

Vírusy

a


antivírusové systémy






Vírusy

Vírus má nasledovné typické vlastnosti:

 je schopný samostatne sa množiť (t.j. vytvárať svoje funkčné kópie, ktoré prostredníctvom siete alebo výmenných pamäťových médií napádajú iné programy)

 nemôže existovať ako samostatný súbor, ale na svoju existenciu potrebuje hostiteľský program, ktorý napadne, ukryje sa v ňom a využíva ho na svoje spustenie v operačnej pamäti. Ukrýva sa do súborov, alebo do systémových oblastí diskov a diskiet („boot sektory“).

Virusy

V praxi sa stretávame aj s ďalšími formami počítačových infiltrácií, ktoré síce vykazujú s vírusmi mnohé spoločné znaky a často bývajú s vírusmi zamieňané, ale niektorými svojimi vlastnosťami a prejavmi sa od vírusov odlišujú:

Trojský kôň

Červ

Makrovírusy

Bootovacie vírusy

Hoax



Trójsky kôň (Trojan Horses)



Trójsky kôň (Trojan Horses)

je program ktorý na pozadí vykonáva činnosť o ktorej vôbec netušíme. K pôvodnému obsahu spustiteľného súboru sa pripojí tak, že užívateľ po jeho spustení ani nespozná že nejaký vír aktivoval. Je samostatným programom ktorý nepotrebuje žiadneho hostiteľa, ale nedokáže sa šíriť sám k tomu využije napr. e-mail červa. Príklad: po spustení na prvý pohľad neškodného šetriča obrazovky síce vykoná k čomu bol určený ale skryte sa snaží pripojiť k internetu a odoslať súbory/heslá s vášho počítača.

Makrovirusy



Pre zvýšenie užívateľského komfortu sa rozhodla firma Microsoft zakomponovať do svojho produktu MS Office (Word, Excel...) programovací jazyk Visual Basic for Application. Pomocou neho môžu vytvárať makrá, preto dostali pomenovanie makrovírus, makrá umožňujú spúšťať programový kód v dokumentoch automaticky hneď pri otvorení dokumentu. Ich šírenie je jednoduché stačí ak si otvoríte infikovaný document.

Červy (Worms)



Dnes sa pojmom červ definujú virusy, ktoré sa šíria prostredníctvom internetu (el. pošty), využívajúc bezpečnostných medzier operačných systémov alebo aplikácií (napr: e-mail klienta).

Nie sú to pravé červy typu “Code Red”, ale nijak za nimi nezostávajú. Nazývajú ich aj e-mail červy. Využívajú chyby e-mailového klienta (najpoužívanejším je MS Outlook) a dokážu sa šíriť/spustiť aj bez toho žeby boli spustené – stačí ak máte u poštového klienta aktivovaný “náhľad” správy. Typickou vlastnosťou vírusov šíriacich sa poštou sú falšovanie adresy odosielateľa. Obranou je deaktivovať automatický náhľad a neotvárať pochybné správy, prípadne ich najskôr preveriť antivírusovým programom. Rovnako dobré je pravidelne aktualizovať najnovšie update operačných systémoch ktoré odstraňujú bezpečnostné medzery. Úlohou alebo podstatou červa je získať určitý stupeň kontroly nad vaším PC za účelom získania dát, či použiť k iným úlohám.

Backdoor



V preklade zadné dvierka, už názov napovedá, že jeho úlohou je “otvoriť” počítač k útokom z vonku (internetu). Ak útočník prevezme čiastočnú/úplnú kontrolu nad vaším pc, v horšom prípade nad celou sieťou následky môžu presiahnuť vaše očakávania (len malý príklad použije vás ako útočníka na nejaký dôležitý server, alebo ukradne prístupové kody k vašim bankovým účtom).

Hoax – poplašná správa



Šíria sa prostredníctvom e-pošty, využívajúcich neskúsenosť užívateľov.

Príkladom uvedieme :

Nepredstavujú žiadny programový kód ale väčšinou sa jedná o jednoduchú správu vyzývajúcu k vymazaniu súboru o ktorom tvrdí, že sa jedná o vírus. Užívateľ ho v dobrej viere vymaže, pričom ide o súbor patriaci operačnému systému potrebnému k jeho chodu. Vymazaním už nebude fungovať korektne, prípadne vôbec.

Klasický vírus



Najčastejšie majú príponu .exe, ktorú potrebujú spustením aktivovať, no v podstate sa môže jednať o akýkoľvek spustiteľný súbor (.com, .sys). Často sa skrývajú za spakovanými súbormi zip a rar, či viacnásobnými názvami ako napr.: obrázok.gif.exe. Neskúsený užívateľ si myslí, že otvára neškodný obrázok, no neuvedomuje si, že skutočný typ súboru definuje až posledná prípona, všetko pred ňou tvorí názov súboru. O to nebezpečnejšie pokiaľ máte aktivované v systéme “*skrývať koncovky známych súborov*” to príponu .exe neuvidíte vôbec. Po aktivovaní vírusu obvykle vyhľadá a napadne, prípadne poškodí súbory. Infikované súbory prenesú užívatelia do iného PC kopírovaním na médium (hdd, cd/dvd...). K aktivácii vírusu dôjde spustením nakazeného súboru, navyše dokáže sám seba klonovať (kopírovať) a vložiť sa do ďalších programov.



Druhy vírusov

- **Rozdelenie na rezidentné a nerezidentné**

Rezidentné – ak sa dostanú do OP spolu s hostiteľským programom, prevezmú riadenie počítača a ostávajú natrvalo v OP, teda aj po ukončení behu hostiteľského programu. Počas svojho pôsobenia napádajú ďalšie spúšťané programy a vykonávajú rôzne akcie.

Nerezidentné – po preniknutí do OP okamžite vykonajú činnosť – kopírovanie, príp. inú akciu a odovzdajú riadenie hostiteľskému programu. Neostávajú aktívne v OP. Nie sú veľmi rozšírené.



Druhy vírusov

Rozdelenie podľa napádaných oblastí



Súborové

Bootovacie vírusy



Druhy vírusov

Súborové

Napádajú a infikujú súbory, ktoré potom slúžia ako „hostitel“, poskytujú vírusu úkryt a umožňujú vírusu spúšťať sa v OP. Vždy musí ísť o spustiteľné súbory, najčastejšie typov .com, .exe, .ovl, .bin, .obj, .prg atď.

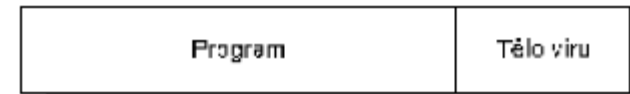
Podľa spôsobu, akým vírusy napádajú hostiteľské súbory, ich ďalej delíme na:

1. Predlžujúce,
2. Medzerové,
3. Prepisujúce,
4. Duplikujúce,
5. Makrovírusy.



Druhy vírusov

Predlžujúce



vírus sa umiestni buď celý na začiatok súboru, alebo na začiatok umiestni svoju hlavičku a telo uloží na koniec súboru. Hostiteľský program nie je vírusom zničený, normálne sa dokáže spustiť, ale spolu s ním sa spúšťa aj vírus. Zväčšenie veľkosti súboru je možné za normálnych okolností zistiť jednoduchým pohľadom cez Prieskumníka, Norton Commanderom, príkazom DIR a pod., ak však vírus používa techniku Stealth, dokáže všetky zmeny vykonané na súboroch ukryť.



Druhy vírusov

Medzerové

pre svoje ukrytie využívajú medzery v niektorých spustiteľných súboroch (napr. command.com), potom nedôjde k predĺženiu hostiteľského súboru.

Duplikujúce

hostiteľský program nezničia, ale vytvoria si jeho kópiu a tú napadnú. Zabezpečia, že nie je spúšťaný „originálny“ program, ale jeho infikovaná kópia.



Druhy vírusov

Prepisujúce vírusy

nepredlžujú veľkosť súboru, ale hostiteľský program priamo prepíšu vlastným kódom („telom“). Potom sa hostiteľský program stáva nefunkčným, pokus o spustenie programu vyvolá len aktivovanie vírusu. Pôsobenie takého druhu vírusu v počítači rýchlo znefunkční väčšinu programov, čím sa ovšem vírus stáva nápadným a je rýchlo odhalený a zničený. Preto sa veľmi nerozširujú.



Druhy vírusov

Makrovírusy

sú vírusy napísané v jazyku Visual Basic ako makro niektorej aplikácie (Word, Excel, AmiPro, AutoCAD). Využívajú schopnosť spomínaných aplikácií uchovávať makrá ako súčasť dokumentu a takto dokážu napádať ďalšie dokumenty a šíriť sa pomocou nich. Mnohé makrovírusy majú schopnosť napádať dokumenty aj spustiteľné súbory – tým sa ich nebezpečnosť ešte zvyšuje. Nebezpečenstvo zo strany makrovírusov je umocnené ešte ďalšími efektami:

Dokumenty patria k najviac vymieňaným súborom; bez možnosti výmeny dokumentov stráca pre väčšinu užívateľov použitie výpočtovej techniky zmysel



Bootovacie vírusy

Tieto vírusy napádajú bootovacie oblasti diskiet a pevných diskov. Oproti súborovým vírusom sú v mnohých ohľadoch účinnejšie: Boot sektor je bežnými prostriedkami užívateľovi neprístupný, má ho každá disketa aj disk formátované MS DOSom, resp. Windows, sú tu umiestnené štartovacie súbory operačného systému, takže okamžite po štarte počítača sa obsah boot sektoru načíta do operačnej pamäti. Vírusy využívajúce boot sektor sú „agresívnejšie“ – vďaka umiestneniu sa dostávajú do operačnej pamäti okamžite po spustení počítača. Prostredníctvom boot sektorov sa infekcia ľahko šíri – infikovať je možné aj diskety, ktoré obsahujú iba jednoduché dátové, prípadne neobsahujú vôbec žiadne súbory. Odhalenie vírusov v boot sektore je obtiažnejšie, ako detekovanie súborového vírusu. Ďalšie nebezpečenstvo týchto vírusov spočíva v tom, že niekedy „omylom“ – chybou práce samotného vírusu - prepíšu FAT tabuľku či inú dôležitú oblasť, obsahujúcu údaje o uložených súboroch na disku a tým dôjde k nevratnej strate všetkých dát uložených na disku.



Infiltrácie šíriace sa e-mailom

Infikovaná príloha



Príloha obsahuje škodlivý spustiteľný kód, ktorý po pokusu o otvorenie prílohy sa načíta do RAM – spustí sa mechanizmus infekcie počítača. Obrana – neotvárať prílohy neznámych e mailov.



Infiltrácie šíriace sa e-mailom

Infikovaná príloha s dvojitou koncovkou



Predchádzajúca technika je „vylepšená“ o použitie dvojitej prípony súboru v prílohe. Využíva sa skutočnosť, že Windows sú štandardne nakonfigurované tak, že ukrývajú príponu (voľba sa dá jednoducho vypnúť, ale väčšina užívateľov necháva z pohodlnosti ukrývanie prípon zapnuté). Príloha s dvojitou príponou potom vyzerá napr. ako súbor „babusky.jpg.vbs“. Vďaka ukrývaniu koncovky sa zobrazí iba „babusky.jpg“ – pre užívateľa príloha vyzerá ako atraktívny obrázok, po jej spustení sa ale spustí v skutočnosti script napísaný vo Visula Basic – koncovka .vbs.



Infiltrácie šíriace sa e-mailom

Infikovaná príloha spúšťaná kódom z tela e-mailu



Predchádzajúce techniky sa spoliehali na neskúsenosť používateľa, ktorý „naletí“ na lákadlo a spustí si škodlivú prílohu sám. Bez spolupráce používateľa sa infekcia nespustí. Nová technika spočíva v tom, že samotné telo emailovej správy je napísané v kóde .html a obsahuje utilitu, ktorá aktivizuje spustenie prílohy okamžite po otvorení správy vo vhodnom prehliadači. Infekcia prebehne už jednoduchým otvorením správy na čítanie – bez otvárania prílohy užívateľom. Uvedenú techniku podporuje aj skutočnosť, že Outlook Express štandardne zobrazuje každú správu automaticky v okne náhľadu, takže škodlivý kód sa spustí automaticky iba pri nastavení kurzoru na hlavičku infikovanej správy. Obrana spočíva v neotváraní podozrivých e-mailov a zákaze používania náhľadového okna.



Infiltrácie šíriace sa e-mailom

Technika automatického rozposielania e-mailov zo zavíreného počítača



Aby vírus zabezpečil svoje efektívne množenie, nespolieha sa na neopatrnosť užívateľa, ale sám aktívne priamo vyhľadá a prečíta adresár s e-mailovými adresami na danom počítači a na objavené adresy rozpošle sám seba, pričom ako telo správy použije náhodné texty zo súborov na lokálnom disku. Ku vírusovej infiltrácii tak pribúda významné a nebezpečné narušenie súkromia, čo je kritické najmä v profesionálnej sfére. Na dokonalé zamaskovanie navyše vírus často sfaľšuje aj adresu odosielateľa (čiže v hlavičke zavírenej správy figuruje falošná, ale skutočná, podstrčená adresa odosielateľa - vírus použije náhodne adresu z adresára napadnutého počítača.



Antivírusy

Pri detekovaní vírusov používajú antivírusy viaceré metódy :

1. skenovanie.

2. heuristická analýza .

3. porovnávanie.

4. Rezidentné skenovanie.



Antivírusy

Skenovanie

- **On demand** prehľadáva klasickým antivírusovým skenerom celý pevný disk ako aj ďalšie záznamové média pripojené k pc (cd/dvd rom).
- **On access** testovanie každého súboru ku ktorému prístupujete v reálnom čase.

Oba prístupy v testovaných súboroch vyhľadávajú reťazce charakteristické pre už známe vírusy. Presnejšie povedané antivírusový program porovnáva reťazce kódov vírusov obsiahnuté v internej databáze programu s reťazcami v skenovaných súboroch. Ak nájde programový kód v súbore zhodujúci sa s kódom v databáze ohlásí vírus a pomenuje ho menom pod akým je v databáze uložený. Spoľahlivosť tejto metódy je plne závislá na aktualizácii vášho antivírusového programu, preto si ich pravidelne aktualizujte !





Antivírusy

heuristická analýza

funguje na princípe analýzy obsahu súboru, teda jeho naprogramovania. Monitoruje podozrivé aktivity programu, napr.: testovaný program sa snaží otvárať iné spustiteľné programy a zapisovať do nich. Preto ho označí ako podozrivý, tak môže nájsť aj nový, neznámy vírus. Taktiež môže za potenciálny vírus označiť súbor ktorý je v poriadku čím sa stane len zdrojom poplašnej správy.





Antivírusy

Porovnávanie

Antivírusový program si po inštalácii vytvorí databázu o súboroch uložených v pc. Potom porovná napríklad veľkosť spustiteľného súboru (.exe) keďže sú najčastejším terčom vírusov. Ak došlo k napadnutiu súboru teda aj zmene jeho programového kódu muselo prísť aj k zmene jeho veľkosti.





Antivírusy

Rezidentné skenovanie

Pri štarte PC sa do operačnej pamäte automaticky zavedie rezidentný antivírus, ktorý monitoruje – skenuje činnosť v PC. Pri neobvyklých operáciách – zápis do systémových oblastí disku, modifikovanie (zmena) spustiteľných súboroch a pod. upozorní užívateľa





Koniec