Компьютерлік қатерлердің негізгі түрлері зиянды бағдарламалар қатарына жатады. Зиянды бағдарлама (malware, malicious software — зиянды бағдарламалық жасақтама) – бұл компьютердің компьютерлік ресурстарына рұқсатсыз қол жеткізуді немесе компьютерде сақталған ақпаратты ЭЕМ компьютерлік ресурстарды рұқсатсыз пайдалану мақсатында ақпаратты көшіру, бұрмалау, жою немесе ауыстыру арқылы ақпарат иесіне жəне / немесе компьютер иесіне немесе ЭЕМ компьютер желісінің иесіне зиян келтіруі мүмкін. Зиянды бағдарламалардың негізгі түрлерін қарастырайық. Вирустар (viruses): оларға басқа бағдарламаларға зиян тигізетін бағдарламалар жатады - вирус жұқтырған файлдарды іске қосу кезінде бақылауды алу үшін олар өз кодын қосады. Бұл қарапайым анықтама вирустың негізгі əрекеті - жұқтыруды анықтауға мүмкіндік береді. Вирустардың жылдамдығы құрттарға қарағанда біршама төмен.

***Құрттар (worms):*** зиянды бағдарламалардың осы санаттарын тарату үшін желілік ресурстарды пайдаланады. Бұл санат атауы құрттардың компьютерден компьютерге жіберіп, желілерді, электрондық поштаны жəне басқа да ақпараттық арналарды пайдаланып «еңбектеу» мүмкіндігі негізінде берілді. Құрттардың көбею жылдамдығы жоғары. Олар компьютерге еніп, басқа компьютерлердің желілік мекенжайларын есептеп, көшірмелерін осы мекенжайларға таратады. Желі мекенжайларынан басқа электрондық пошта клиенттерінің мекенжай кітабының деректері жиі пайдаланылады. Зиянды бағдарламалардың осы санатының өкілдері кейде жүйелік дискілерде жұмыс файлдарын жасайды, бірақ олар компьютердің ресурстарына (оперативтік жадынан басқа) қол жеткізе алмайды.

***Троян бағдарламасы (trojans):*** зардап шеккен компьютерлерде рұқсат етілмеген əрекеттерді жасайтын бағдарламалар, яғни қандай да бір жағдайларға байланысты олар дискілердегі ақпаратты бұзады, жүйені ұстап қалады, құпия ақпаратты ұрлайды жəне т.с.с. Зиянды бағдарламалардың бұл класы бұл терминнің дəстүрлі мағынасында вирус емес (яғни, басқа бағдарламаларға немесе деректерге əсер етпейді); Трояндар компьютерлерге өздігінен ене алмайды жəне зиянкестердің пайдалы бағдарламалық жасақтаманың астында таратылады. Бұл жағдайда олардан туындаған залал дəстүрлі вирустық шабуылдан бірнеше есе асып кетуі мүмкін.

***Тыңшы-бағдарламалар:*** жеке қолданушы немесе ұйым туралы ақпаратты олардың рұқсатынсыз жинауға мүмкіндік беретін бағдарлама. Компьютерде тыңшы бағдарламаларының болуы туралы сіз біле алмайсыз. Әдетте олардың мақсаты:

■ компьютердегі пайдаланушы əрекеттерін бақылау;

■ қатқыл дискінің мазмұны туралы ақпаратты жинау; бұл жағдайда, көбінесе компьютерде орнатылған бағдарламалық жасақтама тізімін жасау мақсатында кейбір каталогтарды жəне жүйелік тізімді сканерлеу туралы;

■ байланыс сапасы, интернетке қосылудың жылдамдығы жəне тəсілі туралы ақпаратты жинау жəне т.б. Алайда бұл бағдарламалар ақпарат жинаумен шектелмейді, олар қауіпсіздікке нақты қатер ұсынады. Белгілі бағдарламалардың кем дегенде екеуі - Gator жəне eZula - шабуылдаушы ақпаратты жинауға ғана емес, басқалардың компьютерін басқаруға мүмкіндік береді. Тыңшылық бағдарламалардың тағы бір мысалы - компьютерде орнатылған браузерге жəне трафикті қайта бағыттауға арналған бағдарламалар. Бір веб-сайттың мекенжайының өтініші бойынша толығымен ашылған болса, сіз осыған ұқсас бағдарламалармен кездескен болуыңыз əбден мүмкін. Тыңшылық бағдарламалардың бір түрі фишинг-жіберілім болып табылады.

***Фишинг (phishing):*** поштаны жіберу, оның мақсаты пайдаланушыдан, əдетте, қаржылық сипаттағы құпия ақпаратты алу болып табылады. Мұндай хаттар банктік құрылымдардан, танымал брендтердің компанияларынан келетін жазбалармен жасалуы мүмкін. Мысалы хаттарда оның несие картасының нөмірі жəне басқа да құпия ақпараты сұралатын пайдаланушыдан белгілі бір жалған сайтқа байланыс бар. Бағдарлама-жарнамалары (adware): пайдаланушының рұқсатынсыз жарнаманы көрсету мақсатында бағдарламалық жасақтамада қамтылған бағдарлама коды. Әдетте жарнамалық бағдарламалар тегін таратылатын бағдарламалық жасақтамаға ендірілген. Жарнама жұмыс интерфейсінде орналасқан. Әсіресе бағдарлама деректерін əзірлеушіге пайдаланушы туралы жеке мəліметтерді жинайды жəне аударады.

***Потенциалды қауіпті бағдарламалар (riskware):*** вирус емес, бірақ потенциалды қауіпі бар бағдарламалық жасақтама. Белгілі бір жағдайларда компьютердегі мұндай бағдарламалардың болуы сіздің деректеріңізді қауіп-қатерге ұшыратады. Мұндай бағдарламаларға қашықтағы əкімшілік коммуникациялары Dial-Up байланысын пайдаланатын ақылы Интернет-ресурстар үшін автоматты теру бағдарламалары жатады.

***Қалжың бағдарламалар (jokes):*** компьютерге тікелей зиян келтірмейтін бағдарламалық жасақтама, бірақ мұндай зиянның белгілі бір жағдайларда туындаған немесе пайда болған хабарламаларын көрсетеді. Мұндай бағдарламалар пайдаланушыны қауіп жоқ деп жиі ескереді, мысалы дискіні пішімдеу туралы хабарларды көрсету арқылы (бірақ ешқандай пішімдеу болмаса да), бөлінбеген файлдардағы вирустарды анықтау жəне т.б. Бҥркеуші бағдарламалар (rootkit): бұл зиянды əрекеттерді жасыру үшін пайдаланылатын утилиталар. Олар антивирустық бағдарламаларды табуды болдырмау үшін зиянды бағдарламаларды маскалайды. Сондай-ақ Rootkit'bi операциялық жүйені вирус жұққан компьютерде өзгерте алады жəне өзінің негізгі қатысуын жасырып, шабуыл жасаған əрекеттерді жасырады. Басқада қауіпті бағдарламалар: басқа да зиянды бағдарламаларды жасау, қашықтағы серверлерге DoS шабуылдарын ұйымдастыру, басқа компьютерлерді бұзу жəне т.б. сияқты бағдарламаларды қамтиды. Мұндай бағдарламаларға хакерлік утилиталар, вирустық құрылымдар жəне т.б. жатады.

***Спам (spam):*** қалаусыз сипаттағы анонимді жаппай пошталық коррсепонденциясы. Спам - саяси жəне агитациялық сипаттағы тарату, біреуге көмектесу үшін шақырылған хаттар. Спамның жекелеген санаты үлкен ақша қаражатын немесе қаржы пирамидаларына, сондайақ құпия сөздерді жəне несие карталарының нөмірлерін ұрлауға бағытталған, адамға өз достарына (мысалы, «бақыт туралы хаттар») жəне т.б. сұраным хаттарын жіберу туралы ұсыныстары бар хаттар болып табылады. Спам пошта серверлерінде жүктемені айтарлықтай арттырады жəне пайдаланушыға маңызды ақпаратты жоғалту қатерін ұлғайтады.

***Зиянды бағдарламалардан мүлдем қорғаныс жоқ:*** Sasser немесе Conficker секілді «нөлдік күнделікті пайдаланудан» ешкім сақтандырылмайды. Бірақ кейбір шаралар көмегімен зиянды бағдарламалардың жұқтыру қаупін елеулі түрде азайтуға болады. Қауіпсіздіктің негізгі жəне ең тиімді шаралары мыналар:

■ пайдаланушының рұқсатынсыз маңызды файлдарды өзгертуге мүмкіндік бермейтін қазіргі заманғы операциялық жүйелерді қолданыңыз;

■ өз уақытында жаңартуларды орнатыңыз;

■ егер автоматты жаңарту режимі болса, оны қосыңыз;

■ Зиянды бағдарламалық қамтамасыз етудің сигнатуралық əдісімен антивирустық өнімдерден басқа, қатерлерден белсенді қорғауды қамтамасыз ететін бағдарламалық жасақтаманы пайдаланыңыз (белсенді қорғаныс қажеттілігі антивирус антивирустық деректер базасына əлі енгізілмеген жаңа қауіптерді байқамайтындығына байланысты). Дегенмен оны пайдалану пайдаланушыдан көптеген тəжірибе мен білімді талап етеді;

■ зиянды бағдарламалардың енуіне мүмкіндік бермейтін əкімші емес, тек қана жеке компьютерде жеке қолданушының құқықтарымен жұмыс жасайды. Бірақ бұл шектеулі тіркеу жазатын жəне оқу (мысалы, үй каталогы - GNU / Linux жүйесінде каталогы / home, Windows жүйесіндегі құжаттар мен параметрлер, Windows) немесе пайдаланушы интерфейсінің рұқсаты бар пайдаланушы файлдарына қол жетімді зиянды бағдарламалардан қорғай алмайды (мысалы, экран көріністерін жасау немесе пернетақта таратылымын өзгерту бағдарламалары);

■ бөгде тұлғалардың компьютерге физикалық қол жеткізуін шектеу; Сыртқы жадты тек қана сенімді көздерден пайдаланыңыз;

■ сенімсіз көздерден алынған компьютер файлдарын ашпаңыз;

■ Пайдаланушы орнатқан саясатқа негізделген жеке компьютерден Интернет қосылымын бақылайтын желі аралық экранды (аппараттық немесе бағдарламалық) пайдаланыңыз.

***Компьютерлік вирус -*** бұл əр түрлі компьютерлік бағдарлама немесе зиянды код, оның ерекшелігі – өздігінен көбеюі (өзін-өзі репликация). Сонымен қатар вирустар пайдаланушының білімісіз, соның ішінде пайдаланушыға жəне / немесе компьютерге зиян тигізбейтін басқа да ерікті əрекеттерді орындай алады. Егер вирустың авторы зиянды əсерлерді жасамаса да, вирус амалдық жүйемен жəне басқа бағдарламалармен өзара əрекеттесу үшін ескерілмеген қателердің салдарынан компьютердегі ақауларға əкелуі мүмкін. Бұдан басқа, вирустар əдетте сақтау құрылғыларында орын алады жəне басқа жүйелік ресурстарды таңдайды. Сондықтан вирустар зиянды бағдарламалар деп саналады. Кейбір пайдаланушылар қате компьютерлік вирустарға зиянды бағдарламалардың басқа да түрлерін - тыңшылық бағдарламаларды жəне т.б. жатады. Әлемде интернетте таратылатын он мыңдаған компьютерлік вирустар бар.

***Таралу механизімі.*** Вирустар өздерінің денелерін көшіріп, оны кейіннен орындауды қамтамасыз етеді: басқа бағдарламалардың орындалатын кодын енгізу, басқа бағдарламаларды ауыстыру, авто қосылуға тіркелу жəне т.б. Вирус немесе оның тасымалдаушысы машина кодын қамтитын бағдарламалар ғана емес, сонымен қатар макростар бар Microsoft Word жəне Excel құжаттары сияқты автоматты түрде орындалатын пəрмендерді қамтитын кез келген ақпарат болуы мүмкін. Сонымен қатар, вирус компьютерге ену үшін вирус əйгілі бағдарламалық жасақтаманың (Adobe Flash, Internet Explorer, Outlook) осалдықтарын пайдалануы мүмкін, ол үшін дистрибьюторлар оны əдеттегі деректерге (суреттер, мəтіндер жəне т.б.) қосып, пайдаланатын эксплуатпен енгізеді.

***Тарату каналдары***. Флэш-жинақтағыштар қазіргі кезде дискеттердің орнын ауыстырып, олардың тағдырын қайталайды - вирустар сандық камералар, сандық видекамералар, портативті сандық плеерлер, сондай-ақ 2000-шы жылдардың мобильді телефондары, əсіресе смартфондар (ұялы телефондар вирустары пайда болды) арқылы тарайды. Бұл арнаны пайдалану, ең алдымен, осы файлдағы дискідегі арнайы autorun.inf. файлын жасау мүмкіндігінен туындады, мұндай дискіні ашқан кезде Windows Explorer бағдарламасымен іске қосылған бағдарламаны көрсетуге болады. Windows 7-ден бастап, портативті медиадан файлдарды автоматты түрде жүктеу мүмкіндігі өшірілген. Әдетте электрондық поштадағы вирустар зиянды қосымшалармен: суреттермен, құжаттармен, музыкамен, веб-сайттарға сілтемелермен маскаланады. Кейбір əріптерде тек сілтемелер ғана болуы мүмкін, яғни əріптерде зиянды код жоқ, бірақ мұндай сілтемені ашсаңыз, вирус кодын қамтитын арнайы құрылған веб-сайтқа өтуіңізге болады. Көптеген электрондық пошта вирустары, пайдаланушының компьютеріне түсіп, одан кейін жіберілген Outlook пошта клиенттерінен мекен-жай кітабын өздеріне жіберу үшін пайдаланады. Шұғыл хабар алмасу бағдарламаларын (ICQ жəне т.б.) пайдаланғанда, болжалды фотосуреттерге, музыкаға немесе нақты вирустар бағдарламаларына сілтемелерді тарату кең таралған. Сондай-ақ оларда əртүрлі «белсенді» мазмұнның болғандығына байланысты веб-парақтар арқылы жұқтыруға болады: сценарийлер, ActiveX компоненттері. Бұл жағдайда пайдаланушының ДК орнатылған бағдарламалық жасақтаманың осалдығы немесе сайт иесінің (бұл аса қауіпті, себебі қонақтардың жоғары ағыны бар жақсы сайттар жұқтыруға ұшырайды) бағдарламалық жасақтамасындағы осалдығы пайдаланылады жəне осы сайтқа кіретін күдікті пайдаланушылар өз компьютерін жұқтыру қаупіне ұшырайды. Қҧрттар - жəбірленуші компьютерге пайдаланушының қатысуынсыз еніп кететін вирус түрі. Ол үшін құрттар амалдық жүйенің бағдарламалық жасақтамасындағы тесіктерді (осалдықтарды) пайдаланады. Осалдықтар – машиналық кодты қашықтан жүктеп алуға жəне орындауға мүмкіндік беретін бағдарламалық жасақтаманың қателіктері мен ақаулары, соның салдарынан вирус операциялық жүйеге кіреді жəне басқа компьютерлерге жергілікті желі немесе Интернет арқылы жұқтыруға əрекет жасайды. Шабуылшылар спамның немесе DDoS шабуылдарын жіберу үшін жұқтырылған компьютер қолданушыларын пайдаланады.

***Анықталуға қарсы әрекеттер.*** Вирусқа қарсы сканерлер кеңінен қолданылып, олар қолтаңбалардың қандай да бір кодын енгізуден немесе күдікті əрекеттерді жасамас бұрын тексеруден өткеннен кейін, вирус технологиялары жеткіліксіз болып шықты. Пайдаланушының назарын өзіне артық аудартапау үшін, вирус үрдіс тізімінен немесе каталог ағашынан жасыру негізгі əдіс болып табылады, алайда антивирустық бағдарламамен күресу үшін аса күрделі əдістер қажет. Сигнатураның барлығын сканерден өткізуге қарсы туру үшін кодты шифрлау жəне полиморфизм қолданылады. Бұл əдістер көбінесе бірлесіп қолданылады, өйткені вирустың шифрланған бөлігін шифрлаудан шығару қажет, ол оны сигнатурамен табуға мүмкіндік береді. Демек, деректерді өзгерту үшін полиморфизм қолданылады - орындалатын əрекеттерді өзгертпейтін пəрмендердің кезектілігін өзгерту. Бұл Intel процессорлары үшін əртүрлі жəне икемді командалар жүйесі арқасында мүмкін болады, сол сияқты қарапайым əрекет, мысалы, екі санды қосу командалардың бірнеше рет орындалуы мүмкін. Сондай-ақ, кодты араластыру жеке командалар кездейсоқ тəртіпте бұзылған жəне сөзсіз өтулермен байланысты болғанда қолданылады. Вирустық технологиялардың дамыған фронты метаморфизм болып табылады, ол көбінесе полиморфизммен араласады. Полиморфтық вирустың дефекторы шифрды айырушысы қарапайым болып табылады, оның функциясы вирустың негізгі корпусын енгізуден кейін, яғни оның коды антивирустық бағдарламамен тексерілгеннен кейін жəне іске қосылғаннан кейін шешуге арналған. Ол вирустың шифрланған бөлігінде орналасқан ең көп полиморфтық қозғалтқышты қамтымайды жəне шифр айырушысын өндіреді. Керісінше метаморфтық вирус шифрлауды мүлдем пайдаланбауы мүмкін, өйткені ол барлық кодты əрбір көшірмені қайта жазады.

***Алдын алу және емі.*** Қазіргі уақытта вирустардың ДК-ге кіруіне жол бермеу үшін қолданылатын антивирустық бағдарламалар көп. Дегенмен олар соңғы жаңа өңдеулерді жеңе алатындығына кепілдік бермейді. Сондықтан кейбір сақтық шараларын сақтау қажет. Қажет болған жағдайда артықшылықты тіркеу жазбаларында жұмыс істемеңіз.

1. Күмəнсіз дереккөздерден таныс емес бағдарламаларды іске қоспаңыз.

2. Жүйелік файлдарды рұқсатсыз өзгерту мүмкіндігін болдырмауға тырысыңыз.

3. Жүйенің қауіпті функционалдығын өшіріңіз (мысалы, MS Windows жүйесіндегі автономды медиа, файлдарды жасыру, олардың кеңейтімдері жəне т.б.).

4. Күдікті сайттарға кірмеңіз, браузердің мекенжай жолындағы адресіне назар аударыңыз.

5. Тек сенімді дистрибутивтерді пайдаланыңыз.

6. Маңызды деректердің резервтік көшірмелерін үнемі жасаңыз жəне жылдам орналасу үшін барлық параметрлермен жүйелік кескінге ие болыңыз.

7. Жиі қолданылатын бағдарламалардың, əсіресе бүкіл жүйенің 202 қауіпсіздігін қамтамасыз ететін тұрақты жаңартуларды орындаңыз.