

## Az informatikai biztonság alapjai

# Tartalom

## 1 Kártékony programok

- Fejlett Perzisztens Fenyvegetés
- Terjedés módja: Fertőzött tartalom
- Terjedés módja: Sebezhetőség kiaknázása
- Terjedés módja: Pszichológiai támadás
- Büntető rutin: Rendszer károsítása
- Büntető rutin: Támadó ügynökök
- Büntető rutin: Információszerzés
- Büntető rutin: Lopakodás
- Biztonsági intézkedések

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

## VIII

- G**      **S**      **\**      **/**

---

- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

## Támadói eszközrendszer (Attack Toolkit)

- Régen: egy terjedési mód egy büntető rutinnal  
Most: terjedési módok és büntető rutinok széles skálája
- A fertőzés sebességének maximalizálása céljából többféle terjedési módot és büntető rutint is használnak. Többségük még **update mechanizmusokat** is támogatnak, mely lehetővé teszi aktiválásuk után, hogy megváltoztassák terjedési módjukat és büntető rutinukat. Akár egy *nem szakember* is képes telepíteni és használni.

- Személyes információk (banki információk) megszerzése a felhasználók számítógépeinek megfertőzésével.
- A legfelkapottabb aktív botnet-ek egyike. A **botnet** olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást.
- Többféle módon lopják el a felhasználó identitását, kontrollálják számítógépét.
- HTML kód-injektálás, minden egyes egérekattintásnál lementí a képenyőképet (virtuális billentyűzet ellen) stb.

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ 🔍 ↺



[illegible]

# Fejlett Perzisztens Fenyvegetés (Advanced Persistent Threat (APT))

- **Perzisztens:** A támadók egy **jól meghatározott** céllal tevékenykednek, és többnyire nem véletlenszerűen, találgatás útján próbálnak rájönni, hogy milyen sebezhetőségeket tudnak kihasználni, hanem már felkészülten, **alapos felderítőmunka** után lépnek akcióba. Ameddig el nem érik a céljukat (például meg nem találják az általuk keresett bizalmas adatokat), addig nem hagyják el a rendszert. Gondoskodnak arról, hogy a **hozzáférésük fenntartható** legyen.
- **Fenyegetés:** Ez esetben **célzott, irányított és komplex akciókról** beszélünk, amelyek komoly fenyegetést jelenthetnek az informatikai rendszerekre és az adatokra.

100

- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ↺ 🔍 ↻

# Fejlett Perzisztens Fenyvegetés - Technikák

- **pszichológiai támadás**
- **célzott adathalász e-mail** (spear-phishing e-mail): E-mailek keresztül egy meghatározott személyt, szervezetet vagy vállalatot céloz meg azzal, hogy megszerezze bizalmas adatait vagy kártékony programot installáljon számítógépére.
- **drive-by-downloads**: Támadás, mely egy fertőzött website-on levő kóddal **kiaknázza a böngésző sérülékenységét**, hogy megtámadja a felhasználó rendszerét böngészés közben.
- **nulladik napi támadás** (zero-day exploits): Valamely számítógépes alkalmazás olyan sebezhetőségét használja ki, ami még nem került publikálásra, a szoftver fejlesztője nem tud róla, vagy nem érhető még el azt foltozó biztonsági javítás. A „nulladik napi” támadás az első vagy „nulladik” napon történik, amikor a fejlesztő még nem juttatta el a biztonsági javítást a szoftver felhasználóihoz.

## APT példa: Stuxnet

- Stuxnet az első katonai féreg, mely 2010-ben bukott le egy iráni nukleáris erőmű számítógépén.
- A felfedezés óta bebizonyosodott, hogy a Stuxnet vírus az erőműre közvetlen fenyegetést nem jelentett, mert annak az urániumdúsító berendezések voltak a célpontjai. Közvetett értelemben azonban az a tény mindenképpen fenyegető, hogy egy vírus bejutott a létesítménybe.
- 2010. november 16-án Irán leállította az urándúsítóit, miután a centrifugák több mint 20%-a megsemmisült a Stuxnet tevékenysége nyomán.
- A férget úgy tervezték meg, hogy törölje magát 2012-ben.
- Négy nulladik napi támadást hajtott végre, Microsoft Windows operációs rendszerű gépeken jutott be és a Siemens Step7 mérnöki szoftvert kereste.

1. *Journal of Management Studies*, 1997, 34, 1, 1-14.

- Három modulja:
  - féreg, mely a támadás büntető rutinjait futtatja.
  - kapcsolat fájl, mely automatikusan futtatja a féreg másolatokat.
  - gyökércsomag, mely felelős a kártékony fájlok, processzek elrejtéséért megelőzve az esetleges lebukást.
- Stuxnet egy fertőzött USB pendrive segítségével jutott be.
- A féreg elterjedt a rendszerben.
- Stuxnet gyökércsomaggal módosította a kódot és nem várt parancsokat hajtott végre.

## APT példa 2.

- Információgyűjtés bizonyos alkalmazottakkal kapcsolatosan, begyűjtött információkkal a kezükben phishing emailt küldenek a felhasználónak (cél-releváns tartalmat, például a pénzügyi osztály számára néhány tanácsot a szabályzási kontrollokat illetően).
- A támadó két különböző adathalász emailt küldött két napos periódus alatt. A két email az alkalmazottak két kisebb csoportjának szólt. Az email tárgya: "2011 Recruitment Plan" (2011-es Toborzási Terv). Az email jól meg volt szerkesztve ahhoz, hogy az alkalmazottak egyike kiszedje a levélszemét mappából, és megnyissa a csatolt excel fájlt. A táblázat egy nulladik napi támadást tartalmazott, mely egy hátsó ajtót (a távoli támadó teljes kontrollt kap) telepített egy Adobe Flash sérülékenységet kihasználva (CVE-2011-0609). Megjegyzés: az Adobe azóta orvosolta a sérülékenységet.

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡





- **Fertőző** mechanizmus (infection vector): Mechanizmus, mellyel a vírus **terjed**, sokszorozódik.
- **Indíték**: Esemény vagy feltétel, mely meghatározza **mikor** aktiválódik a büntető rutin. Az ilyen a programokat **logikai bombának** is hívják.
- **Büntető rutin**: Kárt okozó tevékenységek. (pl. törlés)

- **Fertőző** mechanizmus (infection vector): Mechanizmus, melyel a vírus **terjed**, sokszorozódik.
- **Indíték**: Esemény vagy feltétel, mely meghatározza **mikor** aktiválódik a büntető rutin. Az ilyen a programokat **logikai bombának** is hívják.
- **Büntető rutin**: Kárt okozó tevékenységek. (pl. törlés)

- **Boot vírusok:** 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.
- **Alkalmazásvírusok:** A megfertőzött állományokba beírják a saját kódjukat. Két fajtáját különböztetjük meg: **hozzáfűződő** (append) és **felülíró** (replace) vírusokat. Amennyiben egy fertőzött fájlt elindítunk, a vírus betöltődik a memóriába és megfertőzi az összes többi elindított programot.
  - A hozzáfűződő vírusok az alkalmazások végéhez fűződnek, elhelyeznek azonban a program elején egy kódot, hogy az alkalmazás indulásakor előbb ők töltsődjenek be.
  - A felülíró vírusok az alkalmazások elejét írják felül saját kódjukkal, így a fertőzött állomány adatot veszít, az eredeti állapot nem állítható helyre.

## Vírusok célpont szerinti csoportosítása

- **Macrovírusok:** Elsősorban makrókat támogató dokumentumszerkesztő programokat támadnak meg (Word, Excel), általuk készített dokumentumokkal terjednek. Terjedésükhöz elegendő egy fertőzött állomány megnyitása, és a vírus már be is töltődik a memóriába, mely a későbbiekben megnyitott dokumentumokat megfertőzi. Ide sorolhatók a **levelező vírusok** is. 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.
- **Összetett vírus:** Többféle módon, többféle állományt képesek megfertőzni.

1. *Journal of the American Medical Association*, 1997; 278: 1039-1044.

100

- **Polimorf vírus:** Bizonyos fertőzési ciklusonként képesek megjelenési formájukat változtatni. Ezzel a módszerrel a bitminta alapú felismerést lehet nehezebbé vagy lehetetlenné tenni. (pl. titkosítás, más instrukciókat szűrnak be). Azon vírusrész, mely felelős a kulcs generálásért és a titkosításért/visszafejtésért **mutációs motornak** hívjuk. A mutációs motor is módosul minden használat után.
- **Metamorfózisra képes vírus:** Minden egyes alkalommal teljesen felülírják magukat. Megváltoztatják viselkedésüket és "kinézetüket" is.

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

---



- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ 🔍 ↺

# Férgek - Hálózati címek keresési stratégiák

- **Véletlen:** A fertőzött gazdagépek (hostok) véletlen IP címet használnak. Hatalmas Internet forgalmat eredményez, mely észrevehető, így lebukhat.
- **Hit-lista:** A támadó összegyűjti a lehetséges sebezhető gépek címének egy hosszú listáját, és el is kezdi a lista elején levő címeket felhasználni. Minden fertőzött gép kap egy darabot a listából. Rövid ideig történik a próbálgatás, nehéz észrevenni.
- **Topológiai:** A támadó a már fertőzött gép információit felhasználva talál további hostokat.
- **Helyi alhálózat:** Tűzfal mögötti host próbál megfertőzni további hostokat a helyi hálózatban. Az alhálózat címstruktúráját használja.

# Modern férgek

- **Multiplatform:** Többféle platformot is támadnak, főleg a népszerű UNIX variánsokat, illetve többféle népszerű dokumentumok makró és script kódjait.
- **Multi-kihasználás:** Többféle módú behatolási rendszer (Web szerverek, böngészők, e-mail, fájl megosztás, egyéb hálózati alkalmazások stb.)
- **Ultragyors terjedés:** Optimalizálják terjedésüket, hogy rövid idő alatt minél nagyobb valószínűséggel minél több sebezhető gépet próbáljanak.

# Modern férgek

- **Polimorf:** Vírusok polimorf technikáit használja.
- **Metamorf:** Megváltoztatja viselkedését és "kinézetét".
- **Szállítási eszközök:** Ideális többféle büntetési rutin terjesztésére, pl DDOS botok, gyökércsomagok, spam e-mail generátorok, és kémprogram.
- **Nulladik napi támadás:** Azért, hogy maximális meglepetést és terjedést érjen el, a fégnek olyan ismeretlen sebezhetőséget kell kiaknázni, melyet a többség csak végrehajtás után ismer meg.

# Mobiltelefon Férgék

- Első féreg: Cabir worm (2004), Lasco and CommWarrior (2005)
- **Bluetooth** vezeték nélküli hálózaton vagy MMS-en keresztül kommunikálnak.
- Célpontok az **okostelefonok** (applikációk intallálása), Android és iPhone rendszerek.
- **Használhatatlanná** teszik a telefont, **adatok törlése**, költséges **SMS-ek küldése**.
- Bár mobiltelefon férgek léteznek, de nagyobb mennyiségben fordulnak elő trójai alkalmazások, melyek magukat installálják.



© 2006 The Authors  
Journal compilation © 2006 Blackwell Publishing Ltd

- **Malvertising:** A támadó fizet, hogy hirdetések jelenjenek meg a célpont weboldalakon. A hirdetések kártékony programot tartalmaznak. A weboldalak látogatóit fertőzik meg.
- **E-mail kliensek bug-jainak kihasználása:** pl. Klez mass-mailing worm (2001) a Microsoft's Outlook és Outlook Express programokat támadta, hogy automatikusan végrehajtsódjon.
- **PDF-olvasó bug-jainak kihasználása:** PDF-olvasó (sokszor kiegészítő modulok révén, multimédiás tartalmak megjelenítése) kártékony programot installál, amikor PDF dokumentumot nézünk. Ezek a dokumentumok e-mail spammal terjednek, vagy célzott adathalász támadással.

## Kattintáseltérítéssel támadás (Clickjacking)I.

- A támadó célja összegyűjteni a fertőzött felhasználói klikkeket.
- pl.: "Akaratlan lájkolás": Funkciógombnak (jóváhagyás, eltávolítás, bezárás stb.) álcázott like gombok formájában a felhasználók üzenőfalára kikerülnek az üzenetek.
- Ráveszik a felhasználót, hogy tegyen bizonyos dolgokat, pl. kártékony tartalmat lájkolhatunk, és az így becsempészett rosszindulatú kódok villámgyorsan elterjednek az ismerőseink között, vagy egy weboldalt kell megnéznie stb., így installálnak kártékony programokat.
- Pl. Adobe Flash vagy JavaScript segítségével lehet nyomógombokat beszúrni.



◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ 🔍 ↺

# Pszichológiai támadás - Spam e-mail

- Ötlet: "**átverni**" és rávenni a felhasználókat, hogy saját rendszerüket veszélyeztessék vagy kiadjanak személyes információkat.
- A felhasználó megnéz vagy válaszol egy **SPAM e-mailre**, vagy megengedi, hogy felinstallálódjon vagy lefusson egy **trójai** program vagy **script kód**.
- A felhasználó **aktív részvétele** szükséges.
- **Spam e-mail**: Mai becslések szerint az e-mail forgalom **50% vagy annál több** spam e-mail.
- Ez a jelentős növekedés fellendítette a **anti-spam ipart**, mely igyekszik detektálni és kiszűrni a spam e-maileket.

# Spam e-mail

- Kis része a spam-eknek **legális mail szerverekről** küldődnek ki, nagy részük **botnet**-eken keresztül mennek, felhasználva a fertőzött (zombie) gépeket.
- A spamek nagy része csak **reklám**.
- Másrészük **valamilyen kártékony programot hordoz**:  
Csatolmány tartalmaz egy trójait vagy script kódot, melynek futtatásával megfertőzzük a rendszert.
- Spamek használhatók még **adathalászatra** is (spear phishing emails), tipikusan átirányítják a felhasználót egy a támadó által kontrollált weblapra, mely valamely valós szolgáltatás tükörzése.

# Trójai lovak

- A trójai ló egy olyan kártékony program, mely magukat **hasznos programnak** álcázzák de képesek a háttérben segíteni egyéb ártó szándékú programok bejutását, és működését a számítógépen.
- **Nem sokszorozódnak.**
- Mivel hasznos programnak mutatják magukat, ezért leggyakrabban a felhasználó tölti azt le fertőzött honlapokról a számítógépére. Emellett terjedhetnek e-mailben, vagy adathordozókon is.
- Többségük tartalmazza a **hátsó kapu** telepítését, ami a fertőzés után biztosítja a hozzáférést a célszámítógéphez.
- Büntető rutinok: valamely más kártékony program telepítése, kémprogramok, botnet.

# Trójai lovak - Modellek

Három modell:

- A program továbbra is folytatja eredeti funkcióját, de **rajta kívül** még valamilyen büntető rutint is futtat.
- A program továbbra is folytatja eredeti funkcióját, de **módosítja annak működését**, hogy végrehajtsa a büntető rutint (pl. login program gyűjti a jelszavakat)
- Teljes mértékben **lecseréli** az eredeti program funkcióját.

# Mobiltelefon trójaiak

- 2004-ben jelent meg elsőnek: Skuller
- Célpont: okostelefonok, Android és Apple iPhone. A trójaiak általában az **alkalmazás áruházakból** tölthetők le. (pl. Good Weather időjárás előrejelző alkalmazás Google Play áruházban(2017), már visszavonták, büntető rutin: banki adatok ellopása, képernyő lezárása, feloldása )
- Több olyan mobil trójai (Ztorg, Gorpo, Leech) is van, mely root jogosultságokat használ. Az ilyen trójaikkal megfertőzött eszközök általában hálózatba szervezik magukat egyfajta **reklám botnetet** alkotva, amelyet a hackerek különféle **reklámprogram** (adware-ek) telepítésére használnak. Röviddel azután, hogy rootolják az eszközt a trójaik letöltenek és telepítenek egy **hátsó ajtót**. Majd letölt és aktivál két modult, amely képes letölteni, telepíteni és elindítani alkalmazásokat.

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ 🔍 ↺

## Büntető rutinok

- Büntető rutin: tevékenységek, melyek végrehajtódnak a fertőzött rendszeren
- Vannak olyan kártékony programok, melyeknek nincs büntető rutinjuk, céljuk a terjedés.
- Általában van büntető rutinjuk.
- Kategóriák:
  - Rendszer károsítása: adat megsemmisítése, fizikai károkozás, logikai bomba
  - Támadó ügynökök: Botok, zombik
  - Információ lopás: billentyűzetfigyelők (keyloggers), adathalászat (phishing), kémprogramok (spyware)
  - Lopakodás: hátsóajtó (backdoor), gyökércsomag (rootkit)



◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ≡ ≡ ↺ 🔍 ↻

100

- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

100

- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻

## Ransomware fajtái II.

- **Böngészőlezáró** ransomware: Egy Javascript segítségével egyszerűen blokkolja a böngészőket, és figyelmeztető üzenetet jelenít meg. Többnyire illegális tevékenységeket sorol fel, és a börtönbüntetés elkerülése érdekében büntetés megfizetését kéri.



## Ransomware példák

## Petya - 2016. március végén jelent meg

- A támadó egy hitelesnek tűnő e-mailt küld, ami állásra való jelentkezésnek tűnik. Ebben útmutató is van a kapcsolódó önéletrajz letöltéséhez, egy Dropbox-fiókon keresztül.
- Az önéletrajz a ransomware, amely azonnal tönkreteszi a bootrekordot, és kikényszeríti az összeomlást. Az újrainduláskor egy üzenet jelenik meg, amely szerint hibajavításokra van szükség, a folyamat több órába telhet. Ekkor a teljes meghajtót titkosítja a kártevő. A következő rendszerbetöltés alkalmával már a szomorú üzenet várja a felhasználót: fizessen váltságdíjat a Tor böngészőn keresztül, vagy mindene oda van. A váltságdíj hét nap után duplázódik.
- Átvesszi az uralmat a rendszerbetöltési folyamat fölött, és a teljes gépet zárolja. Saját magukat nem terjesztik, a megtámadott rendszerben komoly problémákat okozhatnak.

**NE** fizesse ki a követelt váltságdíjat, mert ez nem segít.

- A büntető rutin **fizikai eszközöket károsít meg**.
- **Csernobil vírus** nemcsak az adatokat károsítja, de megpróbálja **újraírni a BIOS kódot**. A rendszer addig használhatatlan, míg a BIOS chip nincs újraprogramozva vagy kicserélve.
- **Stuxnet** féreg ipari működtető rendszert céloz meg. A féreg az eredeti rendszer kódját módosítja, mely a berendezés meghibásodását eredményezi.

# Logikai Bomba

- Logikai bombák, mint büntető rutinok egy adott feltétel teljesülésével vagy valamely esemény bekövetkeztével "robbannak" (hajtják végre rutinjukat).
- **Indíték:** Bizonyos fájlok megléte vagy hiánya, valamely dátum vagy a hét valamely napjának bekövetkezése, vagy egy szoftver verzió konfigurálása, vagy valamely speciális felhasználó belépése stb.
- "Robbanás": **adatok vagy teljes fájlok módosítása vagy törlése, rendszer leállása**, illetve más károk okozása.



◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

9.

- Pintér-Husztí Andrea Az informatikai biztonság alapjai

- |                     |                                   |
|---------------------|-----------------------------------|
| Pintér Huzsi Andrea | Az informatikai biztonság alapjai |
|---------------------|-----------------------------------|

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ▶ ↺ 🔍 ↻



Hitelesítő adatok (credential) ellopása, billentyűzetfigyelés, kémprogramok

- Billentyűzetfigyelők **összegyűjtik a billentyűlenyomásokat**, hogy a támadó érzékeny adatokat szerezzen be.
- Mivel az összes szöveget begyűjtik, szükséges egy "beépített" **szűrő**, mely csak a megadott kulcsszóhoz kapcsolódó adatokat továbbítja.
- Néhány bank alkalmazás átállt a **grafikus appletek** alkalmazására.
- Válaszul a támadók általánosabb **kémprogram** büntető rutint használnak: **böngésző előzmények figyelése, web oldalak éltérítése** a támadó által kontrolláltakra, és a böngésző és bizonyos web oldalak között kicserélt adatok dinamikus változtatása.
- Valamennyi személyes adat megszerzésére irányulnak.

1. *Journal of the American Medical Association*, 1997; 277: 1039-1043.


- A felhasználó belépési adatainak megszerzésére irányuló másik megoldás, egy a támadó által kontrollált web oldalra mutató link elhelyezése egy kéretlen e-mailben.
- Ez általában valamilyen **sürgős üzenetben** jelenik meg, mely a felhasználói fiók aktiválására kér.
- **Adathalászat**: pszichológiai támadással kihasználják a felhasználók bizalmát úgy, hogy valamely megbízható felet személyesítenek meg.



## Felderítés, kémkedés

- A támadó bizonyos típusú információt szeretne megtudni.
- Operation Aurora 2009-ben egy trójait használt, hogy hozzáférjen (esetlegesen módosítsa is) high tech és biztonsági cégek forráskódjaihoz.
- A Stuxnet féreg 2010-ben összegyűjtött számos hardver és szoftver konfigurációk részleteit, hogy meghatározza hogy tudná -e a célpontokat támadni.
- **Céltott adathalászattal** ipari kémkedéseket vagy más felderítéseket végeznek.

## Célzott adathalászat

- Komolyabb változata: **célzott adathalászat(spear-phishing attack)**. Leveleket küldenek, egy olyan cég/személy nevében, akiben a címzettek megbíznak.
- Talán 5-10 jól kiválasztott embernek küldik csak ki, a támadók tanulmányozzák a kiszemelt célpontokat, mint pl. azok LinkedIn vagy Facebook fiókjainak átolvasásával, vagy az általuk nyilvános blog-okon, fórumokon közzétett üzeneteik vizsgálatával.
- Egy nagyon testre szabott levelet készítenek, amely az érintett célpontok számára relevánsnak tűnhet. Így az egyének nagyobb valószínűséggel válnak a támadás áldozataivá.
- A támadó kifejezetten a felhasználót, vagy a céget akarja támadni, bizalmas információkhoz igyekeznek hozzáférni, mint pl. a cég üzleti titkai, az érzékeny technológiai tervek, vagy bizalmas kormányzati kommunikáció. Lehet hogy egy másik embert/céget akarnak elérni rajtunk keresztül: 

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

## Lopakodás: Hátsóajtó (Backdoor)

- **Lopakodó büntető rutinok:** A kártékony programok azon rutinjai, melyekkel **elrejtik jelenlétüket és hozzáférésüket** a fertőzött gépeken.
- Ez a rutin a rendszer integritását célozza.
- **Hátsóajtó:** A program egy titkos belépési pontja, mely lehetővé teszi, hogy a belépési pont ismerője a biztonságos hitelesítés nélkül kapjon hozzáférést.
- Programozók legálisan használták a hátsóajtókat program tesztelésre. A hátsóajtók veszélyessé válnak, ha a tisztességtelen programozók illetéktelen hozzáférésre használják.
- A védelmi intézkedések szoftverfejlesztésekre és szoftver updatekre irányulnak.

## Lopakodás: Gyökércsomag (Rootkit)

- A **gyökércsomagok** egy programcsomag, mely installálása után fedett hozzáférést biztosít, tart fent a **már fertőzött** géphez adminisztrátori (root) jogosultságokkal. **Hátsóajtó hozzáférést biztosítanak trójaiak számára** úgy, hogy fontos rendszer fájlokat módosítanak.
- Az operációs rendszer valamennyi funkciójához és szolgáltatásához hozzáférést ad.
- Adminisztrátori jogosultsággal, a támadónak teljes kontrollja van a rendszer felett, felrakhat, módosíthat programokat, fájlokat, processzeket monitorozhat, küldhet, fogadhat hálózati forgalmat és hátsóajtó hozzáférést kaphat.
- A gyökércsomag elrejti ezeket a mechanizmusokat.

# Gyökércsomag jellemzői

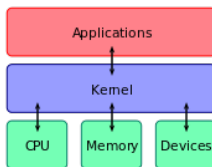
- **Perzisztens:** A gyökércsomag perzisztens helyen tárol kódot, pl. registry-ben és a kódot a felhasználó részvétele nélkül futtatja le.
- **Memória alapú:** Nincs perzisztens kód, tehát újraindítást nem éli túl. Mivel csak a memóriában van, nehezebb detektálni.

## Gyökércsomag jellemzői

- **Felhasználói (user) módú:** Felhasználói szinten működik az operációs rendszerben. Lehallgatja az API hívásokat és módosítja kapott választ. Pl. ha egy alkalmazás egy könyvtár listázását kéri, a lista, amit megkap nem tartalmaz olyan bejegyzéseket, melyek a rootkittal kapcsolatos fájlok beazonosítását segítik.
- **Kernel módú:** A gyökércsomag úgy rejti el jelenlétét, hogy módosítja a kernelt.

## Kernel módú rootkitek

- A rendszermag (kernel) az operációs rendszer alapja (magja), amely felelős a hardver erőforrásainak kezeléséért (beleértve a memóriát és a processzort is).
- A korai rootkitek felhasználói módúak voltak. A változtatásokat detektálni lehetett kernel kódokkal.
- A következő generációs rootkitek egy szinttel lejjebb kerültek, **kernel szintű változtatásokat** hajtottak végre.
- A felhasználói szintű programok a kernellel rendszerhívásokon keresztül teremt kapcsolatot. A kernel szintű rootkitek rejtőzködéséhez az elsődleges célpontok a rendszerhívások.





- 1 **Rendszerhívási tábla módosítása:** A támadó a tárolt rendszerhívások címeit **módosítja**, átirányítva a rendszerhívás mutatóját a legális rutinról a rootkit rutinjára.



**Figure 6.4 System Call Table Modification by Rootkit**



◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ 🔍 ↺ ↻

\_\_\_\_\_

- Valamennyi biztonsági intézkedést "**antivírus**" **mechanizmusnak** hívunk, mivel elsőnek tipikusan a vírusok írtására jöttek létre.
- Ideális megoldás: **megelőzés**. Elsőnek ne engedjük, hogy a kártékony program a rendszerünkbe bejusson. Ha bejutott, blokkoljuk, ne módosíthassa a rendszert.
- Férgek, vírusok, trójaiak terjedésének megelőzése:
  - **Sérülékenység csökkentése**: Összes javítócsomag (patch) alkalmazása, a felszínre került programhibák orvosolására.
  - **Fenyegetés csökkentése**: A rendszer adataihoz, fájljaihoz megfelelő hozzáférés-vezérlés beállítása.
- Pszichológiai támadás megakadályozható megfelelő felhasználói felvilágosítással és oktatással.

## Pszichológiai támadás

- A UK Payment Council nem rég jelentette be, hogy a 2010-es évben elkövetett online banki csalások 22%-kal csökkentek annak ellenére, hogy az adathalászattal kapcsolatos visszaélések 21%-kal növekedtek a vizsgált időszakban. A helyzet változott. A pénzügyi szektornak hét évébe telt egy új védelmi rendszer kifejlesztése a phishing vagy trójai típusú social engineering támadások ellen.

## Biztonsági intézkedések

- Külső adatmentés, szalagos mentés: offline, szalagos mentési rendszer esetén a lementett adatokat a szalagos technológiából fakadóan a zsaroló vírus nem képes titkosítani, TÁROLJUK a havi mentéseket fizikailag is biztonságos külső helyen.
- Folyamatos frissítések, többretegű vírusvédelem: többretegű védelemmel ellátott vírusírtó, frissítése, tűzfal
- Szabályozás kialakítása és betarttatása
- Oktatás, tudatosítás: Ismeretlen feladótól érkezett e-mailekben ne nyissuk meg a mellékletet, főleg ha ez tömörített állomány. Munkahelyünkön figyelmeztessük azon kollégáinkat a veszélyekre, akik főleg külső irányból kapják leveleik többségét (pl. pénzügyi vagy HR osztály).A felhasználóknak ismerniük kell a vírus működését és terjedését, valamint azokat a technikákat, amelyeket a kártékony kód alkalmaz.

## Biztonsági intézkedések: Technikai mechanizmusok

Ha a megelőzés nem sikeres:

- **Detektálás:** Ha a kártékony kód már megfertőzte a rendszert, határozzuk meg **a helyét**.
- **Azonosítás:** Ha detektáltuk, **azonosítsuk be a kártékony kódot**, mely megfertőzte a rendszerünket.
- **Eltávolítás:** Ahogy azonosítottuk, **távolítsuk el a kártékony kód nyomait** valamennyi fertőzött állományból, hogy ne terjedjen tovább.

Ha sikerült detektálni, de se azonosítani, se eltávolítani nem tudjuk, akkor **töltsünk be a tiszta backup verziót.**

- Első generációs: **egyszerű szkennerek**: a kártékony program valamennyi másolatában ugyanaz a struktúra és bitminta kell, hogy legyen. Másik típus a program állományok méretét tárolja és figyeli azok változását.
- Második generációs: **heurisztikus szkennerek**: A szkennerek a kártékony kódhoz kapcsolható programkód részleteket keresik. (pl. polimorf vírusok esetén a titkosítási részből próbálják kinyerni a kulcsot. Másik megoldás az adatintágritás vizsgálata. Egy **ellenőrzőösszeg** (hash érték, MAC) adható meg minden egyes programhoz. Ha a kártékony kód módosítja a programot az ellenőrzőösszeg változtatása nélkül, akkor a változás detektálható. A kulcs külön tárolandó.





## Antivírus szoftver III.

## Fejlett antivírus szoftverek: Viselkedés-blokkoló szoftver

- Viselkedés-blokkoló szoftver valós időben figyeli a kártékony programok működését és megpróbálja blokkolni mielőtt komoly károkat okoz.
- A következő eseményeket figyeli:
  - Fájlok módosítására, törlésére, megnyitására irányuló próbálkozások;
  - Merevlemez formatálása vagy más javíthatatlan művelet;
  - Indítási beállítások módosítása;
  - Futtatható tartalmak küldése e-mailen vagy messenger-en keresztül;
  - Hálózati kommunikáció kezdeményezése;
- A kártékony kód már el kezdi működését mielőtt a tevékenységét detektáljuk.

- • • • •