KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

PROGRAMŲ INŽINERIJOS KATEDRA

Kompiuteriniai virusai

Referatas

Atliko: dokt. Rita Palivonaitė

Priėmė: prof. habil.dr. Rimantas Šeinauskas

KAUNAS, 2011

TURINYS

1. ĮVADAS

Kompiuterinių virusų savoka jau žinoma beveik 30 metų. Kompiuteriui tapus kasdieniniu žmonijos darbo ir pramogų įrankiu, neatsiejama jo dalis tapo ir kompiuteriniai virusai. Kompiuteriniai virusai nuo pat jų atsiradimo evoliucionavo kartu su kompiuteriais ir daro vis didesnę žalą, sugeba greičiau plisti, tampa vis sunkiau aptinkamomis.

Kasmet didėja virusų padaroma žala kompiuteriams ir jų tinklams. Atitinkamai auga ir įmonių bei institucijų išleidžiamų pinigų sumos siekiat apsaugoti savo kompiuterius bei jų tinklus nuo žalingų atakų. Todėl kompiuteriniai virusai tampa svarbia šio amžiaus problema kompiuterizacijos veikiamame pasaulyje, siekiant didesnio informacijos perdavimo saugumo, spartumo bei apdorojimo patikimumo.

Darbo tikslas yra pateikti kompiuterinių virusų sampratą, rūšis ir jų veikimo apžvalgą, o 3 skyriuje pateikiama 2010 m. Kaspersky Laboratorijos kompiuterinių virusų statistika.

2. KOMPIUTERINIAI VIRUSAI

Kompiuteriniai virusai - tai kompiuterinės programos. Nuo įprastų programų jos skiriasi tuo, kad yra piktavališkos ir sugeba pačios plisti, dažnai įgaudamos epidemijos mastus. Dėl pastarojo bruožo kompiuteriniai virusai yra labai panašūs į biologinius virusus. Kompiuteriniai virusai sukelia žalingus padarinius, pavyzdžiui, sunaikina, sugadina, ar net pavagia kompiuteryje esančią informaciją, taip pat gali atlikti kompiuterines atakas prieš kitus kompiuterius, nulemti kompiuterių ir tinklų perkrovas arba perimti kompiuterio valdymą.

Dažniausiai kompiuteriniai virusai plinta elektroniniu paštu bei būna prisegti prie įvairių programų, kurias paleidus, yra aktyvuojamas virusas.

2.1. KOMPIUTERINIŲ VIRUSŲ ATSIRADIMO ISTORIJA

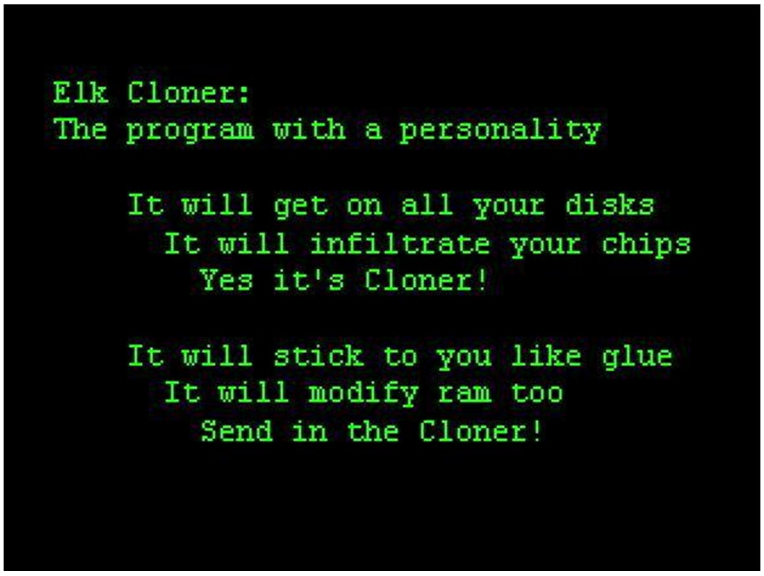
Nėra vieningos nuomonės dėl pirmojo kompiuterinio viruso atsiradimo datos, tačiau chronologiškai galima pažymėti tokius kompiuterinių virusų atsiradimo istorijos įvykius.

1949 m. vengrų mokslininkas matematikas John von Neumann sukūrė save kopijuojančių programų teoriją, tai buvo pirmasis teorinis, pagal šių dienų supratimą, programos-viruso modelis.

Pirmoji programa, turėjusi kompiuterinio viruso bruožų, buvo 1960 m. sukurtas žaidimas *Core War*, tačiau jis nebuvo tikras virusas, galintis daugintis už kūrimo aplinkos ribų. Šio žaidimo kūrėjai, galima sakyti, sukūrė ir pirmąją antivirusinę programą, pavadintą *Reeper,* kuri naikino žaidimo *Core War* sukurtas kopijas. Tačiau apie šio žaidimo egzistavimą buvo paskelbta tik 1983 m. žurnale *Scientific American.*

Pirmuoju tikru kompiuteriniu virusu daugelis tyrinėtojų laiko programą *Elk Cloner,* kurią 1982 m. sukūrė vidurinės mokyklos moksleivis Rich Skrenta. *Elk Cloner* buvo sukurtas kaip pokštas, nes užkrėtė žaidimą, kurį paleidus 50-tąjį kartą juodame ekrane pasirodydavo eilėraštukas apie virusą (1 pav.). Manoma, jog tai pirmasis kompiuterinis virusas paplitęs už kūrimo aplinkos ribų. Šis virusas plito diskeliais, užkrėsdamas Apple DOS 3.3 operacinę sistemą. Virusas pasileisdavo kiekvieną kartą užkraunant kompiuterį iš diskelio. Jis netrukdė dirbti su kompiuteriu, tik stebėdavo sistemos darbą su diskais, užkrėsdamas kiekvieną, dar neužkrėstą, diskelį. Būtent tokiu pačiu principu (užkrėsdavo diskelio ar kietojo disko

formatavimo sektorių ir kiekvieną sykį paleidžiant failus/programas daugindavosi) veikė ir dauguma kitų kompiuterinių virusų iki interneto atsiradimo.



1 pav. Elk Cloner viruso pasirodymo langas

Tuo metu dar nauja operacinė sistema MS-DOS (angl. Microsoft Disk Operating System) jau išsiskyrė iš kitų. Ši sistema turėjo dideles perspektyvas, tačiau ir nemažai trūkumų. 1986 m. ji tapo viruso *Brain* taikiniu. Žalingas šis programos kodas buvo parašytas Pakistane brolių Basit ir Amjad Farooq Alvi, nors iš tiesų jų ketinimai buvo tik apsaugoti savo darbą nuo piratavimo. Virusas užkrėsdavo diskų paleidimo sektorius ir juose esanti informacija tapdavo nepasiekima.

Tais pačiais metais atsirado visiškai naujos rūšies virusas – *trojanas* arba *Trojos arklys* (angl. *Trojan*), kuris apsimesdavo esąs kita, žinoma programa. Buvo manoma, kad jis vykdo naudingus veiksmus, o iš tikro trojanai iškart pradėdavo destrukciją, dažniausiai vogdami iš apkrėstojo kompiuterio duomenis. Pirmasis trojanas buvo pavadintas *PC-Write*, kuris pasirodė kaip teksto procesorius. Programą paleidus ekrane buvo matomas įprastas tekstas, tačiau vartotojui dirbant, *PC-Write* trindavo ir gadindavo kompiuterio kietajame diske esančius failus.

Labai greitai virusų kūrėjai suvokė, kad užkrėsti failai gali būti dar žalingesni kompiuterinėms sistemoms. 1987 m. pasirodė virusas *Suvir-02*, kuris užkrėsdavo COM (angl. *Computer Output on Microfilm*) failus ir atverdavo kelią liūdnai pagarsėjusiems virusams *Jerusalem* arba *Viernes 13*. Tačiau, vienas tų laikų žalingiausių virusų buvo kirminas *Morris worm* pasirodė 1988 m. ir užkrėtė tais laikais įspūdingą skaičių 6000 kompiuterių.

Iki 1995 pasirodė dauguma šiomis dienomis žinomų žalingų programų: pirmieji makro virusai, polimorfiniai virusai ir pan. Kai kurie iš jų, tokie kaip pvz. *MichaelAngelo* 1992 m. net sukėlė epidemiją. Tai buvo pirmasis per programuotojų neapdairumą plačiai paplitęs ir išgarsėjęs virusas, jis kasmet pradeda veikti per šio menininko gimtadienį, tačiau jis nebuvo labai pavojingas. Tačiau būtent jis paskatino garsiai apie virusus kalbėti visame pasaulyje.

Masinis interneto ir elektroninio pašto naudojimas iš esmės pakeitė virusų plitimo mastus. 1999 m. pasirodė *Melissa*, pirmasis virusas, sukėlęs pasaulinę epidemiją ir pradėjęs naują kompiuterinių virusų erą. Kompiuterinių virusų kūrėjų tikslu tapo užkrėsti kiek įmanoma daugiau kompiuterių. *Melissa* pasirodymas tapo ir ekonomine problema, nes kompanijos atkreipė dėmesį į daromą žalą ir pradėjo investuoti į apsisaugojimo priemones, taigi prasidėjo platus antivirusinių programį naudojimas. Tai naujas iššūkis žalingų programų kūrėjams, nes tenka sukti galvą, kaip apeiti apsaugos sistemas.

Apeinant šią ,,problemą"virusų kūrėjai atsirado viena efektyviausių strategijų apgauti vartotojus: įterpti klaidingą pranešimą, kuris neatrodytų panašus į virusą. Garsiausias pavyzdys *LoveLetter*, leidęs jo gavėjams manyti, kad jiems parašė meilės laišką.

Interneto plitimas leido atsirasti ir netikriems virusams, vadinamiems *Hoaxs* vardu. Šie virusai žalos kompiuteriams nedaro, tačiau pranešdami apie netikrus virusus ar kitą informaciją ir priversdami interneto vartotojus persiųsti tokius laiškus kitiems, paralyžiuoja interneto tinklus [1,2].

2.2. KOMPIUTERINIŲ VIRUSŲ RŪŠYS

Kompiuteriniai virusai gali būti klasifikuojami pagal įvairiausius kriterijus: kilmę, technologiją, failus, kuriuos jie puola, slėpimosi būdą ir vietą, jų daromos žalos pobūdį, operacinės sistemos rūšį, kuri yra atakuojama tam tikro viruso. Netgi paprastas virusas, jei jis yra kompleksinio pobūdžio, gali priklausyti keletui kategorijų. Tuo tarpu nauji virusai gali priversti antivirusinių programų kūrėjus iš naujo sudaryti virusų klasifikavimo kategorijas ar net sukurti naujas.

Įvairioje literatūroje galima rasti įvairiai išskiriamus virusų tipus, ir šioje dalyje apžvelgiamos pagrindinės, pasaulyje labiausiai paplitusios kompiuterių kenkėjų rūšis. [3,4]

Trojanai (angl. *Trojans* arba *Trojan horses*) – virusų atmaina, kuri veikia panašiai kaip mitologijoje minimas Trojos arklys. Trojanai į kompiuterį dažniausiai patenka per kitas užkrėstas programas, kurios išoriškai atrodo kaip naudingos, tačiau realiai sukeliančios kenksmingus padarinius. Šie virusai negamina savo kopijų kaip kirminai ir neplinta užkrėsdami failus kaip virusai, bet aktyvavus programą, už kurios jie slepiasi, kartu aktyvuojamas ir virusas. Užpuolę sistemą jie turi galimybę ištrinti bylas, sunaikinti kitą kietojo disko informaciją bei atidaryti prieigą pašaliniams vartotojams, pasiekti ir vogti informaciją iš užkrėsto kompiuterio. Pastaroji virusų galimybė ypač pavojinga, kadangi įmanoma, jog svarbi informacija pateks į svetimas rankas, kompiuteris nebus kontroliuojamas jo šeimininko. Populiariausi yra paslėpti trojanai (angl. *backdoors torjans*), trojanai šnipai (angl. *Trojan spies*), slaptažodžius vagiantys ir įgaliojantys trojanai (angl. *Trojan proxies*), kurie užkrėstą kompiuterį paverčia šlamšto (angl. *spam*) platinimo priemone [3,4].

Kirminai (angl. *worms*) – virusų, kurie patys sugeba daugintis atmaina, pagal paplitimą aplenkę pačius virusus. Didžiausią pavojų kelia jų sugebėjimas daugintis dideliais kiekiais. Kirminai, patekę į sistemą, gali keliauti savarankiškai. Plisdami iš vieno kompiuterio į kitą tai daro automatiškai, užvaldydami kompiuterio funkcijas, kurios gali perkelti failus ar informaciją. Kirminai gali atlikti ne vieną funkciją, o tiek, kiek jų yra užprogramuota.

Kirminai dažniausiai plinta be vartotojo veiksmų ir platina savo kopijas tinkluose, jie gali nesustodami daugintis tol, kol išnaudos kompiuterio duomenų talpą arba išplis po visą tinklą ir sutrikdys jo darbą. Kirminai gali užimti kompiuterio atmintį arba tinklo ryšį, ir taip kompiuteris gali nustoti reaguoti į vartotojo veiksmus. Kadangi kirminams nereikalinga programa ar failas, prie kurio jie turėtų prisikabinti, jie gali sukurti tunelį į vartotojo kompiuterį ir perleisti kontrolę bei valdymą kitiems vartotojams.

Makrovirusai (angl. *macro virus*) - virusų rūšis, kuri pažeidžia dokumentus, sukurtus su taikomosiomis programomis, kuriose galimas makrokomandų (angl. *macros*) naudojimas – tai Word, Excel, PowerPoint, Access ir kitų programų dokumentai. Atitinkama programa turi savo rūšies virusą veikiantį tik ta programa sukurtus failus. Dokumentas yra užkrečiamas paleidžiant jį programos lange, jei nėra uždraustas automatinis makrokomandų vykdymas. Šis virusas prilimpa prie atitinkamų programų šablonų taip, kad visi nauji dokumentai jau turėtų viruso kodą ir patekę į kitą kompiuterį užkrėstų šio programas. Apsisaugoti galima tik Microsoft Word ar Excel programoje uždraudus automatinį makrokomandų vykdymą.

Žinomiausias makrovirusas yra Melissa.A. Šis virusas kompiuterius pasiekia per el. laiškus su užkrėstais Word dokumentais. Paleistas jis nuskaito pirmuosius 50 el. pašto adresų iš Outlook programos ir jais išsiunčia el. laiškus su prisegtais užkrėstais dokumentais. Melissa.A nėra žalingas virusas, nes išvedamos iš rikiuotės tik kai kurios Word funkcijos ir sugadinami kai kurie dokumentai virusui įterpiant tekstus į failus su galūnėmis *.doc.

Paleidžiamieji virusai (ang. *boot virus*) – vieni pirmųjų kompiuterinių virusų, kurie plito per diskelius ir veikdavo kompiuterio DOS (angl. *Disk Operating System*) sistemą. Šio tipo virusai pažeidžia paleidžiamąsias (angl. *boot sector*) diskelių ar kietųjų diskų dalis. Ši sritis yra ypač svarbi kompiuteriui dėl to, kad joje yra laikoma pagrindinė informacija apie diską, kartu su programa, kuri gali paleisti kompiuterį. Paleidžiamieji virusai labiau veikia diskus, kuriuose yra užkrėsti failai, bet ne pačius failus. Pirmiausia jie puola paleidžiamuosius diskų sektorius, o tuomet ir patį kietąjį diską. Tokių virusų plitimo mastai nebuvo dideli, ir šiuo metu praktikoje jų beveik nepasitaiko.

Polimorfiniai virusai (angl. *polymorphic virus*) – vieni pavojingiausių kompiuterinių virusų. Šie virusai kiekvieną sykį užkrėsdami sistemą koduojami ir dekoduojami naudojantis skirtingus algoritmus ir (de)kodavimo raktus. Toks maskavimo būdas labai apsunkina antivirusinių programų paieškas, nes praktiškai tampa neįmanoma aptikti virusų duomenų eilutes ar jų „parašus“.

Polimorfinis kodas naudojamas tokių virusų kėlė daugybę problemų antivirusinėms programoms. Kaip ir koduojami virusai šie virusai užkrečia bylas su užkoduota savo versija, kuri yra dekoduojama atitinkamo modulio, tačiau kiekvienąsyk užkrečiant bylas šis dekodavimo modulis yra modifikuojamas. Antivirusinės programos šiuos virusus gali aptiki tik specialiais būdais pamėgdžiodamos ar kopijuodamos virusus arba atlikdamos tam tikrą analizę. Tam, kad veiktų viruso polimorfinis kodas ir būtų galima kurti naujus tokio tipo kodus, virusas privalo turėti vadinamąjį polimorfinį variklį (angl. polimorphic engine), kuris yra įterpiamas į koduojamą viruso dalį.

Kartais polimorfinis virusų kodas tampa jų dauginimosi greičio reguliatoriumi. Pavyzdžiui, virusas gali būti suprogramuotas lėtai mutacijai arba iš viso nemutuoti užkrėtus naujas bylas. Lėtos viruso mutacijos privalumas tas, kad ieškant tokių virusų sunku rasti

patikimų pavyzdžių, nes vieno puolimo metu užkrėsti failai turės identiškus arba labai panašius virusų pavyzdžius. Tai savo ruožtu labai sunkina šių virusų aptikimą.

Metamorfiniai virusai (angl. metamorphic viruses) - dar sunkiau aptinkami nei polimorfiniai virusai, kurie yra visiškai perrašomi po kiekvieno atakos. Tam jiems reikalingas metamorfinis variklis. Šie virusai dažniausiai yra kompleksinai ir užima daug vietos.

Virusai „gyventojai“ (angl. *resident viruses*) – vieni dažniausiai pasitaikančių virusų. Šie virusai ilgą laiką slepiasi kompiuterio operatyviojoje atmintyje. Iš čia jie gali kontroliuoti ir perimti įvairias sistemos operacijas: sugadinti programas ir failus, kurie yra atidaromi, uždaromi, kopijuojami ir t.t. Šie virusai gali būti laikomi failų užkrečiamaisiais virusais. Kai virusas patenka į kompiuterio atmintį, jis ten lieka, kol kompiuteris nėra perkraunamas ar išjungiamas (laukia tol, kol dėl tam tikrų priežasčių jis galės aktyvuotis). Tuo tarpu iki paleidimo „gyventojai“ nieko nedaro.

Tiesioginių veiksmų virusai (angl. *direct action viruses*). Pagrindinis šių virusų tikslas yra daugintis ir pradėti veikti, kai yra paleidžiami. Atsiradus sąlygoms šie virusai pradeda veikti ir infekuoja failus ar failų aplankus, kurie yra tam tikrose direktorijose, arba direktorijas, per kurias eina kelias iki autoexec.bat failo. Šis paketinis failas (angl. *batch file*) visuomet yra talpinamas pagrindinėje kietojo disko direktorijoje ir atlieka tam tikras operacijas, kai kompiuteris yra paleidžiamas. Šiais virusais užkrėsti kompiuteriniai failai gali būti išvalyti ir pilnai atkurti.

Perrašantys virusai (angl. *overwriting viruses*) taip vadinami todėl, kadangi jie iština informaciją, kuri yra talpinama užkrėstuose failuose, paversdami juos visiškai ar iš dalies nenaudojamais. Užkrėsti failai nepakeičia savo dydžio, nors pats virusas užima daugiau vietos nei pats failas. Taip nutinka todėl, kad virusas nesislepia faile, o pakeičia jo turinį. Vienintelis būdas sunaikinti šiuos virusus yra užkrėstų failų sunaikinimas kartu su visa informacija juose.

Direktorijos virusai (angl. *directory virus*). Operacinės sistemos failus randa sekdamos tam tikru keliu, kuris nurodo failo buvimo direktoriją. Direktorijos virusai sugadina šiuos kelius. Paleidus programą (failus, kurių galūnės *.exe arba *.com), kurią infekavo virusas, mes nežinodami paleidžiame virusinę programą, tuo tarpu originalus failas yra pašalinamas ir nebepaleidžiamas. Užsikrėtus šiais virusais originalių failų nebeįmanoma rasti, todėl tenka perinstaliuoti visą operacinę sistemą.

Koduoti virusai (angl. *encrypted viruses*). Šie virusai buvo sukurti taip, kad galėtų slėptis nuo antivirusinių programų ir būtų užkoduoti iki puolimo momento. Tam tikru momentu jie atsikoduoja ir pradeda savo veiklą, o po atakos vėl pereina į ramybės būseną.

Kodavimas naudojamas tam, kad virusai būtų sunkiau aptinkami. Tokie virusai susideda iš dekodavimo modulio ir užkoduotos viruso kodo kopijos. Šie virusai kiekvieną sykį yra koduojamas su skirtingasi raktais, nepakitęs išlieka tik viruso dekodavmo modulis. Dėl to antivirusinės programos negali tiesiogiai aptikti vadinamųjų „viruso parašų“. Šiuo atveju programos turi ieškoti viruso dekodavimo modulio. Dažniausiai virusų dekodavimo sistemos nėra sudėtingos ir (de)koduojant kiekvieną baitą naudojasi tam tikromis loginėmis operacijomis (angl. *xoring*), naujus virusų raktus išsaugo motininiai virusai.

Daugialypiai virusai (angl. *multipartite virus*). Šie virusai sukelia sudėtinius failų užkrėtimus, naudodamiesi keletu užkrėtimo būdų (susideda iš keleto dalių, kurios atitinkamai gali sukelti užkrėtimą) – būtent dėl to jie yra laikomi ypatingai pavojingais. Daugialypiai virusai puola visus kompiuterio elementus, kurie gali tapti „šeiminikais“ – failus, programas, makrokomandas, diskus ir t.t.

Bylų užkrėtėjai (angl. *file infectors*). Šis virusų tipas puola programas ir vykdomuosius failus (su *.exe ir *.com plėtiniais). Kai tokia programa yra paleidžiama, kartu paleidžiamas ir virusas, kuris pradeda atlikti tuos veiksmus, kurie yra suprogramuoti. Dauguma virusų priklauso būtent šiai kategorijai ir toliau gali būti klasifikuojami pagal atliekamus veiksmus.

FAT virusai (angl. *FAT viruses*) šie virusai puola kietųjų diskų FAT zoną (angl. *file allocation table*). Ši zona labai svarbi viso kompiuterio funkcionavimui, nes ja kompiuteris naudojasi norėdamas pasiekti atitinkamą kietajame diske laikomą informaciją. Virusas sutrikdydamas prieigą prie svarbių failų gali sukelti daug žalos. Dažniausiai dėl šio viruso prarandama informacija iš individualių bylų, o kartais ir visos direktorijos.

Virusai „kompanionai“ (angl. *companion viruses*) yra rezidentinių ir tiesioginių veiksmų virusų mišinys. Šie virusai patekę į sistemas nepradeda veiklos, o laukia kol bus paleistos paprogramės, kurias jie gali pulti (rezidentinių virusų bruožas), o tada pradeda labai greitai daugintis (tiesioginių veiksmų virusai).

Netikri virusai. Šie virusai dažnai yra palaikomi tikrais virusais, tačiau taip nėra, ir jie nekelia jokio pavojaus kompiuteriui. Šiam tipui priskiriami hoax virusai ir vadinamieji „juokeliai“ (angl. joakes). Hoax virusai yra klaidinantys el. pašto laiškai, kurie įspėja apie

netikrus ir neegzistuojančius virusus. Jų tikslas sukelti paniką tarp kompiuterių vartotojų. Dažniausiai tokiose žinutėse yra techninių terminų, kurie suklaidina vartotojus, kartais tokių pranešimų pradžioje paminimos žinomos firmos (pvz., žinių agentūros ar antivirusinių programų kompanijos), kas dar labiau įtikina tokių pranešimų gavėjus, jog informacija yra apie tikrus virusus. Dažnai juose būna nurodyta ir atitinkami veiksmai, kaip apsisaugoti nuo kompiuterinių virusų. Hoax ir „juokelių“ žala – sugaištas vartotojų laikas, pilnos el. pašto dėžutės ir perkrauti interneto tinklai. Į tokius pranešimus nereiktų kreipti dėmesio ir nepersiųsti jų kitiems.

2.3. KOMPIUTERINIŲ VIRUSŲ KENKSMINGUMAS

Virusai gali būti skirstomi pagal įvairius požymius, viena svarbiausių kenksmingumas. Pagal kenksmingumą virusai gali būti skirstomi į:

- Nepavojingus virusus, kurie kompiuterio veikimui nesukelia esminės žalos. Tokie virusai patys daugindamiesi užima tam tikrą kompiuterio atminties dalį, be to, jie gali patys pateikti į kompiuterio ekraną grafinius vaizdus, pranešimus, imituoti įvairius garsus ir pan.
- Pavojingus virusus, kurie gali sutrikdyti kompiuterio darbą. Tokie virusai sistemoje veikia vartotojui nematant ir iš pradžių nesukelia įtarimų,tačiau vėliau gali atsirasti įvairūs sistemos darbo sutrikimai, tokie kaip atskirų programų ar kompiuterio procesoriaus darbo sulėtėjimas, nenumatytų programose simbolių, pranešimų, paveiksliukų ar kitų pašalinių efektų atsiradimas,bylų turinio ar dydžio pasikeitimas ar virusui pasiekiamos atminties dydžio sumažėjimas.
- Labai pavojingus virusus, kurie naikina kitas programas ir kompiuteryje esančius duomenis, išvagia vertingą informaciją, ištrina būtiną kompiuteriui sisteminę informaciją (pvz.,bylų išdėstymo lenteles).Taip pat virusas gali tapti labai pavojingas, kai nekontroliuojamai dauginasi plisdamas kompiuteriniais tinklais taip, kad sutrikdo viso tinklo darbą [3].

  Taip pat virusus galima skirstyti atsižvelgiant į jų paplitimą ir daromą žalą:

- mažo pavojingumo (mažai paplitę ir mažai žalingi);
- vidutiniškai pavojingi (virusai mažai paplitę, bet gana pavojingi, arba paplitę, bet mažai pavojingi);

- pavojingi (virusas labai paplitę ir pavojingi arba paplitę ir labai pavojingi);
- labai pavojingi (virusai labai paplitę ir labai pavojingi).

Skaičiuojant viruso paplitimo lygmenį yra nustatomas užkrėtimo dažnis (t.y. užkrėstų kompiuterių skaičius bendram kompiuterių skaičiui). Yra skiriami tokie paplitimo lygmenys:

- epidemija (užkrėstų kompiuterių skaičius viršija 10%);
- labai paplitę (7,5-10%);
- vidutiniškai paplitę (1-2,5%);
- mažai paplitę (<1%). [3]

Patys garsiausi ir daugiausiai žalos padarę kompiuteriniai virusai laikomi šie:

Nimda – failus užkrečiantis kompiuterinis kirminas, pasirodęs 2001 m. rugsėjį, tuo metu buvo vienas iš piktybiškiausių ir sudėtingiausių iki tol pasirodžiusių virusų. Dėl kelių sklidimo krypčių per 22 minutes virusas tapo labiausiai paplitusiu kirminu visame pasaulyje, užkrėtęs šimtus tūkstančių kompiuterių. Virusui patekus į vieną kompiuterį, jis automatiškai plito po kitus į tą patį tinklą sujungtus kompiuterius. *Nimda* automatiškai išsisiųsdavo elektroniniu paštu su priesaga ,,readme.exe“. Be to, šis kirminas išvesdavo iš rikiuotės interneto serverius, nes į ,,Microsoft“ interneto informacijos serverio (IIS) programinę įrangą įrašydavo nematomą kodo eilutę, kuri apkrėsdavo bet kokį kompiuterį, kurio vartotojas apsilankydavo to serverio tinklapyje. Pavadinimas "*Nimda*" yra atvirkščiai įrašytas žodis "admin" - įprastinė santrumpa sistemų administratoriui įvardyti.

Netsky virusas, taip pat kirminas, pasirodė 2004 m. labiausiai įžymus dėl programos kode esančių komentarų, įžeidžiančių *MyDoom* ir *Bagle* virusų autorius. Dėl to tais metais sparčiai gausėjo minėtųjų virusų variantų. *Netsky* kirminas buvo išsiunčiamas elektroniniu paštu, atidarius prikabintą failą, jis nuskaitydavo elektroninio pašto adresus ir jais persisiųsdavo kitiems adresatams.

Storm kirminas pasirodė 2007 m. ir plito per elektroninius paštus su antrašte „230 dead as storm batters Europe”. Šis kirminas išnaudodavo operacinėje sistemoje esančias spragas. Kai kurios *Storm* kirmino versijos suteikdavo galimybę nuotoliniu būdu valdyti užkrėstą kompiuterį. Šis kirminas, daugiausiai buvo naudojamas per kompiuterių tinklą platinti spamo laiškus.

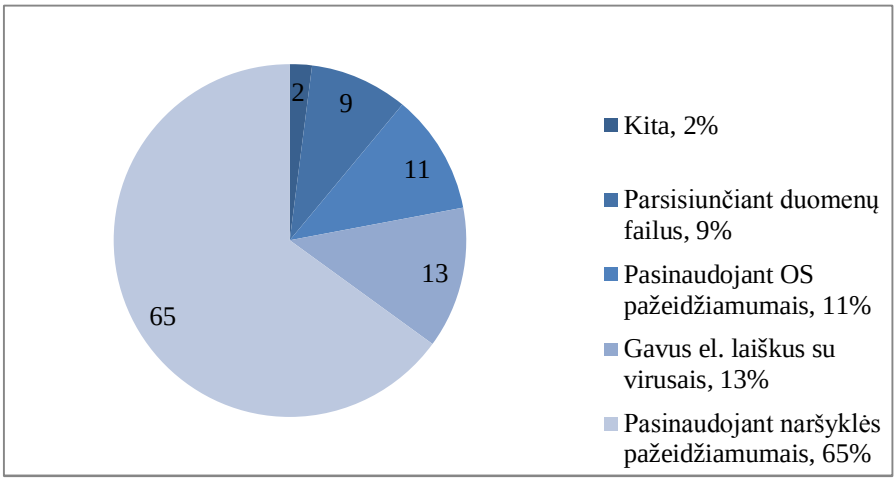
Slammer virusas 2003 m. yra turbūt daugiausiai žalos padaręs virusas iš kada nors paleistų į interneto platybes. Virusas atakuodavo serverius su SQL duomenų bazėmis (tai viena iš populiariausių serverių duomenų struktūros sudarymo programų) ir sustabdydavo jų veiklą. Nuolat skenuodamas prievadus (angl. – port) – jis sugebėdavo platinti tinkle pats save. Milžiniški kiekiai informacinių "šiukšlių" greitai perkrovė ryšio kanalus visame pasaulyje.

Melissa virusas buvo sukurtas David L. Smith`o. *Melissa* virusas į pasaulį buvo išleistas 1999 m. Virusas plito elektroniniu paštu per prisegtą priedą kurį atidarius laiškas persiunčiamas 50-imčiai vartotojų esančių elektroninio pašto programos adresų knygutėje. Šio viruso dėka buvo padarytą tokia didelė žala, kad kai kurios kompanijos išjungė savo elektroninio pašto programas iki tol, kol virusas bus nukenksmintas.

LoveLetter arba *ILOVEYOU* kirminas atsirado 2000 m. Šis virusas, kaip ir *Melissa* plito elektroniniu paštu išsiuntinėdamas savo kopijas adresatams, įrašytiems į Microsoft Outlook adresų knygą - laiško pavadinimas skambėjo "Aš tave myliu", o viduje prisegtas priedas su dvigubu plėtiniu .txt.vbs. Kai atidaromas toks priedas, kirminas pradeda įvairias būdais plisti. Kirminas nusikopijuoja į aukos kompiuterį ir sukuria kelis registro įrašus. Įsiveisęs virusas atsisiunčia slaptažodžių vagimo programą kuri vagia įvairią asmeninę informacija. Tuomet *ILOVEYOU* naudoja elektroninį paštą arba pokalbių programas, kad save išplatintų į kitus kompiuterius. Kai kurie šaltiniai tvirtina, kad šis virusas pridarė žalos už 10 milijardų dolerių.

2.4. KOMPIUTERINIŲ VIRUSŲ PLITIMO IR SLAPSTYMOSI BŪDAI

Dažniausiai kompiuteriai užkrečiami virusais esant naršyklės pažeidžiamumams (65 %), gavus el. laiškų su virusais (13 %), esant operacinių sistemų pažeidžiamumams (11 %), parsisiunčiant duomenų failus (9 %) ir kita (2 pav.) [3].



2 pav. Užsikrėtimo kompiuteriniais virusais būdai

Virusai patenka į kompiuterius kanalais, kurie naudojami informacijos mainams. Pagal plitimo būdus, kompiuteriniai virusai gali būti skirstomi į plintančius internetu, tinklais ir diskais.

Internetas tapęs labiausiai naudojamu informacijos siuntimo ir priėmimo kanalu, kartu tapo geriausiu keliu plisti virusams, o el. paštas - greičiausiu būdu virusų plitimui. Būtent el. paštui priskiriama didžiausia dalis pasaulio kompiuterių užkrėtimų. Taip yra todėl, kad informacija elektroniniu paštu keliauja labai greitai, interneto vartojimas auga labai sparčiai, modernūs virusai sugeba nuskaityti ir išsiųsti laiškus elektroninio pašto adresų knygelėse esančiais adresais. Naršant interneto puslapius taip pat galima nesunkiai pasigauti virusų, nes šie nesunkiai prikimba prie puslapių veikimą palaikančių programų ar serverių, kai kurie virusai gali nukreipti vartotojus prie jau infekuotų virusų. Failų mainų protokolas (FTP) dar vienas būdas plisti virusams, nes iš FTP serverių failai tiesiogiai nukopijuojami į vartotojo kompiuterį, taip kartu gali būti nukopijuojami ir virusai. Naujienų grupėse, ICQ, Skype ir pan. programomis siunčiamos žinutės taip pat gali būti su prilipusiais virusais, kurie tokiu būdu gali žaibiškai plisti.

Tinklai spartina informacijos perdavimą ir lengvina darbą su ja, tačiau tą patį daro ir su virusų plitimu. Kompiuteriai, kurių kietųjų diskų informacija yra prieinama tinklo vartotojams, labai padidina savo galimybę būti užkrėstais iš kitų tinkle esančių kompiuterių plintančių virusų. Jei darbo stotys reguliuojančios tinklo veiklą ir interneto ryšį nėra pakankamai apsaugotos, virusai nesunkiai gali patekti į visus valdomus kompiuterius bei serverius (iš serverių taip pat galimas atvirkštinis tinklo užkrėtimas). Nors dažniausiai virusai turi tuos pačius tikslus, tačiau veikia skirtingais būdais. Tinklu plintantys virusai gali naudotis programavimo klaidomis, atakuoti tam tikrus failus ar pašto serverius. Didžiausias virusų pavojus - jų galimybė sparčiai plisti, todėl virusui patekus į vieną tinklą, turėtų būti užkisti keliai plisti toliau.

Diskai būdami informacijos talpyklomis kartu tampa užkrėstos informacijos pernešėjais. Diskeliai, kuriais vieninteliais galėjo plisti paleidžiamieji virusai, jau eina užmarštin, tačiau vis labiau populiarėjantys ir daugiau informacijos talpinantys CD-R ir DVD diskai, bei USB atmintinės didina tikimybę, jog tarp sukauptos informacijos bus užkrėstų bylų. Įrašant informaciją į diskus ji ne visada skenuojama nuo virusų, todėl jais perkeliama informacija gali būti virusų plitimo šaltiniu.

Virusai slepiasi nuo antivirusinių ir kitų saugumą užtikrinančių įrenginių naudodamiesi daugybe metodų.

- Veikimas slapčia

  Virusai, kurie naudojasi šiuo metodu, slepia savo buvimo išskirtinius bruožus, kurie leidžia aptikti jų veikimą. Pavyzdžiui failo dydis kai jis užkrėstas paprastai didėja, tačiau virusas įterpia savo kodą laisvose failo sekcijose, tokiu būdu užtikrinant sistemą, kad failo dydis nepakito. Užkrėtimo metu yra registruojama failo modifikavimo data ir laikas, tačiau kai veikia šie virusai, jie nekeičia šių atributų palikdami ankstesnius parametrus kaip ir prieš užkrėtimą. Norint išvengti įtarimo, kad failas buvo koreguojamas, virusai keičia failo atributus, kad negalima būtų jų peržiūrėti.

- Tunelio efektas (angl. *tunneling*)

  Tunelio efektas pakankamai sudėtingas reiškinys. Virusai, siekdami išvengti antivirusinių programų, naudodamiesi šiuo būdu tiesiogiai įterpia į operacinę sistemą prižiūrėtojus, kurie efektyviai slepia virusą nuo antivirusinės programos.

- Apsišarvavimas

  Virusai, kurie naudojasi šia technika, užslepia savo kodą, kad jo nebūtų galima nuskaityti. Antivirusinė programa, tam kad aptikti šį virusą turi naudoti euristinius nuskaitymo metodus (badymų ir klaidų metodas virusams aptikti).

- Pats savęs kodavimas.

  Šie virusai užkoduoja savo kodą, kad antivirusinei programai būtų sunkiau juos aptikti.

- Polimorfizmas

  Šie virusai kiekvieną sykį užkrėsdami sistemą koduojami ir dekoduojami naudojantis skirtingus algoritmus ir (de)kodavimo raktus.

Dauguma MS-DOS sistemos virusų stengiasi maskuotis nepakeisdami užkrėsto failo modifikavimo datos, tačiau dabartinės antivirusinėms programoms tai nėra didelė kliūtis.

- Kai kurie virusai užkrėsdami failus sugeba nepakeisti jų dydžio – tai vadinamieji *užpildantys virusai* (angl. *cavity viruses*). Jie tai sugeba padaryti perrašydami neišnaudotas failų vietas.
- Kitos bylos, kurių stengiasi vengti virusai yra vadinamieji failai-masalai (angl. bait

files).“ Tai antivirusinių programų ar profesionalų sukurti failai skirti virusų užkrėtimui. Jais naudojantis profesionalai gali aptikti virusų pavyzdžius, nesukeliant didesnės žalos kompiuteriui; virusų gaudytojams taip lengviau stebėti virusų elgseną ir nustatyti tinkamus virusų aptikimo būdus; kuomet tokio pobūdžio failai yra modifikuojami, antivirusinė sistema iš karto gauna pavojaus signalą, jog virusas yra sistemoje.

- Failo-masalo metodas nėra veiksmingas tada, kai virusas veikia atsitiktiniu būdu (angl. sparce infection) – t.y., kai failai puolimui yra pasirenkami atsitiktine tvarka arba virusas aktyvuojamas tik esant tam tikrom sąlygom.
- Šiuolaikinės antivirusinės programos randa virusus pagal tam tikrus virusų modelius programose skenuodamos taip vadinamus virusų parašus (angl. virus signatares). Šie parašų modeliai nurodo, kad virusas priklauso tam tikrai kenkėjų šeimai. Antivirusinė programa radusi tokį modelį nustato, kad failas yra užkrėstas. Tačiau šiuolaikiniai virusai naudoja tam tikras technikas kas daro tokį kovos būdą mažiau veiksmingą. Vieni jų naudojasi paprastomis modifikacijomis, pakeisdami paprogrames savo kode, tačiau kiti virusai modifikuoja savo kodus po kiekvieno užkrėtimo, o tai leidžia sukurti skirtingas virusų atmainas. Būtent šiais būdais veikia koduoti, polimorfiniai ir matamorfiniai virusai.

Dažniausi požymiai, rodantys, kad kompiuteris gali būti užkrėstas:

- Kompiuteris veikia lėčiau nei įprasta.
- Kompiuteris nebeatsako arba dažnai užrakinamas.
- Kompiuteris užstringa, tada kas kelias minutes paleidžiamas iš naujo.
- Kompiuteris automatiškai paleidžiamas iš naujo. Be to, kompiuteris neveikia kaip įprasta.
- Kompiuteryje esančios programos veikia netinkamai.
- Diskai arba diskų įrenginiai yra nepasiekiami.
- Negalite tinkamai atspausdinti elementų.
- Rodomi keisti klaidų pranešimai.
- Rodomi iškraipyti meniu ar dialogo langai.
- Neseniai atidarytame priede yra dvigubas plėtinys, pavyzdžiui, .jpg, .vbs, .gif arba .exe.
- Kažkodėl išjungiama antivirusinė programa. Be to, jos negalima vėl paleisti.

- Kompiuteryje negalima įdiegti antivirusinės programos arba jos neįmanoma paleisti.
- Darbalaukyje atsiranda naujų piktogramų, kurių ten nedėjote, arba jos nėra susijusios su jokia pastaruoju metu įdiegta programa.
- Netikėtai per garsiakalbius pasigirsta keisti garsai arba leidžiama muzika.
- Iš kompiuterio dingsta programa, nors jos specialiai nepašalinote. [6].

2.5. APSAUGA NUO KOMPIUTERINIŲ VIRUSŲ

Dažniausias ginklas prieš kompiuterinius virusus – antivirusinės programos, kurios aptinka ir naikina virusus po naujų programų suinstaliavimo ar paleidimo. Antivirusinės programos veikia įvairiais būdais. Kai kurios iš jų nuskaito visus kompiuteryje (kartu ir diskų įrenginiuose) esančius failus ir tikrindamos, ar juose nėra virusų parašų, kurių pavyzdžiai sukaupti programos duomenų bazėje. Kai kurios programos nuskaito jau atidarytus failus, kitos gali pateikti vartotojui įtartinus failus pagal jų tipą.

Kuriant programas kovai su kompiuteriniais virusais skiriami kovos būdai – mikroskopinis ir makroskopinis. Jau minėtus antivirusinių programų veikimo būdus galima priskirti mikroskopiniam kovos būdui, nes šiais atvejais tikrinama, ar failuose nėra atitinkamų virusų šablonų. Tuo tarpu makroskopiniai būdai remiasi vartotojų elgsena. Šiuo būdu galima kovoti net nežinant viruso struktūros (tokiu atveju virusas nesunaikinamas, bet sustabdomas jo plitimas), todėl manoma, kad ateityje jis taps vis efektyvesnis ir plačiau naudojamas.

Ne visos antivirusinės programos yra vienodai efektyvios ir naudingos dėl vėluojančių atnaujinimų, duomenų bazėse sukauptų virusų pavyzdžių skaičiaus, kompiuterio veikimo stabdymo. Antivirusinės programos nedaro pakeitimų programinėje kompiuterių įrangoje tam, kad apsisaugoti nuo kitų virusų atakų (nors buvo bandymų tą daryti, bet tai pasirodė neveiksminga dėl didelės failų rūšių įvairovės).

Vartotojai taip pat naudoja užkardas (angl. *firewall*). Tai programa veikianti kaip apsauginis užtvaras, tikrinantis ir ribojantis informaciją, kuri keliauja tarp vartotojo kompiuterio ir paslaugų teikėjo tinklo arba interneto. Taip užkertamas kelias bandymams iš

išorės patekti į kompiuterį be vartotojo žinios, padedama kontroliuoti visus tinklo duomenų srautus [3,4].

3. 2010 METŲ KOMPIUTERINIŲ VIRUSŲ STATISTIKA

Šiame skyriuje pateikiama 2010 m. Kaspersky Laboratorijos metinis pranešimas. Didelių pasikeitimų, lyginant su ankstesniais metais, vertinant žalingas programas neužfiksuota. Pagrindinės to priežastys: kai kurių trojanų, ypač žaidimų trojanų, aktyvumo sumažėjimas, antivirusinių programų prekiautojų ir telekomunikacinių ryšių tiekėjų griežti žygiai prieš nelegalius prekiautojus ir kompiuterinius nusikaltėlius, griežtėjantys įstatymai. Tačiau žalingų programų skaičiaus stabilizacija nereiškia, kad sumažėjo kompiuterinių atakų skaičius, kurios gali būti skirstomos į:

- atakas per Internetą (aptiktos tinklo antivirusinėmis programomis);
- lokaliniai incidentai (aptiktos vartotojų kompiuteriuose);
- tinklų atakos (aptiktos įsibrovėlių aptikimo sistemomis IDS (angl. *Intrusion Detection System*));
- incidentai elektroniuose paštuose;

2010 m. bendras aptiktų incidentų skaičius viršija 1,5 mlrd., iš kurių 30 proc. atakų įvykdyta per naršykles. Kartu atsirado daug pažeidžiamų taikomųjų programų vietų ir būtent per jas buvo skverbiamasi į vartotojų kompiuterius. Pagal užfiksuotų incidentų skaičių 2010 metų lyderiai Microsoft ir Adobe programa ir jos taikymai.

2010 m. kitas svarbus žalingos informacijos tunelis P2P tinklai. Beveik visų tipų virusai, paslėpti trojanai ir kirminai plito per P2P tinklus. Pažangiems ir sudėtingiems priskiriami Mariposa, ZeuS, Bredolab, TDSS, Koobface ir pan, botnet tinklai paveikė milijonus kompiuterių. Jie plito daugiausiai elektroniniu paštu ir buvo novatoriai socialiniuose ir P2P tinkluose, kai kurie iš jų pirmieji pažeidė 64-bitų platformas.

Žalingų programų kūrėjų išradingumas pasireiškė kuriant Stuxnet kirminą. Jam išanalizuoti ir pilnai suprasti jo komponenčių darbą prireikė daugiau kaip 3 mėnesių. Taigi vyrauja tendencijos, kad virusai sudėtingės ir tai didins antivirusinės produkcijos apimtis. Šiomis dienomis neužtenka pažinti 99 % žalingų programų ir nesugebėti aptikti ir paveikti, kad ir vienos, bet labai sudėtingos, pažangios, ir dėl to labai plačiai paplitusios grėsmės.

Socialinių tinklų, tokių kaip Facebook, ar Twitter populiarėjimas taip pat atkreipė žalingų programų kūrėjų dėmesį. Naujojo tipo ataka 2010 m. gegužės mėnesį buvo

paremta Facebook'o "Like" mygtuko funkcija. Vartotojai buvo viliojami patraukliomis nuorodomis, bet jos vedė į specialiai sukurtą puslapį, kur JavaScript kodas patalpino nematomą "Like" mygtuką ir fiksavo bet kokį paspaudimą, nepaisant to, kur stovėjo kursorius.Tokios nuorodos kopija atsirasdavo vartotojo sienoje ir pasiekdavo jo draugus bei draugų draugus ir t.t. Kiekvieną kartą vartotojui patekus į tą puslapį, kompiuteriniai nusikaltėliai dėl reklaminių puslapio tikslų gaudavo nedidelę sumą pinigų.

2010 m. Kaspersky Lab užfiksavo 580 371 937 atakas prieš jų antivirusinių programų vartotojus (2009 m. 73 619 767).

Internetinės atakos. 1 lentelėje pateikta 2010 m. dažniausių žalingų programų atakų per internetą prieš vartotojus penketukas.

1 lent. 2010 m. internetinių atakų skaičius (Kaspersky Lab duomenys)

Vieta	Vardas	Atakų skaičius	% nuo visų atakų
1	Blocked	347,848,449	59.94%
2	Trojan.Script.Iframer	37,436,009	6.45%
3	Trojan.Script.Generic	19,601,498	3.38%
4	Trojan-Downloader.Script.Generic	13,887,220	2.39%
5	Trojan.Win32.Generic	9,515,072	1.64%

Tinklų atakos. Užkardos (angl. *firewalls*) yra svarbi šio tipo atakų apsaugos priemonė. 2 lentelėje pateikti duomenys naudojant Kaspersky Internet Security sistemą, turinčią įsibrovėlių detekcijos sistemą (IDS), kuri 2010 m. aptiko 1 311 156 130 tinklų atakų (2009 m. apie 220 mln.).

2 lent. 2010 m. tinklų atakų skaičius (Kaspersky Lab duomenys)

Vieta	Vardas	Atakų skaičius	% nuo visų atakų
1	Intrusion.Win.NETAPI.buffer-overflow.exploit	557,126,500	42.49%
2	DoS.Generic.SYNFlood	400,491,518	30.54%
3	Intrusion.Win.MSSQL.worm.Helkern	262,443,478	20.02%
4	Scan.Generic.UDP	45,343,780	3.46%
5	Intrusion.Win.DCOM.exploit	14,134,307	1.08%

Kita dalis atakų – vietinės infekcijos, kurios prasiskverbia į vartotojų kompiuterius ne internetu, elektroniniu paštu ir tinklais. 3 lentelėje pateiktos 5 populiariausios programos, aptiktos vartotojų kompiuteriuose, 2010 m. užfiksuota apie 1,5 mlrd. tokių atakų.

3 lent. 2010 m. vartotojų kompiuterių atakų skaičius (Kaspersky Lab duomenys)

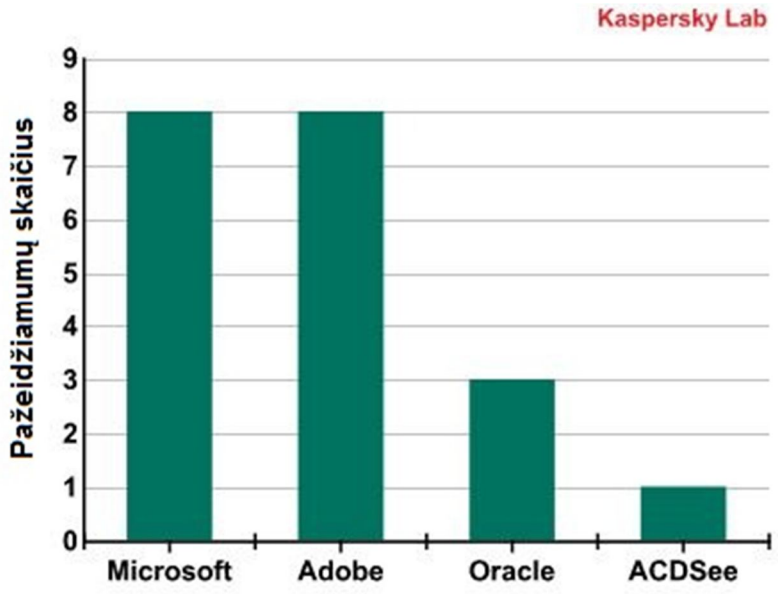
Vieta	Vardas	Atakų skaičius	% nuo visų atakų
1	Trojan.Win32.Generic	9,226,235	20.16%
2	DangerousObject.Multi.Generic	8,400,880	18.36%
3	Net-Worm.Win32.Kido.ih	6,386,762	13.96%
4	Virus.Win32.Sality.aa	4,182,229	9.14%
5	Net-Worm.Win32.Kido.ir	3,785,066	8.27%

2010 m. programų pažeidžiamumų analizė pateikta 4 lentelėje, iš viso jų buvo aptikta 510.

4 lent. 2010 m. kompiuterių programų pažeidžiamumai (Kaspersky Lab duomenys)

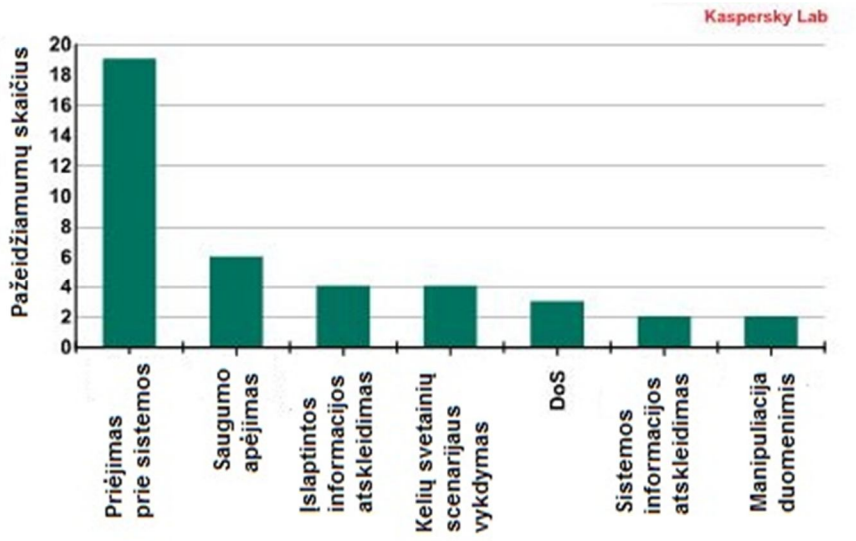
Pažeidžiamumas	% visų kompiuterių, kur buvo aptiktas	Vardas	Poveikis	Įvertinimas	Išleidimo data
31744	26.98%	Microsoft Office OneNote URI Handling	Priėjimas prie sistemos	Labai pavojingas	09.09.2008
35377	26.64%	Microsoft Office Word	Priėjimas prie sistemos	Labai pavojingas	09.06.2009
38805	24.98%	Microsoft Office Excel	Priėjimas prie sistemos	Labai pavojingas	09.03.2010
37255	23.18%	Sun Java JDK / JRE	Priėjimas prie istemos, DoS, informacijos atskleidimas, manipuliacija duomenimis, apsaugos apėjimas	Labai pavojingas	31.03.2010
38547	17.41%	Adobe Flash Player DomainSandbox	Apsaugos apėjimas	Vidutiniškai pavojingas	12.02.2010

3 paveiksle pateikta 2010 m. 20 dažniausių pažeidžiamumų programinės įrangos kūrėjai.



3 pav. 2010 m. 20 dažniausių pažeidžiamumų programinės įrangos kūrėjai

Jeigu šiuos dažniausius pažeidžiamumus skirstytume pagal vykdomos operacijos tipą, gautume 4 paveiksle pavaizduotą skirstinį [8,9].



4 pav. 2010 m. dažniausių pažeidžiamumų operacijos

4. IŠVADOS IR ATEITIES PROGNOZĖS

Pirmieji kompiuteriniai virusai buvo santykinai nežalingi ir plisdavo lėtai, tai nuo praėjusio amžiaus paskutiniojo dešimtmečio antros pusės, atsiradus internetui, virusai gali plisti greičiau nei per valandą ir visame pasaulyje, padarydami milijardines žalas.

Norint apsaugoti kompiuterį nuo žalingos veiklos būtina imtis visų saugumo priemonių: parsisiųsti atnaujinimus, saugiai naršyti internete, neatidarinėti įtartinų failų.

Apibendrinant galima pasakyti, kad pastarąjį dešimtmetį pagrindinės tendencijos paveikusios ir virusų kūrėjus buvo:

- Mobilumas ir priemonių miniatūrizacija – vis mažesnės (dydžiu) priemonės pasiekti internetą, bevieliai tinklai;
- Virusų kūrimo orientacija į kompiuterinius nusikaltimus;
- Windows vis dar operacinių sistemų lyderis;
- Socialiniai tinklai ir paieškos varikliai – svarbiausios šių dienų interneto funkcijos;
- Internetinė bankininkystė ir prekyba internetu;

Norint suprasti, kas laukia ateityje, reikia išanalizuoti kompiuterinių atakų tikslus, metodus ir surasti organizatorius. 2011 m. laukia nauja karta dar labiau organizuotų ir žalingesnių kompiuterinių programų kūrėjų, žalingų informacinių atakų finansiniais tikslais, naujos kartos vagysčių priemonės *Spyware*2.0 iškilimas ir dar gausesnės atakos prieš programų pažeidžiamumus ir spragas.

Bandant prognozuoti, kas laukia artimiausiąjį dešimtmetį, išryškėja tokios tendencijos: Windows praras operacinių sistemų lyderio pozicijas ir naujų operacinių sistemų atsiradimas ir jų skaičiaus augimas veiks virusinių programų kūrimą – kompiuteriniai nusikaltėliai nesugebės sukurti žalingų kodų dideliam skaičiui platformų. Taip pat prognozuojama, kad atakų kūrėjai pasiskirstys į dvi grupes: tie, kurie atakuos verslo struktūras, ir tuos, kurių tikslas bus dalykai, kurie daro įtaką kasdieniniam gyvenimui, pvz. transporto sistemos. Taip pat akivaizdu, kad mobiliųjų technologijų naudojimas augs eksponentiškai, o senas posakis „Kas valdo informaciją, tas valdo pasaulį“ bus aktualus kaip niekad anksčiau.

5. LITERATŪRA

1. History of Computer Viruses. Prieiga per internetą: http://www.antivirusworld.com/articles/history.php
2. A Short History of Computer Viruses and Attacks. Washington Post, 2002. Prieiga per internetą: http://www.washingtonpost.com/wp-dyn/articles/A50636-2002_Jun26_2 .html
3. Virus, Worms, antivirus and Security Information. Prieiga per internetą: http://www.pandasecurity.com/homeusers/security-info/
4. Kompiuteriniai virusai. Prieiga per internetą: http://www.esaugumas.lt/index.php?-1030858023
5. Computer Virus: The Types of Viruses Out There. Prieiga per internetą: http://www.spamlaws.com/virus-types.html
6. Kompiuterinių virusų požymiai. Prieiga per internetą: http://support.microsoft.com/kb/129972
7. Interneto grėsmės. Lietuvos rytas, 2008. Prieiga per internet: http://m.lrytas.lt/-12036729681201335918-p1-interneto-gr%C4%97sm%C4%97s.htm
8. Kaspersky Security Bulletin. Malware Evolution 2010. Prieiga per internetą: http://www.securelist.com/en/analysis/204792161/Kaspersky_Security_Bulletin_Malware_Evolution_2010
9. Kaspersky Security Bulletin. Statistics, 2010. Prieiga per internetą: http://www.securelist.com/en/analysis/204792162/Kaspersky_Security_Bulletin_2010_Statistics_2010
10. Cybercrime outlook 2020 from Kaspersky Lab. Prieiga per internetą: http://www.securelist.com/en/analysis/204792165/Cybercrime_Outlook_2020_From_Kaspersky_Lab