Hozzászólás vírusügyben

Több alkalommal írtak lapjukban és a *Mikrovilágban* is vírusokról szóló cikkeket. Ezek többnyire külföldi példákra hivatkoztak.

A vírus azonban hazánkat is elérte. Jó nevű felsőoktatási intézményünk több gépe is elfertőződött már. Még belegondolni is rossz, mi történik, ha minden felhasználó továbbadja barátainak, környezetének a veszélyes kórt. Most a vírusok egyik legkellemetlenebb fajtájáról lesz szó. Terjedése igen gyors, és mivel beleír a FAT táblába, teljes adatvesztést okozhat. További kísérőjelenség még, hogy a képernyőkarakterek időnként „lezuhannak" az alsó sorba. Ez azonban csak XT gépen fordul elő. E rövid ismertetővel segítséget szeretnék nyújtani a számítógépeseknek, hogy mi a teendő fertőzésgyanús esetben.

A vírus jelenléte felismerhető a PC-Tools 4.xx-es verziójával. A program F(ind) funkcióját kell meghívni, és a következő hexa-sorozatot keresni: 01 FA 8B EC E8 00 00 5B 81 EB. Először a winchestert, majd utána minden egyes hajlékonylemezünket végig kell vizsgálni. Ha találtunk ilyen karaktersorozatot, az egyértelműen jelzi, hogy fertőzött a lemezünk. Az érintett program nevét a PC-Tools kiírja. Könnyen észrevehetjük a vírus jelenlétét úgy is, hogy írásvédett lemezt teszünk a meghajtóba, és katalógust kérünk. Ekkor az „Error on drive A, Attempt to write on write protected disk" hibaüzenetet kapjuk.

A vírus a DOS-utasításokkal is terjed, tehát ha egy gépen „csak" a winchester vírusos, hajlékonylemezünkre egy sima **dir a:** parancs is életveszélyes lehet. A rendszerállományok hosszát szintén megnézhetjük: a DOS 3.3-as COMMAND.COM eredeti hossza 25 307 bájt. Indításakor 1701 bájttal lesz hosszabb az eredeti program. A vírus az .EXE és a .COM állományokat támadhatja meg. Egy programhoz többször is hozzámásolódhat.

Ha már a gépünkben van, akkor csak a merevlemez újraformázása segít, abból is a kemény, vagyis fizikai formázás. Erre azért van szükség, mert van a vírusnak olyan formája, amely több DOS-formázást is elvisel a winchesteren. Megfelelő erre a célra például a Disk Manager vagy a diagnosztikai lemez. Ezt vírusmentes gépen másoljuk hajlékonylemezre, és onnan indítsuk el. A rendszert és a használatban levő programjainkat utána kizárólag biztos forrásból másoljuk vissza.

Ha „tiszták" vagyunk, elég arra vigyázni, hogy a jövőben új programokat csak a fent leírt ellenőrzés után másoljuk be winchesterünkre. A vizsgálat előtt még katalógust sem szabad kérni! További védekezésként, különösen ha többen is dolgoznak egy gépen, hasznos lehet egy rövid programot írni a COMMAND.COM hosszának figyelésére, és ezt az AUTOEXEC.BAT-ba beleírni.

Csizmazia D. István