Bulgarian Security Info

- Българското списание за сигурност.
- Брой 3 - 2008 година
- www.virusinfo-bg.org
- Bulgarian Security Research Center
- LOD TS, Bulgarian Portal Network

- Център по компютърна вирусология

- Bulgarian Security Research Portal:
- info@virusinfo-bg.org Информация, запитвания и проблеми.
- newvirus@virusinfo-bg.org нови вируси, заплахи и съмнителни файлове изпращайте тук.

Bulgarian Security Info

- Седмично списание за компютърна сигурност.

- Съдържание:

Как да разберете дали сте заразени с компютърен вирус?

- 1-Първият вариант е от време на време да извършвате пълно сканиране на компютърната система, по план или спонтанно. Добър подход е да правите пълно сканиране поне веднъж в седмицата.
- 2-Вторият вариант за проверка не зависи от вас - ако забележите различни проблеми по време на работа с компютъра, значи вероятността да сте заразен е много голяма. Например, ако започнат да се появяват съобщения за грешки, липсващи файлове или "увисвания" на системата. Все пак трябва да знаете, че подобно поведение на системата не означава непременно, че компютърът е инфектиран. Затова при появата на смущаващи симптоми, изпълнете пълно сканиране на системата.
- Преди да стартирате пълното сканиране, трябва да обновите вирусните дефиниции на използвания от вас антивирусен софтуер. Също трябва да изключите възстановяването на системата. Ето как става в Windows XP: Натиснете бутона "старт" (Start), десен клик върху "моят компютър" (My Computer) и изберете "свойства" (Properties). Оттам изберете възстановяване на системата (System Restore) и сложете отметка в "изключи възстановяване на системата". След това изберете "приложи" (Apply) и на появилия се прозорец натиснете върху "да" (Yes).
- Добра идея е да проверите и кои програми се стартират заедно с операционната система. Някои вируси указват път към изпълнимите си файлове и има възможност да се стартират преди антивирусната програма и да попречат на правилното й функциониране. Отстраняването на този проблем можете да направите по следния начин: бутон Start, след това Run и в появилия се прозорец написвате "msconfig" и избирате Startup, където можете да изберете коя програма да се стартира заедно с операционната система. Важно е да не променяте нищо, ако не знаете на 100% какво правите, тъй като можете да провалите нормалната работа на системата.

Почистване(лекуване) на заразата

- 1-За да започнете „излекуването“, трябва да влезете в така наречения Safe режим, което става по следния начин: рестартирайте компютъра и преди да започне зареждането на операционната система Windows, натиснете бутона F8 от клавиатурата. След като сте влезли в безопасния режим на Windows, можете да стартирате антивирусната си програма и да направите пълно сканиране на системата. Когато приключи сканирането и заразените файлове бъдат изтрити, погледнете статистиката и вижте дали броят на намерените инфектирани файлове е същият като изтритите. Ако не е, вижте кои вируси не са изтрити и потърсете инструменти за премахването им. Всеки производител предлага подобен род мини приложения, предназначени за изчистване на точно определен вирус.След като всичко е минало благополучно и вирусите са били изчистени, върнете системата в първоначално състояние, като отново включите възстановяването на системата (от System Restore).
-
- Превенция

- Много е важно вашето поведение в мрежата, за да избегнете заразяване на компютъра, а в някои случаи и загуба на информация. Затова ето няколко съвета, които ако бъдат спазвани, възможността да инфектирате вашия компютър е нищожна

- 1-Никога не стартирайте програми от неизвестен източник, например свалени от Интернет. Ако все пак не можете да се сдобиете по друг начин с необходимата програма, преди да я стартирате, задължително сканирайте изпълнимия файл.
- 2-Избягвайте посещението на порнографски или хакерски сайтове.
- 3- При получаване на електронно писмо, преди да го отворите, вижте кой е подателят и ако ви е непознат, по-добре не рискувайте с отварянето му.
- 4-При получаване на електронно писмо с прикачен файл винаги сканирайте файла, преди да го отворите, дори подателят да ви е познат.
-
- Тези елементарни мерки може да ви предпазят от сериозни беди. Друг е въпросът за избора на антивирусна програма, която в днешно време е задължителна. В компаниите с по-сложни компютърни инфраструктури мерките също са различни от описаните в статията. За сигурността на системите в добрия случай там се грижат професионалисти и дори цели отдели, които защитават фирмените мрежи с помощта на развити технически средства, обикновено комбинация от софтуер и хардуер.

- Автор:**mihnev_sz**
- М. Михнев
- e-mail: mihnev_sz@abv.bg
- Skype: mihnev_sz

Проактивните технологии

- „Знанието е сила , а силата успех”! Добре известна поговорка , но дали всеки я спазва , когато става дума за сигурността на данните ?
- Както писахме в последния брой на Bulgarian Security Info , съвсем логично е Интернет да е основната причини за развитие на каквито и да е било заплахи . Всички днес сме свързали домашните и работните си компютри най-малко в мрежа с други компютри - тези на нашия интернет доставчик , редовно увеличаваме скоростите за достъп то Мрежата … Скоростта , с която получаваме и изпращаме информация до други машини може да се използва както и по наше желание , така и от всяка една програма , която е инсталирана на компютъра ни и има права да го направи . Днешните заплахи придобиват „супер права” и използват тази скорост , за да изпълнят мисията си . Колкото по-бърза е връзката ни с Мрежата , толкова по-зле . Следователно колкото повече технологиите се развиват , толкова по-бързо ще се развиват и съвременните заплахи , защото е много по-трудно за dial-up потребител да се зарази и заплахата всъщност да краде информация.
- Именно огромните темпове , с които технологиите се развиват , и респективно нарастващите рискове за кражба на информация за „нула време” , карат компаниите , които се занимават с разработката на защитен софтуер да се опитат да са една крачка през врага . Нараствайки , скоростта води след себе си и друг недостатък , който не може да бъде избегнат поради простата причина , че е естествен процес . Скоростта расте , а времето намалява ; хората са едни и същи . Заплахите се увеличават и се разпространяват все по-бързо , а антивирусните компании са в постоянно надпреварване и надбягване . Процесът изглежда безкраен и трябва да бъде спрян . Единственият начин , по който може да бъде осуетен е чрез прекъсване на порочния кръг – заплахите са същите , но загиват много по-бързо , даващо повече време на хората .
- Проактивните технологии са ,най-общо, начини , чрез които антивирусните продукти могат да засекат и евентуално елиминират дадена заплаха без преди да са я срещали или формулирано по друг начин- да убият потенциална заплаха за сигурността на информацията , да я елиминират и да не и позволят да се възползва от напредъкът на цивилизацията за да извършва зловредни действия .

Проактивните технологии

- През 2003 година антивирусните компании получавали средно около 100 заплахи дневно . През 2007 година се появяват нови заплахи обикновено всяка минута и на антивурусните компании им се налага да обработват прекалено много информация ежедневно / ежеминутно . Това е непосилно за хората . Проактивната технология спомага за откриването на голям набор от нов зловреден код , спестявайки много време и ресурси и давайки много по-голяма защита на потребителите не само от заплахите , които са се появили вчера , но и от тези , които ще се появят утре .
- Евристичните технологии и програми за наблюдение на поведението са двата клона на проактивните технологии . Всяка една от тях има множество подразновидности , но най-общо евристичните технологии наблюдават за общо поведение на зловреден код чрез анализ на съдържанието/кода на файла , докато програмите за наблюдение на поведение следят какво дадена програм е извършива току-що , преценяват дали то е било опасно за системата и моментално алармират/блокират и биха могли да върнат назад *повредите* .
- Обикновен разбираем пример за това какво е проактивна технология:
- Известно е , че години наред всички крадци и обирджии са използвали черни шапки , които са поставяли на главите си . Проактивната технология веднага ще реагира , когато забележи индивид , облечен с точно такава шапка , защото знае , че това е типично поведение на престъпник.

Проактивните технологии

- Но нали само през 18 и 19 век крадците са слагали точно такива шапки ? Днес определно е по-сложно >>> Ситуацията е идентична и при зловредните програми . Сега е не може да се разпознае зловредна програма само по един или два признака . Интелигентна е само тази проактивна технология , която успее да улови всички признаци и да блокира само наистина опасните приложения . В днешно време не можем да кажем , че даден индивид е крадец само защото носи черна шапка на цялата си глава . Направим ли така , допускаме огромна грешка . Случи ли се това при проактивните технологии , излагаме на риск системите си – генерира ли се false positive може да е неприятно , конфузно , но и опасно .
- Единствено и само интелигентната система може да ни помогне да сме една крачка през врага и умело да различи приятеля от врага , докато самите ние се научим да мислим , защото “Интелигентността вече не е привилегия само на човешките същества” © ESET

- Автор:**ASpace**
- А. Спасов

Обща информация за вирусите част 3-та

- Някои вируси търсят да заразят определени файлове, например основният шаблон за документи, използван с Microsoft (MS) Word — normal. dot. Други извършват търсене на целия компютър за определени файлови типове, например такива с разширения . exe или . com.
- Паразитно прикрепване към файл-гостоприемник
- Вирусите се прикрепват като паразити към съществуващ файл-гостоприемник на даден компютър. Например ако игра с име tank.exe съдържа 10 000 байта код, той може да стане 12 000 байта, след като програмата бъде заразена с вирус.
- Когато заразената програма бъде стартирана, кодът на вируса се изпълнява заедно с кода на tank.exe. Вирусът е зависим от приемащата програма и може да се разпространи в системата само след като се прикрепи към съществуващи файлове. След като вирусът се стартира, той се прехвърля на друг файл в системата и може също така да се опита да се изпълни и в паметта.
- Вируси, които се изпълняват в паметта
- Вирусите TSR (Terminate and Stay Resident — „стартирай и остани резидентен") под DOS се опитват да се изпълняват в паметта, след като бъдат стартирани от заразен файл-гостоприемник. Веднъж оказал се в паметта, кодът на вируса работи за заразяване на най-различни файлове в цялата система, докато компютърът не бъде изключен. Той може да работи също с цел скриването си от потребителя или от антивирусна програма, инсталирана на компютъра.
- Много TSR вируси се опитват да заразяват стартови файлове, така че да бъдат отново стартирани в паметта при следващо рестартиране на компютъра.
- Репродуциране на макровируси
- Кодът на макровирус се изпълнява при отваряне на заразен файл на Microsoft Word. Макровируси като например Cap действат бързо, за да се прикрият, като изключват елемента Macro от менюто Tools в Microsoft Word. Същевременно те се опитват да заразят файла normal. dot на PC и normal на Macintosh — глобалният шаблонен файл по подразбиране на Microsoft Word, който се отваря всеки път при стартиране на приложението.
- Всеки файл на Microsoft Word, който бъде отворен след първоначалното заразяване, в общия случай се заразява от макровируса. Това е изключително ефективен метод за разпространяване на вируси в мрежова среда,

Обща информация за вирусите част 3-та

- тъй като файловете на Microsoft Word обикновено се обменят между пот-ребители. Макровирусите са в състояние да контролират работната среда след отваряне на Microsoft Word, като заразяват всеки отворен или ново-създаден файл, понякога без да бъдат разкрити дълго време.
- При положение че потребителят не забележи никакви странични дей-ности от заразяването с вирус, той може дори да архивира заразените файлове на дискета. След като вирусът бъде отстранен от системата, по-късно той може да бъде повторно внесен в нея чрез архивните копия на файлове. Ето защо е изключително важно потребителите да инсталират сканиращ софтуер с незабавен достъп, който ще помогне за защита сре-щу заразяване, докато потребителят работи с компютъра. Потребител, който разчита на ръчно сканиране с антивирусна програма от време на време, може да зарази повторно системата си и да продължи да разпрос-транява макровируса за дълъг период от време.
- Ориентация на вирусите към репродуциране
- Вирусите разчитат повече на репродуциране, отколкото на унищожа-ване или кражба на поверителни данни. Цялата идея на традиционните вируси е да заразяват колкото е възможно повече компютри и мрежи. При наличие на такава философия унищожителните действия са срав-нително рядко явление.
- Значително по-малко от 10 процента от най-разпространените на сво-бода вируси днес носят зловреден товар. Независимо че някои вируси задръстват сървъри за електронна поща или повреждат файлове, преди да бъдат отстранени от дадена система, като цяло те не са предназначе-ни да й навредят. Вируси, които са нарочно злонамерени, като Chernobyl и Love Letter, не са толкова често срещани, но пълнят вестникарските заглавия, когато бъдат открити „в зоопарка" или „на свобода".
- За щастие повечето силно разрушителни вируси не са толкова изобилни на свобода както беше Chernobyl през 1999 г. и Love Letter през 2000 г.
- Важно е да се отбележи, че вирусът Chernobyl имаше голямо разпрос-транение в Азия, където порази около 600 000 компютъра на 26 април 1999 г., а нещо подобно се случи през 2000 г. с Love Letter. Пораженията в тази част на света бяха толкова големи, от една страна, поради разпрос-траняването на пиратски софтуер и липсата на превантивни мерки. Голя-ма част от поразените потребители бяха купили нелегално записани ком-пактдискове с операционни системи, върху които е записан и Chernobyl. В САЩ бе съобщено за незначителен брой случаи на заразяване с Chernobyl в резултат на липсата на нелегален пазар на софтуер и засилено внимание от страна на медиите, което доведе до засилване на превантивните мерки от корпоративните среди и домашните потребители.

Обща информация за вирусите част 3-та

- Нови заплахи за сигурността
- С промяна на технологията се наблюдава и промяна на съществува-щата заплаха от вируси. Много нови технологии, като например т. нар. „бисквитки" (cookies) и JavaScript, карат потребителите да се замислят за нови типове злонамерен софтуер. Докато „бисквитките" не са изпъл-ними програми, JavaScript е добър пример за това как някакъв нов код може да проникне злонамерено или да разруши работната компютърна среда на потребителя. JavaScript може .да се изпълнява в Web браузър, за Да извежда фалшиви съобщения и предупреждения, да отваря непре-къснато прозорци на приложения — докато се достигне до проблем с паметта, и дори да изключи браузъра.
- Други нови заплахи, като например BubbleBoy, използва един бъг, за да заразява системи. Един компютър може да бъде подложен на риск от на пръв поглед елементарно свойство, каквото е Auto-Preview в програ-мите за електронна поща MS Outlook, комбинирано с неподходящ конт-рол на сигурността. При функцията Auto-Preview, когато е избрано съ-общение в електронната поща, програмата автоматично стартира код, който да изобрази съобщението в прозорец за предварителен изглед. Но-ви злонамерени програми като BubbleBoy използват това действие, за да заразят системата с вирус или да пуснат заразяващ скрипт в стартовата папка (Start Up) на твърдия диск.
- Защо биват създавани вируси?
- Първоначално вирусите били разработвани от изследователи, за да се установи какво е поведението на определен софтуер при такава заплаха за компютърната система. Днес вирусите биват създавани за голямо раз-нообразие от цели, обхващащи неща от чисто предизвикателство — до кибервойна.
- Профил на автора на вируси
- Създателите на вируси са от деца — до възрастни хора. Повечето от тях са от мъжки пол и попадат в три основни възрастови категории — юноши, младежи (студенти) и възрастни (в общия случай — под 40 години). Мотивацията на трите възрастови групи е различна. Средният програмист на вируси няма експертни умения в тази област. По-умелите програмисти понякога членуват в групи като например 29A.

Обща информация за вирусите част 3-та

- Често срещани мотиви
- Създаването на един вирус се счита за безотговорно деяние, но етика-та на повечето създатели на вируси включва някакво оправдание на техните злодеяния. Някои професионални създатели на вируси работят само за да разкриват пробиви в сигурността или да създадат злонамерен софтуер, който ще бъде забелязан от пресата и публикуван в списъка WildList на Джо Уелс.
- Преобладаващите мотиви за създаване на злонамерен софтуер включ-ват гордост и желание за слава, предизвикателство и вандализъм. След-ва списък с възможните мотиви.
- *Гордост и желание за слава.* Вниманието от страна на пре-сата, „плодовитостта" на даден вирус на свобода, жертвата на зараза, „първооткривателството" на слабо място в защи-тата или нов метод за заразяване — всичко това понякога носи определена слава на някои създатели на вируси.
- *Предизвикателство.* Много от ентусиастите, създаващи ви-руси, търсят и се наслаждават на предизвикателствата, кои-то им отправят новите технологии.
- *Отмъщение/вандализъм.* Някои вируси са предназначени спе-циално да нанесат удар на определена компания или лич-ност. Познати са случаи, когато недоволни служители съз-дават злонамерен софтуер и го „засаждат" с цел да унищожи работната среда, когато имат оплаквания или бъдат уволне-ни. Други създатели на вируси са обикновени вандали, кои-то нямат друг мотив, освен да повреждат или унищожават компютърни системи.
- *Власт.* Някои създатели на вируси изпитват усещане за власт, когато успеят да изтрият данни или да проникнат в повери-телна информация.
- *Разкриване на слаби места в защитата.* Някои програмис-ти използват злонамерен софтуер, за да докажат наличие на „дупка" в защитата на даден софтуерен пакет.
- *Финансова изгода.* Цените на акциите на компании, които създават антивирусен софтуер, в много случаи се определят от избухването на „епидемии" или настъпване на други съ-бития, свързани с вируси.
- *Шпионаж/нападение.* Получаването на поверителна или сек-ретна информация за корпоративни инициативи, правителс-
- Автор:**LORD OF DARK**
- Ц. Угринов
- Skype: LORDOFDARK E-Mail: info@virusinfo-bg.org

Седмично електронно списание за компютърна сигурност

- Благодарости на ASpace, че се съгласи да се включи в този брой на списанията и се надяваме и за напред да се включва и да дава полезна информация.
- Специална благодарност и на mihnev_sz за статията.
- Virus Info се спонсорира с любезното съдействие на Eset.bg

Други проекти на Bulgarian Portal Network:

- www.potal-bg.info Софтуерни новини
- www.bg-windows.info Помощ за Windows, статии, новини, трикове и други

Bulgarian Security Research Portal:

- info@virusinfo-bg.org Информация, запитвания и проблеми.
- newvirus@virusinfo-bg.org нови вируси, заплахи и съмнителни файлове изпращайте тук.