Компютърен вирус е компютърна програма, която може да копирате самия и заразят компютъра, без разрешение или знанието на потребителя. Терминът "вирус" е често използван, но погрешно да се позове на други видове зловреден софтуер, рекламен и шпионски програми, които не разполагат с репродуктивната способност. Истински вирусът може да се пренесе от един компютър на друг (в някаква форма на изпълним код), когато тя се взема предвид целта компютър, например, защото когато потребител го е изпратил по мрежа или Интернет, или на сменяем носител като дискета, CD или USB устройство. Вирусите могат да увеличат шансовете си за разпространение към други компютри от инфектирането на файлове в мрежа файлова система или на файловата система, който е достъпен от друг компютър. [1] , [2]

Вируси се бъркат с компютърните червеи и троянски коне, които те са технически различни. Червеят може да се разпространи към други компютри, без да е необходимо да бъдат прехвърлени като част от по-домакин, както и троянски кон е програма, която изглежда безобидно, но има скрит дневен ред. Червеят и троянският, като вируси, които могат да причинят вреда на компютъра или системата, данни, функционални резултати, или в мрежовата производителност, когато са изпълнени. Някои вируси и друг зловреден софтуер имат симптоми забележимо с компютърния потребител, но повечето са подмолни. Това ги прави по-трудно забележими за средния потребител на информация, затова има специализирани програми за борба с тези злонамерни програми.

Повечето персонални компютри са свързани към Интернет и локална мрежа, улесняващи разпространението на опасения код. Днешните вируси също могат да се възползват от услуги на мрежата, като World Wide Web, електронна поща, незабавни съобщения и споделяне на файлове системи за разпространение. Освен това, някои източници използват алтернативни терминология, в която вирусът е всяка форма на самооценка възпроизвеждане на злонамерен софтуер.reeper вирусът е бил открит за първи по ARPANET - предшественик на Интернет в началото на 1970-те.
[3]
Creeper вирусът е експериментална самостоятелно възпроизвеждаща програма написана от Боб Томас от BBN през 1971 година.
[4]
Creeper използвали ARPANET да зарази DEC PDP -10 компютри работещи на TENEX операционна система. Показвал съобщението, "Аз съм Creeper, хвани ме, ако можеш!". The Reaper е програма създадена, за да изтриете Creeper.
[5]

Погрешно схващане е, че програмата, наречена "Rother J" е първият компютърен вирус. Тя беше, все пак, първият вирус да зарази компютри "в дома си." Написано през 1982 г. от Richard Skrenta, и приложен към Apple DOS 3.3 операционна система и разпространението й чрез флопи диск [6] .Този вирус беше първоначално шега, създадена от гимназията студент. Той е бил създаден в една игра на флопи диск. На своето 50-то използване Elk Cloner вирусът се активира, заразявайки компютъра и показване на кратко стихотворение началото " Elk Cloner: The program with a personality."

За първи път когато се използва BOOT сектора на диска е dubbed (C) Brain [7] , създаден през 1986 г. от Farooq Alvi Brothers, работещи в Лахор, Пакистан. Те са създали вируса да възпрат пиратските копия на софтуерите който са написали. Въпреки това анализаторите са твърди, че Ashar вирус, вариант на Brain .

Преди компютърните мрежи да станат широко разпространени, повечето вируси се разпространяваха по сменяемите носители - флопи дискове. В ранните дни на персоналния компютър, много потребители редовно обменят информация и програми по дискети. Някои вируси се разпространяват и инфектират програми съхранявани на тези дискети, а други инсталирани в диска Boot сектор, като се гарантира, че те ще бъдат изпълнени, когато потребителят стартира диска на компютъра си, обикновено по невнимание. В ерата на персонални компютри първия опит за зареждане от флопи ако някой е бил оставен в устройството. Това беше най-успешната стратегия на инфекция от флопи дискове в продължение на много години. [8]

1. Видове компютърни вируси.

Видовете вируси са няколко основни с множество от подвидове. В тази версия са описани 30 вида вируси и 8 вида вирусоподобни програми. Често вирусите представляват няколко от тези "видове" събрани в един вирус. Пример: резидентни и Stealth едновременно или други качества като често пъти са по много. Комбинациите между тези "видове" е най-коварното при вирусите. Вирусите са написани като изпълним код който се самозаписва някъде из програмата като модифицира програмата да изпълнява този код или кода се записва с стартовите сектори на дискетите или харддиска за да се изпълни. Така вирусът става активен и нанася своят удар върху софтуера. Има и вирусоподобни програми които помагат на вирусите.

- Резидентни - те остават резидентни в паметта така както остава някой драйвер. (до изключването или рестартирането на компютъра). От паметта вируса може да се размножава и да смущава работата на компютъра и да повреждa файлове и цели

програми;

- Boot - тези вируси се самокопират в зареждащия сектор на дискетите и на харддиска като копират системните файлове (ако харддиска е системен или дискетата е системна) на друго място на дискетата или на харддиска. Така при опит да се зареди от заразената системна дискета вирусите се зареждат успоредно с ОС нанасят своите удари върху софтуера;
- Вируси с директно действие - са вируси които се стартират нанасят своят удар върху софтуера и се "самоизключват", но остават като инфекция;
- Stealth - вирусите са най - коварните защото те причиняват големи щети и остават резидентни в RAM. Те още прикриват симптомите на вирусната инфекция и взаимодействат с различни антивирусни програми като принуждават програмата да каже че няма вируси. Тези вируси не показват промени по размерите на файла който са инфектирали което ги прави трудни за засичане и обезвреждане! Самият вирус лесно се укрива и трудно се премахва. Секторите от харддиска и (или) дискетата където е записан оригинала на вируса се маркират като лоши (механично повредени) въпреки че не са повредени по никакъв начин. Всички антивирусни програми който проверяват харддиска или дискетите "виждат" маркираното - "лош сектор" и го прескачат и не засичат вируса. Друга мярка за защита е заетата техника от полиморфичните вируси на самопроменящ се код на вируса за допълнителна самозащита;
- Макровируси [9] - вируси специално написани на "Word macro language" и на "Visual Basic Macro language" като създават отделни макроси - вируси. Тези вируси често предизвикват правописни и стилистични грешки по текстовете на "WinWord"; "MacWord"; "DosWord" а също и по таблиците на "DosExcel", "WinExcel и "MacExcel" . Тези вируси не правят разлика между отделните версии на Word и Excel. Макро вирусите се пренасят като макроси по документи и таблици със записани макроси. Стартирането на макросите стартира и макро вирусите. Макро вирусите нападат първо файла Normal.dot (когато става дума за Word) или Normal.xlt (когато става дума за Excel), а после и всеки отворен документ;
- Логическите вируси - предизвикват не само множество щети но предизвикват и много логически грешки по време на работа. Те се активират ако определени условия се изпълнят правилно;
- Time-bomb - вирусите са вируси с назначена дата на активиране. Ако попаднат в компютъра преди датата на активирането им те само се размножават без да предизвикват повреди. На датата на активирането или след нея вирусите се активират и нанасят своят удар. Пример за такъв вирус е CIH (т.нар. Чернобил), който се активира на 26-ти април;
- MBR (Master Boot Record) - вирусите работят на принцип близък на Boot вирусите. С тази разлика че те не копират системните файлове а се "смесват" с тях и ги модифицират за да приемат вируса като част от тях което прави невъзможно премахването им. Когато от заразен системен харддиск или заразена от системна дискета се зарежда ОС, вирусите се зареждат отново успоредно с ОС и нанасят своят жесток удар върху софтуера;
- BIOS вирусите - това са тези вируси които освен че причиняват щети правят и промени по BIOS-а на компютъра или се записват там. Най-честите промени са свързани с флопитата често се обявява че флопитата не са инсталирани и компютъра не може да ги използва. Разбира се и често пъти вирусите така разбъркват данните от

BIOS-а че компютърът не може да се стартира. Вирусите причинили всякакви промени промени по BIOS-а не позволяват нормалното преконфигуриране Трети вируси се самозаписват в BIOS-а и се самостартират от там още преди ОС да е заредена. Борбата с тези вируси е най-сложна защото те контролират целият хардуер и софтуер;

- Размножаващи се - тези вируси само се размножават без да причиняват никакви повреди и каквито и да било други щети и последици;
- Joke programs - всъщност те не са вируси, а шегаджийски програми които се разпространяват като вирусите. Тези програми не причиняват никакви щети. Те само извеждат глупави съобщения и още по-глупави шеги;
- Virus creating tool viruses [10] - не са вируси а инструменти за създаване на вируси в големи количества. Вирусите създадени от тези инструменти обикновено са шифровани и лесно засечими както и лесно отстраними;
- ANTI-VIRUS viruses - не са вируси, а антивирусни програми които се разпространяват като вирусите и обикновено са блок за самотестване срещу вируси. Желателно е да не ги допускате по диска (дисковете) и дискетите си;
- Хардуерните вируси са вируси които спъват работата на хардуера по всякакви начини: симулирайки хардуерни проблеми, механически повредени сектори, по дисковете и дискетите, повреди по тях, провалят тестовете на дисковите контролери и принуждавайки компютъра да не работи с дадени компоненти от хардуера. Вируса FireBurn е точно такъв с цел самосъхранение блокира клавиатурата и мишката;
- COM вирус е този вирус който напада и заразява само .COM файлове;
- EXE вирус е този вирус който напада и заразява само .EXE файлове;
- COM/EXE - вирус е този вирус който напада и заразява както .COM, така и файлове и .EXE файлове;
- Суматорните вируси са предвидени да събират и закръглят стойности предизвиквайки много големи бъркотии. Започвайки от най-ниските нива на Excel и стигат до най-високите нива на счетоводни и ведомствени и подбанкови и банкови нива и функции. Тези вируси могат да объркат сметки, подменят стойности и резултати и знаци в зависимост от индентификацията на дадено действие и сумите и вида на стойностите. Често тези вируси вкарват в обръщение неверни стойности представяйки ги за верни както и да отхвърлят верните стойности като ги представят за грешни;

- Псевдорутерните са вируси които само смущават трансфера на данни като предизвикват частични задръствания по мрежите и трансферните линии. Попаднали на подходящо устройство или в главният компютър на мрежа те започват да се размножават и да предизвикват тотални задръствания по мрежите и трансферните линии и препращат информацията по различни вектори където тя се губи. E-mail и локалните мрежи са главното им поле на действие;
- Информационни замърсители са вируси с функции като на псевдорутерните само че за да предизвикат тотално задръстване и объркване на мрежите и на трансферните линии не е необходимо да са в главен компютър или устройство а където и да било по мрежата и устройствата. Често тези вируси пращат пратка на адрес различен от този който потребителя е посочил или обявяват съществуващ адрес в мрежа за невалиден или ако се набере грешен адрес вирусите го приемат за валиден и пращат информацията в различни вектори на трансфер където тя се губи;
- Полиморфните вируси [11] са много трудни за засичане, идентифициране и

премахване защото те постоянно променят своят код. Няма два еднакви кода на един и същ полиморфичен вирус който е способен да направи хиляди самомодификации с цел да се самопредпази от антивирусните програми. Принципа на полиморфията при вирусите е всяко копие да се кодира различно;

- Биокомпютърните вируси [12] [13] са много интересни. Те представляват нещо като един вирус разделен на две "половини", които са програмирани да се търсят взаимно (една-друга) и когато се открият да се съединят и да образуват вируса. Всяка (коя да е)"половина" поотделно е безобидна но ако двете се съберат заедно вируса образува и се активира и нанася своят удар срещу софтуера;

- Бинарни вируси са вирусите които са написани на машинен език и също като биокомпютърните вируси са в две части които взаимно се търсят една друга Това че са написани на машинен език ги прави малки и трудно засечими;
- RAM вирусите са вируси които само се размножават и седят в оперативната памет (RAM) и окупират голяма част от нея и не се улавят от антивирусните програми сканират които RAM за резидентни вируси. Те не причиняват никакви щети но бързо и лесно се размножават. Тези вируси също често пъти заставят програмата да не стартира и да изведе съобщение за не достатъчно RAM-памет въпреки че компютъра в повечето случай има достатъчно количество RAM-памет за да изпълни програмата;
- Companion вирусите с вируси които са нещо средно между шегаджийските програми (joke programs) RAM-вирусите и размножаващите се вируси. Този тип вируси се записват в началото на програмата и при нейното изпълнение вируса задава някакъв въпрос. при правилен отговор вируса стартира програмата. При грешен отговор вируса или блокира компютъра или го рестартира;
- Вируси убийци - по непотвърдени данни съществува и такава категория вируси. Те не повреждат данни или каквото и да било друго, но убиват оператора. Такъв вирус са използвали в КГБ като крайна мярка на защита на компютрите им през студената война. Вируса се е казвал 666 и е объркал до такава степен мозъчните вълни че е причинявял невероятно главоболие и смърт. Много любопитни хакери, кракери и американски експерти и програмисти са се опитвали да откраднат вируса но никой още не е успял...;

- FAT Scrabmlers - тези вируси така разбъркват двете копия на FAT че всичко записано на диска става негодно за каквито и да е манипулации. Двете Копия на FAT се разбъркват Всяко по различен начин с цел максимални щети. Няма Друг изход освен Форматиране от BIOS и след това предформатна подготовка с FDISK и повторно форматиране с Format /u /c /s;
- Java вируси - това са вируси които могат да заразяват само Java програми и заразяват всякакви компютри и операционни среди защото се стартират не от ОС а от браузера;
- E - Mail вируси [14] - особено актуална категория вируси разпространява се чрез електронна поща и използва адресната книга за да нападне нови компютри;

- WAP вируси [15] - току що появила се категория с засега единствен представител - Timofonica нападат GSM, Palm PC и лаптопи ако те използват WAP. за сега няма данни за вредни кодове но се очаква да се получи нещо като разбъркване на мрежите, сривове, раздуване на телефонни сметки, разпращане на телефонни номера или

адреси.

Забележка: вирусите за PC не могат да заразяват Power Machintosh и вирусите за Power Machintosh не могат са заразяват PC компютри [16] , защото има разлики в интерфейса на двете групи хардуер. Двете групи са взаимно несъвместими. Тази забележка не важи за Java вирусите.

1. Вирусоподобни програми:

- Червеи (Worms) - Програми които се самокопират но и заразяват други програми но не винаги причиняват щети;
- Host червеи - Имат нужда от локална мрежа за да се самокопират и за да могат да функционират;
- Net Worm - разпространява части от себе си по мрежа и има нужда от мрежа за да може частите му да работят съвместно. Може да съществува и на единичен компютър но се самокопира на различни места и/или дялове на харддиска;
- Троянски кон - това са програми които са скрити в други програми. Тази система е ефективна. докато основната програма върши нещо то в фонов режим се имплантира вирус или се създават други проблеми. Пример за това е FreeWare програмата ProMail 2000 v. 1.02 която служи като оптимизатор на мрежовия трафик и разпределение на пощата. Програмата създава файла ACCOUNT.INI в който се съдържат всички имена пароли и привилегии за достъп на всички потребители и информация за степента на защита на мрежата който файл се копира и копието му се изпраща като прикачен файл по електронна поща до създателя на програмата;
- "Терористи" (Droppers) - програми направени за заобикаляне на антивирусните защити. При създаване се използва мощна криптираща система със защитна цел. Тази криптираща система прави невъзможно откриването от антивирусни програми. "Терористите" най често транспортират и имплантират вируси;
- Бомби - Тези програми изчакват определено събитие на компютъра, което събитие ще ги стартира и те ще инсталират вируса който носят със себе си. Тези програми имат много и разнообразни начини на действие (все вредни) и се стартират от разнообразни събития в компютъра ви или в определени дни;
- INI програми - тези програми са във формат на стандартен INI файл. Много опасни и силно разрушителни. Модифицират се системните файлове на Windows. Това реално са вредни опции в INI файловете;
- BAT инфектори - асоциират се с BAT файлове. Може да се асоциират всякакви унищожителни програми съвместими с PC. Това е или елементарен BAT код или е програма която се извиква с модифицирани BAT файлове.

1. Троянски коне от типа remote administration tool.

През последните месеци огромно разпространение сред потребителите на Интернет получиха програми от типа "Троянски кон", които се използват за кражба на акаунти. В следващите редове ще се опитаме да разясним опасностите и средствата за защита от такива програми.

Троянски кон е програма, която под прикритието на някаква полезна функция (или обещание за извършване на такава) извършва скрити от потребителя действия. Троянският кон не е вирус защото не може да се разпространява сам и единственият начин за неговото разпространение е чрез измама от страна на създателите му и благодарение на лековерие от страна на потребителите. Създадени са специални разновидности на троянските коне, основната цел на които е кражба на акаунти за достъп до Интернет. Възможностите, които те дават на създателите си (респ. на злонамерените разпространители) обаче далеч надхвърлят тази цел. Този тип троянски коне се базират на една отдавна съществуваща група софтуерни продукти известни като Remote Administration Tools (RAT). Типичен представител на този тип програми е PC Anywhere на Norton. Идеята е да се осъществи отдалечен мрежов достъп до даден компютър, така че да е възможно пълно използване на ресурсите - все едно, че седим зад клавиатурата и мишката му. Инсталирането и използването на програма от такъв тип без знанието на собственика на компютъра обаче води до големи опасности за потребителите на Интернет. В интервалите от време, когато такъв компютър е online, т.е. свързан е към Интернет, е възможен пълен дистанционен контрол на абсолютно всичките му ресурси от всяка точка на земното кълбо!

За да предотвратят конкурентна намеса на заразени от тях машини разпространителите на RAT в повечето случаи имат възможност да изберат парола с която да кодират връзката си, така че други хакери да не могат да се възползват от техния троянски кон. Това ограничение обаче не се отнася до авторите на RAT софтуера (и хората запознати в тънкости с дадената разновидност), които винаги имат възможност да осъществят пълен контрол над даден заразен компютър независимо от използваната от конкретния разпространител парола.

Разпространители най-често са не особено компютърно грамотни тинейджъри. В желанието си да откраднат акаунти за достъп до Интернет те дават възможност на злонамерени хакери с по-висока компютърна грамотност да осъществят неоторизиран достъп до данните от хиляди компютри по цял сват. Този факт прави

разпространенитето на RAT много по-опасно за потребителите от колкото изглежда на пръв поглед. Напълно реалната възможност за изтичане на важна фирмена или лична информация в никакъв случай не трябва да бъде пренебрегвана.

В момента чрез Интернет в различна степен са разпространени над различни RAT троянски коне, създадени предимно за осъществяване на неоторизиран дистанционен контрол над включени в мрежа компютри. Най-разпространени в момента са Back Office, TeamViewer, VNC, Netbus. Възможностите, които те дават на разпространителите си с малки нюанси са едни и същи а именно:

- изтегляне на произволен файл
- записване на произволен файл (вкл. подмяна на инсталирани програми, които търсят троянски коне!)
- търсене и декодиране на записани на диска пароли
- записване на всеки натиснат клавиш (всички пароли, които не са записани се въвеждат от клавиатурата)
- блокиране/рестартиране на компютъра
- извеждане на съобщения на екрана
- записване изображението на екрана
- изпращане на писма от името на собственика на заразения компютър

1. Spyware.

Spyware е компютърен софтуер, който е инсталиран тайничко на личен компютър, за да вземе частичен контрол или контрол върху потребителя, без информирано съгласие на потребителя.

Въпреки, че терминът подсказва, шпионски софтуер, който тайно следи потребителско поведение, функциите на шпионски разшири отвъд простите мониторинг. Spyware програми могат да събират различни видове лични данни, като сърфиране в интернет навиците, сайтове, които са посетили, но също така може да се намесва с потребителски контрол на компютъра по други начини, като например инсталиране на допълнителен софтуер, както и пренасочване на Уеб браузъра дейност. Spyware е известно, за да промените настройките на компютъра, в резултат на бавни скорости на връзката, различни вътрешни страници и / или загуба на Интернет или функциите на други програми. При опит да се повиши разбирането на шпионски софтуер, по-официална класификация на видовете, включени софтуер е заловен в рамките на срока за конфиденциалност-инвазивни софтуер.

В отговор на появата на шпионски софтуер, започнаха да се занимават с анти-шпионски софтуер различните фирми разработващи антивирустни програми. Редица юрисдикции са преминали анти-шпионски закони, които обикновено целта софтуер, който е инсталиран тайничко да контролират компютъра на потребителя. В САЩ Федералната търговска комисия е поставен на интернет страницата за съвети на потребителите,за това как да намалят риска от инфекция с шпионски софтуер, включително и списък от "DOS" и "don'ts." [17]

1. Най-интересните вируси за 2008 г.

Panda Security [18] състави списък с най-интересните компютърни вируси, които макар да не са причинили големи епидемии, по една или друга причина са станали забележителни през втората половина на миналата година. [19]

P2PShared.U. Този опасен код се разпространява с помощта на пощенски съобщения с тема „McDonalds ви желае весела Коледа!“. В съобщението става дума за купон, даващ правото на безплатен обяд във веригата McDonald's. Именно този купон е носител на вируса. По този начин безплатният обяд може да ви излезе скъпо.

Agent.JEN. Представете си куриер, които ви звъни на вратата със съобщение, че има пратка за вас. Но ако вратата бъде отворена, пълчища мошеници завземат дома ви. Именно до това може да доведе Agent.JEN, ако се докопа до компютъра ви. Той се разпространява в пощенски съобщения, привидно изпратени от куриерската служба UPS. Всеки който свали или отвори прикрепения файл пуска троянски кон, който веднага започва да вкарва други видове вреден код в компютъра ви.

Banbra.FXT. Преструвайки се на съобщение от бразилски съд, Banbra.FXT съобщава на жертвите, че те се намират под следствие и предлага да покаже подробен отчет за хода на делото. Този отчет реално е троянец, който попаднал в компютъра краде банкови пароли и друга лична информация.

Banker.LGC. Състезателят от Формула 1 Фернандо Алонсо е катастрофирал? Нищо подобно – това е просто поредната история, измислена от троянски кон с цел да ви

накара да отворите видеофайл. Всички, които го правят получават троянец, падащ си по банкова информация.

Sinowal.VTJ. Един от най-чудатите вируси за 2008 г. Той се разпространява чрез пощенски писма от неизвестен подател, които твърдят че получателят им е изпратил вируси и го заплашват с полиция. Всички усилия са насочени към това, потребителят да отвори и разпечата приложение, което е „явно доказателство за вината му в разпращане на опасни съобщения“. В резултат в компютъра се вмъква Sinowal VTJ.

BatGen.D. Този вирус е специалист в приготвянето на опасни торти. Той попада в компютъра във вид на файл с название personalcake.bat. На практика вирусът представлява инструмент за създаване на вреден софтуер, който след това пита потребителя как би искал да нарече творението си (seleccionaelnombredelpastel – изберете име за тортата).

Aidreden.A. Вирусът предсказва бъдещето, и то в съвсем мрачни краски. Когато компютърът ви е заразен, на екрана се извежда съобщение „Вие ще умрете през следващия месец“. Този диалогов прозорец е снабден с опция-бутон OK. Едва ли някой потребител би се съгласил спокойно с това предсказание.

Banker.LLN. Този троянски кон попада в компютъра във вид на файл с название barackobama.exe и иконка изобразяваща флага на САЩ. Естествено, вирусът няма нищо с изборите за президент, а спокойно си краде банкова информация.

Banbra.GDB. Когато на вратата ви чука полиция, по-добре е да й отворите. Но не и когато това е троянски кон. Banbra.GDB попада в компютъра във вид на съобщение, привидно изпратено от бразилската полиция. В писмото се казва, че вашият компютър участва в незаконна дейност. На потребителя се предлага да свали отчет, съдържащ доказателства за това твърдение. Ако той се съгласи, и стартира приложението, в компютъра започва да шета банков троянец.

Spammer.AKE. Това е червей, разпространяващ се в пощенски съобщения, съдържащи призиви за приятелство и любов. Не се връзвайте. В противен случай, компютърът ви ще бъде използван за разпращане на спам.

1. Начини за справяне с злонамерния софтуер и вирусите - антивирусни програми.

На базата на проучването, което направих в Интернет и на личният ми опит с голяма част от анти вирусните програми, това са тези от тях, които Ви препоръчвам :

Kaspersky [20] - Тази програма е съвършена за средният домашен потребител. Има препоръчителни настройки и лесен за намиране бутон

” Сканирай “, след натискането на който мигновено ще започне сканиране на вашият компютър на базата на тези настройки.

Това е най-бързата антивирусна програма - на нея и трябват само 8 мин. за да сканира 80 GB твърд диск.

Обновява се автоматично на всеки един час, което означава че е почти невъзможно да бъде създаден нов вирус, който да зарази вашият компютър за толкова кратко време, без Kaspersky да реагират на това.

Ако програмата открие вируси във вашият компютър има доста опции, от които можете да избирате какво да бъде направено с заразеният файл - той да бъде дезинфекциран, да бъде изтрит, само да ви предупреди че е намерен заразен файл или да запомни информацията за по-късна употреба.

Единственият недостатък, който мога да посоча от личният ми опит с тази програма е големият размер на обновленията, които се събират с течение на времето.

Kaspersky осигуряват пълна поддръжка на своите продукти. Можете да се свържете с тях чрез имейл адрес, по-телефона или чрез онлайн форума.

Определено може да бъдете сигурни, че след нейното инсталиране няма да имате никакъв проблем с вирусите.

Има Free OnLine Virus Scanner но не изтрива вирусите.

ESET Nod32 [21] - Това е една първостепенна антивирусна програма, която предлага няколко нива на защита.

Подредбата на контролният център е малко объркана и терминологията е прекалено техническа. Nod32 определено не е програма за хора, които тепърва ще се занимават с компютри.

Nod32 имат претенциите, че те първи са открили и блокирали едни от най-големите вируси, като Melissa, LoveLetter и CIH много преди останалите антивирусни програми. Програмата не се обновява през определен период от време, а само тогава, когато е необходимо.

Nod32 е замислена за по напреднали потребители с възможност за промяна на много различни настройки, включително и по-време на инсталацията на самата програма.

Може да избирате между пет различни режима на сканиране. На програмата са и необходими 24 мин. за да сканира 80 GB твърд диск.

Има денонощна поддръжка чрез телефон, връзка с имейл и достатъчна помощна документация.

Лично аз не съм доволен от нея! Много е лесна за променяне и имах много главоболия с нея!

Trend Micro Antivirus [22] - програмата има много приятен интерфейс, с който се работи съвсем лесно.

Разполага с протокол за защита на компютрите от вируси, червеи, троянски коне, както и Spyware, Rootkits и Malware. Сканира всички постъпващи файлове в реално време, включително и електронните пощи, свалящите се файлове от Интернет и от преносими устройства за съхранени на данни.

Необходимото време на програмата за да сканира 80 GB твърд диск е 30 мин.

Обновлението на Trend Micro се извършва ежедневно, което може би е достатъчно за да се осигури защита срещу повечето ново излязли вируси, но мисля че би било по-добре ако програмата можеше да се обновява на няколко часа.

Поддръжката се осъществява чрез електронна поща, телефон и онлайн чат. Има възможност да ви изпращат и помощна информация за работа с програмата.

Общо взето Trend Micro се представя почти толкова добре, колкото нейните конкуренти, но за същата цена Kaspersky може да сканира компютърът ви доста по-бързо и разполага с по-чести обновления.

Има Free OnLine Virus Scanner - изтрива вирусите.

F-Secure Anti-Virus [23] - Със своят елементарен за употреба интерфейс, тази антивирусна програма е подходяща за начинаещи потребители.

Тя върши добра работа при осигуряването на защитата на вашият компютър от потенциални опасности. Само в рамките на няколко часа след появата на нов вирус,

вашият компютър ще бъде снабден с защита срещу него.

Програмата се обновява по-няколко пъти на ден. Имате достъп и до график на обновленията, така че вие винаги можете да проверите, кога последно е била обновена и кога предстои да бъде обновена отново.

F-Secure не само сканира за вируси, но също има и вграден Anti Spyware скенер. Тя сканира в реално време входящата и изходящата електронна поща и защитава регистрите на Windows от хакерски атаки и от програми, които се опитват да ги променят за да могат след това да се стартират автоматично с Windows.

Необходими са и 35 мин. за да сканира 80 GB твърд диск.

Поддръжката на програмата се осъществява чрез имейл и телефон. На уеб-сайта на F-Secure има достатъчно помощна документация, както и световна карта, на която можете да видите статистиките за вирусите по-целият свят и съответно вашето местно състояние.

От личният ми опит с програмата мога да кажа само, че работи перфектно и не натоварва излишно работата на вашият компютър.

Има Free OnLine Virus Scanner - изтрива вирусите.

McAfee VirusScan и Total Protection [24] - Програмата има вграден ScriptsStoper, който предотвратява вирусите да се разпространяват от ден компютър на друг, както и през електронната поща.

Ако използвате настройките по подразбиране, програмата ще ви предостави много добра защита срещу вируси, троянци, червеи и злонамерени ActivX и Java.

Вие можете да настроите VirusScan и Total Protection да сканира вашият компютър в предварително зададено от вас време. Програмата е доста по-бавна от останалите и и е необходим 1ч. за да сканира 80 GB твърд диск.

McAfee автоматично сваля обновленията на вирус дефинициите от Интернет ежедневно.

Програмата има авариен антивирусен екип, който непрекъснато наблюдава развитието на световните вируси за да може да ви осигури възможно най-голяма безопасност.

Снабдена е с много помощна документация, включително и поддръжка по-телефон, чат и имейл.

Има Free OnLine Virus Scanner но не изтрива вирусите.

От личният ми опит с програмата McAfee Total Protection , която си купувам вече 4 /четвърта/ година съм много доволен.

Norton AntiVirus [25] - Интерфейса на програмата е приятен и лесен за използване. Настройките по подразбиране предоставят защита срещу вируси, SMTP червеи и троянски коне.

При откриване на заразени файлове имате възможност да ги поставите под карантина, като по-този начин те ще останат изолирани на вашият твърд диск докато не бъдат дезинфектирани.

Програмата се нуждае от 35 мин. за да сканира 80 GB твърд диск.

В Norton AntiVirus има вградени и инструменти за откриване на Spyware и Adware. Тя открива и блокира високо рискови Spyware и Adware програми още преди те да бъдат инсталирани на вашият компютър.

Програмата се обновява веднъж седмично, което е прекалено рядко според мен за да бъде защитен вашият компютър от ново излязлите вируси.

Поддръжката се осъществява чрез имейл и помощната документация, която е достъпна до всеки потребител.

От личният ми опит с програмата, като минуси мога да отбележа това, че инсталационният файл е прекалено голям, за разлика от другите анти вирусни програми и определено забавя нормалният работен процес на компютъра. Недостатък също така е и това, че може да ви бъде предоставена поддръжка по телефон само ако си закупите някой от платените пакети за поддръжка.

Има Free OnLine Virus Scanner но не изтрива вирусите.

AVG Anti-Virus Pro [26] - Програмата разполага със сравнително лесен за използване интерфейс. Системната икона на AVG е многоцветна, когато всички компоненти работят правилно. Ако има някакъв проблем тя се оцветява в сиво. Само с едно кликване върху нея имате достъп до контролният панел на програмата.

При откриване на заразени файлове също имате опция да ги поставяте под карантина, докато те не бъдат дезинфекцирани. Сканирането се извършва доста бързо, като на програмата са и нужни 24 мин. за да сканира 80 GB твърд диск.

Обновленията на програмата се извършват автоматично, винаги когато има налични такива, средно веднъж дневно.

Поддръжката на програмата се осъществява чрез имейл и онлайн чат. Има и достатъчно помощна информация. Като минус мога да посоча, че не се предлага поддръжка по телефон.

Има и безплатна версия с ограничени възможностти.