KOMPIUTERIŲ VIRUSAI

Kompiuterinio viruso sąvoka

- Įvairios kenkėjiškos kompiuterinės programos, sutrikdančios kompiuterio veikimą ar trukdančios dirbti, vadinamos bendru **kompiuterinių virusų** vardu. Programuotojo požiūriu virusas - tai kompiuterinis kodas, kuris savo plėtimusi turi pažeisti (infekuoti) kurią nors programą.
  Paprastai kompiuterinis virusas infekuoja kitas programas, įjungdamas į jas programos - viruso kodą. Virusas dauginasi ir, prisijungęs prie programų ar kitų bylų bei ten „pasislėpęs", „keliauja" nuo vieno kompiuterio prie kito. Virusai kuriami (programuojami), siekiant atlikti įvairius kenkėjiškus veiksmus: trinti standžioje disko informaciją keisti ar naikinti tam tikras bylas ir pan.
  Virusai gali slėptis diskelyje, standžiajame diske arba net kompiuterių tinkle.

Virusų tipai

- Šiuo metu žinoma labai daug virusų. Specialistai juos klasifikuoja pagal įvairius požymius. Vienas jų - viruso algoritmo ypatybės ir veikimo būdas. Pagal šį požymį virusai skirstomi į kelias grupes, iš kurių paminėsime tokias:
  - **tikrieji virusai** - mažos apimties programos, „prisiklijuojančios" prie kitų programų ir atgyjančios, kai infekuotoji programa ruošiama vykdyti. Jie užkrečia kitas programas, bet infekuotos programos dažniausiai veikia įprastai;
  - **programos - kirminai**, kurie visą laiką dauginasi, užimdamos vis didesnę atmintinės sritį, taip sutrikdydamos kompiuterio darbą;
  - **loginės bombos**, pradedančios veikti, įvykus konkrečiam loginiam įvykiui (pavyzdžiui, prisijungus prie tinklo naujam vartotojui);
  - **laiko bombos**, pradedančios veikti („sprogstančios") iš anksto numatytu laiku (pavyzdžiui, jei mėnesio 13 diena - penktadienis);
  - **Trojos arkliai** - programos, įterptos į kitas programas; jos atrodo kaip naudingos programos, tačiau atlieka kenkėjiškus veiksmus (pavyzdžiui, groja nustatytą melodiją);
  - **nematomi virusai** - programos, paslepiančios jų atliktus pakeitimus bylose ar išorinės atmintinės sektoriuose. Tie pakeitimai pakeičia sistemines funkcijas, kurias naudoja tas bylas ar sektorius skaitančios programos.

Virusų kenksmingumas

- Pagal kenksmingumo lygį virusai skirstomi į **nepavojingus, pavojingus** ir **labai pavojingus**.
  Nepavojingieji virusai kompiuterio darbui ypatingai nekenkia, tik į ekraną išveda įvairius pranešimus, imituoja įvairus garsus ir pan. Pavojingieji virusai gali gerokai sutrikdyti kompiuterio darbą, o labai pavojingi virusai naikina programas ir duomenis, ištrina reikalingą sisteminę informaciją (pavyzdžiui, bylų išdėstymo lenteles).
  Virusai, užkrėtę sistemą, gali jai pakenkti įvairiai:
  - sumažinti sistemos darbo greitį;
  - neleisti atlikti kai kurias operacijas (pavyzdžiui, įkelti sistemą);
  - nepastebimai modifikuoti duomenis (pavyzdžiui, sukeisti skaičius vietomis);
  - ištrinti kai kurias bylas;
  - sunaikinti bylų sistemą;
  - modifikuoti bylų sistemos duomenis (pavyzdžiui, katalogus, bylų išdėstymo lenteles);
  - fiziškai sugadinti kai kuriuos įrenginius (pavyzdžiui, nuolat rašant į tą patį disko takelį, nusitrina magnetinės medžiagos sluoksnis).

  Pagal užkrėtimo būdą virusai skirstomi į **rezidentinius** ir **nerezidentinius**. Rezidentiniai virusai savo programos dalį laiko pagrindinėje atmintinėje ir yra aktyvūs iki kompiuterio išjungimo.
  Nerezidentiniai virusai kompiuterio atmintinės neužkrečia ir yra aktyvūs tik tam tikrą laiko tarpą.

Kaip pasireiškia virusai?

- Infekuotos sistemos veikimas išoriškai pradžioje gali atrodyti kaip ir neužkrėstos. Tačiau vėliau gali atsirasti įvairūs sistemos darbo sutrikimai. Tai gali būti:
    - sistemos spartos pastebimas sumažėjimas;
    - nenumatytų programose simbolių, paveiksliukų, garsų ir kitų pašalinių efektų atsiradimas;
    - bylų turinio ir apimties pasikeitimas.

Kaip užsikrečiama virusais?

- Kompiuteriai vis dažniau užsikrečia virusais, - skelbia Tarptautinės kompiuterių saugumo asociacijos (ICSA) atliktas tyrimas. Jo duomenimis, nuo 1997 m. kasmet užsikrėtimų kompiuteriniais virusais padvigubėja. Didžiausią poveikį daro virusai, platinami elektroniniu paštu. Anot tyrimo, daugiausiai (56%) buvo užsikrėsta virusais elektroniniu paštu. Kažkada populiariausia virusų plitimo priemonė - diskeliai - tapo nebe tokia pavojinga: jie buvo kalti tik dėl 39% atvejų (palyginti su 80% prieš dvejus metus). Tik 16% virusų buvo „pasigauta" atsisiunčiant bylas iš Interneto.

Word virusai

- **Winword** sistemos dokumentų bylas (.doc tipo) puola virusai, kurie plinta per makrokomandas. Jie užkrečia naujus dokumentų bylas ir šablonų bylas (.dot tipo). Šiuo metu Cap yra vienas dažniausiai pasitaikančių Word Macro virusų. Cap nėra pavojingas, bet trukdo dirbti. Virusą dažniausiai sudaro dešimt užkoduotų makrokomandų.
  Darbinis šablono bylas užkrečiamas atvertus jau infekuotą MS Word dokumentą. Kartu ištrinamos esamos makrokomandos. Kiti dokumentai užkrečiami, kai jie atverčiami, užverčiami ir išsaugomi, taip pat kai išeinama iš **MS Word** redagavimo terpės.

Virusai Internete

- Internete virusus galima suskirstyti į kelias grupes.
    - Pirmąją sudaro virusai, **„migruojantys" kartu su bylomis**.
    - Antroji grupė - **netikrieji virusai arba „virusai apgavikai"**. Trečiajai grupei priklauso šiuo metu bene daugiausia diskusijų sukėlusios kenkėjiškos Java, JavaScript bei ActiveX programėlės.
      Pirmosios grupės virusai patys plisti Internete negali. Išplatinti tokį virusą gali tik vartotojas, paskleidęs juo užkrėstą bylą Internete (pavyzdžiui, palikęs jį paslaugų kompiuteryje ar pan.). „Geras" pavyzdys - Microsoft kompanijos išplatintas Wazzu virusas. Apsauga nuo panašių virusų yra gana paprasta - tiesiog reikia įprasti tikrinti ir bylas, paimtus iš Interneto paslaugų kompiuterių).
      Antrosios grupės virusai įdomūs tuo, kad jie dažniausiai neegzistuoja ir net negali egzistuoti. Kenkia ne virusai, o pranešimai apie juos. Didėjant virusų įvairovei, kompiuterių vartotojai pradėjo naudotis Internetu kaip pigia, patogia priemone įspėti apie naujausius virusus savo kolegas. Tačiau atsirado ir norinčiųjų papokštauti. Pastarieji elektroniniu paštu ėmė siųsti pranešimus apie kažkur kibernetinėje erdvėje klaidžiojančius fantastinius virusus. Pranešimo pabaigoje prašydavo persiųsti gautą laišką kuo didesniam skaičiui vartotojų. Nesunku įsivaizduoti, kaip per trumpą laiką gali padaugėti tokių pranešimų kopijų, ypač jei jos dar būtų išplatintos ir naujienų padaliniuose. Toks nereikalingas „balastas" užteršia kompiuterinius tinklus, sumažindamas naudingos informacijos persiuntimo spartą. Gavę pranešimą apie netikrą virusą, ne persiųskite kitiems, o ištrinkite jį.
      Gavę laišką su „prikabinta" byla, būkite atsargūs. Saugiausia būtų tokias bylas atskirti nuo laiško ir, įrašius į diską, patikrinti juos turimomis antivirusinėmis priemonėmis.
      Taip pat patartina turėti naujausią tinklo naršyklę. Microsoft ir kitos kompanijos gana greitai reaguoja į pranešimus apie naršyklėse rastas „skyles" bei kitus trūkumus ir operatyviai juos ištaiso. Todėl galima tikėtis, kad naudodami naujausią naršyklę, būsite apsaugoti bent nuo tuo

metu žinomų kenkėjų.
Jeigu dirbate internete, jūsų kompiuteris turi būti aprūpintas antivirusinėmis programomis, kurios tikrina patenkančias į kompiuterį bylas ir reaguoja, jeigu tokia byla yra infekuota virusu.

Apsisaugojimas nuo kompiuterinio viruso

- Siekiant apsisaugoti nuo virusų naudojamos:
  - bendrosios informacijos apsaugos priemonės;
  - specializuotos kovos su virusais priemonės;
  - profilaktinės priemonės.

Bendrosios informacijos apsaugos priemonės

- Bendrosioms informacijos apsaugos priemonėms priskiriamas duomenų rezervinis kopijavimas ir kreipties į bylas apribojimas. Atsarginės duomenų kopijas reikėtų saugoti išoriniuose kaupikliuose - diskeliuose, kompaktiniuose diskuose, magnetinėse juostose. Jei sukurtos naujos bylos ar kurios nors pakeistos, pasidarykite jų kopijas. Prieš kopijuodami patikrinkite, ar bylos neužkrėstos virusais. Toks reguliarus kopijavimas reikalauja mažiau sąnaudų, nei jų reikėtų prarastoms byloms atkurti. Kreipties apribojimas padeda išvengti nesankcionuoto informacijos naudojimo ir kartu apsaugo duomenis nuo užkrėtimo virusu.

Specializuotos kovos su virusais priemonės

- Specializuotos kovos su virusais priemonės - tai techninė ir programinė antivirusinė įranga.

Profilaktinės priemonės

- Profilaktinės priemonės taip pat gali realiai sumažinti užsikrėtimo virusu tikimybę. Rekomenduojami tokie veiksmai:
  - apsaugoti nuo įrašymo tuos diskelius, iš kurių informacija tik skaitoma;
  - standžiajame diske reikėtų sukurti tokį apsaugotą nuo įrašymo loginį diską kuriame laikysite nekeičiamą informaciją (programas ir duomenis);
  - vengti perrašinėti informaciją iš kitų kompiuterių, nes ji gali būti užkrėsta;
  - prieš perkeliant bet kokią informaciją iš diskelio, jį būtina patikrinti antivirusine programa;
  - visą gautą programinę įrangą (ypač demonstracinę ar nemokamai prieš įkeliant būtina patikrinti antivirusine programa;
  - vengti leisti naudotis kompiuteriu kitiems asmenims (ypač pašaliniams);
  - reguliariai atnaujinti turimas ir įsigyti naujas antivirusines programas;
  - visada atsargai turėkite sisteminį diskelį su svarbiausiomis operacinės sistemos komandomis.

Ką daryti pastebėjus (įtarus) virusą kompiuteryje?

- Pastebėjus ar įtariant tokį faktą, visų pirma nepanikuokite. Jeigu apie tai jus informavo antivirusinė programa, tai greičiausiai toks virusas bus neutralizuotas ir žalos jums nepadarys.
jeigu dirbate didelėje įstaigoje, tai pastebėję ar įtardami viruso požymius, elkitės taip, kaip nustatyta įstaigos duomenų saugumo užtikrinimo taisyklėse.
Jeigu viruso požymiai atsirado jūsų asmeniniame kompiuteryje, tai kreipkitės į specialistą, kad problema būtų pašalinta.

Antivirusinė programinė įranga