Злонамерен софтвер и заштита од него

1. Вируси

Вируси се злонамерни програми кои ги користат секоја заразена програма или диск за понатаму да се шират со правење свои копии. Тоа се остварува така што **вирусот се прикачува за некоја програма (извршна датотека најчесто од тип .exe или .com)** и се извршува секој пат кога се извршува и програмата. Тие обично **се сокриваат во оперативниот систем или во апликативните програми на корисникот.**

Некои вируси не работат ништо освен што **се репродуцираат**, некои прикажуваат **пораки** на екранот, додека некои можат да **избришат податоци.**

Вирусите обично се направени **за одреден оперативен систем и ги напаѓаат дисковите содржат макро наредби** (вментнати мали програми за автоматизација на задачи), најчесто Microsoft Office документи. **Макро вирусите можат да се шират преку email прилози (atach). Тие вируси се нарекуваат email вируси.**

2. Црви (worms)

Слично како и вирусот, црв (**worm**) е програма или серија од програми кои **ги користат компјутерите домаќини за понатаму да се репродуцираат.** Но за разлика од вирусите, **црвите се самостојни програми и не им е потребна програма за која ќе се прилепат.** Црвите се размножуваат со огромна **брзина најчесто како додаток на email пораки**. Тие имаат способност понатаму да **се препратат на речиси сите адреси кои се запишани во адресарот на е-поштата.**

3. Тројански коњи

Тројански коњи (Trojan horse programs) се навидум корисни програми, но тие ја загрозуваат безбедноста и нанесуваат голема штета на компјутерот. Слично со легендата според која и го добиле името, овие програми се **претставени како атрактивни програми (игри, корисни алатки и сл.) и корисниците сами ги преземаат од Интернет мислејќи дека доаѓаат од сигурен извор.** Кога таква програма ќе се покрене, таа може да избрише датотеки, да измени или да украде податоци или да предизвика друг вид штета. Тројанските коњи **можат да се најдат во бесплатен софтвер кој се презема од Интернет.** Тие ретко се размножуваат но можат да нанесат големи штети и да предизвикаат големи проблеми во компјутерските системи.

Логичка бомба е вид тројански коњ, тоа е програма која се активира како реакција на некое дејство, на **пример ако се внесе специјална шифра, ако се логира одреден корисник или ако се извршат одредени наредби**. Ако програмата се активира во одредено време тогаш се нарекува **темпирана бомба.**

4. Спам пораки

Спам пораките се непосакувани, комерцијални електронски пораки, кои се сместуваат во електронските поштенски сандачиња на корисниците. Овие пораки често се придружени со прикачени документи кои доколку бидат отворени, можат да го заразат компјутерот со вирус. Некои спам пораки ги мамат примачите да ги откријат **своите лозинки и други вредни информации што би можело да ја наруши безбедноста на податоците и на работата**.

5. Adware и Spyware

Adware е софтвер кој се појавува на екранот на корисникот во вид на **светлечка рекламна** порака во текот на извршувањето на друга програма. Овој софтвер редовно го **забавува работењето** на системот.

Spyware е софтвер кој без дозвола надгледува работа на корисникот и испраќа информации за неговите online активности со цел стекнување на корист за трето лице. Овој софтвер, за разлика

од вирусите и црвите, **обично не се размножува, туку е дизајниран да ги искористува заразените компјутери за комерцијална добивка**. Типично применувани тактики се**: активирање на небарани pop-up реклами; крадење на личните податоци (на пр. броеви на кредитните картичкии или лозинки), набљудување на активности и навики на корисниците на Интернет во рекламни цели и сл.**

6. Заштита од злонамерен софтвер

Опасноста од злонамерниот софтвер веќе секојдневно се зголемува и со самото ширење на Интернетот. Секојдневно се пишуваат стотици нови штетни програми затоа е од голема важност компјутерот соодветно да се заштити од секојдневните закани

- Антивирусни програми

Најдобриот начин да се ослободи од малициозните програми и од хакерите е инсталирање на антивирусна програма. Антивирусни програми (AV softver) се проектирани да бараат вируси, да го известат корисникот кога ќе најдат вирус и истиот да го отстранат од заразениот диск, документ или програма.

Сите модерни антивирусни програми имаат неколку компоненти:

- **дел за проверка** на датотеките (scan)
- **дел за чистење** на заразените датотеки (clean) и
- **дел што секогаш е активен и ги надгледува влезните и излезните операции на компјутерот со цел да спречи евентуално навлегување на вируси** (monitor).

Делот за проверка (**скенирање**) ја проверува содржината на дискот и ги бара вирусите. Доколку се најде вирус автоматски се **покренува делот за чистење**. Чистењето се врши така што во заразената датотека се **брише** кодот кој представува вирус. Некогаш единственото решение е да се избрише цела датотека, што е и најдоброто решение и треба да се применува секогаш кога тоа е можно.

Делот за надгледување автоматски се стартува со вклучување на компјутерот.

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 антивирусни програми кои го задоволуваат ова барање.

Антивирусната програма Avast може да се преземе од веб страницата: www.avast.com.

Антивирусната програма AVG може да се преземе од веб страницата: www.grisoft.com.

Меѓу најпопуларните антивирусни програми се вбројуваат и **McAfee Virus Scan и Norton AntiViru**s, 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 поголемиот дел на антивирусни програми **автоматски ги преземаат програмските дополнувања од Интернетот (update).**

За намалување на ризик од заразување на компјутер со злонамерен софтвер се препорачува:

- софтвер да се набавува по легален пат,
- да се одбегнува 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 да ли истата е заразена.

7. Огнен ѕид

Антивирусите не се совршени, тие ги откриваат само оние вируси кои им се познати и се наоѓаат во нивната база, така што нови вируси, **особено тројански коњи, можат да поминат, а антивирусот да не ги открие**. Најдобрата заштита од тројанските коњи е **огнениот ѕид (firewall).**

Тоа е програма или хардверски уред кој ги надгледува сите податоци што компјутерот или локалната мрежа ги праќа или ги прима преку Интернет и нема да им дозволи на сомнителните програми да поминат. За исправно работење на огнениот ѕид, потребно **е прецизно да се одреди** низа од правила кои одредуваат што претставува дозволен сообраќај, а што забранет сообраќај. Денес многу антивирусни програми даваат и **firewall заштита.**