9. ДЕСТРУКТИВЕН СОФТВЕР

Деструктивен или малициозен софтвер (скратено **malware** од **mal**icious soft**ware)** е општ поим за „лош“ софтвер. Хакерите го користат злонамерниот софтвер со цел неовластено пристапување до компјутери од каде можат да преземат доверливи информации, да нанесат штета на сопственикот со бришење на податоци, итн.

9.1. Видови на деструктивен софтвер

Постојат различни видови деструктивен софтвер, како:

- Компјутерски вируси
- Компјутерски црви
- Тројанци
- Логички бомби
- Spyware
- Adware
- Spam

Компјутерските вируси (computer viruses) се мали софтверски програми кои се направени така што при извршување или се репродуцираат самите или инфицираат други компјутерски програми на тој начин што ги модифицираат. Со тоа тие ја попречуваат нормалната работа на компјутерот. Притоа се мисли на можното оштетување или бришење на податоците. Се манифестираат со значително зголемена искористеност на процесорот, меморијата и/или тврдиот диск. Вирусите се поделени во неколку групи:

- Boot sector вируси
- Master Boot Record вируси
- File infector вируси
- Macro вируси

***Boot sector* вирусите** го заразуваат **boot** секторот на тврдиот диск, флопи дисковите или флеш мемориите. Теоретски тоа може да го направат и на CD или DVD медиумите. Кога заразениот компјутер ќе се покрене, овие вируси преминуваат во работната меморија и од таму се пренесуваат на сите нововнесени медиуми за снимање податоци. За среќа, со се помалата употреба за флопи дисковите се намалува ризикот од нив, но од друга страна употреба да флеш дисковите го зголеми ризикот од нивно распространување.

***Master Boot Record* вирусите** се многу слични на претходните само што тие го заразуваат MBR (Master Boot Record).

***File infector* вирусите** се специјално дизајнирани да ги заразат екзекутивните фајлови

чија екстензија е .exe или .com. Вообичаено овие вируси се сместуваат во работната меморија како резидентни програми и од таму ги заразуваат специфичните фајлови.

***Macro* вирусите** се направени да заразуваат специфични фајлови како што се word, excel или powerpoint документи. Тие го користат Visual basic macro програмскиот јазик што е вграден во Microsoft Office. Макро вирусите може да се шират преку email додатоци (attachments). Овие вируси се нарекуваат email вируси. Еден од најпознатите email вируси е вирусот **Mellisa** од 1999-тата година. Работел како и повеќето email вируси: корисникот прима „важна порака“ од пријател која содржи документ со примамлива содржина. Документот всушност содржи макро вирус и откако корисникот ќе го отвори документот, вирусот веднаш започнува со праќање на заразениот документ на првите 50 адреси од адресарот на корисникот.

Компјутерските црви (worms) се само-реплицирачки програми кои самостојно се пренесуваат низ компјутерски мрежи. За разлика од компјутерските вируси ним не им е потребен програм-домаќин, туку самостојно може да се реплицираат и да „шетаат“ низ Интернет. Целта им е собирање или испраќање податоци, како и оптоварување на мрежните ресурси. Повеќето нови црви самостојно се закачуваат на e-mail пораките и на тој начин се шират.

Тројанците (Trojan horse programs) се деструктивни програми кои најчесто се маскираат како безопасни апликации што се нудат бесплатно на Интернет. Слично како и легендата по која го добиле името, овие програми се претставуваат како атрактивни (игри, корисни алатки и сл.) и корисниците сами ги преземаат од Интернет мислејќи дека доаѓаат од сигурен извор. Целата им е да направат „отворен пат“ до вашиот компјутер и преку него да трансферираат различни информации. Понекогаш тоа се лозинките што се снимени на заразениот компјутер или пак други лични информации за корисниците на заразениот компјутер. Овие информации се трансферираат до сервери што се специјално направени од „креаторите“ на Тројанците и преку нив може да ја преземат целосна контрола врз компјутерите-жртви.

Овој вид на деструктивен софтвер најчесто се пренесува преку додатоците на електронските пораки, но може да се пренесе и преку Yahoo или Windows Messenger како и Skype. Затоа треба многу внимателно да се користат овие широкораспространети програми и да се внимава многу на содржината на електронските пораки. *Многу корисен совет е да не се отвораат пораките од непознати испраќачи*.

Логичките бомби се специјален деструктивен софтвер што „лежат“ скриени сè додека не се случи некоја предвидена активност во компјутерот, како на пример да се прими некоја специфична порака или да се достигне даден датум во годината. Значи, најчесто тие го проверуваат системскиот датум и реагираат во зависност од тоа зашто се програмирани. Логичките бомби како заштита се вградени во речиси сите видови на

trial софтвери. Всушност станува збор за посебен вид на логички бомби што реагираат *ако не се направи нешто*. Имено, trial верзиите на програмите по истекот на пробниот период го оневозможуваат користењето на софтверот ако истиот не се плати. Притоа, може да се случи дури и програмот ненамерно да избрише некои информации со што ќе го оневозможи користењето на компјутерскиот систем во целина.

Spyware е деструктивен софтвер што се инсталира на компјутерот тајно најчесто кога се инсталираат shareware (пробни) програми или се посетуваат некои веб-страници. Цел им е да собираат информации за интернет активностите на корисникот на комјутерот-домаќин. Потоа, овие информации се препраќаат до оној што го креирал spyware-от пришто може да дојде до значително оптоварување на интернет конекцијата како и процентот на искористеност на процесорот. Многу често се смета дека spyware-от ја нарушува приватноста, но од друга страна пак комерцијалните компании имаат огромна корист. Затоа, се препорачува корисникот да има поголема контрола врз „колачињата“ (cookies) кои се инсталираат на компјутерот кога се посетуваат некои веб-страници.

Adware се рекламни програми кои се многу слични на spyware програмите. Тие предизвикуваат прикажување на рекламни банери и pop-up прозорчиња. Понекогаш се инсталираат заедно со бесплатни или shareware програми. Може да се инсталираат и при сурфање на Интернет. Најчесто, тешко се отстрануваат откако ќе се „сместат“ на компјутерот-домаќин. Заради тоа треба да се внимава што се одговара кога се поставуваат прашања при посета на некои веб-страници или при инсталирање на програми и игри.

Spam е непосакуван email кој многу често се дистрибуира до email корисниците. Во најголем број случаи spam-от е со комерцијални карактеристики и е наменет за продажба и реклама на разни производи, но понекогаш во прашање е криминален spam кој ги убедува „наивните“ email корисници да ја напишат својата банковна сметка или да извршат електронско плаќање на лажни комерцијални веб-страници. Имајќи го предвид начинот на кој функционира spam-от, целосна заштита од него е доста тешко да се направи. Затоа треба да се внимава на содржината на примените email пораки.

Како да се заштитиме

Од погоре кажаното може да се заклучи дека голем број и разновидни опасности ги „демнат“ интернет корисниците. Најчесто заразувањето на компјутерот е заради несовесноста на корисниците, но понекогаш едноставно заразувањето ќе се случи колку и да се внимава. Од друга страна, секојдневно се пишуваат нови штетни програми, па затоа логично се поставува прашање како да се заштитиме кога сме на Интернет?

Слика 9.1. Како да се заштитиме кога сме на Интернет?

Како прво треба редовно да се прави **update на оперативниот систем** преку обновување со последните надградби од официјалната веб-страница на производителот. Потоа, многу важно е да се има **антивирусна заштита**, при што треба да се има предвид кои се побарувањата на антивирусната програма во смисла колкава работна меморија побарува и колкава е оптовареноста на процесорот додека се резидентни. Иако постојат голем број бесплатни антивирусни програми, мал е бројот на оние кои не го оптоваруваат системот, односно не ја намалуваат неговата брзина. Avast и AVG се примери на антивирусни програми кои го задоволуваат ова барање. Меѓу најпопуларните антивирусни програми се вбројуваат McAfee Virus Scan и Norton AntiVirus, но за разлика од претходно спомнатите антивирусни програми, нивното користење не е бесплатно.

Сепак, не постои антивирус кој може да ги открие сите вируси и тие постојано мора да ја надополнуваат својата база на познати вируси како би можеле да ги најдат најновите вируси. Денес поголем дел од антивирусните програми автоматски ги преземаат програмските дополнувања од Интернет (**updates**). Многу антивирусни програми може да се обноват преку веб-страницата на нивниот производител.

За намалување на ризикот од заразување на компјутерот со злонамерен софтвер се препорачува:

- софтверот да се набавува по легален пат,
- да се избегнува размена на датотеки со непознати корисници,
- антивирусните програми редовно да се надополнуваат,
- да не се отвора електронска пошта од непознати корисници,
- при секоја размена на датотеки да се провери дали истата е заразена.

http://www.toptenreviews.com/software/security/best-antivirus-software/