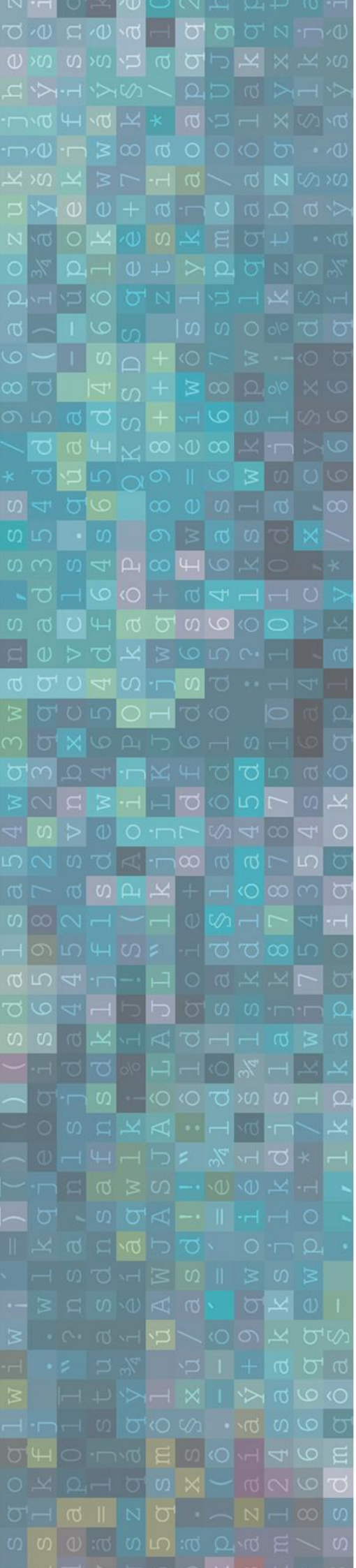
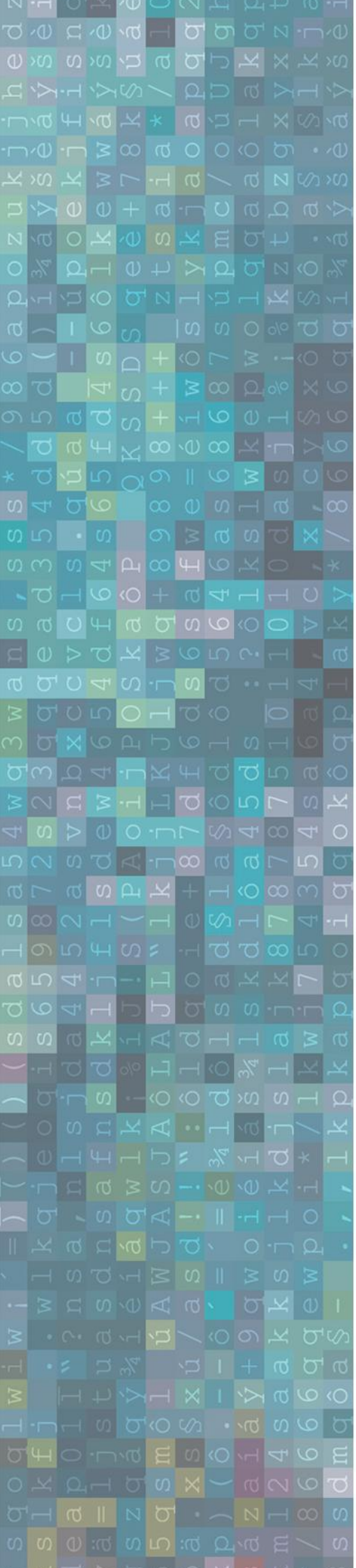


NOD32 antivirus system

felhasználói kézikönyv a 2.70-es verzióhoz

Tartalomjegyzék



1. Bevezető

1.1. A számítógépek károkozói

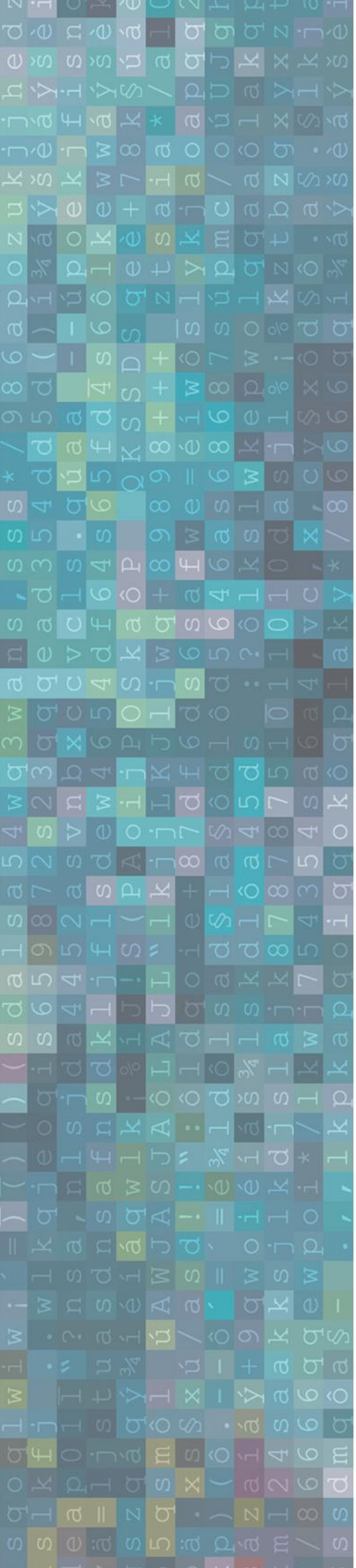
Napjainkban egyre gyakrabban lehet hallani interneten terjedő férgekről, a gépeken hátsó kaput nyitó trójai programokról, különböző vírusjárványok által okozott jelentős károkról. Még inkább felkapott téma a reklám- és kémprogramok (Adware, Spyware) terjedése, az ellenük történő védekezés módja és a legújabb kártevők, a rootkitek elleni megfelelő védekezés kérdése.

Mik ezek tulajdonképpen, és ki van kitéve a veszélynek?

A válaszra következtethetünk a híradásokban hallható óriási számokból: az otthoni és irodai számítógépek jelentős része ki van téve ennek a veszélynek. Az internetre kapcsolt számítógépek döntő többsége Windows alapú operációs rendszert futtat, így a vírusírók kiemelten foglalkoznak ezen operációs rendszerek sebezhetőségeivel. Munkánk során elektronikus leveleket küldünk és fogadunk, dokumentumokat és egyéb fájlokat cserélünk – így az ártalmas programok ártalmatlannak tűnő fájlok és dokumentumok formájában könnyen számítógépünkre kerülhetnek.

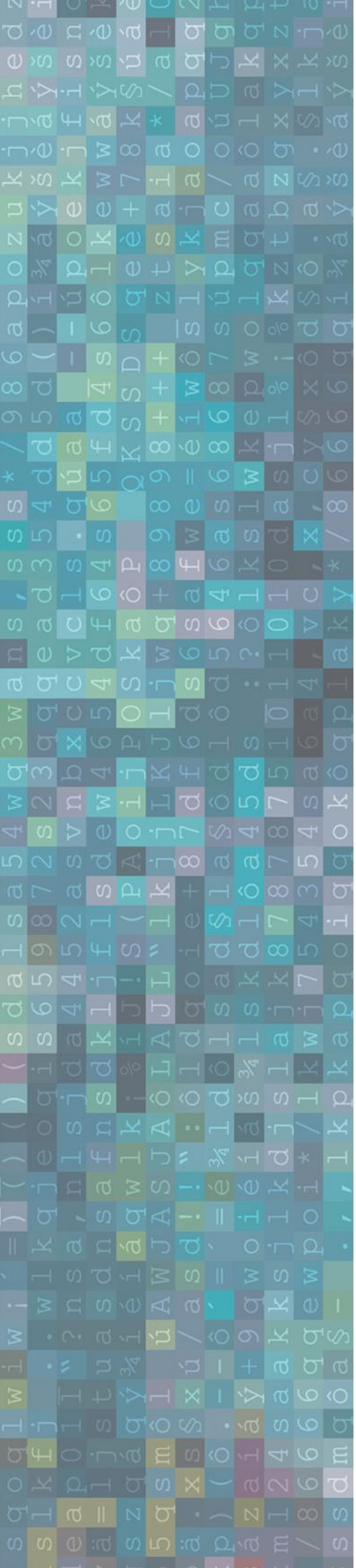
Természetesen a veszély mértéke sem minden számítógépen egyforma, ahogy egy legyengült emberi szervezetet is könnyebben megtámadnak a kórokozók, mint egy egészséges testet. A számítógépek „egészsége” is több összetevőből áll, ebből a két legfontosabb a képzett felhasználó és a naprakész frissítések. A képzett felhasználó legfontosabb tulajdonsága, hogy véletlenül sem futtat ártalmas kódot a számítógépen (például, nem indít el megbízhatatlan e-mailhez csatolt futtatható fájlokat). A naprakész frissítések azért fontosak, mert a programok hibáit javítják ki, amely hibákat kihasználva tudnak az elektronikus kártevők legkönnyebben terjedni. Az előző két dolgot egészíti ki a vírusvédelmi termékek két alapvető jelentőségű eleme: az állandó (memória-rezidens) fájl rendszer védelem és a bejövő e-mailek szűrése.

Fontos tudnunk, hogy minden alkalommal, amikor fájlokat másolunk, adatokat fogadunk gépünkre, fennáll a fertőzés veszélye, tökéletes védelem gyakorlatilag nem létezik. Kártevők ezrei fáradoznak azon, hogy újabb és újabb ötleteket bevetve rosszindulatú támadásokat intézzenek számítógépes rendszereink ellen. Szerencsére a teljesen új ötlet meglehetősen ritka, a Windows javítócsomagokat és a vírusirtókat fejlesztő szakemberek pedig gyorsan reagálnak minden újszerű támadásra.



Ezekkel az eszközökkel (fájlrendszer védelem, bejövő e-mailek szűrése) tulajdonképpen egy egészséges géptől tartjuk távol a vírusokat és egyéb kártevőket: az e-mail szűrés megtisztítja, vagy törli a vírusos vagy vírus-gyanús leveleket és csatolt fájlokat, míg az állandó fájlrendszer védelem az adathordozókról származó fertőzéseket veszi észre, mielőtt azok aktivizálhatnák magukat. Tehát elméletileg a fájlrendszer védelem által nyújtott védelem teljes: hiszen nem kerülhet futtatásra ártalmas kód mindaddig, amíg a védelem aktív. Viszont a fájlrendszer védelem nem mindig aktív, mert a számítógép bekapcsolásakor be kell töltődnie, mint minden más programnak, ezért előtte a gép védtelen és bármilyen ártalmas kódot futtathat. Ezért fontos, hogy a számítógépünk merevlemezei bekapcsoláskor ne tartalmazzanak kártékony programokat – erről a kézi indítású vírusirtó gondoskodik, ami részletesen végignézi a lemezeken tárolt fájlokat és eltávolítja a kártevőket. Így már a védelmünk majdnem teljes: a számítógép egészséges állapotba hozható a vírusirtó lefuttatásával, majd a következő bekapcsoláskor már nem indulhat el ártalmas kód, illetve az állandó fájlrendszer védelem és levélszűrés biztosítja, hogy ne juthasson a működés során új vírus a számítógépbe.

Fontos, hogy mind az operációs rendszer, mind a vírusvédelem naprakész legyen. Ennek nincs más módja, mind a *Windows Update* rendszeres futtatása (célszerű ezt automatikusra állítani vagy ezen a beállításon hagyni) és az elérhető frissítések haladéktalan letöltése és telepítése. Az operációs rendszer sebezhetőségeit az okozza, hogy az egyes részegységek is tartalmazhatnak hibákat, és egy célzott, az adott hiba kihasználásra irányuló kód rendellenes viselkedést válthat ki a számítógépből (például kényszerítve azt a kikapcsolásra). Ezeket a hibákat Microsoft Windows XP, illetve elődei esetén döntő többségben már kijavították a szakemberek, de egy frissítések nélküli operációs rendszer ugyanúgy sebezhető marad, hiába létezik már akár évek óta javítása a biztonsági résnek. Ezért létfontosságú, hogy minden frissítést azonnal telepítsünk, amint azok elérhetővé válnak, és természetesen a már meglévők is kivétel nélkül legyenek feltelepítve számítógépünkre. Szerencsére ez a folyamat ma már beállítható teljesen automatikusra, így a háttérben futva nem zavarja munkánkat, csak az esetleges újrainditásról kell gondoskodnunk.



Összefoglalva, a Microsoft Windows alapú számítógépek az alábbi veszélyeknek és károkozóknak vannak kitéve:

kártékony kód (vírus/féreg/trójai/stb.) futtatása, fertőzött dokumentum megnyitása (véletlenül vagy szándékosan, a felhasználó tudtával vagy anélkül): a Windows biztonsági rendszere sajnos nem elégséges a számítógépeken „elszabaduló" vírusok ellen, ezért ezek viszonylag szabadon törölhetnek, károsíthatnak fájlokat, vagy tehetnek elérhetővé bizalmas adatokat, illetve akár az egész számítógép felett is átvehetik az irányítást.

Trójai programok és férgek

Napjainkban a trójai programok és a férgek jelentik a fő fenyegetést. Ezek a kártékony kódok miután valamilyen álcázás alkalmazva bejutottak a számítógépbe (ahogy a görög faló Trójába) és elindultak, gyakran szabadon tehetnek bármit, amire csak a vírusíró „megtanította" őket.

Ritkán fordul elő, de bizonyos esetekben az adatok megsemmisítése és a rombolás is cél lehet: valamilyen rendszer szerint vagy véletlenszerűen adatfájlok törlése, módosítása a merevlemezen, esetleg az operációs rendszer tönkretétele valamilyen sebezhetőség kihasználásával.

Kifinomultabb cél lehet a jelszavak, személyes adatok, hitelkártya számok összegyűjtése, majd ezek kijuttatása valamilyen formában például a vírus írójához: ilyen esetben a program nem pusztít, hisz az a célja, hogy a háttérben futva minél tovább felfedezetlen maradjon, működéséről mindössze a gyanús hálózati forgalom árulkodhat.

Egy napjainkra jellemző cél a számítógép felhasználása különböző illegális tevékenységekre: több ezer megfertőzött számítógép egyszerre indíthat egy célzott támadást egy hálózati pont ellen, mindezt úgy, hogy az egyes gépek felhasználói mit sem sejtenek arról, hogy számítógépük épp részt vett például egy fontos szolgáltatás megbénításában. Gondolhatunk továbbá a kéretlen reklámlevelek küldésére is: minden nap több ezer "zombi" számítógép küldi szét a világba kéretlen reklámlevelek millióit a felhasználók tudta nélkül, a számítógépeiken futó trójai programok segítségével.

Hallhatunk olyan fertőzésekről is, amik a modemes internetezők életét keserítik meg: lefuttatásuk után bontják a telefonos kapcsolatot és egy emelt díjas (gyakran külföldi) számot tárcsáznak, mindezt úgy, hogy a képzetlen felhasználó sajnos csak a telefonszámláján veszi észre a károkozó tevékenységét.

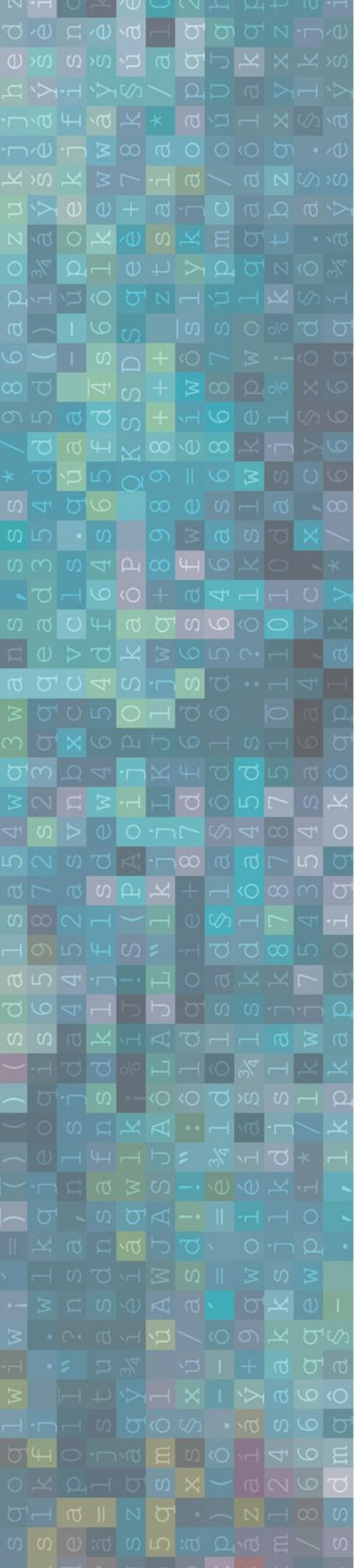
Érdekesség, de néha terjednek „jótékony" fertőzések is, amelyek egy-egy vírusjárvány közben eltávolítják az előző vírusokat a számítógépről és megkísérlik a szükséges Windows frissítés letöltését, amivel a számítógép későbbi sebezhetősége megszüntethető – annak ellenére, hogy mindezt a beleegyezésünk nélkül teszik, világos színfoltként működnek a vírusok sötét világában.

Rootkit technológiát alkalmazó kártevők

Napjaink leggyakrabban hangoztatott kifejezése a „Rootkit", amely olyan technikák gyűjtő neve, amelyek lehetővé teszik egy Trójai program, féreg, reklám- vagy kémprogram –egyszerűbben: bármilyen elektronikus kártevő- számára, hogy fertőzéskor és utána észrevétlen maradjon. Alapvető célja ez minden kártevőnek, hiszen minél tovább fejtheti ki hatását a fertőzött rendszerben, annál nagyobb a hatékonysága: több számítógépet tud megfertőzni, több reklámot képes megjeleníteni, több spam-levelet képes kiküldeni.

Reklám- és kémprogramok

Ebbe a kategóriába olyan programok tartoznak, melyek nagyrészt az emberi kíváncsiságot és figyelmetlenséget kihasználva a felhasználó engedélyével települnek a számítógépre. Az internetet böngészve mindenki találkozott már azzal a jelenséggel, hogy a megtekinteni kívánt weboldal gyakran csak sok felugró figyelmeztető ablak után jelenik meg. Ezekre a figyelmeztetésekre, kérdésekre hajlamosak vagyunk gondolkodás nélkül „Igen" gombot nyomni, melynek következménye hogy mi magunk engedjük meg, hogy az történjen rendszerünkkel, ami a figyelmeztetésben le volt írva, anélkül hogy azt elolvastuk volna. Ha a figyelmeztetésben például az található, hogy „az igen gombra kattintással hozzájárulunk, hogy a feltelepülő program internetezési szokásainkról információt küldjön egy adatgyűjtéssel foglalkozó szervezet számára", akkor ezek után a csendben feltelepülő program – teljesen jogosan – ezt fogja tenni. A hasonló kártevők tevékenységi köre széleskörű, általában ezek haszonszerző céllal készülnek.



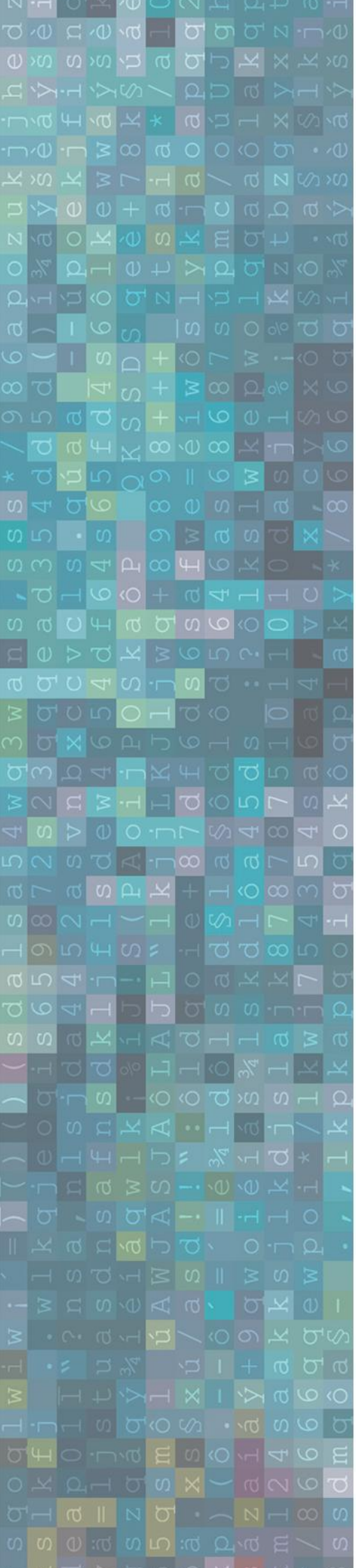
Az ilyen ártalmas programok feltelepülésekor amennyiben például az Internet Explorer biztonsági beállításai alacsonyra vannak állítva, nem is jelenik meg a fent említett figyelmeztető üzenet, ezen a biztonsági szinten a figyelmeztetés automatikusan elfogadásra kerül. Ezért a biztonsági beállításokat, illetve a folyamatos frissítést az interneten kommunikáló programok esetén még komolyabban kell venni, valamint nagyon fontos a folyamatos tájékozódás ezen a területen.

A kártevők létrehozói, a (vírusírók, spammerek, stb.) trójai programok, férgek, és Adware /Spyware programok tulajdonságait és lehetőségeit kihasználva ötvözik a technikákat, és az egyik fertőzés hozza maga után a másikat. Tipikus példa, hogy bizonyos (külön ilyen céllal létrehozott) internetes oldalakat meglátogatva, figyelmetlenségünket kihasználva feltelepül egy ActiveX vezérlőprogram, ami automatikusan elkezd letölteni egy trójai programot, mely megfelelő védelem hiányában a számítógépre érkezve elindul, és feltelepít további kártékony programokat, és így tovább.

Makró- és script vírusok

A makróvírusok mindig egy dokumentumba beágyazottan érkeznek, például egy Word szövegben vagy Excel táblázatban. Sok termék lehetővé teszi a programozhatóságot (script vagy makró írást) például egy táblázatkezelőben, hogy bonyolultabb műveleteket is meg lehessen valósítani az egyszerű számadatok és képletek mellett. A makró programozhatóság elsődleges célja a termék, például a táblázatkezelő szoftver felhasználhatóságának növelése. Természetesen ezek is tartalmaznak különböző hibákat és sebezhetőségeket, amivel kártékony kódot is meg tudunk „fogalmazni” a dokumentumokban.

Jellemzően a scriptek és makrók szigorú biztonsági előírások között futnak, ezért sokkal nehezebb a dolguk, mint a szabadon futó trójai társaiknak. Ennek ellenére a beépített biztonsági rendszerekben rejlő hibák miatt sokak számára csak a makrók/scriptek teljes körű letiltása nyújt biztonságot a megfelelő vírusvédelem hiányában.



Az operációs rendszerek sebezhetőségei

Ahogy már korábban említettük, a Windows operációs rendszerekben első kiadásuk óta sok biztonsági résre derült fény, melyek azonnali befoltozása elengedhetetlen. A figyelmeztetések ellenére mégis sokan nem foglalkoznak a frissítések feltelepítésével, ezért terjedhetnek napjainkban olyan vírusok, melyek elvileg már nem is működhetnének: ha minden számítógépen a legfrissebb Windows verziók futnának, a legtöbb vírus terjedése ellehetetlenülne. Az esetek többségében már a vírusjárványok kitörése előtt az operációs rendszert fejlesztő Microsoft elérhetővé teszi a szükséges Windows frissítéseket, a járványok mégis azért tudnak kitörni, mert ezek a javítások nem jutnak el időben minden számítógépre.

Az operációs rendszer sebezhetőségei lehetőséget nyitnak idegen, fertőzött fájlok merevlemezre-vitelére és azok futtatására. Fontos, hogy az állandó vírusvédelem nem tudja megszüntetni a biztonsági lyukakat, mindössze a bekerült vírusokat tudja hatástalanítani (blokkolni, törölni), amikor azok futtatásra kerülnek.

Fontos kihangsúlyozni, hogy minden elérhető Windows frissítést késlekedés nélkül telepítsünk fel; nem elegendő, ha csak a vírusvédelmi rendszerünket tartjuk naprakészen!

Egyéb szoftverek sebezhetőségei

Ahogyan az operációs rendszer is tartalmaz biztonsági réseket, úgy tetszőleges felhasználói programok is tartalmazhatnak: például egy webböngésző vagy egy FTP szerver, rosszabb esetben pont a biztonságtechnikai programok, például tűzfalak, lehetnek hálózati támadások célpontjai.

A Windows sebezhetőségekhez hasonlóan ezek is különböző kapukat nyithatnak a kártékony kódoknak. A megoldás itt is a termékek lehető legfrissebb változatra való frissítése, hiszen minden új változattól elvárhatjuk, hogy a fejlesztő megszüntette a korábban nyilvánosságra került (és akár vírusjárványokat is okozó) sebezhetőségeit.

1.2. A NOD32 által biztosított védelem

A *NOD32 antivirus system* részegységei az alábbi kórokozók ellen nyújtanak védelmet:

részegység neve és leírása	*védelmet nyújt*
AMON: Állandó (memória rezidens) fájlrendszer-védelem	Vírusok, trójaiak, férgek, reklám- és kémprogramok, valamint rootkitek ellen, megakadályozva a fertőzött fájlhoz való hozzáférést
DMON: Dokumentumok és automatikusan letöltődő internet tartalom védelme	fertőzött Microsoft Office dokumentumok és a Microsoft Internet Explorer által automatikusan letöltött kártékony tartalom ellen
IMON: POP3 levelezés és web-böngészés (HTTP) védelem	internet felől e-mailben, illetve a weboldalak böngészése közben érkező ártalmas kód ellen
EMON: Outlook levelezés védelem	internet felől e-mailben érkező ártalmas kód ellen
NOD32: Kézi víruskereső és vírusirtó alkalmazás	Vírusok, trójaiak, férgek, reklám- és kémprogramok, rootkit technikákat alkalmazó kártevők felfedezésére és eltávolítására

1.3. Az irtható vírusokról

Ebben a részben arról a gyakran felmerülő kérdésről lesz szó, hogy milyen vírust nevezünk irthatónak, illetve, hogy miért nem tud a NOD32 bizonyos fertőzéseket eltávolítani, például a vírusriasztás ablakban.

Nem választható ki a Vírusirtás

A vírusirtás gyakran csak törléssel valósítható meg. Vírusirtáskor egy feltehetően értékes dokumentumból vagy programból távolítjuk el a „hozzánőtt" kártevőt, míg a törlés a teljes fertőzött programfájl eltávolítását jelenti a meghajtóról. Manapság a leggyakoribb vírusfertőzéseket interneten terjedő férgek és trójai programok okozzák, melyek nem fertőznek meg dokumentumokat vagy programfájlokat, hanem az egész fájl kizárólag a kártevőt tartalmazza. Másképpen fogalmazva, a program nem tartalmaz hasznos információt, csak kártékony kódot, ezért a vírusirtás után nem maradna belőle semmi – ezért nevezzük az ilyen esetekben a vírusirtást törlésnek.

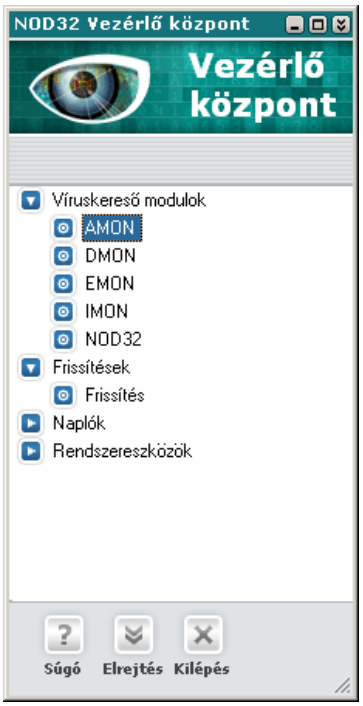
Összefoglalva tehát a vírusfertőzésekről elmondható:

- a trójai programok és férgek nem fertőznek meg más alkalmazásokat, nem írthatók csak törölhetők, hasznos információt nem tartalmaznak
- a reklám- és kémprogramok az emberi figyelmetlenséget illetve a rosszul beállított rendszereket kihasználva „engedéllyel" fertőznek
- a rootkitek elrejtik magukat az operációs rendszer elől, megnehezítve felfedezésüket a védelmi szoftverek és a szakemberek számára
- a makróvírusok dokumentumokat (például Word, Excel fájlok) fertőznek és ezeken keresztül terjednek. Ezek gyakorlatilag kivétel nélkül irthatók, így nem szükséges az eredeti dokumentumok törlése.
- a régi fájlvírusok a makróvírusokhoz hasonló módon program fájlokat fertőztek meg, ezek is szinte kivétel nélkül irthatók, de elterjedtségük ma már minimálisnak mondható.

2. A NOD32 antivirus system fogalmai

2.1. Moduláris felépítés

A *NOD32 antivirus system* Microsoft Windowsra telepíthető munkaállomás és szerver védelme moduláris felépítésű. A különböző víruskereső modulokat a Vezérlő központon keresztül tudjuk menedzselni. A Vezérlő központon keresztül tudjuk frissíteni a vírus-adatbázist, illetve a program-komponenseket, itt tudjuk ütemezni a víruskeresési feladatokat, kezelni a karantén tartalmát, megtekinteni a naplókat, vagy személyre szabni a vírusvédelmi beállításokat.



A NOD32 Vezérlő központot a tálcán levő NOD32 ikonra kattintással tudjuk megjeleníteni.

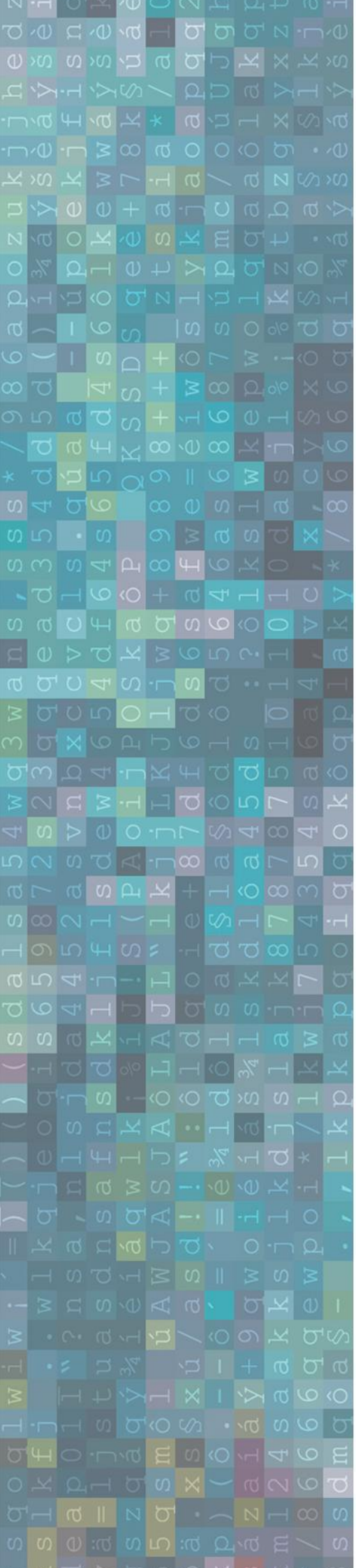
2.2. Profilok

A NOD32 úgynevezett profilok használatával lehetővé teszi, hogy különböző, előre definiált beállítások között gyorsan válthassunk. Egy profil tartalmazza a frissítési beállításokat (pl: AV- kezdetű felhasználói név és jelszó, mely az elektronikus licenc e-mailben szerepel), valamint a NOD32 kézi indítású víruskereső modul beállításait (pl.: mit tegyen egy kártevő felfedezése esetén, vagy milyen típusú és kiterjesztésű fájlokat vizsgáljon a program)..

Alapértelmezésben négy profilt tartalmaz a NOD32.Az úgynevezett *„Saját profil”* tartalmazza a frissítési alapbeállításokat, 3 további profil víruskeresések indítására szolgál. A víruskeresési profilok menedzselését (új profil hozzáadása, profil törlése, stb.) a NOD32 kézi indítású víruskereső program *„Profilok”* ablakábanlehet elvégezni.

2.3. Tükrözés *

A NOD32 antivirus system Administrator változata valósítja meg a frissítések szétosztását helyi hálózatokon. A Tükrözés modul letölti és eltárolja (tükrözi) az internetes vírusadatbázis és programfrissítéseket, és elérhetővé teszi egy helyi hálózaton belül a



többi NOD32 számára. Például, ha egy irodai hálózatban egyetlen számítógép rendelkezik internet eléréssel, akkor az itt futó, Tükrözés modult tartalmazó *NOD32 Administrator* változat segítségével elég, ha mindössze az a számítógép frissít rendszeresen az internetről, és a többi NOD32 a hálózatban erről a munkaállomásról frissül. További információt a következő dokumentumban talál: http://www.nod32.hu/dl/nod32_lan_ebook.pdf

* A Tükrözés modult kizárólag az Administrator jelzéssel ellátott NOD32 programok tartalmazzák.
Ezt a programváltozatot 2 vagy több munkaállomásos licenccel lehet letölteni, és használni.

2.4. Karantén

A karanténban a NOD32 futásra és megnyitásra képtelenül, biztonságosan tárolja a felfedezett vírusokat és fertőzött fájlokat. A karanténból visszaállíthatjuk a fertőzöttnek vélt fájlokat..

2.5. Feladatütemező

A NOD32 feladatütemező segítségével általános víruskereséssel és vírusirtással kapcsolatos feladatok indíthatók el automatikusan. A feladatütemezőt használhatjuk egyaránt az automatikus frissítések időpontjának megadására, vagy a kézi indítású vírusirtás automatikus, tetszőleges gyakoriságú futtatására.

2.6. Naplók

A NOD32 futása során három különböző naplót tart nyilván: ezek az Eseménynapló, a Vírusnapló és a NOD32 víruskeresési napló.

Az *eseménynaplóba* kerülnek a NOD32 kliens különböző moduljai által generált üzenetek, pl.: sikeres frissítés vagy a hibajelzések. A *vírusnaplóba* kerülnek az AMON, az IMON és az EMON által generált vírusriasztások. A NOD32 kézi indítású víruskereső üzenetei (a vírustalálatok is) a *NOD32 víruskeresési naplóba* kerülnek

2.7. Távadminisztráció

A *NOD32 Remote Administrator* program segítségével egy számítógépről felügyelhető egy helyi hálózatban működő összes NOD32 antivirus system.

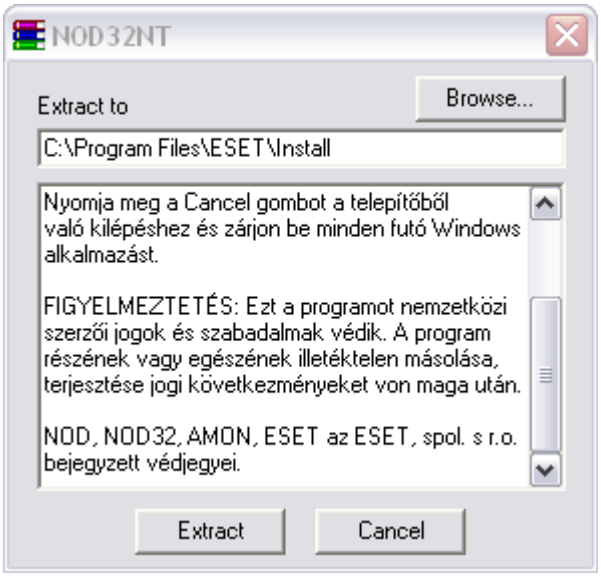
A NOD32 helyi hálózatokon alkalmazandó beállításairól olvassa el honlapunkról letölthető szemléletes útmutatónkat: http://www.nod32.hu/dl/nod32_lan_ebook.pdf

A *NOD32 Remote Administrator* program a NOD32 kliensek távoli felügyeletére szolgál, nem valósít meg helyi hálózaton belüli frissítést. A helyi hálózaton belüli frissítés a NOD32 Administrator programmal valósítható meg, mely egy NOD32 vírusvédelmi program, úgynevezett Tükrözés modullal kiegészítve.

3. A NOD32 telepítése

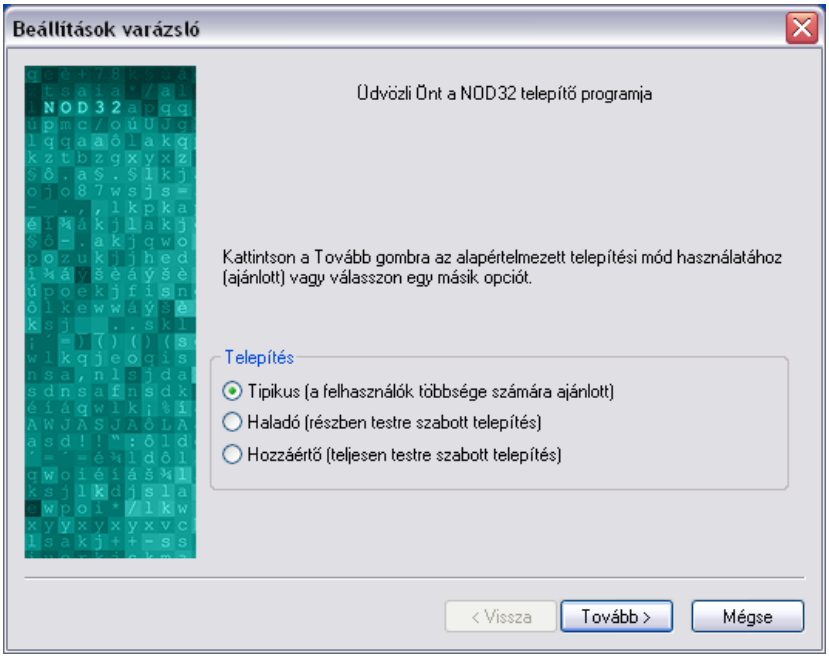
Telepítés „Tipikus" módban

A letöltött, vagy a CD-n található önkicsomagoló telepítő fájl elindításával kezdetét veszi a telepítési folyamat. Első lépésben meg kell adni az önkicsomagoló telepítő fájlnak azt a mappát, amelybe a program a telepítéshez szükséges átmeneti fájlokat másolhatja. Célszerű a felkínált útvonalat elfogadni.



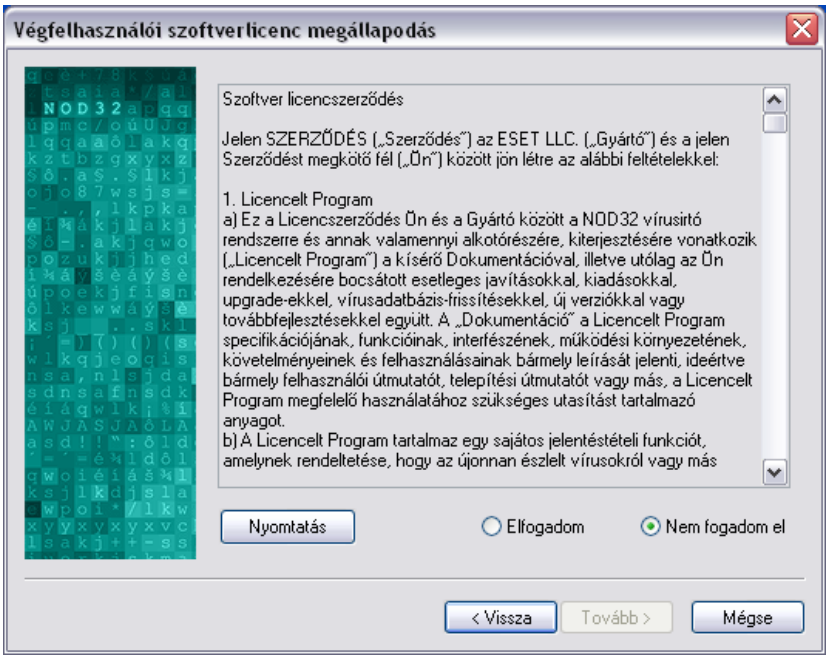
Nyomja meg az Extract (kitömörítés) gombot a telepítés folytatásához. A telepítéshez szükséges átmeneti fájlok a felkínált mappába másolódnak!

Az átmeneti fájlok kicsomagolása után elindul a NOD32 telepítő programja. Itt kiválaszthatja, hogy a telepítés milyen üzemmódban történjen (Tipikus, Haladó és Hozzáértő telepítési módok).
A Tipikus telepítési mód a legtöbb felhasználó számára jól használható alapbeállításokat tartalmaz, célszerű ezért a Tipikus telepítési módot választani.



Hagyja a Tipikus telepítési módot kijelölve és nyomja meg a Tovább gombot a telepítés folytatásához!

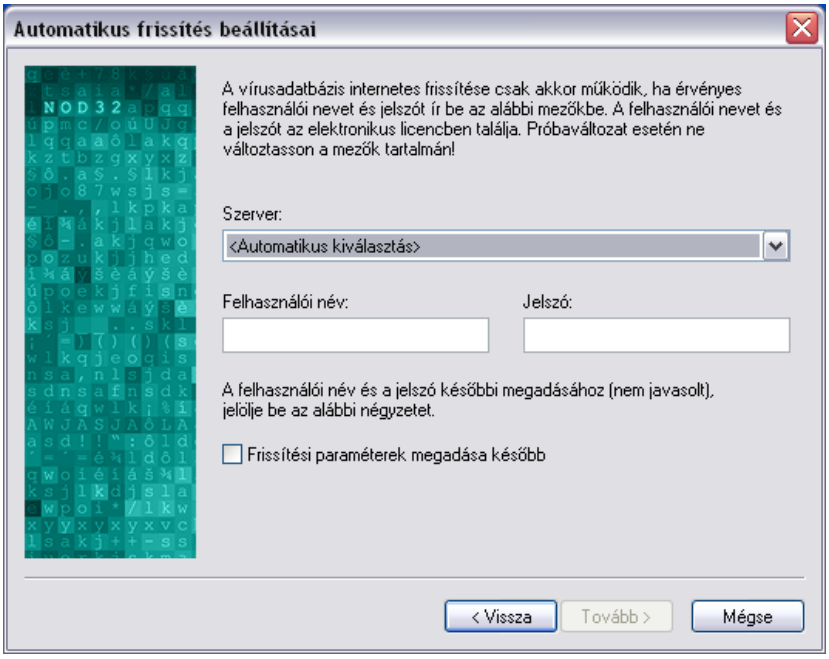
A telepítési folyamat folytatásához el kell fogadnia a Végfelhasználói szoftverlicenc megállapodást. Kérjük, alaposan olvassa el a licencszerződést. Amennyiben egyetért az abban foglaltakkal és maradéktalanul elfogadja a licencben szereplő feltételeket, kattintson az Elfogadom feliratra, majd a Tovább gombra. A Mégse gombbal megszakíthatja a telepítési folyamatot.



A telepítés folytatásához kattintson az Elfogadom feliratra és nyomja meg a Tovább gombot, amennyiben maradéktalanul egyetért a végfelhasználói licencszerződésben foglaltakkal!

A következő ablakban az automatikus frissítés beállítására kerül sor. Bármely víruskereső program használata esetén - így a NOD32 esetében is – a hatékony működéshez elengedhetetlen, hogy a lehető legfrissebb vírusadatbázist használjuk. Ehhez rendszeres frissítésre van szükség. A NOD32 minden gépindításkor, az Internet-kapcsolat létrejöttekor, valamint minden órában próbál a frissítési szerverek valamelyikéhez kapcsolódni, hogy letöltse a legújabb frissítéseket. Ehhez érvényes AV- kezdetű felhasználói névre és jelszóra van szükség, amit elektronikus úton történő vásárlás, vagy a dobozos NOD32 változat regisztrációja során kap meg, az Ön által megadott e-mail címre.

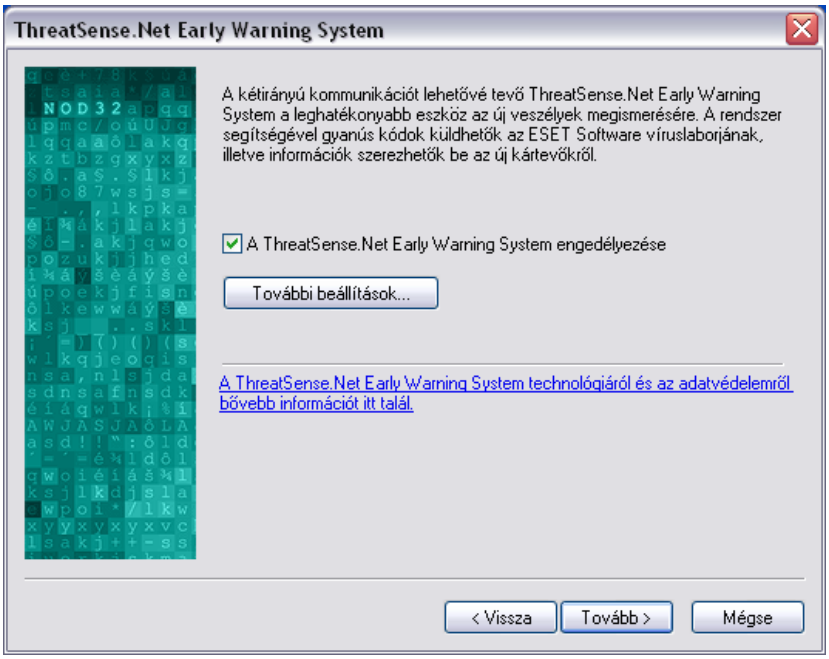
Amennyiben dobozos NOD32 változattal rendelkezik, és még regisztrálta a terméket, kérjük, látogassa meg a **http://www.nod32.hu/regisztracio** oldalt, majd a regisztrációhoz kövesse az ott olvasható utasításokat.



Írja be licencében szereplő AV- kezdetű egyedi felhasználói nevét és a hozzá tartozó jelszavát a megfelelő mezőkbe, ügyelve a kis- és nagybetűkre! Nyomja meg a Tovább gombot a telepítés folytatásához!

Az új vírusok és egyéb kártevők elleni hatékony védekezés eszköze a *ThreatSense.Net Early Warning System*. A *ThreatSense.Net* engedélyezésével hozzájárul ahhoz, hogy a számítógépét támadó eddig ismeretlen kártevőt a program az adatvédelmi jogok teljes tiszteletben tartásával, anonim formában elküldje az *Eset Software* víruslaborjába, így ön is hatékonyan közreműködik abban, hogy új víruskitörés esetén a lehető leghamarabb ismertté váljon a kártevő, és ezzel elősegíti saját maga és az internetes társadalom hatékonyabb védelmét.

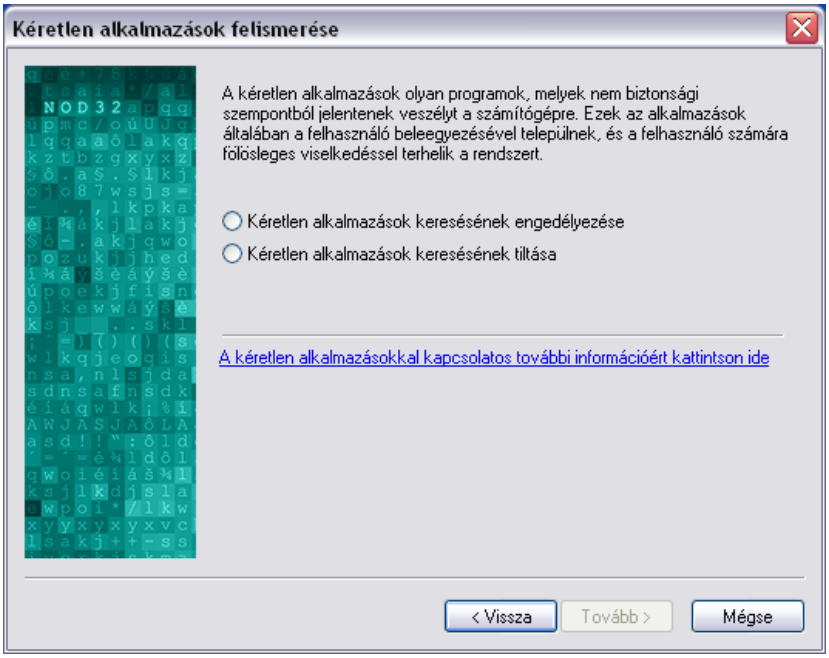
Adatvédelmi és egyéb információkért nyissa meg a *ThreatSense.Net* súgóját az aláhúzott „ThreatSense.Net Early Warning System technológiáról és az adatvédelemről bővebben információt itt talál” szövegre kattintással, vagy az F1 billentyű lenyomásával.



Hagyja bejelölve a „ThreatSense.Net Early Warning System engedélyezése” opciót, és nyomja meg a Tovább gombot a telepítés folytatásához.

A NOD32 2.7-es változatában megjelent „Kéretlen alkalmazások keresése” opció bekapcsolásával a NOD32 azon alkalmazásokat is felismeri és blokkolja, melyek nem esnek a Reklám és kémprogramok definíciója alá, azonban a felhasználók általános véleménye alapján nem kívánatos szoftverek.

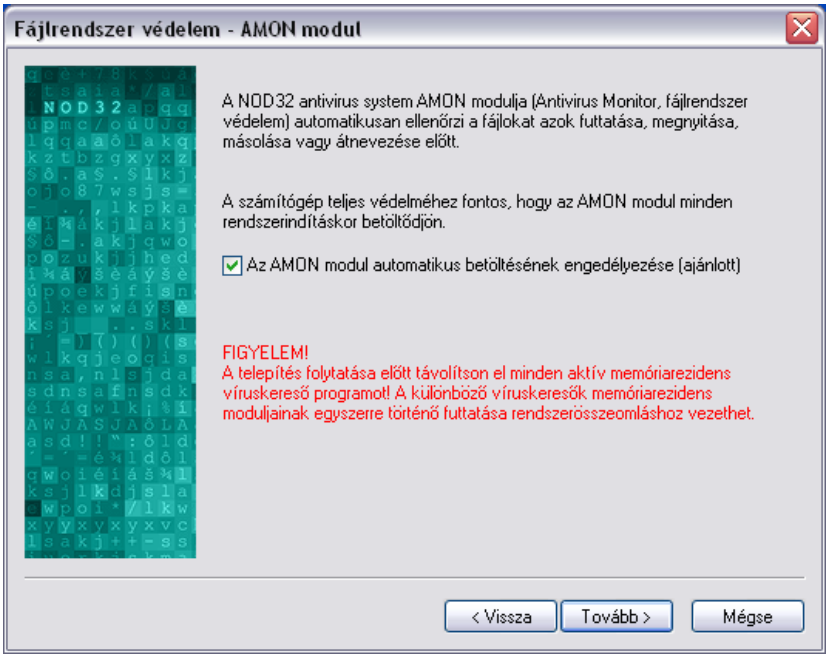
További információért nyissa meg a *NOD32* súgóját az aláhúzott „A kéretlen alkalmazásokkal kapcsolatos további információért kattintson ide” szövegre kattintással, vagy az F1 billentyű lenyomásával.



Jelölje be a „Kéretlen alkalmazások keresésének engedélyezése" opciót és kattintson a tovább gombra a telepítés folytatásához.

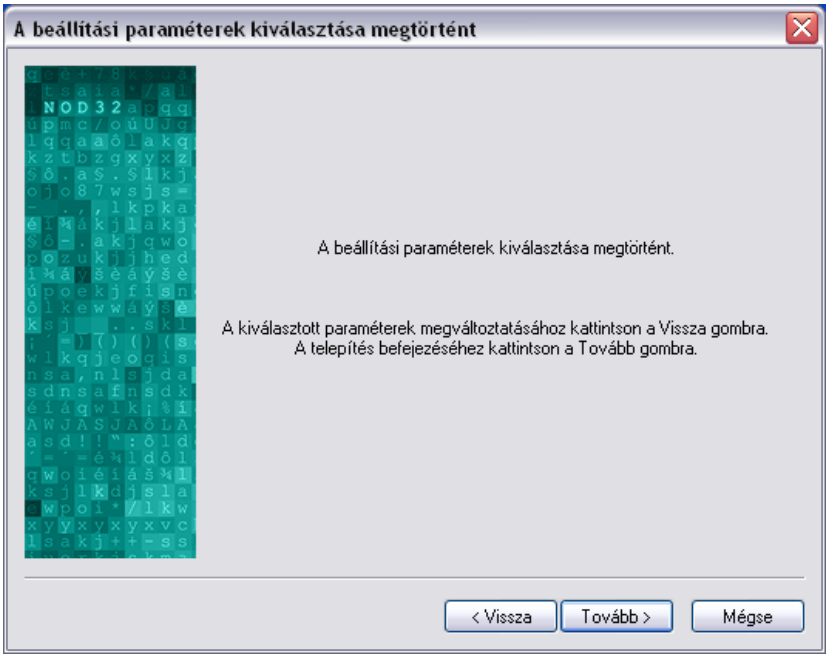
A telepítés következő részében a legfontosabb modul, a fájlrendszer védelem beállítására kerül sor. Fontos, hogy ne legyen a NOD32-n kívül más típusú memóriarezidens víruskereső program feltelepítve a számítógépre, mert két különböző memóriarezidens vírusvédelmi program egyidejű futása rendszerösszeomláshoz vezethet.

A fájlrendszer védelem (AMON modul), akkor hatékony, ha automatikusan elindul a számítógép indulásakor, ezért pipálja ki az *„Az AMON modul automatikus betöltésének engedélyezése (ajánlott)"* jelölőnégyzetet.

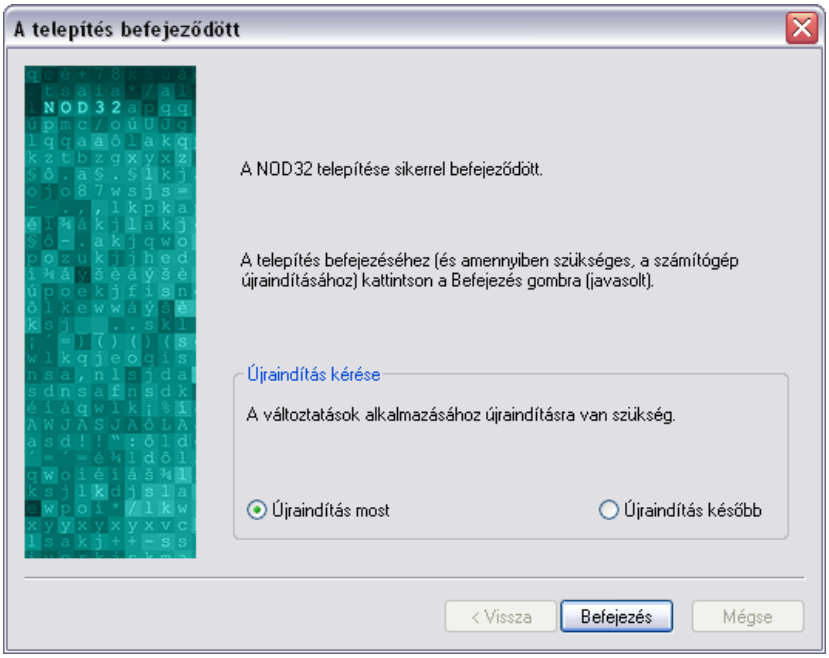


Hagyja bejelölve az „Az AMON modul automatikus betöltésének engedélyezése (ajánlott)” jelölőnégyzetet és nyomja meg a Tovább gombot

---



A beállítási paraméterek kiválasztása megtörtént. Nyomja meg a Tovább gombot a telepítés véglegesítéséhez. (Figyelem! Ezután már nem tud változtatni a telepítési beállításokon, csak a számítógép újraindítása után)



A NOD32 telepítése befejeződött. A vírusvédelem elindításához a számítógép újraindítására van szükség. Mentse el jelenlegi munkáit és zárja be az összes futó alkalmazást. A NOD32 telepítőjében hagyja bejelölve az *„Újraindítás most”* opciót és nyomja meg a *Befejezés* gombot.
A számítógép újraindítását követően a sikeresen feltelepített, NOD32 program helyes működését a tálcán megjelenő zöld-fehér NOD32 ikon jelzi.

4. A NOD32 moduljai

A *NOD32 Vezérlő központban* az alábbi víruskereső modulok találhatók:

AMON	Antivirus Monitor, memóriarezidens fájlrendszer védelem – a legfontosabb modul
DMON	Document Monitor, Microsoft Office dokumentumok védelme
EMON	Email Monitor, Microsoft Outlook programba beépülő védelmi modul (MAPI, IMAP és POP3 protokoll ellenőrzése)
IMON	Internet Monitor, internetes védelem és általános levelezés védelem (POP3 és HTTP protokollokon)
NOD32	kézi indítású víruskereső program

A Vezérlő központon keresztül tudja a modulokat beállítani (például ki- és bekapcsolás, naplók megtekintése, ütemezett feladatok beállítása).

A továbbiakban az egyes modulokról olvashat bővebben.

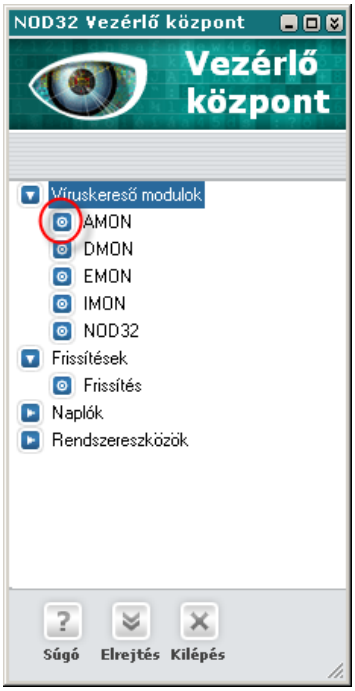
4.1. AMON

Az AMON látja el a folyamatos fájlrendszer védelmet. A számítógépre potenciálisan veszélyes fájlok létrehozása, másolása, megnyitása vagy futtatása esetén az AMON blokkolja a fájlhoz való hozzáférést. Az AMON a fájlokon túl vizsgálja a lemezek boot-szektorát, valamint a távoli meghajtókat is.

A NOD32 antivirus system legfontosabb modulja a folyamatosan futó (memóriarezidens) fájlrendszer védelem. Ha az AMON kikapcsol, a NOD32 ikonja a tálcán zöld-fehérről (normális működés) piros-fehérre (memóriarezidens védelem inaktív) vált. Kérjük, figyeljen arra, hogy az AMON mindig be legyen kapcsolva!

Az AMON háromféle állapotban lehet:

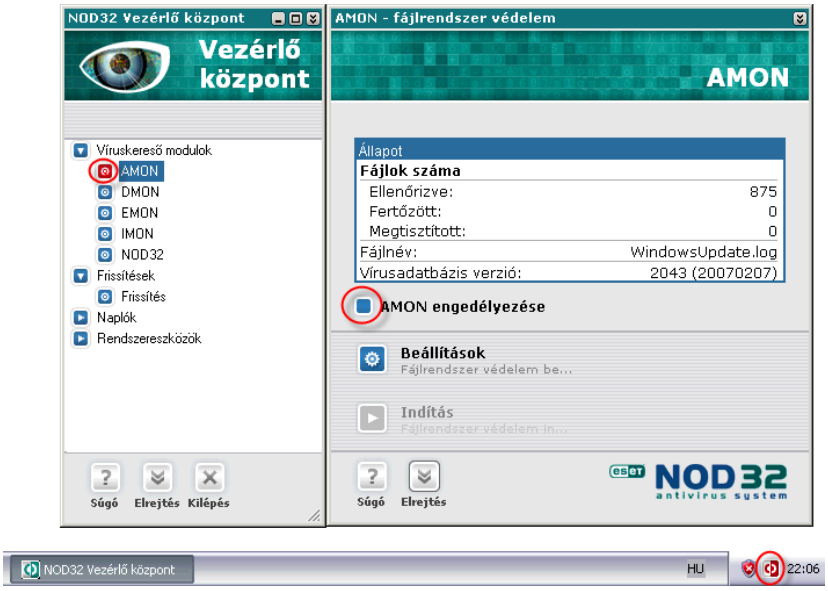
1. a modul betöltődött a memóriába, és be van kapcsolva (a Vezérlő központban az AMON felirat melletti négyzet kék színű, valamint a tálcán a NOD32 ikon zöld-fehér színű - ez az ajánlott beállítás)



2. a modul betöltődött a memóriába, de ki van kapcsolva (a Vezérlő központban az AMON felirat melletti négyzet piros színű, valamint a tálcán a NOD32 ikon piros-fehér színű - ilyenkor az AMON nem biztosít védelmet!)

3. a modul nem töltődött be a memóriába (a Vezérlő központban az AMON felirat melletti négyzet szürke színű, valamint a tálcán a NOD32 ikon piros-fehér színű - ilyenkor az AMON nem biztosít védelmet!)

Az AMON modul ki- és bekapcsolását a NOD32Vezérlő központban, az AMON beállító panelén lehet elvégezni. Az *„AMON engedélyezése”* felirat melletti pipa eltávolításával tudja kikapcsolni a memóriarezidens fájlrendszer védelmet (ilyenkor a Vezérlő központban az AMON felirat melletti négyzet piros színűre, a tálcán látható NOD32 ikon piros-fehér színűre vált, ezzel jelezve, hogy az AMON nem biztosít védelmet).



Figyelem: Ha átmenetileg ki akarja kapcsolni a memóriarezidens fájlvédelmet, az *„AMON engedélyezése”* felirat melletti pipát távolítsa el.

Az AMON működésének részletes beállításához (pl: ellenőrizendő meghajtók, vizsgált fájltípusok, ellenőrzésből kizárt fájlok és mappák, stb) nyomja meg a *Beállítások* gombot a Vezérlő központ AMON panelén. Részletes információt a Súgóban talál, melyet a Súgó gombra kattintással, vagy az F1 billentyű lenyomásával hívhat elő.

4.2. DMON

A DMON (Document Monitor) segítségével a NOD32 antivirus system a Microsoft Office dokumentumokat és az Internet Explorer által automatikusan letöltendő fájlokat (például a Microsoft ActiveX vezérlők) ellenőrzi, ezáltal a DMON kiegészítő védelmet nyújt az AMON (Antivirus Monitor, a memóriarezidens fájlellenőrző modul) részére.

A DMON modul csak olyan alkalmazásokkal tud együttműködni, amelyek támogatják a Microsoft Antivirus API interfészt. Ilyen alkalmazások például a Microsoft Office 2000 (9.0-s vagy későbbi változat) vagy a Microsoft Internet Explorer (5.0-s vagy későbbi változat)

A DMON modul ki- és bekapcsolását a Vezérlő központon keresztül lehet végezni. A *„DMON engedélyezése”* felirat melletti pipa eltávolításával tudja kikapcsolni a DMON-t (ilyenkor a Vezérlő központban a DMON felirat melletti négyzet piros színűre vált, ezzel jelezve, hogy a DMON nem biztosít védelmet).

A DMON beállításairól részletes információt a Súgóban talál, melyet a Súgó gombra kattintással, vagy az F1 billentyű lenyomásával hívhat elő.

4.3. IMON

Az IMON (Internet Monitor) modul az első védelmi vonal az Internet felől érkező elektronikus kártevők ellen. Az IMON látja el a levelezésvédelmet, oly módon, hogy a levelezőprogramok külön beállítására nincs szükség. Védelmet nyújt bármely levelező program esetén (Outlook Express, a The Bat!, Eudora), amennyiben a levelek letöltése POP3 protokollon történik. Szintén az IMON véd a böngészés közben (HTTP protokollon) érkező kártevők ellen és a hálózaton terjedő férgek ellen.

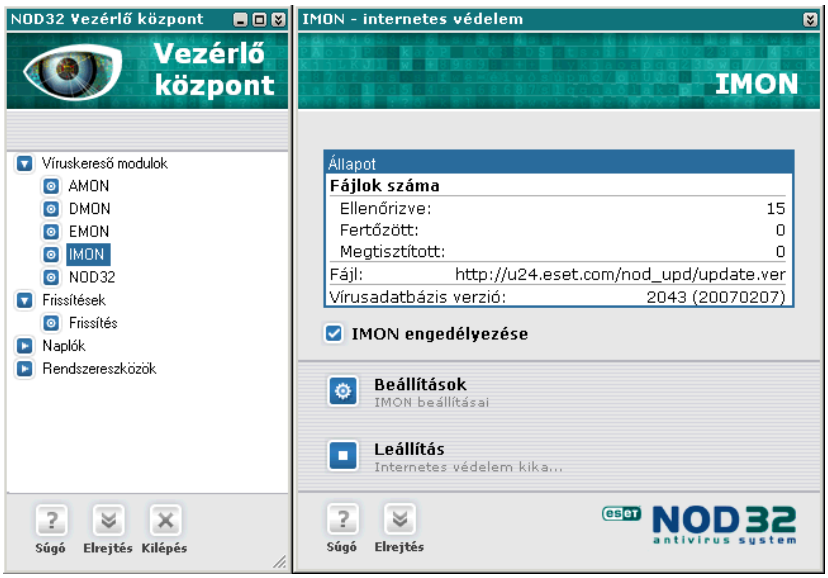
Az IMON modul háromféle állapotban lehet:

1. a modul betöltődött a memóriába, és be van kapcsolva (a Vezérlő központban az IMON felirat melletti négyzet kék színű - ez az ajánlott beállítás)

2. a modul betöltődött a memóriába, és ki van kapcsolva (a Vezérlő központban az IMON felirat melletti négyzet piros színű - ilyenkor az IMON nem biztosít védelmet!)

3. a modul nem töltődött be a memóriába (a Vezérlő központban az IMON felirat melletti négyzet szürke színű - ilyenkor az IMON nem biztosít védelmet!)

Az IMON modul ki- és bekapcsolását a Vezérlő központon keresztül lehet elvégezni. Amennyiben az IMON modul betöltődött a memóriába, az *„IMON engedélyezése”* felirat melletti pipa eltávolításával tudja ideiglenesen kikapcsolni az IMON által nyújtott védelmet (ilyenkor a Vezérlő központban az IMON felirat melletti négyzet piros színűre vált, ezzel jelezve, hogy az IMON nem aktív). A Vezérlő központ IMON panelén látható egy *Leállítás* gomb is, ezt csak akkor használja, ha az IMON-t teljesen el akarja távolítani a memóriából.



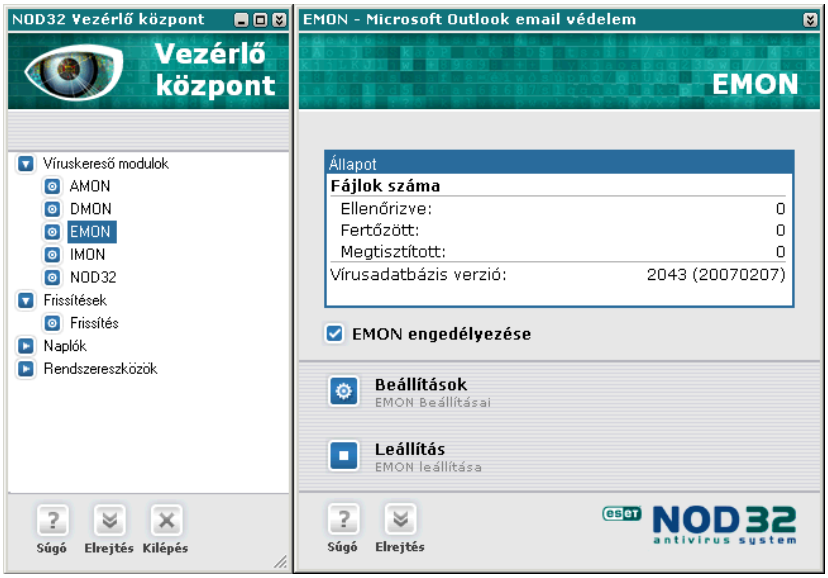
Figyelem: Ha csak átmenetileg akarja kikapcsolni az IMON-t, távolítsa el az *„IMON engedélyezése”* felirat melletti pipát.

Az IMON beállításairól részletes információt a Súgóban talál, melyet a Súgó gombra kattintással, vagy az F1 billentyű lenyomásával hívhat elő.

4.4. EMON

Az EMON, (Email Monitor) a modul látja el a Microsoft Outlook (2000 vagy későbbi) programon (MAPI interfészen) keresztül érkező kártevők elleni védelmet. Az EMON modul csak akkor kerül feltelepítésre, ha ilyen levelező programot használ ezért nem biztos hogy az Ön gépén látható lesz az EMON modul a Vezérlő központban.

A Vezérlő központ EMON panelén található *"EMON engedélyezése"* opció ki/bekapcsolásával (kipipálás, illetve a pipa eltávolítása) tudja az EMON működését ideiglenesen engedélyezni vagy letiltani. Az alap állapotban rendszerindításkor a memóriába töltődik. A *Leállítás* gomb megnyomásával az EMON eltávolítható a memóriából, ebben az esetben rendszerindításkor sem fog újra betöltődni. Bekapcsolt állapotban a Vezérlő központban az EMON felirat melletti négyzet kék színű; kikapcsolt állapotban a Vezérlő központban az EMON felirat melletti négyzet piros színű (ilyenkor az EMON nem biztosít védelmet!).



Az EMON beállításairól részletes információt a Súgóban talál, melyet a Súgó gombra kattintással, vagy az F1 billentyű lenyomásával hívhat elő.

4.5. NOD32 kézi indítású víruskereső

A NOD32 kézi indítású víruskeresőt többféleképpen is futtathatjuk. Egy lehetőség, hogy az Asztalon lévő NOD32 ikonra duplán kattintunk, vagy a Start menüből (az *Eset* programcsoportból) indítjuk a programot. Ebben az esetben a *„Saját profil”* nevű beállítással indul el a kereső. A vezérlő központ NOD32 „modulját” választva többféle beállítással (profillal) is indíthatunk víruskeresést.

A különböző módok különböző mélységű és különböző célterületekre (Helyi lemezek, Floppy, stb.) irányuló keresést indítanak. A különböző beállításokról további információ a Súgóban található, mely a Súgó gombra kattintással, vagy az F1 billentyű lenyomásával hívható elő.

"Helyzetérzékeny menü profil" nevű beállításokkal indul el a kereső, ha a Windows Intézőben egy fájl, könyvtár vagy meghajtó fölött a

jobb egérgombbal kattintunk, és az előugró menüből kiválasztjuk a *"NOD32 antivirus system "*-et.

Lehetőség van még *"<Parancssorból konfigurált profil >"* beállításokkal is indítani a NOD32-t: a *"Helyi lemezek" / Floppy* feliratra kattintva a Vezérlő központ NOD32 panelén, vagy a parancssorból indítva és a lehetséges paraméter-kapcsolókat használva.

Amennyiben egy profil beállításait megváltoztatja, a változtatások elmenthetők, így legközelebb már a módosított beállításokkal fog futni a keresés. A profilok (beállítások) mentését a program kilépésnél automatikusan felajánlja.

Figyelem: a *"Helyzetérzékeny menü profil"*-ban alapértelmezésben nincsenek bejelölve a futtatás közbeni tömörítők, a tömörített fájlok és az email fájlok, valamint a módszerek között Kiterjesztett heurisztikus keresés és az egyéb kártékony alkalmazások keresése. Amennyiben mélyreható ellenőrzést szeretne végezni az érintett fájlokon, kérjük, jelölje be a fenti opciókat a *Beállítások* fülön. Ha a profil beállításait kilépéskor elmenti, a következő alkalommal a megjegyzett mélyreható keresés fog elindulni.

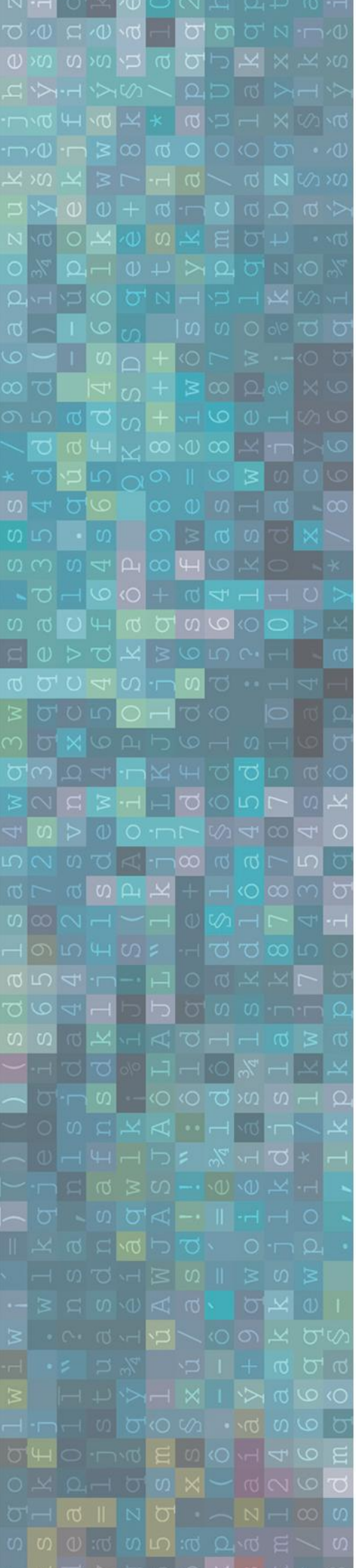
A NOD32 antivirus system kézi indítású víruskereső programja (*on-demand scanner*) öt beállítási fület tartalmaz. Ezek:

- **Ellenőrzési célterületek**
- **Víruskeresési napló**
- **Akciók**
- **Beállítások**
- **Profilok**

A képernyő jobb alsó felén található vezérlő gombok a következők:

- **Víruskeresés** – ebben az üzemmódban a NOD32 nem irtja, csak keresi a vírusokat!
- **Vírusirtás**
- **Kilépés**
- **Súgó**

A beállítási fülek használatáról a Súgó nyújt bővebb tájékoztatást, melyet a Súgó gombra kattintással, vagy az F1 billentyű lenyomásával hívhat elő.



4.5.1. Parancssori paraméterek

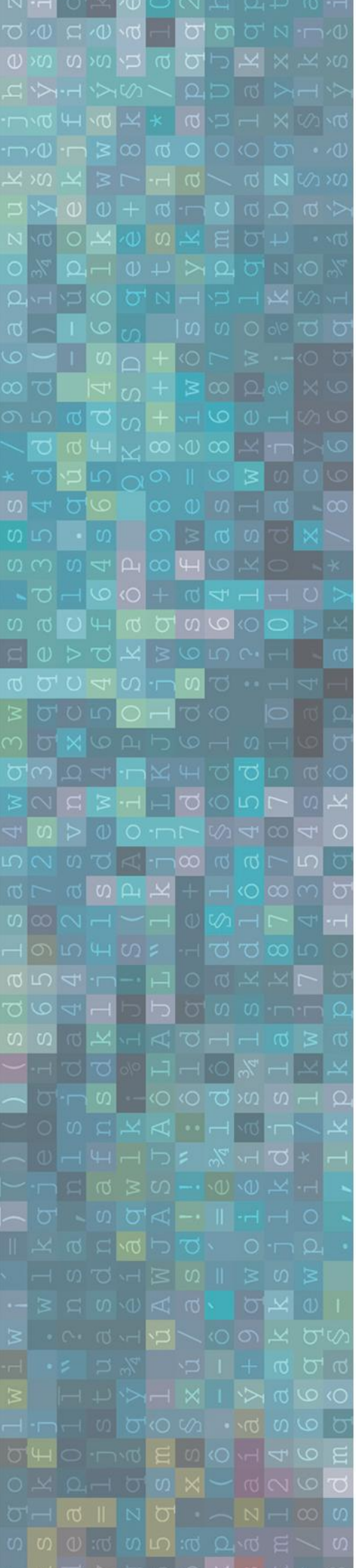
Amikor a vírusellenőrzést parancssorból futtatjuk, számos paraméter és kapcsoló alkalmazására van lehetőség a különféle opciók kiválasztásához. Sok paraméter a plusz (+) és a mínusz (-) jellel engedélyezhető vagy tiltható le. Például ahhoz hogy a program saját magát is megvizsgálja (önellenőrzés) a *"/selfcheck+" kapcsoló használatára*, az önellenőrzés letiltásához a *"/selfcheck-" kapcsoló* használatára van szükség.

Általános parancssori paraméterek:

• **/help**	Megmutatja a program kapcsolóinak a listáját
• /**selfcheck+(-)**	Önellenőrzés engedélyezése (letiltása)
• **/expire+(-)**	A program lejártáról szóló értesítés engedélyezése (letiltása)
• **/subdir+(-)**	Alkönyvtárak ellenőrzésének engedélyezése (letiltása)
• **/multi+(-)**	Többszörös lemezellenőrzés engedélyezése (letiltása)
• **/sound+(-)**	Hangjelzés engedélyezése (letiltása)
• **/list+**	Minden vizsgált objektum felvétele a napló listájára
• **/list-**	Csak a fertőzött objektumok felvétele a napló listájára
• **/break+(-)**	Az ellenőrzés szüneteltetésének engedélyezése (letiltása)
• **/scroll+(-)**	A napló legördüléses megjelenítésének engedélyezése (letiltása)
• **/quit+(-)**	Vírusellenőrzés után a program kilép (nem lép ki)

Vírusészleléssel kapcsolatos parancssori paraméterek:

• **/pattern+(-)**	Vírusadatbázis alapján történő ellenőrzés engedélyezése (letiltása)
• **/heur+(-)**	Alap heurisztikus keresés engedélyezése (letiltása)
• **/ah**	Kiterjesztett heurisztikus keresés engedélyezése (Advanced Heuristics)
• **/scanfile+(-)**	Fájlok ellenőrzésének engedélyezése (letiltása)
• **/scanboot+(-)**	A boot szektor ellenőrzésének engedélyezése (letiltása)



- **/scanmbr+(-)** A master boot record (MBR) ellenőrzésének engedélyezése (letiltása)
- **/arch+(-)** Az archívumok (ZIP, ARJ, RAR) ellenőrzésének engedélyezése (letiltása)
- **/pack+(-)** A belső, futtatás közbeni tömörítők (internal runtime packer) ellenőrzésének engedélyezése (letiltása)
- **/sfx+(-)** Önkicsomagoló tömörített fájlok vizsgálatának engedélyezése (letiltása)
- **/local** Minden helyi, nem kivehető médium ellenőrzése
- **/network** Minden hálózati meghajtó ellenőrzése
- **/ext=<LIST>** Új kiterjesztés hozzáadása az ellenőrzendő fájlok listájához. (Több bejegyzés is engedélyezett, pl. /ext=EXT1,EXT2)
- **/all** Minden fájl ellenőrzése a kiterjesztéstől függetlenül
- **/adware** Adware, Spyware, Riskware keresése
- **/unsafe** Veszélyes alkalmazások keresése

Heurisztikus kereséssel kapcsolatos parancssori paraméterek:

- **/heursafe** A *Biztonságos* alap heurisztikus érzékenység beállítása (minimalizálja a téves riasztások számát)
- **/heurstd** A *Standard* alap heurisztikus érzékenység beállítása
- **/heurdeep** A *Mély* alap heurisztikus érzékenység beállítása
- **/ah** Kiterjesztett heurisztikus keresés engedélyezése (Advanced Heuristics)

Naplózással kapcsolatos parancssori paraméterek:

- **/log+(-)** Naplófájl létrehozásának engedélyezése (letiltása)
- **/wrap+(-)** A naplófájl szövege sortörésének engedélyezése (letiltása)
- **/logappend** A naplófájl hozzáfűzési opciójának engedélyezése (letiltása)
- **/logrewrite** A naplófájl felülírási opciójának engedélyezése (letiltása)
- **/logsize=N** A naplófájl legnagyobb kiterjedésének a megadása: KB-ban

- **/log=<FILENAME>** A naplófájl nevének a megadása (pl.: /log=NOD.LOG)

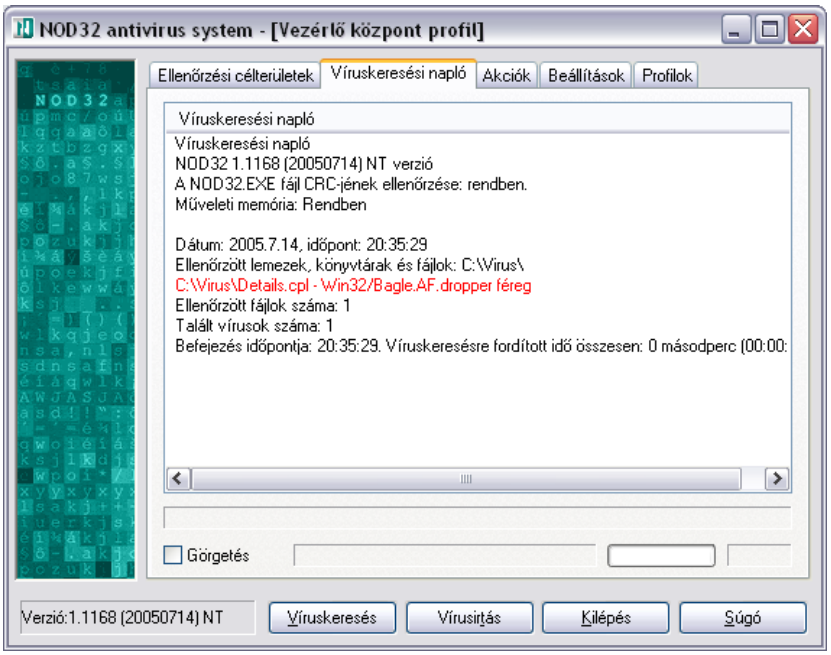
Vírusirtással kapcsolatos parancssori paraméterek:

- **/clean** A fertőzött objektumok vírusirtása (ha lehetséges)
- **/prompt** Javaslattétel vírusészlelés esetén
- **/rename** Fertőzött fájlok átnevezése
- **/delete** Fertőzött fájlok törlése
- **/replace** A boot szektor fertőzött kódjának kicserélése a megfelelő szabványos kóddal

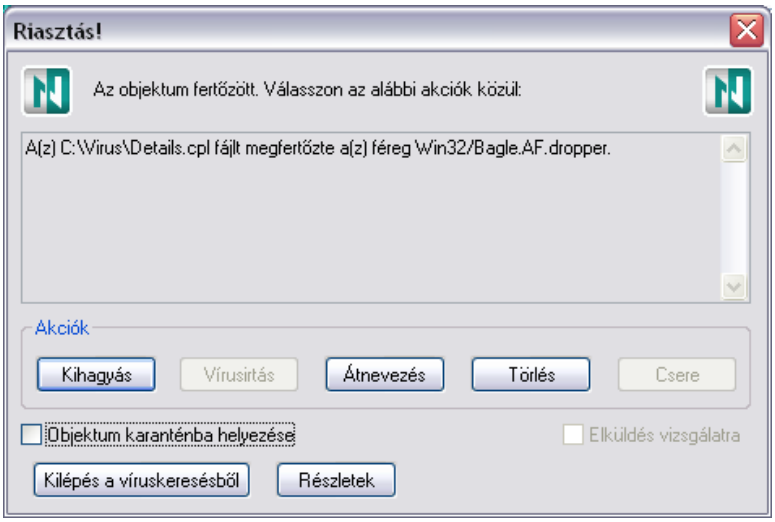
Megjegyzés: *ha a /prompt, /rename, /delete vagy /replace kapcsolókat a /clean kapcsolóval együtt használjuk, a megfelelő akció végrehajtására csak akkor kerül sor, ha a vírus irtható. (Az írható és csak törölhető vírusokról a kézikönyv elején, az 1.3 -as, „Az irtható vírusokról" című fejezetben olvashat.)*

4.5.2. Ha a NOD32 vírust vagy egyéb kártékony kódot talál

A NOD32 kézi indítású víruskereső programjának Víruskeresési napló fülén piros színű felirat mutatja, ha a NOD32 fertőzést észlel. Az alábbi példában megtalált *Bagle.AF* esetében is így történt: mozgassuk az egér mutatóját a piros feliratra, majd nyomjuk meg a jobb oldali egérgombot. Ekkor egy helyzetérzékeny menüt kapunk, melynek három eleme van: Napló törlése, Vírusirtás és Információ.



Válasszuk ki a **Vírusirtás** opciót! Az alábbi ablakot kapjuk:

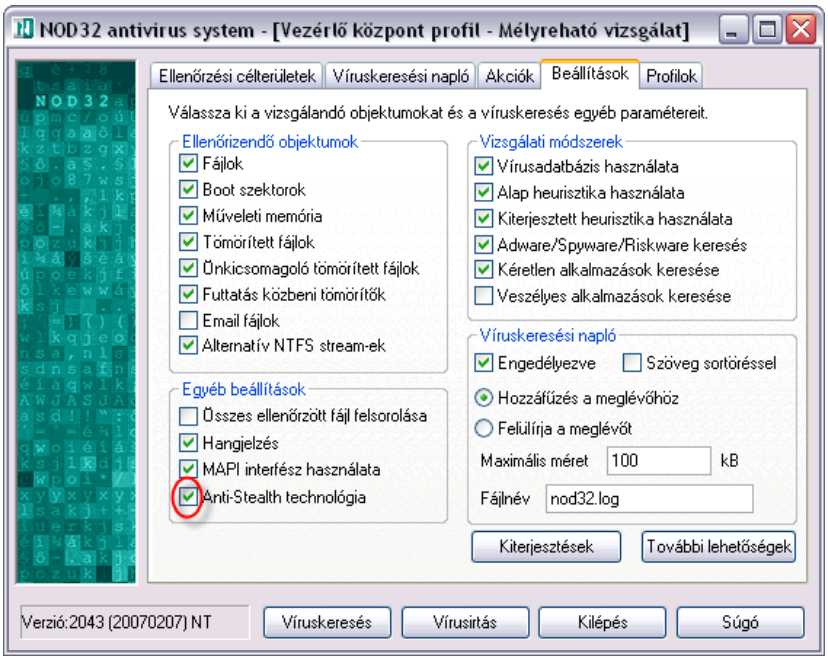


Hasonlóan az AMON illetve az IMON *Riasztás* ablakához, itt is ki tudjuk választani a megfelelő akciókat.

Megjegyzés: vannak olyan fertőzések (a férgek is ilyenek, így a Bagle is), amelyekből nem lehet eltávolítani a fertőzést, ugyanis az egész program maga ártalmas, nincs „hasznos része”. Ilyenkor választhatunk, hogy töröljük-e a fájlt, esetleg átnevezzük – így nem lehet a későbbiekben közvetlenül futtatni. Az „Karanténba helyezés” opció segítségével a választott akció végrehajtása előtt a karanténba kerül a fertőzött fájl.

4.5.3. Hasznos vírusirtási tanácsok

A NOD32 kézi indítású víruskereső pontos beállításával, és különböző profilok elmentésével elérhető, hogy mindig a legoptimálisabb víruskeresést hajtsa végre a program. Példákat a kézikönyv utolsó fejezetében talál.
A NOD32 2.7-es változatában megjelent Anti-Stealth technológia vírusirtás közbeni alkalmazásával elérhető, hogy az operációs rendszer által elrejtett, a szakemberek számára is észrevehetetlen, lopakodó (u.n. Rootkit) technológiákat alkalmazó kártevőket is felfedezze és kiirtsa a NOD32. A kézi indítású víruskeresőben a Beállítások panelen tudja bekapcsolni az Anti-Stealth technológia használatát.

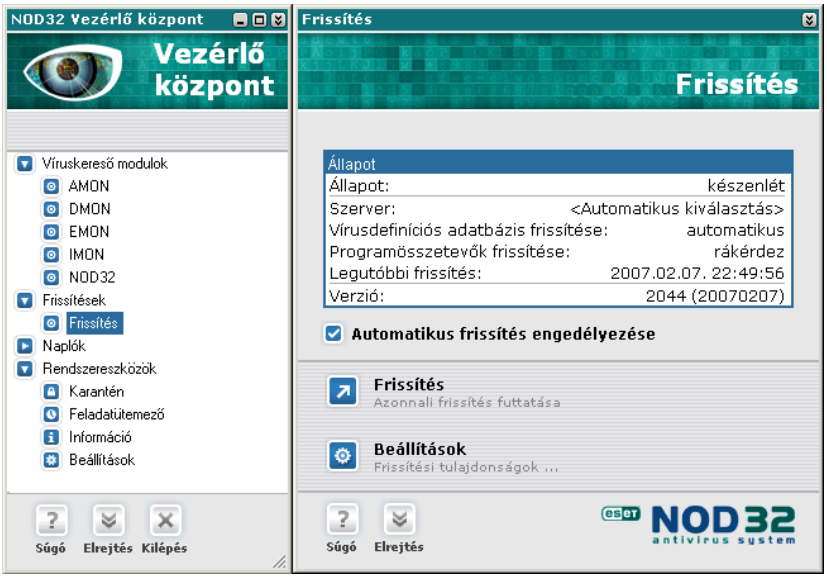


A rejtőzködő kártevők hatékony kereséséhez a kézi indítású víruskereső Beállítások panelén kapcsolja be az Anti-Stealth technológiát.

Amennyiben számítógépe működés alapján fertőzöttnek tűnik (lassan töltődnek be az ablakok, weboldalak, szakadozik az internet kapcsolat) végezzen úgynevezett teljes vírusirtást az alábbi helyről letölthető, szemléletes útmutató alapján: http://www.nod32.hu/dl/virusirtas.pdf

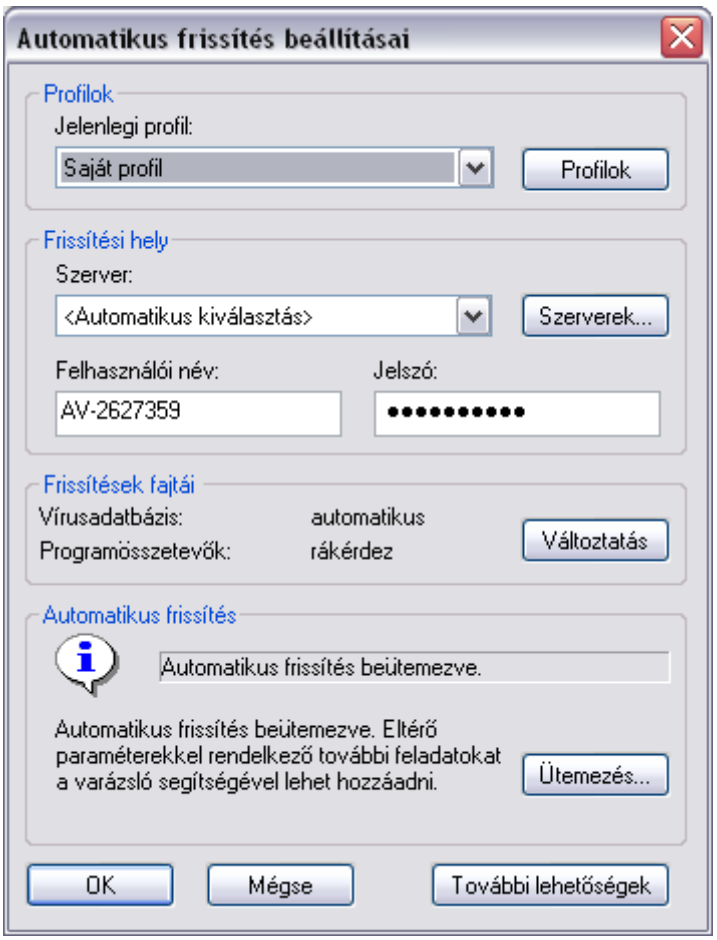
5. A Frissítés modul

A Frissítés modul a NOD32 egyik legfontosabb része, az általa nyújtott szolgáltatás minden vírusvédelmi rendszer kulcsfontosságú eleme. Segítségével a licenc teljes időtartama alatt a *NOD32 antivirus system* tetszőleges gyakorisággal frissíthető. A frissítés egyaránt kiterjed a vírusadatbázisra és a legújabb programösszetevőkre. A *Feladatütemező* segítségével a frissítések teljesen automatizálhatók. Régi vírusadatbázis esetén a modul figyelmeztet a frissítés szükségességére – amely legkönnyebben az interneten keresztül végezhető el. A lehetséges alternatív frissítési módokról is ebben a fejezetben olvashat.



Kérjük, győződjön meg időközönként arról, hogy az Ön gépén is a lehető legfrissebb NOD32 található. Ehhez a Frissítés panelen nyomja meg a **Frissítés** gombot: amennyiben naprakész az adatbázis, a következő üzenetablak jelenik meg: *"Az Ön NOD32 programja a lehető legfrissebb változatú fájlokat használja."* Ha a NOD32 *„Csendes üzemmódban”* fut, akkor nem fog ilyen ablakot kapni, mindössze azt láthatja, hogy a frissítés gyorsan véget ér és a legutóbbi frissítés időpontja nem változik.

A NOD32 alapértelmezett beállítása szerint az internetről próbálja letölteni a frissítéseket. Lehetősége van ezen kívül CD-ről, a lokális hálózat megosztott könyvtárából, vagy saját NOD32 HTTP alapú frissítési szerverről is elvégezni a termékfrissítéseket. Az ehhez szükséges beállításokat az *"Automatikus frissítés beállításai"* ablakban végezheti el.



Nyomja meg a *Szerverek…* gombot új frissítési szerver hozzáadásához. A megjelenő *Szerverek* ablakban nyomja meg a *Hozzáadás* gombot. Az előugró ablak beviteli mezőjébe az alábbi három forma közül kiválasztva a megfelelőt, adja meg a frissítési útvonalat:

Helyi lemezek (floppy, merevlemez, CD, stb.) esetén az alábbi formában adjuk meg:

X:\PATH

ahol X: a meghajtó jele, PATH pedig az elérési útvonal.

Pl.: E:\NOD_UPD

Lokális hálózati meghajtók esetén az alábbi formát használjuk:

\\SERVER\PATH

ahol SERVER a kiszolgáló neve, PATH pedig az elérési útvonal.

Pl.: \\nod32mirror\nod_upd

Figyelem: csatlakoztatott meghajtók nem használhatók frissítési útvonalként!

NOD32 HTTP frissítési szerver esetén a következő formát használhatjuk:

http://server:port

ahol a mezőket értelemszerűen adjuk meg.

Pl.: http://10.0.0.2:8081

Az egyedi frissítési szerverek hozzáadása után az *„Automatikus frissítés beállításai”* ablakban a *Szerver* legördülő menüből ki kell választani a kívánt frissítési szervert. Miután az *OK* gomb megnyomásával véglegesítette a beállításokat, kérjük, a **Frissítés** gomb megnyomásával ellenőrizze le, hogy valóban jól működnek-e a beállítások.

Helyi hálózatok helyes beállításáról, a tükrözések és a Remote Administrator lehetőségeiről kérjük, olvassa el a *nod32.hu* honlapon található *„NOD32 telepítése helyi hálózatok esetén”* című útmutatónkat! (http://www.nod32.hu/dl/nod32_lan_ebook.pdf)

6. Naplók

A NOD32 Vezérlő központ *Naplók* részében találhatók az Eseménynapló, a Vírusnapló és a NOD32 víruskeresési napló.

Az *eseménynaplóba* kerülnek a NOD32 kliens különböző moduljai által generált üzenetek (pl.: sikeres frissítés, hibajelzések)
A *vírusnaplóba* kerülnek az AMON, az IMON és az EMON által generált vírusriasztások.
A NOD32 kézi indítású víruskereső üzenetei (a vírustalálatok is) a *NOD32 víruskeresési naplóba* kerülnek.

7. Rendszereszközök

A Vezérlő központ *Rendszereszközök* menüpontja alatt található a Karantén, a Feladatütemező, az Információ és a Beállítások panel.

7.1. Karantén

A karantén mappa a fertőzött vagy gyanús fájlok ártalmatlan formában történő tárolásának kényelmes módja.

A *Karantén* a számítógép egy megadott könyvtára (alapértelmezésben a *Program Files\Eset\Infected*, ez a *Beállítások* részben módosítható), ahol a felismert elektronikus kártevők, valamint a vírusgyanús fájlok kódolva tárolódnak, így azok nem veszélyeztetik a gépet.

Használata csak tapasztalat felhasználóknak javasolt, például olyan esetben, amikor egy programfájlról (pl.: egy .DLL fájlról) nem dönthető el biztosan, hogy az fertőzött, de ha a karanténba zárás után minden program továbbra is hibátlanul működik, akkor nagy valószínűséggel a fertőzés része volt. Ellenkező esetben a karanténból az eredeti helyére visszaállítható a gyanús fájl.

7.2. Feladatütemező

A NOD32 hatékony feladatütemező és tervező modullal rendelkezik.

Az ütemezett feladatok lehetnek:

- NOD32 - kézi indítású vírusellenőrzés (*on-demand scan*)
- A NOD32 frissítése
- Külső alkalmazás futtatása (a NOD32 segítségével)

Minden ütemezett feladathoz egy előre beállított profil tartozik. Egy profil azt határozza meg, hogy milyen módon hajtja végre a NOD32 az adott feladatot, és hogy milyen paraméterek kapcsolódnak hozzá a végrehajtás során.

Az *ütemezett feladatok* ablak az egyes feladatok listáját tartalmazza azok nevével, fajtájával, az érintett modul megadásával, a végrehajtás módjával, esetenként különleges beállításokkal, végül azzal az időponttal, amikor a feladat legutóbbi végrehajtására sor került.

Az ablakban található *Hozzáadás* gombbal új feladatot tud létrehozni egy varázsló segítségével, a *Törlés* gombbal pedig az épp kiválasztott feladatot lehet az ütemezett feladatok listájából eltávolítani.

Minden feladatot egyszerűen engedélyezhetünk, vagy letilthatunk a feladat sorában, a neve előtt szereplő jelölőnégyzet ki/bekapcsolásával.

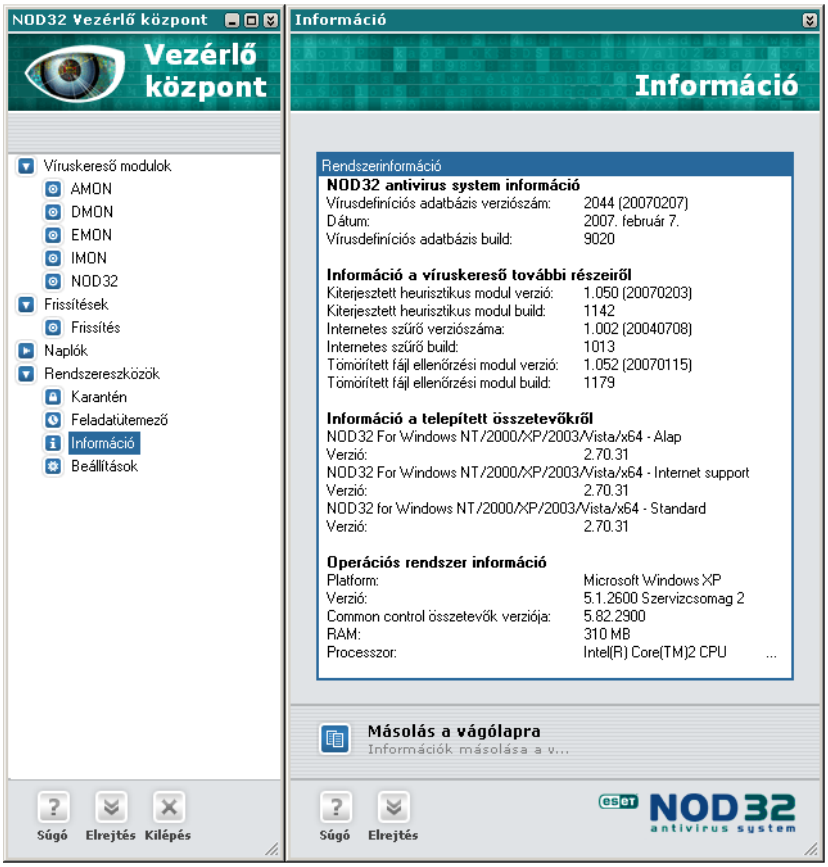
Az ütemezett feladatok listájában, egy sorban való dupla kattintás egy összegző ablakot jelenít meg a kiválasztott feladatról. Egy feladat sorában jobb-gombbal való kattintás pedig egy előugró menüt hoz fel, amiből a megfelelő menüpontokat választva a kijelölt feladat szerkesztésére is lehetőségünk nyílik.

Új feladat hozzáadásához:

1. Kattintson a *Hozzáadás* gombra az ütemezett feladatok ablak bal alsó sarkában!
2. Válassza ki a kívánt feladat jellegét a legördülő menüből!
3. Írja be a feladat nevét, jelölje be időzítését vagy a feladat végrehajtását kiváltó eseményt a jelölőnégyzetek valamelyikébe!
4. Adja meg a kiválasztott feladathoz kapcsolódó részleteket!
5. Válassza ki a végrehajtandó akciót arra az esetre, ha a feladat nem teljesíthető a megadottaknak megfelelően!
6. Ellenőrizze a beütemezett feladat részleteit!
7. Kattintson a *Befejezés* gombra a specifikáció megadásának befejezéséhez vagy a *Vissza* gombra a beállítások módosításához!
8. *Külső alkalmazás futtatása* esetén adja meg a program részleteit, míg *víruskeresés* vagy *frissítés* esetén válasszon ki egy profilt a meglévők közül.
9. Kattintson az *OK* gombra a feladat hozzáadásának véglegesítéséhez.

7.3. Információ

Az *Info* panel összesíti a NOD32 állapotával kapcsolatos adatokat, melyek nagyon fontosak lehetnek az esetleges hibakereséskor.



Kérjük, amennyiben terméktámogatási kérdése van, e-mailben küldje el a feltelepített NOD32 komponensek pontos leírását. Ezt úgy tudja megtenni, hogy a *„Másolás a vágólapra”* gomb megnyomása után a vágólapra került információkat beilleszti a terméktámogatást kérő email szövegébe (például a CTRL-V gombok együttes megnyomásával).

7.4. Beállítások

A Beállítások ablakban összefoglalva megtekinthetők a NOD32 keretrendszer mindenkori beállításai. A *Beállítások* gombra kattintva megváltoztatható a kertrendszer működése. A fejezetben az egyes füleken elvégezhető beállítási lehetőségekről olvashat részletesen.

7.4.1. Általános Beállítások fül

Grafika

A NOD32 Microsoft Windows rendszerekre telepíthető változatának kezelőfelületét meg lehet jeleníteni az Eset Software által tervezett grafikus felülettel, valamint a szabvány Windows-megjelenítéssel. Ebben a csoportban lehet kikapcsolni a rendszerinduláskor megjelenő NOD32 nyitóképernyőt is.

Csendes üzemmód

Ha a *"Csendes üzemmód engedélyezése"* jelölőnégyzet ki van pipálva, csak a legfontosabb üzenetek jelennek meg, például a vírus-adatbázis frissítésekről nem fog többet felugró ablakban értesülni.

A beállítások védelme

A NOD32 beállításait el lehet látni jelszavas védelemmel. A védelem beállításához kattintson a *Beállítások...* gombra, majd adja meg a jelszót. Amennyiben levédte a programot, és elfelejtette a jelszót hívja a NOD32 terméktámogatást a www.nod32.hu weboldalon található telefonszámon.

Alapbeállított rendszerfeladatok

Az alapbeállított rendszerfeladatok (naplókezelés, rendszerindítás-védelem) szükségesek a NOD32 megfelelő működéséhez. Alaphelyzetben rejtve maradnak ezek a feladatok, de a jelölőnégyzet kipipálásával meg lehet őket nézni. Ennek az opciónak az aktiválása nem ajánlott, mert ez által lehetővé válik a helyes működést segítő rendszerfeladatok módosítása a Feladatütemezőben..

7.4.2. Értesítések fül

Az Értesítések fülön beállítható, hogy milyen módon kommunikáljon a NOD32 - a program működéséről távoli értesítést váró - rendszergazdával.

Két típusú üzenetet tud küldeni a program:
• Vírusriasztás-üzenet
• Különböző eseményekről tájékoztatás

Az üzeneteket vagy SMTP szolgáltatás használatával e-mailben, vagy helyi hálózaton Windows Messenger segítségével tudja eljuttatni a NOD32 antivirus system.

Az E-mail riasztás beállításához:

Jelölje be az *„Értesítések küldése SMTP-n keresztül”* opciót!

A *Szerver* mezőben adja meg az SMTP szerver címét!

A *Küldő címe* mezőben lehetősége van megadni a figyelmeztető levél feladóját.

(Például: Számítógép_neve@sicontact.hu)

A *„Vírusriasztások küldése”* mezőben megadott pontosvesszővel elválasztott e-mail címekre fognak a vírusnapló riasztásai eljutni, míg az *„Egyéb riasztások”* mezőben megadott e-mail címekre az eseménynapló riasztásai továbbítódnak.

Helyi hálózaton, Windows Messenger használatával történő riasztáshoz:

Jelölje be a *„Riasztások küldése LAN számítógépre”* opciót!

A megjelenő szövegmezőben ';' (pontosvessző) használatával felsorolhatja azon munkaállomások azonosítóit, melyekre a riasztások továbbítódnak. elküldésre kerülnek. A riasztások ilyen módon történő küldéséhez a hálózaton engedélyezni kell a Windows Messenger szolgáltatást

A *További lehetőségek* részben szereplő változók segítségével személyre szabhatja a riasztási üzenetek formátumát.

7.4.3. Naplókezelés fül

A NOD32 minden, a program működésével kapcsolatos fontosabb eseményről naplóbejegyzést készít. Annak érdekében, hogy az így keletkezett naplók ne legyenek túlságosan nagy terjedelműek, be lehet állítani a naplók élettartamát a *Beállítások* ablak *Naplókezelés fülén*. Az alapbeállított értéket (30 nap) célszerű változatlanul hagyni.

A *Napló élettartama* csoport két jelölőnégyzetet tartalmaz. A felső jelölőnégyzet az általános események (pl. frissítés) és a memóriarezidens víruskereső modul, az AMON bejegyzéseire

szolgál. Az alsó jelölőnégyzet csak a kézzel indítható víruskeresés naplóbejegyzéseire vonatkozik.

A *Naplókezelés csoport* a különböző naplófájlok töredezettségmentesítésére szolgál. Az alapbeállított érték megváltoztatása nem ajánlott.

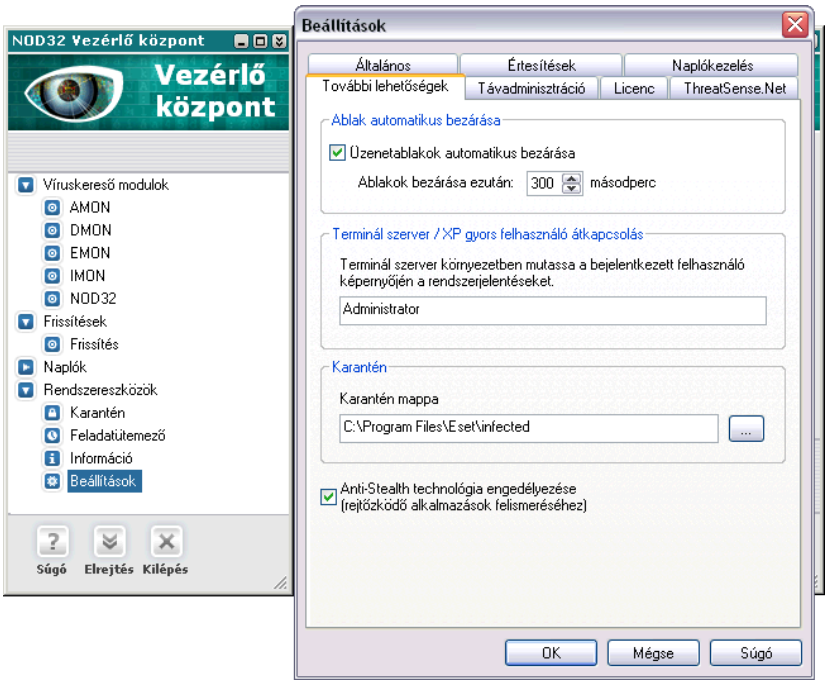
A kézzel indított töredezettségmentesítéshez nyomja meg a *Töredezettségmentesítés* gombot.

7.4.4. További lehetőségek fül

A További lehetőségek fülön a NOD32 Vezérlő központ néhány különleges beállítása érhető el.

Anti-Stealth technológia:
(Lopakodó kártevők – Rootkitek- elleni védelem)

NOD32 2.7-es verziójában megjelent továbbfejlesztett heurisztikus motor lehetővé teszi a rejtőzködő vírusok és kártékony kódok felismerését a fertőzés pillanatában, illetve a fertőzést követően is. A technológia nem igényel felhasználói szakértelmet, egy beállítással engedélyezhető vagy kikapcsolható a NOD32 Vezérlő központjában. Az Anti-Stealth technológia használata ajánlott, segítségével az operációs rendszer megtisztítható az esetleges rejtőzködő kártevőktől. Amennyiben szükséges, kikapcsolásához Válassza a Rendszereszközök panelen a Beállítások gombot, majd a További lehetőségek panelen vegye ki a pipát az opció mellől.



Üzenetablakok automatikus bezárása
Ha automatikusan szeretné az esetleges üzenetablakokat bezárni, válassza ki ezt az opciót és adja meg azt az időtartamot másodpercben, amíg az üzenetablak látható legyen.

Terminál Szerver / XP gyors felhasználó átkapcsolás
A figyelmeztető üzenetek ahhoz a felhasználóhoz kerülnek, akinél a figyelmeztetés keletkezett. Ha egy felhasználó nem azonosítható (pl. ha a figyelmeztető üzenetet maga a rendszer váltotta ki), a szövegmezőben megadott felhasználóhoz fognak továbbítódni az üzenetek.

Karantén mappa
A szövegmezőben a karantén könyvtár helyét tudja módosítani.

7.4.5. Távadminisztráció fül

A különálló, vállalati környezetbe szánt NOD32 Remote Administrator programmal lehetőség van a munkaállomásokat védő NOD32 program példányok távoli menedzselésére. A Távadminisztráció fülön csatlakoztatható a NOD32 egy NOD32 Remote Administrator szerverhez.

A *Szerver címe* mezőben megadhatjuk a központi menedzsment szerver IP címét vagy hálózati azonosítóját. A *http://* előtagot ebben a mezőben ne használja!

7.4.6. Licencek

A NOD32 program bizonyos változatainak (pl: NOD32 for MS-Exchange) működéséhez érvényes licenc kulcs-fájlra van szükség, ezek kezelhetők a Licencek fülön.

7.4.7. ThreatSense.Net

Online kapcsolat a víruslaborral

A ThreatSense.Net Early Warning System lehetővé teszi, hogy a NOD32 program példányok által elfogott eddig ismeretlen kártevők akár teljesen automatizált módon eljussanak az Eset Software víruslaborjába, analizálásra. A technológia fejlesztésénél elsődleges szempont a személyiségi jogok figyelembe vétele volt, tehát a program csak anonim adatokat továbbít. Néhány kivétel adódhat, (például mikor a felhasználó Windowsos felhasználóneve megegyezik valós nevével), azonban ezek az adatok egyik esetben

sem tartalmaznak aggodalomra okot adó információt, csak a kártevők megismerésének célját szolgálják.

A Beállításokról és adatvédelemről a súgóban olvashat bővebben, melyet a „ThreatSense.Net Early Warning System technológiáról és az adatvédelemről bővebben információt itt talál” szövegre kattintással vagy az F1 billentyűvel hívhat elő.

Az Early Warning System oly módon is beállítható, hogy minden egyes küldés előtt engedélyt kérjen, így felülbírálható a kommunikációs folyamat. Az Early Warning System használatával nagyban hozzájárul a kártevők elleni küzdelemhez.

8. NOD32 Használati példák

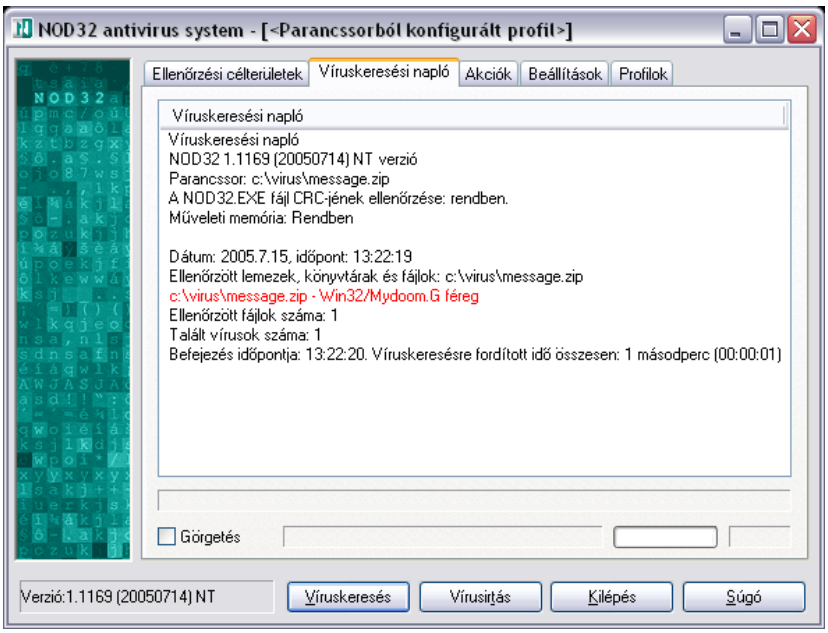
8.1. Példa: Parancssori paraméterek

A példában a NOD32 kiterjesztett heurisztikus keresőmotorjának tesztelését végezzük el parancssori paraméterek segítségével.

Az alábbi példán keresztül szeretnénk bemutatni a parancssori paraméterek használatát. Elmentettük a C: meghajtó Virus alkönyvtárába a Win32/Mydoom.G férget tartalmazó message.zip nevű állományt.

Parancssorból indítva a NOD32 kézi indítású víruskeresőjét, az alábbi képernyőképet kapjuk:

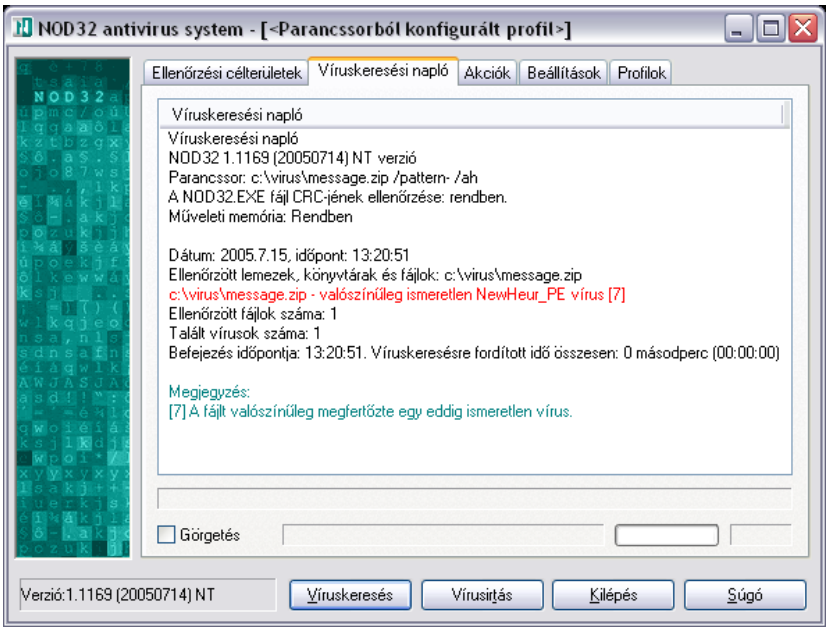
```
nod32.exe c:\virus\message.zip
```



Látható, hogy a NOD32 felismeri a Win32/Mydoom.G férget, ugyanis parancssori paraméterként csak a fájl nevét adtuk meg.

Ha bekapcsoljuk a kiterjesztett heurisztikus keresést (/ah) és letiltjuk a vírusdefiníciós adatbázis használatát (/pattern-), a következő képernyőt kapjuk:

```
nod32.exe c:\virus\message.zip /pattern- /ah
```

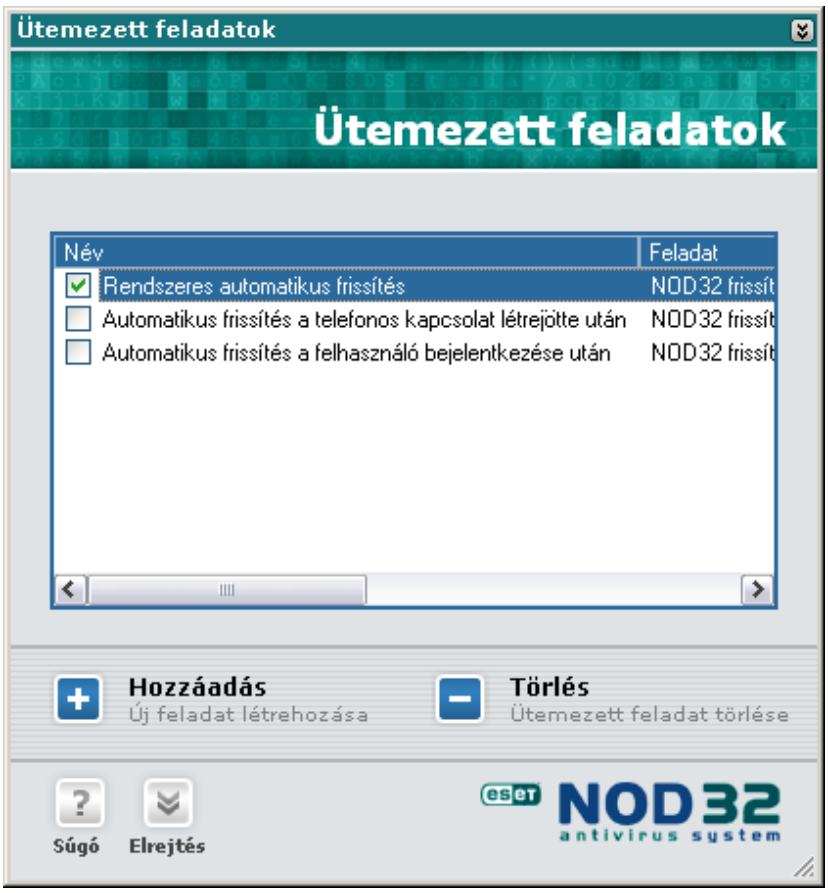


Látható, hogy a NOD32 vírusdefiníciós adatbázisát sikerült kikapcsolnunk a **/pattern-** kapcsoló segítségével, ugyanis a NOD32 így nem tudta a fertőzést teljesen pontosan azonosítani, e helyett a kiterjesztett heurisztika (**/ah** kapcsoló) „valószínűleg ismeretlen NewHeur_PE vírus” néven jelezte.

8.2. Példa: Ütemezés

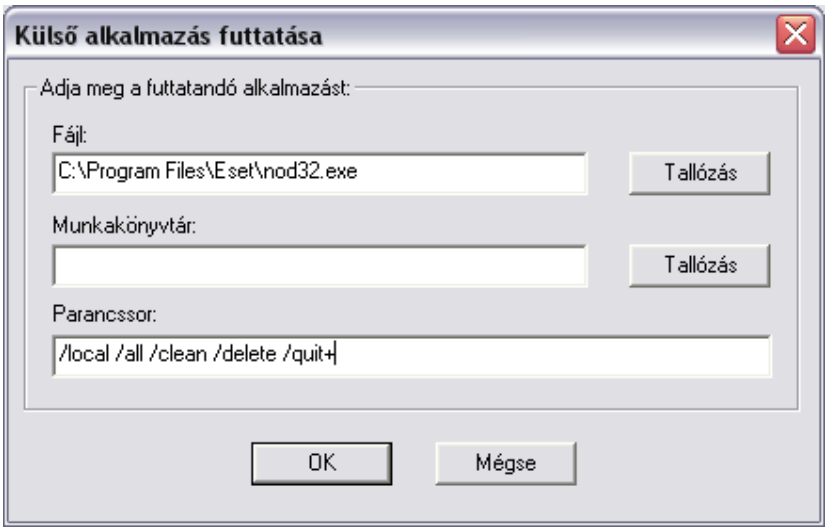
A példában a NOD32 kézi indítású víruskeresőt automatizáljuk az ütemezett feladatok segítségével.

A NOD32 Vezérlő Központ Rendszereszközök csoportjának *Feladatütemező* elemére kattintva a jobb oldalon megjelenik az *„Ütemezett feladatok”* panel.



1. Adjunk hozzá egy új ütemezett feladatot a *Hozzáadás* gombra kattintva!
2. Az előugró ablak legördülő menüjében válasszuk ki a *„NOD32 Kernel – Külső alkalmazás futtatása”* elemet, majd nyomjuk meg a *Tovább* gombot!
3. Adjunk nevet a létrehozandó feladatnak, pl. Vírusirtás!
4. Válasszuk ki, hogy milyen rendszerességgel hajtsa végre a NOD32 az ütemezett feladatot (pl. hetente), majd nyomjuk meg a *Tovább* gombot!
5. Válasszuk ki, a hét mely napjain, illetve milyen időpontban hajtsa végre a program, majd nyomjuk meg a *Tovább* gombot!
6. Válasszuk ki, mi történjen, ha a NOD32 nem tudja végrehajtani a feladatot a megadott időben (pl. *„Hajtsa végre a feladatot az első adandó alkalommal”*), majd nyomjuk meg a *Tovább* gombot!
7. Ellenőrizzük a feladat beállításait, amelyeken a *Vissza* gombok használatával tudunk változtatni. Ha mindent rendben találtunk, nyomjuk meg a *Befejezés* gombot!
8. A futtatandó alkalmazást a *Fájlnál* a *Tallózás* gomb segítségével válasszuk ki. Ez a futtatandó alkalmazás a NOD32 kézi indítású parancssori keresője, a *nod32.exe* legyen!

9. Adjuk meg a parancssori paramétereket: */local /all /clean /delete /quit+* (a NOD32 vizsgáljon meg minden fájlt a helyi lemezeken, tisztítsa meg a fertőzött fájlokat, illetve nem irtható fertőzések esetén törölje a fájlt, majd lépjen ki az alkalmazásból a vírusirtás befejezése után)



Nyomjuk meg az *OK* gombot a feladat hozzáadásának befejezéséhez!

Az így létrejött feladatot az ütemező a kiválasztott időpontokban, a megadott paraméterekkel fogja lefuttatni, így a példa esetében a NOD32 minden héten, minden merevlemezt végig fog ellenőrizni.

9. További információk

A NOD32 antivirus system további dokumentációi, kézikönyvei és hasznos segédletei találhatók magyar és angol nyelven a ***www.nod32.hu*** *honlapon, illetve angolul a* ***www.nod32.com*** *címen.*

A felmerülő kérdéseivel kérjük, forduljon bizalommal kollégáinkhoz, technikai kérdésekben a support@sicontact.hu, minden más kérdésben pedig az info@sicontact.hu e-mail címen várjuk leveleiket!