

Ak, tie virusai (kompiuterių virusų istorija)

Kas yra virusas

Išgirdęs sąvoką „virusas“, nieko gero tikėtis negali, nes lotyniškai *virus* reiškia *nuodus*. **Virusas** – kompiuterio programa, kuri prisijungia prie vykdomųjų failų, gamina savo kopijas ir jomis užkrečia kitus failus. Kompiuterių virusas gali pažeisti sistemą, sutrikdyti programų darbą, sunaikinti duomenis ir sugadinti aparatinę įrangą. Jis taip pat gali pasisavinti asmeninę informaciją: asmens kodus, įvairius prisijungimo slaptažodžius ir perduoti piktavaliams žmonėms. Kompiuterių virusas gali būti stebėtinais įžūlus – pavyzdžiui, kompiuterinėje erdvėje karaliaujantis internetinių žaidimų virusas gali fiksuoti kiekvieną jūsų klaviatūros mygtukų paspaudimą, taip sužinodamas prisijungimo duomenis ir slaptažodžius.

Viruso sąvoka pasirinkta neatsitiktinai, nes kompiuterių virusas ir biologinis virusas yra labai panašūs. **Biologinis virusas** – parazitinis mikroorganizmas, galintis išgyventi tik įsiskverbęs į kitą organizmą. Patekęs į ląstelę, jis pažeidžia čia esančią genetinę informaciją ir užgrobia ląstelės gyvybinių procesų valdymą, taip susikurdamas sau galimybę daugintis. Panašiai elgiasi ir kompiuterių virusas – radęs neužkrėstą programos failą, pakeičia jo kodus taip, kad galėtų kurti savo paties kopijas. Abiem atvejais tiek kompiuterių, tiek biologinis virusas perima sistemos valdymą ir kenkia.

Kompiuterių virusas – intelektinis žmogaus produktas. Kaip žmogus sukūrė programas, kenkiančias kitoms programoms?

Viruso atsiradimo istorija

Pirmosios programos, turinčios kompiuterių viruso bruožų, buvo žaidimai – juose priešininkų programos stengdavosi nugalėti kitas programas ir užimti jų vietą atmintinėje.

9-ame dešimtmetyje dėl neatsargumo, smalsumo ar neatsakingumo buvo sukurtos tokios programos, kurios tapo nekontroliuojamos – jos skverbdavosi į kitas programas ir pakeisdavo jų vykdomuosius failus. Tai buvo pirmieji kompiuterių virusai. Vienas pirmųjų tikrųjų kompiuterių virusų, plitęs 5,25 colio lankščiaisiais diskeliais, buvo sukurtas 1986 m. Virusą „Brain“ („Smegenys“) sukūrė du broliai pakistaniečiai, turėję programinės įrangos firmą ir norėję apsaugoti savo programas nuo plagijavimo. Virusas užkrėsdavo kompiuterius, į kuriuos buvo įkeliamos nelegaliai nukopijuotos programos. Jis užkrėsdavo įkelties sektorių (*boot*) ir mokėjo labai gerai

slėptis – kai naudotojas tikrindavo, ar viruso nėra, virusas pasirūpindavo, kad toks įrašas atsirastų! „Brain“ virusui pagauti 1988 m. buvo sukurta pirmoji antivirusinė programa pasaulyje. Bet virusas išnyko pats, kai 5,25 colio diskelius pakeitė mažesni – 3,5 colio diskeliai.

Programuotojai entuziastai kurdavo virusus kaip įdomius uždavinius, norėdami patikrinti savo galimybes.

Pirmasis kompiuterių tinklo virusas – kirminas „Cornell/Aparnet“, pridaręs labai daug žalos, buvo sukurtas 1988 metų rudenį „Bell“ bendrovėje. Jį, nenorėdamas nieko blogo, sukūrė Kornelio universiteto diplomantas Robertas Morisas (*Robert Morris*). Virusas pradėdavo veikti tada, kai kuris nors naudotojas surinkdavo tam tikrą slaptažodį. R. Morisas slaptažodžių rinkinį sudarė iš labai paprastų dažnai vartojamų žodžių – žmonių ar jų augintinių vardų. Įdomu tai, kad tuos pačius slaptažodžius žmonės naudojo skirtinguose miestuose ar net skirtingose šalyse, tad virusas tinklais pradėjo plisti labai greitai. Išėjęs iš bendrovės ribų, virusas per penkias dienas „apkeliavo“ visą Ameriką, išvesdamas iš rikiuotės daugiau nei 6000 kompiuterių, vėliau, patekęs į internetą, persikėlė į Europą ir Australiją.

Kaip virusai patenka į kompiuterį

Virusas – kompiuterio programa, todėl į kompiuterį jis gali patekti taip pat, kaip ir kiti failai – elektroniniu paštu, internetu, vietiniu tinklu, iš kompaktinių diskų, atmintukų. Labiausiai kompiuterių virusai mėgsta elektroninį paštą. Atveriant neaiškius laiškus ir jų priedus, galima užkrėsti kompiuterį labai pavojingais virusais.

Virusų rūšys

Specialistai mano, kad pasaulio kompiuteriuose klaidžioja apie milijonas skirtingų virusų, tad suskirstyti juos į grupes pakankamai sudėtinga. Yra keletas kriterijų, pagal kuriuos virusai skirstomi.

1. Pagal kenksmingumą:

- *nekenksmingi* – kompiuterio darbui nedaro žalos, tik užima atmintinės vietą;
- *nelabai kenksmingi* – užima atmintinės vietą ir krečia įvairius pokštus, pasireiškiančius garso, grafikos efektais;
- *kenksmingi* – pavojingi, trikdančios kompiuterio darbą, stabdantys programas;
- *labai kenksmingi* – naikinantys programas, duomenis, informaciją, reikalingą operacinei sistemai, gadinantys įrenginius.

2. Pagal veikimo pobūdį:

- *failų* arba *programų virusas* įsiterpia į failus ir juos pakeičia; dažniausiai užkrečiami failai, kurių prievardžiai yra .com, .exe, .bat, .sys, .dll, .doc;
- *įkelties virusai* užgrobia pirmąjį (paleidimo) disko, diskelio, atmintuko sektorių (*boot*) ir įrašo ten savo programą; (pradėdama dirbti, operacinė sistema pirmiausia kreipiasi į įkelties sektorių ir vykdo ten įrašytas komandas, net ir tuomet, kai jas duoda ten esantis virusas);
- *tinklo virusas* plinta kompiuterių tinklais; tinklais gali plisti ir failų, ir įkelties virusai.

3. Virusai-bombos:

- *laiko bombos* pradeda veikti nustatytu laiku, pavyzdžiui, virusas „CIH“, veikė tik balandžio 26 dieną, kai įvyko avarija Černobylio atominėje elektrinėje;
- *loginės bombos* pradeda veikti, kai nutinka konkretus įvykis, pavyzdžiui, prisijungia naujas naudotojas.

Ypač „gudrūs“ yra **polimòrfiniai virusai**, kurie suaktyvuoti kaskart pakeičia savo programos kodus. Tokius virusus sunkiai aptinka antivirusinės programos.

Dar yra atskiros grupės kompiuterio programų-kenkėjų, vadinamų bendrinium virusų vardu: **kirminai (worms)** ir **Tròjos arkliai (trojan)**. Kompiuterių **kiřminas** yra kenkėjiška programa, kuri kopijuoja save ir platina veikiančias savo kopijas kompiuteryje arba kompiuterių tinkle. Kirminui, skirtingai nei virusui, nereikia prisitvirtinti prie programų ir jis nenaikina failų. Bet labai sparčiai besidaugindami kirminai gali užtvindyti visą kompiuterio atmintį ar kompiuterių tinklą.

Tròjos arklis – programa, kuri slepiasi po kokia nors naudinga programa ir, vos šiai pradėjus veikti kompiuteryje, pradeda veikti. Trojos arklis nesidaugina kaip kirminai ir negadina failų bei programų. „Trojanų“ tikslas – padaryti kuo daugiau spragų kompiuterio apsaugoje ir įsileisti į kompiuterį įsilaužėlius, kurie gali vogti informaciją ir valdyti virusu užkrėstą kompiuterį.

Kai kompiuterį užpuola virusas, jam gali padėti **antivirusinė programa. Ši programa aptinka ir sunaikina kompiuterių virusus.** Yra nuolat budinčių antivirusinių programų ir veikiančių tik tada, kai naudotojas jas paleidžia. Budinčios antivirusinės programos nuolat seka kompiuteryje esančius ir į jį patenkančius duomenis. Aptikusios virusą, programos klausia naudotojo, ką su juo daryti – naikinti, pervardyti, perkelti į laikinąją saugyklą ir pan.

Pasaulinėje kompiuterių rinkoje sukurta daug antivirusinių programų: „Kaspersky“



, „AntiVir“



, „AVG“



ir kitų. Daugelyje

Lietuvės mokyklų naudojama lengvai įgyjama, sulie-tuvinta programa „Dr. Web“. Antivirusinių programų nuostatose galima nurodyti, kad antivirusinė duo-menų bazė būtų atnaujinama automatiškai, galima

nustatyti tikrinimo laiką, elektroninių laiškų tikrinimo sąlygas ir kt. Įdiegus antivirusinę programą kompiu-terijoje, darbalaukio užduočių juostos dešiniajame kampe atsiranda programos piktograma, pavyzdžiui,



(„Dr. Web“).

Norėdami, kad jūsų kompiuteris būtų pakanka-mai apsaugotas nuo įvairių kompiuterio kenkėjų, turėtumėte įdiegti visą saugos programų rinkinį – **tiūklo užkardą** (saugiasienę), **antišnipinėjimo** ir **antivirusinės programos**. Tinklo užkarda apsaugo nuo įsilaužėlių („hakerių“), užkrečiančių kompiuterį kenkėjiškomis programomis – „Trojos arkliais“. An-tišnipinė programa saugo nuo virusų, vagiančių ir siuntinėjančių piktavaliams žmonėms asmeninius kompiuterių naudotojų duomenis, o antivirusinė programa saugo nuo virusų.

Kaip išvengti virusų (patarimai kompiuterio naudotojui)

Pirmiausia, įsigykite antivirusinę programą.

Pati brangiausia antivirusinė programa neapsaugos nuo virusų, jei ja nesisinaudosite – nuolat tikrinkite, ar jūsų kompiuteryje neapsigyveno virusai.

Jei neketinate kopijuoti informacijos į diskelį, atmintuką, uždrauskite įrašymą.

Prieš įrašydami naują informaciją į savo išorinę atmintinę, įsitikinkite, ar neparsinešite kartu ir dovanėlės – viruso.

Mainydamiesi dainomis, filmais ar kitokiais failais internetu, įsitikinkite, kad mainotės ne virusais.

Kuo dažniau atnaujinkite antivirusinę duomenų bazę – pasaulyje yra jau milijonas skirtingų virusų ir visi jie tikisi surasti savo šeiminką.

Visą naujai gautą (net ir licencinę) programinę įrangą prieš diegdami patikrinkite antivirusine programa. Virusai gali gyventi ir nuo įrašymo apsaugotuose kompaktiniuose ar skaitmeniniuose vaizdo diskuose.

Neatverkite neaiškių laiškų ir priedų – labai mėgstama virusų slėptuvė yra elektroniniai laiškai.

Nesigundykite spustelėti tinklalapiuose įtartinų nuorodų – ten gali laukti virusas.

Naudokite tik teisėtai įsigytas arba laisvai platinamas programas – neteisėtai platinamose (vogtose) programose dažnai slepiasi virusai. O ir naudotis svetimais autorių darbais draudžiama.

Nenaudokite nepatikrintų išorinių laikmenų – kompaktinių ar skaitmeninių vaizdo diskų, diskelių, atmintukų, mp3 formato grotuvų. Labai populiarus virusas „INF/Autorun“ gyvena diskeliuose, standžiuosiuose diskuose ir atmintukuose, neleisdamas automatiškai jų atverti.