuzuje na vir – nejperspektivnější - není závislý na tom, zda je virus známý či ne – zachytí až 70% novinek

Antivirové techniky - II

- ***Léčky na viry*** – úmyslné simulování operací, na které by virus v PC reagoval – vytvoření a spuštění programu a kontrola velikosti a obsahu
- ***Rezidentní kontrola PC*** – program se startuje co nejdříve po startu PC a převezme kontrolu nad službami operačního systému (diskové operace a operace se soubory) – pro každodenní práci, ne pro důslednou antivirovou ochranu
- ***Kombinace technik*** – efektivní antivirový program musí obsahovat více funkcí – scanner pro rychlou kontrolu na známé viry, heuristickou analýzu pro detailnější, časově náročnější test, test integrity spouštěný v pravidelných intervalech pro posouzení korektního vzniku změn a doplněný o rezidentní kontrolu.

Antivirové programy

AVG
Kaspersky Anti-Virus
F-Secure Antivirus
F-PROT
TBAV
SCAN
pro sítě NET-PROT
Avast
Norton AntiVirus
McAfee Viruscan

Zásady antivirové ochrany

- Používejte antivirový program
- Pravidelně aktualizujte
- Pozor na přílohy u elektronické pošty – př. obrazek.jpg.exe
- Pravidelně získávejte informace – www.viry.cz, www.virusbtn.com, www.grisoft.cz, www.viruslist.com
- Pravidelně zálohujte
- Nedůvěřujte nikdy, nikomu a ničemu
- Dodržujte tato pravidla

Co je to HOAX ?

HOAXy = poplašné zprávy

Varování před nějakým extrémně nebezpečným, dramaticky rychle se šířícím virem a následujícím požadavkem na nějakou uživatelskou akci.

V lepším případě vyzývají adresáta zprávy k jejímu přeposlání na všechny známé a partnery.

V horším případě vyzývají uživatele ke smazání údajného viru, přičemž údajným virovým souborem bývá někdy naprosto regulérní systémový soubor, jehož smazání může vést i k vážným problémům (nefunkčnost některých aplikací, celého systému, atp.)

Nejlepší obranou uživatele elektronické pošty je vlastní rozum + informace - **www.hoax.cz**