«ԻՆՏԵՐԱԿՏԻՎ ԿՐԹՈՒԹՅԱՆ ԶԱՐԳԱՑՈՒՄ» ՀԻՄՆԱԴՐԱՄ

ՀԵՐԹԱԿԱՆ ԱՏԵՍՏԱՎՈՐՄԱՆ ԵՆԹԱԿԱ ՈՒՍՈՒՑԻՉՆԵՐԻ ՎԵՐԱՊԱՏՐԱՍՏՄԱՆ ԴԱՍԸՆԹԱՑ 2022

ՀԵՏԱԶՈՏԱԿԱՆ ԱՇԽԱՏԱՆՔ

ԹԵՄԱ	Համակարգչային վիրտուալներ վնասատու ծրագրեր
ԱՌԱՐԿԱ	Ինֆորմատիկա
ՀԵՂԻՆԱԿ	Կարինե Անդրեասյան
ՄԱՐԶ	Արմավիր
ՈՒՍՈՒՄՆԱԿԱՆ ՀԱՍՏԱՏՈՒԹՅՈՒՆ	Հայկաշենի Գ. Կիրակոսյանի անվան միջն. դպրոց

Բովանդակություն

ՆԵՐԱԾՈՒԹՅՈՒՆ

Թեմայի արդիականությունը: Համակարգչային վիրուսը ծրագիր է, որը կարող է ինքն իրեն պատճենվել և տարածվել՝ վարակելով համակարգիչն առանց օգտագործողի թույլտվության կամ իմացության: Մի քանի տարի առաջ վիրուսների մեծամասնությունը սահմանափակվում էր համակարգչային սկավառակների և ծրագրերի աղտոտմամբ: Հիմնականում վնասը սահմանափակվում էր տվյալների կորստով, քանի որ վիրուսները մաքրում կամ (երբեմն) փչացնում էին սկավառակի վրայի տվյալները: Այժմ ամեն ինչ այլ է: Այսօր կիբեռանվտանգության ապահովումը լայնածավալ խնդիր է: Վնասակիր ծրագրերը գրվում են անօրինական ճանապարհով այլ համակարգիչների օգտագործմամբ տեղեկատվություն ստանալու նպատակով, իսկ համակարգչային տեխնոլոգիաների կիրառումը կամ օգտագործումը զարգանում է շատ արագ: Այժմ կյանքի բոլոր ոլորտներում տեղեկատվական տեխնոլոգիաների զարգացման և համատարած ներդրման հետ կապված արդիական խնդիր է համարվում հուսալի տեղեկատվական համակարգերի կազմակերպումը և ապահովումը: Դասապրոցեսի ընթացքում ևս հանդիպել ենք նման իրավիճակների, ինչը պատճառ է հանդիսացել աշխատանքի թեմայի ընտրության հարցում:

Հետազոտության նպատակը և խնդիրները: Հետազոտական աշխատանքի նպատակն է համակարգչային վիրուսների ուսումնասիրությունը, դրանց տեսակների նկարագրությունը և հասցվող վնասներից խուսափման միջոցառումների իրականացումը: Այժմ կյանքի բոլոր ոլորտներում տեղեկատվական տեխնոլոգիաների զարգացման և համատարած ներդրման հետ կապված արդիական խնդիր է համարվում հուսալի տեղեկատվական համակարգերի կազմակերպումը և ապահովումը, որոնք կլինեն կազմակերպությունների աշխատանքների ապակայունացման ազդեցության կամ տեղեկատվության գողությունների դեմ դիմացկունության, ինչպես նաև մշակվող և պահպանվող տվյալների արժանահավատության պահպանման հիմնական միջոցը:

Հետազոտության օբյեկտը և առարկան: Հետազոտական աշխատանքի օբյեկտ է հանդիսանում համակարգչի համակարգային տարածքը, դրայվերները, փաստաթղթերը, հասարակ խմբագիր-ծրագրերի կողմից ստեղծված փաստաթղթերը, տվյալների բազաների ֆայլերը և այլն: Իսկ ուսումնասիրության առարկա հանդիսացող համակարգչային վիրուսը, որն իրենից ներկայացնում է ծրագիր, կարող է ներթափանցել համակարգիչ և վարակել մի կամ միանգամից մի քանի օբյեկտներ, ինչի հետևանքով կլինեն տվյալների կորուստներ, համակարգի

կախում, համակարգչի առանձին մասերի խափանում և այլն: Հատկանշական է, որ տեքստային բնույթ կրող ֆայլերը վիրուսակիր չեն լինում, սակայն վիրուսը կարող է փոփոխման ենթարկել դրանք:

Հետազոտության տեսական, մեթոդաբանական և տեղեկատվական հիմքերը:

Աշխատանքի կատարման համար տեսական և մեթոդաբանական հիմք են ծառայել թեմային առնչվող դասագրքերը, ՀՀ իրավական ակտերը, ինտերնետային կայքերը: Օգտագործվել են ինչպես հայրենական այնպես էլ արտասահմանյան գրականություն:

Հետազոտական աշխատանքի տեսական նյութը և առաջարկված մեթոդները կարելի է կիրառել հանրակրթական դպրոցում տվյալ թեմաների դասավանդման ժամանակ:

Ավարտական աշխատանքի կառուցվածքը: Ավարտական աշխատանքը բաղկացած է բովանդակությունից, ներածությունից, ավարտական աշխատանքի հիմնական նյութից, եզրակացությունից և օգտագործված գրականության ցանկից:

Գլուխ 1

Համակարգչային վիրուսների էությունը և նշանակությունը

Ժամանակակից անհատական համակարգչով աշխատելիս օգտագործողներին (հատկապես սկսնակ) կարող են հետապնդել շատ անհաջողություններ՝ տվյալների կորուստ, համակարգի կախում, համակարգչի առանձին մասերի խափանում և այլն: Պատճառներից մեկը կարող է հանդիսանալ վիրուսային ծրագրերի ներխուժումը համակարգչային համակարգ: Վիրուսները համարյա թե ամենավտանգավոր թշնամիներն են համակարգչի համար: Այդ ծրագրերը կենսաբանական վիրուսների նման բազմանում են՝ գրանցվելով սկավառակի համակարգային տարածքում, կամ կցվելով ֆայլերին՝ կարող են կատարել տարբեր ոչ ցանկալի գործողություններ:

Համակարգչային վիրուսի առաջին «համաճարակը» տեղի ունեցավ 1986 թվականին, երբ Brain (ուղեղ) անվամբ վիրոռավ սկսեցին «վարակվել» ճկուն մագնիսական սկավառակները: Ներկայումս հայտնի են մոտ 5 հազարից ավելի վիրուսներ, որոնք տարածվելով համակարգչային ցանցով՝ վարակում են դրանց հետ համագործակցող համակարգիչները[1]:

[1] Ինֆորմատիկա 8-րդ դասարան, դասագիրք, Ս.Ս Ավետիսյան, Ս.Վ. Դանիելյան; մասն. խմբ. Ռ.Վ. Աղգաշյան – Երևան: Տիգրան Մեծ, 2013, – 168 էջ

Ընդհանուր առմամբ վիրուսը փոքրածավալ ծրագիր է, որի ստեղծողներն այն մեծապես օժտում են նաև **«ինքնաբազմացման»** ունակությամբ: Վիրուսակիր ծրագիրը կարող է ամենատարբեր գործողությունների **«հեղինակ»** հանդիսանալ՝ սկսած ամենաանմեղներից՝ էկրանին բերվող պատկերի աղավաղում, երաժշտական հոլովակների ցուցադրում և այլն, մինչև լրջորեն վնասելը՝ համակարգչային տվյալների ոչնչացում և նույնիսկ համակարգչի առանձին միկրոսխեմաների անսարքության առաջացում: Համակարգիչը վարակելուց հետո վիրուսը կարող է **«թաքնվել»** ու **«հարձակման անցնել»** որոշակի իրադարձությունից՝ շաբաթվա որևէ օրվանից, կոնկրետ ամսաթվից, կիրառական որևէ ծրագրի աշխատելուց, փաստաթուղթ բացելուց հետո միայն:

Վիրուսակիր ծրագրերը կարող են տեղակայվել հաճախակի կիրառվող ծրագրային ֆայլերի տարբեր մասերում՝ դրանց սկզբում, միջնանասում կամ վերջում:

Համակարգչային վիրուսները կցվում են որևէ ծրագրի կամ ֆայլի դրանց աշխատանքի ժամանակ: Սակայն վիրուսները անպայմանորեն չեն վարակում բոլոր աշխատող ֆայլերը: Շատ հաճախ վիրուսներից շատերը գրվում են միայն մեկ կամ մի քանի տեսակի ֆայլերի համար: Ավելին, վիրուսներից շատերը վարակում են ոչ թե օգտագործողի կողմից ստեղծված, այլև շատ հաճախ՝ հենց համակարգային ֆայլերը: Որքան երկարատև է վիրուսը աշխատում համակարգչում այնքան ավելի ու ավելի շատ ֆայլեր է այն վարակում: Տարածվելով մի ֆայլից մյուսին, և համապատասխան պահի սպասելով, վարակը կարող է կցվել էլեկտրոնային նամակին կամ վարակելով ցանցային ֆայլային համակարգը անցնել ցանցի ներսում գտնվող հաջորդ համակարգչին:[2]

Համակարգչային վիրուսների շարքին հաճախ սխալմամբ դասում են բազմաթիվ վնասակար ծրագրային միջոցներ (malicious software-MALWARE), որոնք իրականում վիրուսներ չեն, կարող են ունենալ կամ չունենալ վերարտադրվելու հատկություն և շատ հաճախ կարող են զգալի վնաս հասցնել օգտագործողին և նրա կողմից օգտագործվող համակարգին: Այնուամենայնիվ այս վնասակար ծրագրերը նույնպես դիտարկվում են որպես անցանկալի և դրանք շատ հաճախ դիտվում են վիրուսների հետ մեկ շարքում[3]:

Ծրագրային վնասակար միջոցների թվին են պատկանում՝

- որդերը (WORMS),

[2] https://totalsec.wordpress.com

[3] *А.Савицкий.* Опрос: Самая непонятная киберугроза. Лаборатория Касперского (10 февраля 2014).

- գովազդային՝ օժանդակվող ծրագրային միջոցները (Advertising-supported software-ADWARE),
- հետախուզական՝ գաղտնի ծրագրային միջոցները (Spy Software-SPYWARE),
- դեպի օգտագործողի համակարգիչ չարտոնված մուտքի շնորհման՝ գաղտնի աշխատող ծրագրային միջոցները (Root Kit-ROOTKIT),
- կեղծ անվանումով և օրինական ծրագրի դիմակով աշխատող՝ իրականում ծածուկ վնաս հասցնող ծրագրային միջոցները (Trojan Horse-TROJAN),
- իրականում վնասակար՝ օգտագործողի համակարգչի համար օգտակար ծրագրի դիմակի տակ աշխատող և այդ «օգտակարությունը» ամեն կերպ խարդախությամբ լավ կողմից ներկայացնող ծրագրային միջոցները (scaring software- SCAREWARE),
- ինտերնետային հանցագործության համար ստեղծված որևիցե վնասակար ծրագրային միջոց (վիրուս) (crime software-CRIMEWARE):

Գլուխ 2

Համակարգչային վիրուսների տեսակները

Համակարգչային վիրուսները իրարից տարբերվում են նրանով, թե ինչպիսի օբյեկտներում են նրանք տեղավորվում, այսինքն ինչ են վարակում: Որոշ վիրուսներ կարող են վարակել միանգամից մի քանի օբյեկտներ: Վիրուսների մեծամասնությունը տարածվում են վարակելով կատարողական ֆայլերը՝ ֆայլեր որոնք ունեն exe և com ընդլայնումներ: Այս վիրուսները կոչվում են ֆայլային: Վիրուսը, որը գտնվում է վարակված կատարողական ֆայլերում, սկսում է իր աշխատանքը այն ծրագրի բեռնման ժամանակ, որում գտնվում է ինքը: Մեկ այլ վիրուսների տարածված տեսակ, որը ներխուժում է կոշտ սկավառակի սկզբնական սեկտոր, որտեղ գտնվում է օպերացիոն համակարգը բեռնող ծրագիրը: Այսպիսի վիրուսները կոչվում են բեռնային վիրուսներ: Այս վիրուսները սկսում են իրենց աշխատանքը համակարգչի բեռնման ժամանակ: Բեռնային վիրուսները համարվում են ռեզիդենտ և վարակում են համակարգչի մեջ տեղակայված սկավառակները: Որոշ վիրուսներ կարողանում են վարակել դրայվերներ: Դրայվերում գտնվող վիրուսը սկում է իր աշխատանքը տվյալ դրայվերի բեռնման (CONFIG.SYS ֆայլից) ժամանակ: Սովորաբար վիրուսները, որոնք վարակում են դրայվերները վարակում են նաև կատարողական

ֆայլերը, քանի որ այլ կերպ այդ վիրուսները չէին կարողանա տարածվել: Շատ հազվադեպ են հանդիպում վիրուսներ, որոնք վարակում են համակարգային DOS ֆայլերը (IO. SYS կամ MSDOS.SYS): Սովորաբար այդպիսի վիրուսները վարակում են նաև սկավառակի բեռնման սեկտորները, քանի որ այլ կերպ նրանց չի հաջողվի տարածվել: Հազվադեպ են հանդիպում վիրուսներ, որոնք վարակում են հրամանային ֆայլերը: Սովորաբար այդպիսի վիրուսները հրամանային ֆայլի հրամանների միջոցով ձևակերպում են սկավառակի վրա կատարող ֆայլ, բաց են թողնում այն, այնուհետև տեղի է ունենում վիրուսների բազմացումն ու տարածումը, որից հետո ֆայլը մաքրվում է սկավառակից: Այս վիրուսները սկսում են իրենց աշխատանքը հրամանային ֆայլի կատարման ժամանակ, որտեղ նրանք գտնվում են: Վիրուսը իրենից ներկայացնում է ծրագիր, այդ պատճառով օբյեկտները, որոնք ծրագրային կոդ չեն պարունակում, չեն կարող վարակվել վիրուսով: Այդպիսի օբյեկտները կարող են միայն վրուսների հետևանքով փչանալ: Այդպիսի օբյեկտների թվում են պատկանում հասարակ խմբագիր-ծրագրերի կողմից ստեղծված փաստաթղթերը և տվյալների բազաների ֆայլերը[4]:

Իրենց պահելաձևից ելնելով վիրուսները բաժանվում են երկու խմբի. ռեզիդենտ և ոչ ռեզիդենտ վիրուսների:

Ռեզիդենտ (կամ նույն է թե մշտապես տեղակայված) այս տեսակի վիրուսների վարակիչ կոդերը (վերարտադրվող մոդուլը) իրենց բեռնում են օպերատիվ հիշողության մեջ (ասել է թե մշտապես տեղակայվում են այնտեղ), որևէ վարակված ծրագրին կցված լինելով, և սպասում այնտեղ ակտիվ վիճակում այնքան ժամանակ մինչև օպերացիոն համակարգը կամ օգտագործողը չաշխատացնի այլ ծրագիր: Վերջինս վարակվելով, վերահսկողությունը հանձնում է արդեն նոր տիրոջը և սպասում իր հաջորդ «զոհին»: Ռեզիդենտ վիրուսները հաճախ բաժանում են արագ վարակող կամ դանդաղ վարակող վիրուսների: Արագ վարակող ռեզիդենտ վիրուսները կարող են վարակել բոլոր այն ֆայլերը, որոնք այդ պահին սկսում են աշխատել: Նման դեպքում անգամ հենց ինքը հակավիրուսը, եթե չի հայտնաբերել, որ վիրուսի կիրառական մոդուլը նստած է հիշողության մեջ և այն չի վերացրել, կարող է պատճառ դառնալ ամբողջ համակարգչի ֆայլերի վարակմանը: Այդ դեպքում, հակավիրուսի ընդլայնված սքանավորման ժամանակ, յուրաքանչյուր ֆայլի վրա անցնելիս, ակտիվացնում է վերջիններիս դրանով իսկ թույլ տալով վիրուսին տեսնել և վարակել դրանք: Դանդաղները, հակառակը՝ փորձում են հնարավորինս քիչ ֆայլեր վարակել և դրանով իսկ անտեսանելի մնալ: Ի տարբերություն ռեզիդենտ վիրուսների, ոչ ռեզիդենտները ունեն երկու

[4] https://hy.wikipedia.org

մոդուլ՝ փնտրման և վերարտադրվելու: Երբ վիրուսը վարակում է համակարգիչը նրա փնտրման մոդուլը անմիջապես փնտրում է նոր ֆայլեր և գտնելով այն դիմում է վերարտադրման կամ վարակիչ մոդուլի օգնությանը, որպեսզի վերջինս վարակի այն:

Ի տարբերություն ռեզիդենտ վիրուսների, ոչ ռեզիդենտները ունեն երկու մոդուլ՝ փնտրման և վերարտադրվելու: Երբ վիրուսը վարակում է համակարգիչը նրա փնտրման մոդուլը անմիջապես փնտրում է նոր ֆայլեր և գտնելով այն դիմում է վերարտադրման կամ վարակիչ մոդուլի օգնությանը, որպեսզի վերջինս վարակի այն: Օգտագործողներից շատերը չեն էլ գիտակցում վիրուսի ներկայության մասին՝ չնայած որ հաճախ վիրուսների առկայությունը երևում է այս կամ այն ախտանշանից:

Կախված այն բանից, թե ինչ տիպի ծրագրեր են վարակում՝ վիրուսները կարելի է բաժանել հետևյալ տիպերի.

· **ֆայլային.** սրանք վարակում են սկավառակների վրա եղած ծրագրեր և փաստաթղթեր պարունակող ֆայլերը:

 Մակրովիրուսներ - Վերջերս հատկապես տարածում են գտել այնպիսի **մակրովիրոաներ,** որոնք ունակ են ներդրվելու միանգամից մի քանի հավելվածներում. այդպիսին է, օրինակ Nriplicate անունը կրող վիրուսը: Նման վիրուսակիր ծրագրի աշխատանքը սկսելուց հետո վիրուսը տեղակայվում է համակարգչի օպերատիվ հիշողության մեջ և կարող է մինչև մեքենան անջատելը վարակել այդ ընթացքում կիրառված ծրագրերը:

 Ցանցային վիրուսներ -կարող է փոխանցել համակարգչային ցանցեր ձեր ծրագրի կոդը և գործարկեք այն այս ցանցին միացված համակարգիչների վրա: Ցանցային վիրուսային վարակը կարող է առաջանալ, երբ աշխատում եք էլեկտրոնային փոստով կամ համաշխարհային սարդոստայնով «ճանապարհորդելիս»:

· **բեռնավորվող.** սրանք վնասում են սկավառակների այն տիրույթները, որոնք ծառայում են օպերացիոն համակարգի բեռնավորման համար: Նման վիրուսի օրինակ է հայտնի Win95CIH **«Չեռնոբիլ»** անվամբ վիրուսը, որը 1998 թվականի գարնանը հազարավոր համակարգիչներ շարքից հանեց:

· **տրոյական.** սրանք այն վտանգավոր վիրուսներն են, որոնք ունակ են **«գաղտնի»** աշխատելու: Այդ ընթացքում կարող են ոչ միայն համացանց մտնելու Ձեր գաղտնաբառը, այլև վարկային կտրոնի համարն իմանալ, այնուհետև այդ տեղեկություններն Համացանցով այլ համակարգիչ ուղարկել: Հիմնավորվելով վերջինիս վրա՝ նման վիրուսներն

այնուհետև սկսում են գործել Ձեր անունից:

Համակարգչային վիրուսներն ազդեցության աստիճանով[5]:

Վիրուսների մեծամասնությունը չեն կատարում ինչ-որ գործողություններ, բացի իրենց տարածումից (վարակելով այլ ծրագրեր, սկավառակներ և այլն) և երբեմն արտածում են հաղորդագրություններ, կամ վիրուսի հեղինակի կողմից ստեղծված այլ էֆեկտներ՝ խաղեր, երաժշտություններ, համակարգչի կախում, մոնիտորին հայտնվում են նկարներ, ստեղների ֆունկցիայի փոփոխում, համակարգչի աշխատանքի դանդաղեցում և այլն: Բայց այդ վիրուսները ինֆորմացիային լուրջ վնաս չեն հասցնում: Այդպիսի վիրուսները պայմանականորեն կոչվում են անվնաս: Ի դեպ, անվնաս վիրուսներն էլ կարող են պատճառել մեծ անհաջողություններ (օրինակ. համակարգչի վերաբեռնումը ամեն 5 րոպեն մեկ ձեզ թույլ չի տալիս հանգիստ աշխատել): Եթե տվյալների վնասումը կատարվում է պարբերաբար և դա չի ունենում ծանր հետևանքներ, ապա այդ վիրուսները կոչվում են վտանգավոր: Իսկ եթե վնասումը կատարվում է հաճախակի, կամ վիրուսները հասցնում են լուրջ վնասներ (կոշտ սկավառակի ֆորմատավորում, տվյալների սիստեմատիկ փոփոխում սկավառակի վրա և այլն) ապա այդպիսի վիրուսները կոչվում են շատ վտանգավոր: Այսպիսով,

- **Ոչ վտանգավոր/ անվնաս** - որպես կանոն, այս վիրուսները բազմապատկելով խցանում են համակարգչի հիշողությունը և կարող են կազմակերպել փոքրիկ կեղտոտ հնարքներ՝ նվագարկել դրանց մեջ ներկառուցված մեղեդի կամ ցուցադրել նկար;
- **Վտանգավոր**- այս վիրուսները կարող են որոշակի խանգարումներ ստեղծել ԱՀ-ի աշխատանքի մեջ՝ խափանումներ, վերագործարկում, ԱՀ-ի սառեցում, համակարգչի դանդաղ աշխատանք և այլն;
- **Շատ վտանգավոր**- վտանգավոր վիրուսները կարող են ոչնչացնել ծրագրերը, ջնջել կարևոր տվյալները, սպանել բեռնախցիկի և համակարգի տարածքները կոշտ սկավառակ, որը հետո կարելի է դեն նետել:

[5] https://wisemotors.ru/

Գլուխ 3

Համակարգչային վիրուսներից պաշտպանություն: Հակավիրուսային ծրագրեր

Վիրուսները համակարգիչ կարող են ներխուժել սկավառակների հետ կամ էլեկտրոնային փոստի հաղորդագրության հետ: Որպեսզի չդառնալ վիրուսների զոհը, ամեն մի օգտագործող պետք է իմանա համակարգչային վիրուսներից պաշտպանվելու սկզբունքները, քանի որ վիրուսները վերջնականապես ոչնչացնելու ոչ մի հույս չկա:

Վիրոսով վարակված ֆայլի ակտիվացման ժամանակ ղեկավարումը միանգամից փոխանցվում է վիրուսին, որը կատարում է իր ավերիչ գործողությունները, նաև զուգահեռ կցվում է այլ ծրագրերին և ֆայլերին: Այնուհետև տեխնոլոգիապես կատարվում է հետադարձ այն գործողություններին, որոնք կատարվել են համակարգչի վրա: Համակարգչի բարձր և արագ գործողության ժամանակ նմանատիպ շեղումը օգտագործողի համար մնում է աննկատ: Հասցված վնասը կարող է նկատվել ոչ միանգամից: Վիրուսի ներկայության արտաքին դրսևորումները համակարգչի մեջ կարող են լինել ամենատարբեր տեսակների.

- համակարգչի աշխատունակության նվազում (այն սկսում է դանդաղ աշխատել՝ երկար «մտածել»),
- համակարգչով աշխատելու ընթացքում օպերացիոն համակարգի ավտոմատ վերաբեռնավորում,
- տեքստային փաստաթղթերի աղավաղում,
- կիրառական ծրագրերի աշխատանքի վթարային ելք,
- ճկուն և կոշտ սկավառակների վրա եղած ֆայլերի բազմաթիվ կրկնօրինակների ստեղծում և այլն:

Իսկ ինչպե՞ս պաշտպանվել նման վտանգ ներկայացնող վիրուսներից:

Հին ժամանակներից հայտնի է, որ ցանակացած թույնի համար ուշ թե շուտ կգտնվի նրա հակաթույնը: Համակարգչային աշխարհում այդ հակաթույները կոչվում են հակավիրուսներ: Համակարգչային վիրուսը հատուկ, որպես կանոն, փոքր ծավալի ծրագիր է, որը կարող է գրանցել իր պատճենները համակարգչի համակարգային տարածքում, դրայվերներում, փաստաթղթերում և այլ տեղերում: Վիրուսի պատճենի ներխուժումը մեկ այլ ծրագիր կոչվում է վարակում, իսկ ծրագիրը, որը պարունակում է վիրուսը՝ կոչվում է վարակված: Այսօր գիտությանը հայտնի է մոտ 40 հազար համակարգչային վիրուսներ: Բիոլոգիական վիրուսների նման համակարգչային

վիրուսներին տարածվելու համար անհրաժեշտ են «կրիչներ»՝ առողջ ծրագրեր կամ փաստաթղթեր: Ինքը, վիրուսը, մեծ ծավալի ծրագիր չէ, հիմնականում չի գերազանցում մեգաբայթը: Այն պահին, երբ օգտագործողը ոչինչ չկասկածելով բաց է թողնում վարակված ծրագիրը, վիրուսը ակտիվանում է և սկսում է իր վտանգավոր գործունեությունը: Բացի ծրագրեր վնասելուց՝ կան ժամանակակից վիրուսներ, որոնք կարող են վնասել «երկաթը», օրինակ՝ ոչնչացնում են BIOS-ի պարունակությունը կամ վնասում են կոշտ սկավառակը: Առաջին համակարգչային վիրուսները եղել են հասարակ և օգտագործողից չեն թաքնվել, այլ մոնիտորին արտապատկերել են նկարներ և կատակներ: Բացահայտել այդպիսի վիրուսները դժվար չէր: Նրանք կպչում էին *.com և *.exe ֆայլերին՝ փոփոխելով նրանց իսկական չափսերը: Հետագայում վիրուսները սկսեցին թաքցնել իրենց ծրագրային կոդը այնպես, որ ոչ մի հակավիրուս չէր կարողանում հայտնաբերել: Այդպիսի վիրուսները կոչվում էին «անտեսանելի»: 90-ական թվականներին վիրուսները սկսեցին արագ փոխել իրենց ծրագրային կոդը, այն թաքցնելով կոշտ սկավառակի տարբեր մասերում: Վիրուսների տարածման մեջ մեծ ներդրում ունեցավ ինտերնետը: 1998-1999 թ-ին աշխարհը ցնցվեց մի քանի կործանիչ վիրուսային գրոհներից: Melissa Win95.CIH և Chernobyl վիրուսների գործունեության արդյունքում շարքից դուրս եկան մոտ 5 միլիոն համակարգիչներ ամբողջ աշխարհում: Այդ վիրուսները փչցնում էին համակարգչի կոշտ սկավառակը և ոչնչացնում էին մայրական հարթակի BIOS ծրագիրը:

Հիմնականում օգտագործողի համար վտանգավոր է համարվում վիրուսի այն գործողությունը, ինչպիսին է կոշտ սկավառակի ֆորմատավորումը, որը բերում է կոշտ սկավառակի վրա պահպանվող ինֆորմացիայի կորստի: Քանի որ վիրուսի ներխուժումից ոչ մի օգտագործողի համակարգիչ ապահովված չէ, հետևաբար վիրուսների կողմից հասցվող վնասները նվազագույնի հասցնելու համար անհրաժեշտ է պահպանել մի քանի հասարակ կանոններ:

Ամեն մի սկավառակ, եթե այն եղել է այլ համակարգչի վրա, անհրաժեշտ է ստուգել կամայական հակավիրուս ծրագրով: Այդպիսի ծրագրերը կարող են ոչ միայն հայտնաբերել վիրուսը, այլ նաև կարող են բուժել սկավառակը: Հատկապես վերաբերվում է խաղային ծրագրերին, քանի որ վիրուսների մեծ մասը տարածվում են հենց խաղերի միջոցով:

Նմանատիպ ստուգումները անհրաժեշտ է կատարել այն ֆայլերի համար, որոնք գալիս են ցանցի միջոցով:

Լայնորեն կիրառվող հակավիրոսային միջոցներից են **Kaspersky, Dr. Web 7, ESETNOD32, NortonInt. Security, BitDefender, Comodo, Avira, Avast** փաթեթները:

Համակարգիչները վիրուսակիր ծրագրերից պաշպանելու համար պետք է՝

- հակավիրուսային ծրագրերի օգնությամբ պարբերաբար ստուգել համակարգչի աշխատունակությունը,
- մինչև սկավառակներից ինֆորմացիա կարդալը՝ ստուգել դրա վրա վիրուսի առկայությունը,
- այլ համակարգիչներով աշխատելիս սկավառակները պաշտպանել դրանց վրա ինֆորմացիա գրանցելուց,
- արժեքավոր տվյալների ֆայլերի կրկնօրինակ ստեղծել, սկավառակը չթողնել սկավառակակրի մեջ,
- չօգտագործել անհասկանալի «պահվածքով» ծրագրեր,
- հակավիրուսային ծրագրերը պարբերաբար թարմացնել (փոխարինել դրանց նոր տարբերակներով)[6]:

Հակավիրուսային ծրագիրը շատ արագ ծերանում է: Դրա համար խորհուրդ է տրվում հաճախակիորեն այն թարմացնել նոր տարբերակով: Սովորաբար այդպիսի թարմացումները տևում են մեկ շաբաթից մինչ երեք ամիս:

Վիրուսի բացահայտման ժամանակ պետք չէ կատարել չմտածված գործողություններ, քանի որ դա կարող է բերել այնպիսի ինֆորմացիայի կորստի, որը դեռ կարելի է փրկել: Այդ ժամանակ ամենից ճիշտ է անջատել համակարգիչը, որպեսզի կանգնեցվի վիրուսի գործունեությունը: Այնուհետև բեռնել համակարգիչը օպերացիոն համակարգի էտալոնային սկավառակից: Որից հետո պետք է բաց թողնել հակավիրուսային ծրագիրը: Եթե ամեն ինչ ճիշտ է կատարվել, ապա հակավիրուսային ծրագիրը օգտագործողին տեղեկացնում է համակարգչից վիրուսների բացակայման մասին:

Պաշտպանություն էլեկտրոնային փոստով տարածվող վիրուսներից

Վերջին շրջանում ցանցում աշխատելիս հատկապես էլեկտրոնային փոստից օգտվելիս, հաճախակի են դարձել վիրուսների ներխուժումը համակարգիչ փոստային հաղորդագրությունների միջոցով: Այդ պատճառով այստեղ նույնպես անհրաժեշտ է պահպանել մի քանի հասարակ կանոններ.

[6] Ինֆորմատիկա 8-րդ դասարան, դասագիրք, Ս.Ս Ավետիսյան, Ս.Վ. Դանիելյան; մասն. խմբ. Ռ.Վ. Աղգաշյան – Երևան: Տիգրան Մեծ, 2013, – 168 էջ

1. Նամակներին կպած ֆայլերը պետք չէ բացել, եթե չգիտես թե ումից է ուղարկված և ինչ է պարունակում։
2. Նամակներին կպած ֆայլերը պետք չէ բացել, որոնք ուղարկված են հակավիրուսային լաբորատորիաներից։ Լաբորատորիաները երբեք ֆայլեր չեն ուղարկում։
3. Նամակներին կպած ֆայլերը պետք չէ բացել, եթե նամակի թեման և ինքը նամակը դատարկ են։
4. Ոչնչացնել բոլոր կասկածելի ֆայլերը։

Եթե համակարգիչների զարգացման սկզբնական շրջանում վիրուսները տարածվում էին սկավառակների միջոցով, ապա այսօր սկավառակներին փոխարինում է էլեկտրոնային փոստը։ Ամեն օր էլեկտրոնային փոստի միջոցով փոխանցվում է միլիոնավոր հաղորդագրություններ, որոնց մեծ մասը վարակված է վիրուսով։ Ցավոք էլեկտրոնային հաղորդագրություններում ներդրված ֆայլերը նաև կարող են շատ վտանգավոր լինել համակարգիչների համար։ Ինչու՞մ է կայանում ներդրված ֆայլերի վտանգը։ Այդպիսի ֆայլի փոխարեն օգտագործողին կարող են ուղարկել վիրուս կամ Տրոյան ծրագիր, երբեմն Microsoft Office ծրագրերով ստեղծված փաստաթուղթ (*.doc, *.xls), վարակված համակարգչային վիրուսով։ Բաց թողելով ստացված ծրագիրը կատարման համար, օգտագործողը կարող է սկզբնայնացնել վիրուսը, կամ ակտիվացնել համակարգչում Տրոյան ծրագիրը։ Դեռ ավելին փոստային ծրագրի ոչ ճիշտ կարգավորումից կամ նրանում եղած սխալներից, ներդրված ֆայլերը կարող են մեխանիկորեն բացվել ստացված նամակները ընթերցելիս։ Այս դեպքում, եթե չձեռնարկել ոչ մի պաշտպանողական միջոց, ապա վիրուսների ներխուժումը համակարգիչ ժամանակի գործ է։ Հնարավոր են վիրուսների ներխուժման այլ փորձեր համակարգիչ էլեկտրոնային փոստի միջոցով։ Օրինակ կարող են ուղարկել հաղորդագրություններ HTML տեսքով, որում ներդրված լինի ActiveX ղեկավարման տրոյան էլեմենտը։ Բացելով այդպիսի հաղորդագրություն դուք կարող եք բեռնել այդ էլեմենտը ձեր համակարգիչ, որից հետո նա դանդաղորեն սկսում է կատարել իր «չար» գործը։

Վիրուսներից և այլ վնասարար ծրագրերից պաշտպանվելու համար անհրաժեշտ է օգտագործել հատուկ հակավիրուսային ծրագրային ապահովում (հակավիրուսներ)։ Վիրուսներից պաշտպանվելու համար, որոնք տարածվում են էլեկտրոնային փոստի միջոցով, պետք է տեղադրել հակավիրուսային ծրագրեր ուղարկողի և ստացողի համակարգիչներում։ Երբեմն այդպիսի պաշտպանությունը պարզվում է անբավարար։ Սովորական հակավիրուսները, որոնք տեղադրվում են ինտերնետից օգտվողի համակարգչում, հաշվարկված են ֆայլերի ստուգման վրա

և ոչ միշտ են կարողանում վերլուծել էլեկտրոնային փոստի տվյալների հոսքը: Հակավիրուսների արդյունավետությունը կախված է մի քանի պարզ կանոններ պահպանումից: Անհրաժեշտ է պարբերաբար թարմացնել հակավիրուսային տվյալների բազան: Ցավոք շատ օգտագործողներ չեն կարողանում ճիշտ օգտվել հակավիրուսային ծրագրերից, կամ չեն թարմացնում հակավիրուսային տվյալների բազան, որը բերում է վիրուսային վարակի:

Առաջին ցանցային վիրուս Creeper-ը հայտնվեց 70-ական թթ.-ների սկզբներին Arpanet ռազմական համակարգչային ցանցում, որը Ինտերնետի նախատիպն էր: Ծրագիրը կարողանում էր մոդեմի միջոցով ինքնուրույն մուտք գործել ցանց և իր իսկ պատճենը պահպանել հեռավար աշխատող համակարգչում: Վարակված համակարգերում վիրուսը հայտնվում էր հետևյալ գրառմամբ.,,Ես CREEPER-ն եմ բռնի՛ր ինձ, եթե կարող ես:Վիրուսն ընդհանուր առմամբ անվնաս էր, սակայն անձնակազմին նյարդայնացնում էր: Անմեղ, բայց կպչուն վիրուսի ոչնչացման համար մի անհայտ անձ ստեղծեց Reaper ծրագիրը: Ըստ էության, դա նույնպես վիրուս էր, որն անտիվիրուսին բնորոշ որոշակի գործառույթներ էր կատարում. Reaper-ը տարածվում էր ցանցով և Creeper վիրուսի հայտնաբերման դեպքում ոչնչացնում էր դրան:

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ

Այսպիսով, առավել խորը ուսումնասիրելով համակարգչային վիրուսների էությունը, տեսակները, եկանք այն եզրահանգման, որ արդի ժամանակաշրջանի կարևորագույն խնդիրներից մեկը անվտանգ միջավայրում աշխատելն է, իսկ անվտանգ միջավայրի ստեղծման համար պետք է.

- ստեղծել հուսալի տեղեկատվական համակարգեր,
- իրականացնել համակարգչային վիրուսների դեմ պայքարի միջոցառումների ծրագիր,
- իրականացնել վիրուսային համաճարակների ժամանակին հայտնաբերման և կանխարգելման միջոցառումներ:

Հիմք ընդունելով ուսումնասիրման առարկա հանդիսացող համակարգչային վիրուսների դեմ պայքարի ծավալների ընդլայնումը, հասկացանք հակավիրուսային ծրագրերի խիստ անհրաժեշտությունն և ուսումնասիրեցինք դրանց յուրահատկությունները:

Ուսումնասիրության արդյունքում հատուկ ուշադրություն ենք դարձրել հատկապես էլեկտրոնային փոստի միջոցով համակարգչային վիրուսների տարածմանն ու դրանց կանխարգելման ուղիներին: Դա հիմնականում պայմանավորված է նրանով, որ ներկայումս ահռելի մեծ ծավալների են հասնում հենց այս տարբերակով համակարգչային վիրուսների տարածումը, ինչը հանգեցնում է շատ մեծ ծավալի ինֆորմացիոն կորուստների և կիբեռհանցագործությունների: Ուսումնասիրության արդյունքում ներկայացրեցինք, թե ինչպես պայքարել, ինչ քայլերի դիմել նման խնդիրներից խուսափելու համար:

Ընդհանուր առմանբ, հաշվի առնելով բոլոր ուսումնասիրություններն ու կանխարգելիչ միջոցառումների իրականացումները, որպես առաջարկություն կարող ենք ներկայացնել.

- Սերվերային տնտեսության առկայության ապահովում
- Հուսալի տեղեկատվական համակարգերի ապահովման համար միջոցառումներ, ներքին ապահով ցանցի ստեղծում
- անձնակազմի/անհատների առավել տեղեկացվածության ապահովում

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

Գրականություն՝

1. Ինֆորմատիկա 8-րդ դասարան, դասագիրք, Ս.Ս Ավետիսյան, Ս.Վ. Դանիելյան; մասն. խմբ. Ռ.Վ. Աղգաշյան – Երևան: Տիգրան Մեծ, 2013, – 168 էջ
2. А.Савицкий. Опрос: Самая непонятная киберугроза. Лаборатория Касперского (10 февраля 2014).

Իրավական ակտեր՝

3. ՀԱՄԱԿԱՐԳԶԱՅԻՆ ՎԻՐՈՒՍԱՅԻՆ ՎՏԱՆԳԻ ԴԵՄ ԱՐԴՅՈՒՆԱՎԵՏ ՊԱՅՔԱՐ ԻՐԱԿԱՆԱՑՆԵԼՈՒ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ ԾՐԱԳՐԻՆ ԵՎ ԺԱՄԱՆԱԿԱՑՈՒՅՑԻՆ ՀԱՎԱՆՈՒԹՅՈՒՆ ՏԱԼՈՒ ՄԱՍԻՆ ՀՀ ԿԱՌԱՎԱՐՈՒԹՅԱՆ ՆԻՍՏԻ ԱՐՁԱՆԱԳՐՈՒԹՅՈՒՆԻՑ ՔԱՂՎԱԾՔ 14 հունիսի 2012 թվականի N 23

Ինտերնետային կայքեր՝

4. www.imdproc.am
5. https://totalsec.wordpress.com
6. https://hy.wikipedia.org
7. https://wisemotors.ru/