**7. tétel**

**Információtechnológiai alapok - Számítógépes architektúrák (1.1.1)**

Töltsön le az Internetről egy ingyenes, vagy egy próbaverziós víruskereső programot, vagy telepítse fel a rendelkezésére bocsátott víruskereső alkalmazást! (Vírusdefiníciós adatbázis frissítése) Végezzen a merevlemez egy partícióján víruskeresést! Amíg a víruskeresés folyamatban van, jellemezze a különböző számítógépes kártevő alkalmazásokat! (vírus, trójai, féreg, spyware, spam stb.)

***Szempontok a tartalom rész értékeléséhez***

o Víruskereső alkalmazás kiválasztása, telepítése, frissítése

o Kártevő alkalmazások jellemzése

o Védekezés ellenük

**Vírusok**

A **számítógépes vírus** olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet. Hatása ellen védekezni megfelelő vírusirtó szoftverrel többnyire lehetséges.

A vírusok manapság jellemzően pendrive, vagy e-mail segítségével terjednek az internetes böngészés mellett, valamint a megbízhatatlan oldalakról történő letöltések által.

A számítógépes vírusok működése hasonlít az élővilágban megfigyelhető vírus viselkedéséhez, mely az élő sejtekbe hatol be, hogy önmaga másolatait előállíthassa.

Ha egy számítógépes vírus kerül egy másik programba, akkor azt *fertőződés*nek nevezzük.

**A vírusok jellemzői:**

A gazdaprogramok megfertőzése és az önsokszorosító viselkedés valamennyi vírusra jellemző. Ezenkívül gyakran rendelkeznek a következő tulajdonságokkal:

* nagyon kisméretűek;
* futtatható állományokat képesek megfertőzni;
* általában ártó szándékkal készítették őket;
* gyakran akár válogatva, időzítve tönkretesznek más fájlokat;
* rejtetten működnek, esetleg akkor fedik fel magukat, ha feladatukat elvégezték;
* egyre fejlettebb intelligenciával rendelkeznek, például változtathatják saját kódjukat és aktivitásukat.

**Bootvírusok**

A boot vírusok az elsőként megjelenő vírusok közé tartoznak. Leggyakrabban akkor terjednek, ha fertőzött lemezzel indítjuk el a rendszert. Ebben az esetben a vírus a merevlemez boot szektorába ágyazódik be, így még az operációs rendszer betöltése előtt aktiválódik. Ennek hatására a fertőzött merevlemez az összes meghajtóba helyezett lemezt megfertőzi. A boot vírusok napjainkban a kevésbé elterjedt vírusfajták közé tartoznak.

**Alkalmazásvírusok**

Az alkalmazás- vagy más néven programvírusok a futtatható kódot tartalmazó (.COM, .EXE kiterjesztésű) állományokat fertőzik meg. A megfertőzött állományokba beírják a saját kódjukat. Két fajtáját különböztetjük meg: hozzáfűződő (append) és felülíró (replace) vírusokat. A hozzáfűződő vírusok az alkalmazások végéhez fűződnek, elhelyeznek azonban a program elején egy kódot, hogy az alkalmazás indulásakor előbb ők töltődjenek be, a program csak később. A felülíró vírusok az alkalmazások elejét írják felül saját kódjukkal, így a fertőzött állomány adatot veszít, és az eredeti állapot nem állítható helyre. Amennyiben egy programvírussal fertőzött fájlt elindítunk, a vírus betöltődik a memóriába és megfertőzi az összes többi elindított programot.

**Makrovírusok**

Elsősorban olyan dokumentumszerkesztő programokat támadnak meg a makrovírusok, melyek elég fejlettek, hogy bizonyos lépéssorozatokat képesek legyenek makrókkal automatizálni. Általában Word és Excel által készített dokumentumokat (.DOC, .XLS) fertőznek meg. Terjedésükhöz elegendő egy fertőzött állomány megnyitása, és a vírus már be is töltődik a memóriába, mely a későbbiekben megnyitott dokumentumokat megfertőzi. A fertőzést általában már csak akkor vesszük észre, amikor már késő.  
A makrovírusok csoportjába tartoznak a levelező vírusok is, melyek elsősorban e-mail útján terjednek. A csatolt fertőzött fájlok megnyitásakor aktivizálják magukat és általában a levelezési listában szereplő partnereknek írnak levelet, melyhez saját maguk másolatát is hozzáfűzik. Ha a levelezési címlistában nagyon sok partner van, akkor olyan mennyiségű levéláradat indulhat, amely megbénítja egy nagyvállalat levelezőrendszerét is.

**Számítógépes férgek**

Egy **számítógépes féreg** *(worm)* egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. A férgek gyakran a számítógép-hálózatokat használják fel terjedésükhöz.

Az első széles körben is ismertté vált féreg a Morris-féreg volt, melyet a Cornell Egyetem egyik diákja, Robert Tappan Morris, Jr. készített el. 1988. november 2-án került ki a szabadba és a korabeli internetre kapcsolt számítógépek közül számosat megfertőzött. Terjedéséhez a BSD Unix-ban található programhibákat használta fel. Morrist az amerikai bíróság a három év felfüggesztett börtönbüntetésre, közmunkára és 10 000 dolláros pénzbírságra ítélte.

Az önsokszorosításon kívül a féreg sokféle dologra beprogramozható, például a fájlok törlésére a gazdarendszeren, vagy önmaga elküldésére e-mailben. Az újabban megfigyelt férgek több végrehajtható állományt is visznek magukkal. Még valódi ártó szándékú kód nélkül is súlyos fennakadásokat okozhatnak, csupán azzal, hogy sokszorozódásuk kiugróan magas hálózati forgalmat generálhat. Például a Mydoom féreg terjedése csúcsán világszerte észrevehetően lelassította az internetet.

**Kémprogramok**

**Kémszoftvernek**, **kémprogramnak** (angolul spyware, ejtsd: szpájver) nevezzük az olyan, főleg az interneten terjedő számítógépes programok összességét, amelyek célja, hogy a felhasználó tudomása nélkül megszerezzék a megfertőzött számítógép felhasználójának személyazonosító, banki vagy más személyes adatait.

A megszerzett információkat általában bűncselekmények elkövetésére használják fel, mások nevében kötött szerződések és más kötelezettségek elvállalására, hamis személyazonosító okmányok készítésére, banki folyószámlák megcsapolására, szolgáltatások vagy üzleti kapcsolatok felmondására.

Enyhébb esetben böngészési szokásaink, érdeklődésünk, ízlésünk megfigyelése a cél, hogy az azoknak megfelelő ajánlatokkal keressenek meg bennünket (lásd még spam).

Feltelepülése általában észrevétlenül történik, a felhasználó figyelmetlenségének és a számítógép böngészőprogramja biztonsági hiányosságainak kiaknázásával. Léteznek magukat álcázó - trójaiakra hasonló - programok is, amik a felhasználó közreműködésével települnek egy rosszindulatú honlapról.

A kémprogramokat a számítógépes kártevők (angolul *malware* - malver) kategóriájába sorolhatjuk. Az ellenük való védekezés az összetett víruskereső programok, intelligens tűzfalprogramok, illetve spyware-ek ellen kifejlesztett specifikus programok segítségével történik. A megelőzésben nem elhanyagolható a felhasználó ébersége sem.

Általában a fertőzött rendszer egyrészt bizonyos helyzetekben nem úgy működik, ahogy kellene, másrészt a gép teljesítménye is észrevehetően csökken. Egy spyware fertőzés lefoglalhatja a CPU-t, a merevlemezt, és a hálózatot is. Gyakori fagyások, rendszerösszeomlások szintén jellemezhetnek egy komolyabban fertőzött rendszert. Ilyen helyzetekben gyakran csak egy teljes, rendszerszintű újratelepítés segíthet. Bizonyos típusú kémprogramok képesek kikapcsolni a tűzfalat és a vírusirtó programot is, ami több hasonló kártékony szoftver beáramlását eredményezheti. Vannak olyan kémprogramok is, amelyek kikapcsolják a rendszeren szintén megbújó konkurens kódokat, nehogy a felhasználó az egyre több gyanús jel hatására takarításba kezdjen.

**Trójai programok**

Számítógépes értelemben a **trójai faló** (röviden *trójai*) egy olyan rosszindulatú program, ami mást tesz a háttérben, mint amit a felhasználónak mutat. Az elnevezés a görög mitológiában szereplő trójai falóból származik, utalva Odüsszeusz cselvetésére, hogy a görögök megnyerjék a trójai háborút. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az ún. hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a célszámítógéphez. A vírusokkal ellentétben általában nem többszörözi önmagát, terjedése főként egyedi támadásoknak és az emberi hiszékenységnek köszönhető.

Az egyszerűbb trójai programok csak kívülről tűnnek hasznos programnak, míg fejlettebb változataik a kémkedés mellett valóban képesek az ígért funkciók elvégzésére is – így csökkentve a lebukás veszélyét.

Trójaival való megfertőződésnek forrása lehet egy e-mail üzenet csatolmánya vagy azonnali üzenetküldő program, de megkaphatjuk CD-n vagy egyéb adattárolón is. A leggyakoribb fertőzési módszert azonban a letöltések és a veszélyes honlapok jelentik.

Trójai program célja lehet…

* Rombolás
* Eszköz vagy identitás kihasználása
* Pénzlopás, váltságdíj
* Adatlopás
* Kémkedés, megfigyelés, tevékenységkövetés

**Hoax, magyarul lánclevél**

Ez nem program. A lánclevél egy hasznot nem hozó, sőt sokszor bosszantó e-mail fajta. Ez az a levél, ami arra kéri olvasóját, hogy minél több példányban küldje tovább. Ennek érdekében általában az érzelmekre próbál hatni, (Ha továbbküldöd a levelet legalább 1000 ismerősödnek, meggyógyulnak az afrikai beteg gyerekek) vagy áltudományos adatokra (új vírus jelent meg, amit csak a levél továbbküldésével lehet kiirtani) hivatkozik. Bár káros tevékenysége nincs, az elolvasásával és továbbküldésével töltött időt más, fontosabb tevékenységtől vesszük el.

A Sophos antivírus kutatói megvizsgálták az e-mailen terjedő hoaxokat, hogy mik a legnépszerűbb lánclevelek közös tulajdonságai:

• Sok nagybetűs szöveget tartalmaznak.   
• Felszólítanak, hogy minél több ismerősünknek, mielőbb küldjük tovább.   
• Ismert nagy cégre hivatkoznak, mely szerint ők is megerősítették a hírt.   
• Többször is elhangzik, hogy mennyire extrém veszélyes kártevőről van szó.   
• Áltudományos nyelvezettel próbálja meggyőzni a kevésbé hozzáértőket.   
• Gyakori a ködösítés, például tegnap (mihez képest tegnap, pl már egy hónapja is bolyonghat az álhír így a neten)

**Spam**

Kéretlen reklámlevél. Legtöbbször teljesen felesleges, a fogadó által nem kért, mégis nagy számban elküldött reklám a spam. Mivel a spameket milliós nagyságrendben küldik, ezért jelentősen terheli az internetet, foglalja a fontos információk elől xa sávszélességet.

A spamek egy része tudatosan megtévesztő, a fogadó kihasználására törekszik (olcsó, nagy nyereséget ígérő befektetésre csalogató, piramisjátékra csalogató, banki azonosítókat, személyes adatokat különféle indokokkal megkérő levelekkel).

Nincsen egységes álláspont arra vonatkozóan, hogy mit kell spamnek tekinteni. A platformfüggetlenség miatt szigorúan technikai tipizálás nem lehetséges. A spam kéretlen elektronikus reklámüzenet, mely terjedhet e-mailben, SMS-ben, de gyakran használják a kifejezést a papírformában terjesztett szórólapokra is.

Az általános álláspont szerint spam az az üzenet, ami:

* a címzett által nem kívánatos,
* tartalma nem a címzett személyére szóló,
* nagy tömegben kiküldött (vagy másképp fogalmazva a feladó nem csak a címzettnek küldi el),
* nagyon gyakran a feladó valódi személyét elrejtő, meghamisító formában érkezik.

Szintén kapcsolódó fogalom a kártevőket (vírus, féreg, trójai) terjesztő e-mail. A kárt okozó program lehet HTML formátumú, színes, grafikákat tartalmazó levél kódjában, lehet a csatolt mellékletben (különösen az EXE, PPS, DOC, FLV, XML, MSI, MHT, MAFF kiterjesztésű fájlokban), vagy annak a honlapnak a nem látható szövegében, amelynek a levélben a címét (linkjét) adják meg, és rákattintva gyakorlatilag a gépünkre töltjük a honlap tartalmán kívül a kártevőt is tartalmazó kódszöveget. Igen könnyen rejtőzhet kártevő az ismeretlen forrástól elindult, sorozatosan továbbküldött „jópofa” mellékletekben. Az ártalmas e-mailek elleni védekezés első számú fegyvere az ismeretlen tartalmakkal szembeni bizalmatlanság.

**Hogyan védekezzünk ellenük?**

A már feltérképezett Trójai vírusok és egyéb rosszindulatú programok ellen számos (akár ingyenes) programmal, vírusirtóval védekezhetünk.

A **vírusirtó** vagy **Antivirus program** a számítástechnikában egy szoftveres vagy hardveres architektúra, amelynek célja annak biztosítása, hogy a hálózatba vagy egy adott számítógépbe ne juthasson be olyan állomány, mely károkozást, illetéktelen adatgyűjtést vagy bármely, a felhasználó által nem engedélyezett műveletet hajt végre.

Fontos a program és a vírusdefiníciós adatbázis rendszeres (automatikus) frissítése, valamint - ha a program rendelkezik vele - az aktív védelmi funkciók bekapcsolása, illetve a tűzfal használata. Ezen programok leggyakoribb forrása az internet, azon belül is kéretlen emailek (csatolmánya, hivatkozása) és egyes kártékony weboldalak, amelyek rendszerint valamilyen (pl. pornográf) áltartalmat kínálnak a látogatóknak. A megelőzés érdekében javasolt az ilyen helyek kerülése is.

A vírusirtó szoftverek két alapelven működnek. Az első az úgynevezett reaktív védelem, ami az úgynevezett vírusdefiníciós adatbázison alapszik. Ebben az esetben a vírusirtó szoftver egy adatbázisból azonosítja a kártevőket. Az adatbázist a vírusirtó szoftver gyártója rendszeresen frissíti, a frissítéseket a legtöbb vírusirtó szoftver automatikusan letölti az internetről.

A második – és napjainkban egyre fontosabb – védelmi módszer az úgynevezett heurisztikus vírusvédelem. Ebben az esetben a vírusirtó a beépített analizáló algoritmusok (mesterséges intelligencia) segítségével azonosítja a vírusokat. A módszer azért nagyon fontos, mert sokszor több nap telik el egy új vírus megjelenésétől addig, amíg a vírusirtó program gyártója az ellenszert elkészíti és beépíti a vírusdefiníciós adatbázisba. A reaktív vírusirtó szoftvernek ilyenkor frissítenie kell magát az internetről, és csak ezután nyújt védelmet az új vírusok ellen.

A heurisztikus módszereket is alkalmazó modern vírusirtók viszont addig is védelmet nyújtanak a legtöbb kártevő ellen, amíg az ellenszer elkészül.

Ezek a modern vírusirtók kombinálják tehát a hagyományos (vírusdefiníciós adatbázison alapuló) védelmet a modern heurisztikus védelemmel, és így nagyobb biztonságot adnak a felhasználóknak.

**Ingyenes vírusírtók:**

* Avast
* AVG
* Avira
* Bitedefender
* Kaspersky
* ZoneAlarm
* FSecure
* Adaware
* NOD 32
* Comodo Free Antivirus
* Panda Antivirus Titanium

**Rosszindulatú programok ellen:**

Bár alapvetően a vírusirtók is képesek felismerni a spyware (kémprogram), malware (rosszindulatú program), ransomware-eket (zsaroló program) és egyebeket de vannak speciálisabb, kifejezetten erre a célra készült védelmi megoldások, amelyek ezek ellen védenek. Illetve képesek a böngészők beállításainak megváltoztatását eszközölő rosszindulatú programok és a reklámprogramok felismerésére is.

Ráadásul ezek általában gond nélkül együttműködnek a vírusirtókkal is, így megduplázható a védelem. Ilyenek a következők:

* Malwarebytes Anti-Malware
* SUPERAntiSpyware Free
* Spybot – Search & Destroy

**Víruskeresés több tíz vírusirtóval egyszerre**

Előfordul, hogy olyan programot kellene futtatnod, vagy fájl megnyitnod, amiben nem bízol meg. Ilyenkor jönnek jól az olyan weboldalak és programok, amelyek lehetőséget adnak számtalan vírusirtóval történő ellenőrzésre.

Ilyenek például a Winja vagy a virustotal.com

**Tűzfalak**

A tűzfalak számos feladatot végeznek, a használatukkal sok egyéb mellett szabályozhatjuk az egyes programok internethez történő hozzáférését. Mindenképpen előnyös a használatuk, viszont ahhoz, hogy igazán hatékonyak legyenek szükséges némi picit mélyebb informatikai ismeret (az automatikus működési módban ez kevésbé igaz, akkor csak minimális felhasználói interakciót kíván).

Az ingyenes megoldások közül mindenképpen a Comodo Firewall ajánlott, ami a tűzfal funkción kívül rendszervédelmi szerepet is betölt. Szabályozhatjuk például, hogy mely programok hajthatnak végre módosításokat, megvédhetjük a böngészőket, stb. De mint a tűzfalhoz, ehhez is szükséges némi informatikai ismeret.