ОБРАЗОВАНИЕ
С НАУКА

Първи въпроси в компютърната вирусология

НЛКВ • БАН

НЛКВ • БАН

Национална лаборатория по компютърна вирусология, Българска академия на науките

Националната лаборатория по компютърна вирусология към БАН е единственото научно звено в България, специализирано в областта на компютърната вирусология, работещо за осигуряване на максимална компютърна сигурност, комуникационна сигурност и сигурност на данните.

“

Ted Nelson

The good news about computers is that they do what you tell them to do. The bad news is that they do what you tell them to do.

НЛКВ • БАН

Национална лаборатория
по компютърна вирусология, БАН

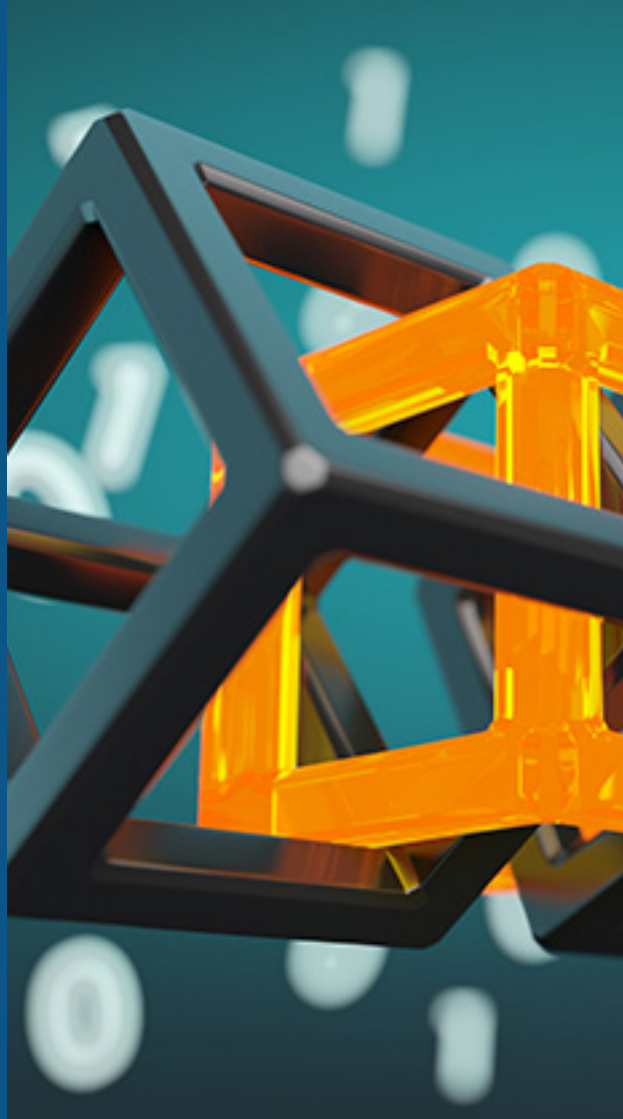
https://nlcv.bas.bg/

e-mail: office@nlcv.bas.bg

София 1113,
ул. “Акад. Георги Бончев”,
блок 8, офис 104

+359 2 9733398

СЪДЪРЖАНИЕ



01. Какво е компютърен вирус?

Най-общо казано, компютрният вирус е програма, която има способността да се саморазмножава. Саморазмножението е както необходимо, така и достатъчно условие една програма да е вирус. Тоест, ако една програма се саморазмножава, то тя е вирус, дори и нищо друго да не прави. Съответно, ако една програма не се саморазмножава, то тя не е вирус, независимо колко и какви други вредителски действия тя извършва.

Възможността да се създават вируси е неотменима част от съвременните компютри с общо предназначение. За да бъдат вирусите невъзможни, необходимо е да е изпълнен поне един от следните три фактора:

- **Компютърът трябва да е програмируем и с общо предназначение –** например вируси за строго специализирани компютри, като този, който управлява пералната машина, са невъзможни.
- **Трябва да има ограничение в обмена на информацията.** Например, ако една програма в компютъра не може да предава информация на друга, то вируси за този компютър са невъзможни.
- **Информационният поток в компютъра не бива да е транзитивен.** Тоест, ако една програма може да предаде информация на друга, а другата – на трета, трябва да е невъзможно първата програма да може да предава информация на третата по какъвто и да е начин. Ако това условие е спазено, вирусите са невъзможни.

За съжаление, кое да е от горните условия е твърде ограничително за практическо приложение, което да не прави компютъра прекалено ограничен и неизползваем. Може би най-близкото приложение са модерните смартфони, работещи под управлението на операционната система Android или iOS. Приложенията, работещи на тях, имат достъп само до собствените си файлове – не и до другите приложения, работещи на телефона. Инсталирането на приложения става само от предназначените за целта хранилища на приложения; не е възможно едно приложение да се прехвърли от един смартфон на друг. Затова, за модерните смартфони вируси на практика не съществуват. Има само редки изключения – например, вируси, които работят само на "разбит" (jailbroken) смартфон, или вируси, които изпращат съобщения до всеки един от контактите на заразения телефон. Тези съобщения се опитват да убедят получателя ръчно да инсталира вируса (претендиращ, че е полезно приложение) от хранилище на приложения, контролирано от автора на вируса.

Има много видове вируси; подробното им описание излиза извън рамките на този материал. По-специален клас вируси са т.нар. "червеи" – това са вируси, които умишлено използват компютърните мрежи, за да се размножават от един компютър на друг.

02. Всички вредителски програми ли са вируси?

Не. Въпреки че за много хора думите “компютърен вирус” и “вредителска програма” са синоними, както видяхме по-горе, за да бъде една програма вирус, тя трябва да е способна да се саморазмножава. Само по себе си, размножаването е вредителска функция (защото използва компютърни и мрежови ресурси без разрешението на собственика им), така че всички вируси са вредителски програми. Но далеч не всички вредителски програми са вируси. Тези, които не се саморазмножават, не са такива. Има много видове вредителски програми, които не са вируси – троянски коне, задни вратички, логически бомби, шпионски софтуер, рансомуер, и др. Събирателно, всички видове вредителски програми (включително вирусите) се наричат за по-кратко “малуер” (“malware”) – от английските думи “**mal**icious” (“вредителски”) и “soft**ware**” (“програма”).

“

Gordon Glegg

Sometimes the problem is to discover what the problem is.

03. Какво е рансомуер и как да се предпазим от него?

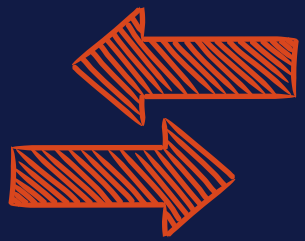
Рансомуер (“ransomware” – от английските думи “ransom” – “откуп” и “software” – “програма”) се нарича класът вредителски програми, които забраняват достъпа на потребителя до собствената му информация и искат изплащането на откуп за освобождаването ѝ. На обикновени компютри тази забрана за достъп се осъществява чрез шифроването на файловете с данни (картинки, документи, и т.н.) на потребителя. На смартфони, където вредителската програма няма достъп до файлове, които не ѝ принадлежат, това обикновено се осъществява чрез заключване на устройството. Единственото изключение са файловете с данни на SD картата на телефона – до тях имат достъп всички приложения и те понякога се шифроват от рансомуера за телефони. За изплащане на откупа обикновено се използват електронни криптовалути като Биткойн и др. (напр. Монеро), които са сравнително анонимни и е трудно да бъдат проследени до авторите на рансомуера.

Този вид вредителски програми е изключително популярен сред кибер престъпниците, защото жертвите често се виждат принудени да платят откупа, тъй като не разполагат с друг начин да си върнат ценната информация. Напоследък организираните банди от кибер престъпници, които специализират в тази област, насочват усилията си към компрометирането на цели мрежи в големи компании и в шифроването (чрез рансомуер) на данните от хиляди компютри в тях. Доходите за престъпниците от един успешен удар срещу средно голяма компания често пъти възлизат на милиони, в случай че откупът бъде платен. А ако не бъде платен, загубите за компаниите понякога могат да достигнат милиарди долари. Напоследък все по-модерна е тенденцията престъпниците да заплашат да публикуват на някое общодостъпно място конфиденциалните данни на компанията, които те са откраднали преди шифроването им, в случай че последната откаже да изплати искания откуп.

Има редица програми, които се опитват да предпазват от нападение на рансомуер. Това са както традиционните антивирусни програми, така и специализиран софтуер, който се опитва да извърши ранно откриване на процеса на шифроване на файловете и да прекъсне работата му. Но нито една от тези програми не дава стопроцентова гаранция за защита.

Значително по-надежден подход, особено за индивидуални потребители и за сравнително малки компании, е редовното правене на резервни копия (“бекъпи”) на всички ценни данни. Тези резервни копия не бива да се правят върху носител, който е постоянно закачен за защитаваният компютър и до който последният има постоянен достъп, защото тогава и рансомуерът има такъв достъп и резервните копия е най-вероятно също да се окажат шифровани.

Правенето на такива резервни копия трябва да се извършва само когато сме сигурни, че машината не е заразена и върху диск, който се закача за нея само временно (за времето за копиране на данните), или през мрежата, през акаунт, който може да чете и копира защитаваните данни, но в който защитаваната машина няма права за запис.



James Scott, Sr.

Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact.

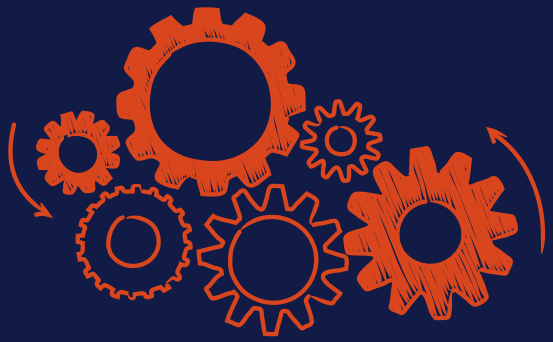
Индивидуалните потребители биха могли да държат по-ценните си данни в мрежови дискове като OneDrive или Dropbox; те съхраняват много различни версии на файловете и могат да възстановят до стара версия, ако последната изведнъж се окаже шифрована. Компаниите, които стоят зад тези мрежови дискове обикновено предоставят безплатно само ограничено дисково пространство (напр. – 2 GB), годно само за най-ценните данни на потребителя. Но значително по-големи капацитети се предоставят на сравнително разумна цена – например един абонамент за Office365 Business Basic струва 5 долара на месец и включва 1 TB дисково пространство в OneDrive.

04. Необходимо ли е да използваме антивирусна програма?

Твърде разпространено е мнението, че от антивирусните програми няма особена полза. Наистина, от една страна непрекъснато чуваме истории за това, как един или друг компютър е бил заразен (въпреки антивирусната си програма), а от друга страна – оплаквания за това, как антивирусната програма само забавяла компютъра и задръствала паметта, или пък пречела на тази или онази игра да работи както трябва.

Доколко е достоверно това?

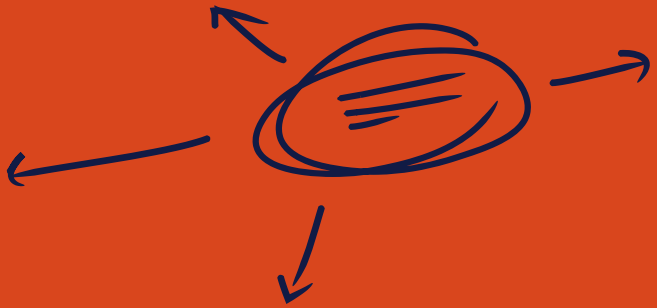
Преди всичко, трябва да се изясни за какъв вид операционна система става дума. Например Apple изрично забранява присъствието на антивирусни приложения в хранилището на приложения за iPhone и iPad. Може да се спори доколко тази политика е разумна, но във всеки случай тя не нанася голяма вреда, защото вредителски програми за iOS практически няма, така че липсата на антивирусни програми за тях няма особено отрицателен ефект.



Вредителски програми за Linux и MacOS (включително и вируси) определено съществуват, но са много малко разпространени. Това е така не защото (противно на разпространеното мнение) тези операционни системи са по-защитени от Windows например, а защото са много по-рядко използвани. Съответно, броят на потенциалните жертви, които ги използват, е относително малък и кибер престъпниците, общо-взето, не си правят труда да се занимават с тях. Затова, неизползването на антивирусна програма при тези операционни системи не е придружено от сериозни рискове.

От друга страна, за операционните системи Android и особено за Windows, съществува огромно множество вредителски програми. Това множество непрекъснато се разраства – например само за Windows, се създават над един милион нови вредителски програми всеки месец. Ако такава машина е свързана към интернет и на нея се работи активно (например за посещаване на уеб сайтове и за четене на електронна поща, да не говорим за сваляне на игри), срещата с някаква вредителска програма е практически неизбежно.

Поради огромното и непрекъснато разширяващо се множество от вредителски програми за тези операционни системи, никоя антивирусна програма не може да гарантира прехващането и спирането на всички възможни такива програми. Именно на този факт се дължат историите, че този или онзи компютър бил заразен, въпреки инсталираната антивирусна програма.



От друга страна обаче, антивирусните програми все пак спират огромна част от известните вредителски програми. Именно затова използването им на тези операционни системи (особено на Windows) е просто задължително, а неизползването им е просто безотговорно. Малкото забавяне на работата на компютъра, предизвиквано от тези програми и проблемите, които в много редки случаи те могат да предизвикат, са нищожна цена в сравнение с риска от заразяване, който те са в състояние да предотвратят.

Така че, да, ако работите на операционната система Windows, използването на някаква антивирусна програма е просто задължително.

Seymour Cray

The trouble with programmers is that you can never tell what a programmer is doing until it's too late.

05. Коя е най-добрата антивирусна програма?

Това е често задаван въпрос, на който е доста трудно да се отговори – предимно защото различните хора имат различни критерии за оценка. За едни е важна цената, за други – доколко се забавя компютърът при използването й, за трети – колко надеждно програмата спира малуера, който би нападнал машината.

Дори да се съсредоточим само на един критерий (качество на защитата), правилната му оценка е изключително трудна. Съществуват толкова много вредителски програми (десетки милиони), че никой не знае точния им брой, да не говорим да тества всяка една от тях дали се открива и от кои антивирусни програми. Освен това различните антивирусни програми използват различни подходи за защита, някои от които е много трудно да бъдат тествани, а резултатите понякога е невъзможно да бъдат сравнявани.

Съществуват поне две международни компании, които се специализират в независими тестове на антивирусни продукти. (Независими, в смисъл, че те не са свързани с нито един производител на такива продукти, въпреки че производителите заплащат тестването на продуктите им.) Това са ***www.av-test.org*** и ***www.av-comparatives***.org. Ако посетите сайтовете им, можете да разгледате докладите, съдържащи резултатите от тестването на редица антивирусни продукти.

www.av-test.org

www.av-comparatives

Може да се спори доколко е високо качеството на тези тестове, но тези компании са най-добрият източник на такива, с каквито разполагаме. При преглеждането на резултатите впечатление прави това, че “оценките”, получени от повечето антивирусни продукти са доста близки помежду си. Това, в общи линии, съвпада и с нашето мнение по въпроса. Не е от особено значение коя точно антивирусна програма ще използвате, стига да е от добре известен производител и да бъде редовно обновявана. Използването на коя да е от тях е значително по-добре от нищо.

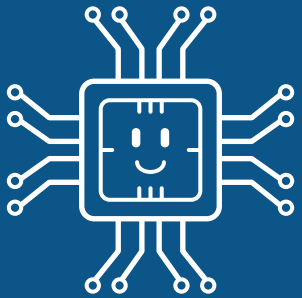
Нашият съвет е да предпочитате платена антивирусна програма пред безплатните, но това не е от особено голямо значение. Дори да не разполагате със средства за платена антивирусна програма, и дори да използвате Windows Defender (безплатна антивирусна програма, която се съдържа в операционната система Windows 10), това ще ви осигури адекватно (но не и абсолютно!) ниво на защита.

Особено внимание трябва да се обърне на това, дали антивирусната програма наистина работи, а не е изключена поради някаква причина, и че се обновява редовно (а не например, че е спряла да го прави, защото е изтекъл лицензът й). Включете всичките й нива на защита – например да сканира файлове при достъп, да проверява линковете на сайтовете, които се опитвате да посетите, да сканира файловете, прикачени към съобщенията, пристигащи по електронната поща и т.н.

Все пак, доверието ви в защитата, предоставяна от антивирусната програма, не бива да бъде абсолютно. Рано или късно някоя вредителска програма вероятно ще успее да я пробие. Затова редовно правете резервни копия на ценната си информация, за да не я загубите в случай на успешна атака.

06. Може ли компютърът ми да бъде заразен, ако сложа в него флашка?

Отново отгорът е – не е така просто, както става по филмите.



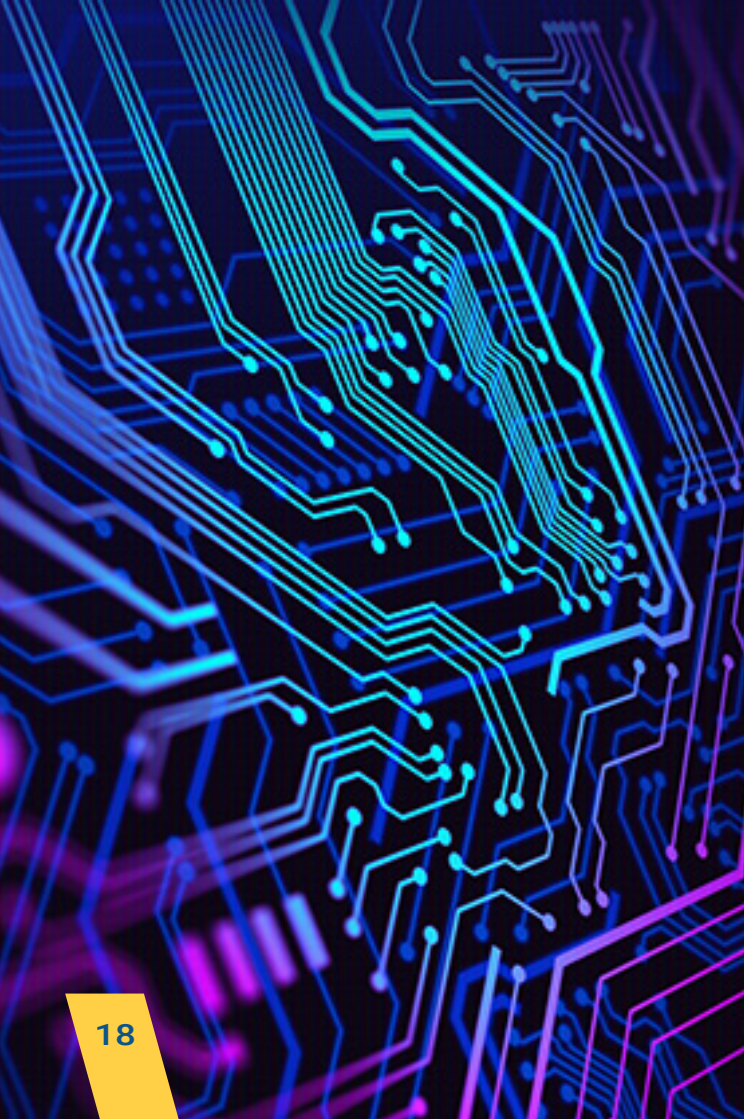
Преди много години, ако главната директория на флащката съдържаше файл, наречен autorun.inf, който представлява текстов файл със специален формат, поставянето й в компютър, работещ под управлението на операционната система Windows, водеше до автоматичното интерпретиране на компандите в този файл. Те можеха да стартират автоматично изпълним файл, намиращ се някъде другаде на флашката, което да доведе до заразяването на компютъра. Редица вируси използваха този метод, за да се разпространяват от един компютър на друг.

Но от много години това не е така. Още през 2006 г., когато най-популярната операционна система беше Windows XP, фирмата Microsoft въведе промени в нея, които доведоха до това, че този файл вече не се интерпретира автоматично от флашки.

Има, обаче, няколко "но".

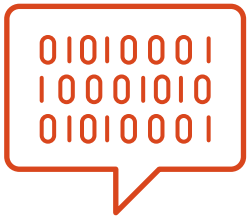
- **Първо,** докато този файл не се интерпретира автоматично от флашки, той все още се интерпретира автоматично от CD-та. А има модели флашки, които съдържат дял, който се държи като CD. Ако поставите в компютъра си флашка от този тип, и споменатият файл се съдържа на дяла й, който се държи като CD, компютърът ви може да бъде заразен.

- **Второ,** (което е донякъде свързано с първото), дадено USB устройство се идентифицира от компютъра като "флашка" (т.е. като диск) като резултат от информацията, намираща се във фирмуера му. Възможно е да се вземе стандартна флашка и тя да се промени по такъв начин, че компютърът, в който се постави, да я идентифицира като друго устройство – например като USB клавиатура или мишка. Тогава така специално приготвената флашка може да започне да дава клавиатурни команди на компютъра, в който е поставена. Тези команди могат да доведат до свалянето (или до създаването) на вредителска програма върху машината и до нейното изпълнение, което от своя страна да доведе до заразяването й.



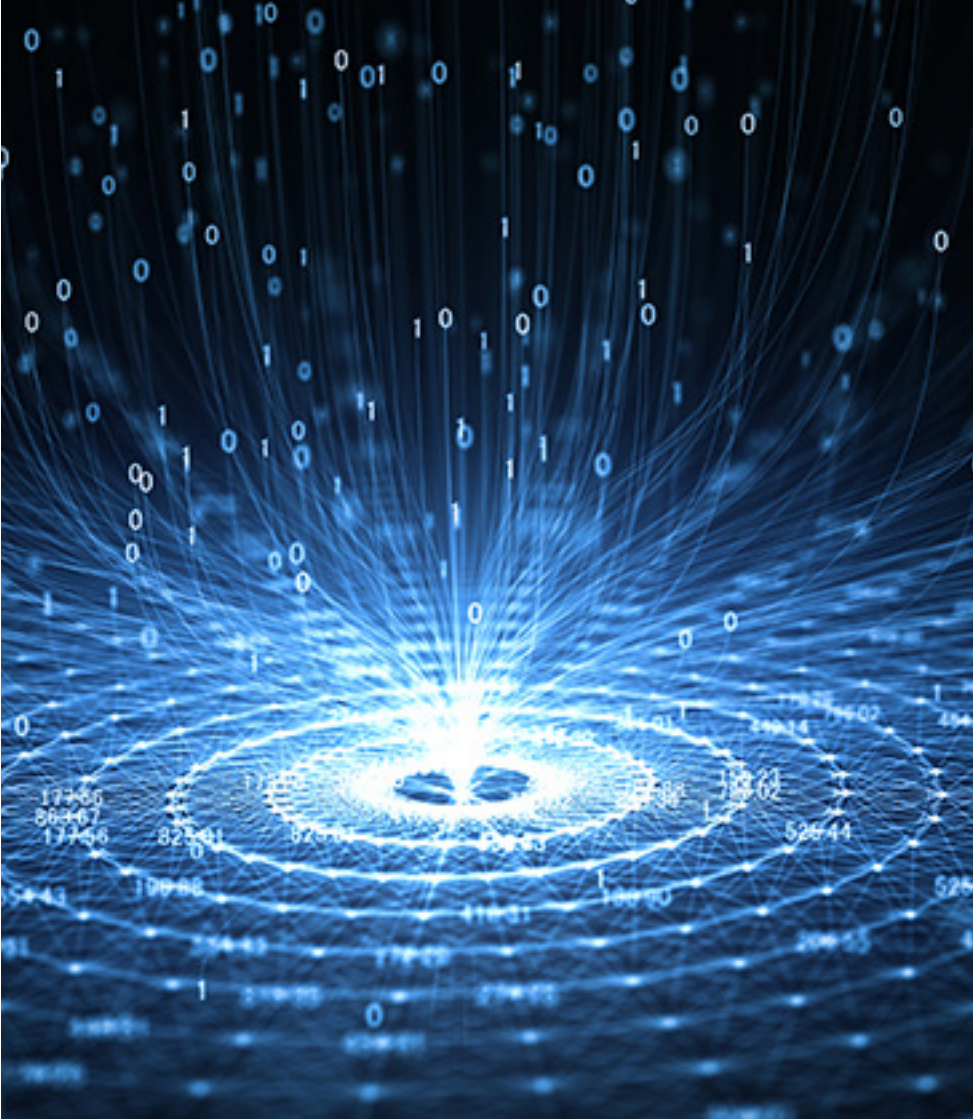
- **Трето,** възможно е на флашката да се съдържа изпълним файл, иконката на който да е напълно еднаква с иконката на директориите. Когато потребителят я види, много е вероятно той да цъкне двойно по нея, “за да види какво има в директорията”, което да доведе до изпълнението на програмата. Съществуват вируси, които използват този трик за да се разпространяват чрез флашки. Макар изпълнението да не е автоматично и да разчита на действията на потребителя, трикът е достатъчно ефективен и често сработва.

Четвърто, възможно е да съществуват неизвестни досега уязвимости в кода на операционната система, който отговаря за разпознаването на флашките. Именно такава уязвимост беше използвана от червея Stuxnet, който беше използван от американското разузнаване за саботиране на иранската програма за обогатяване на уран. Но, това е доста рядка и малко вероятна атака, пък и ако американското (или което и да е друго) разузнаване фигурира сред потенциалните ви нападатели, имате много по-сериозни проблеми от опасността да заразите компютъра си с флашка.



> **Anonymous**
>
> A disaster is often a sequence of apparently harmless, little mistakes.

Все пак, поради всички тези възможни методи на атака, желателно е да не слагате в компютъра си флашки, които не са ваши и на които не може да се има пълно доверие.



“

When you look at the dark side, careful you must be ... for the dark side looks back.