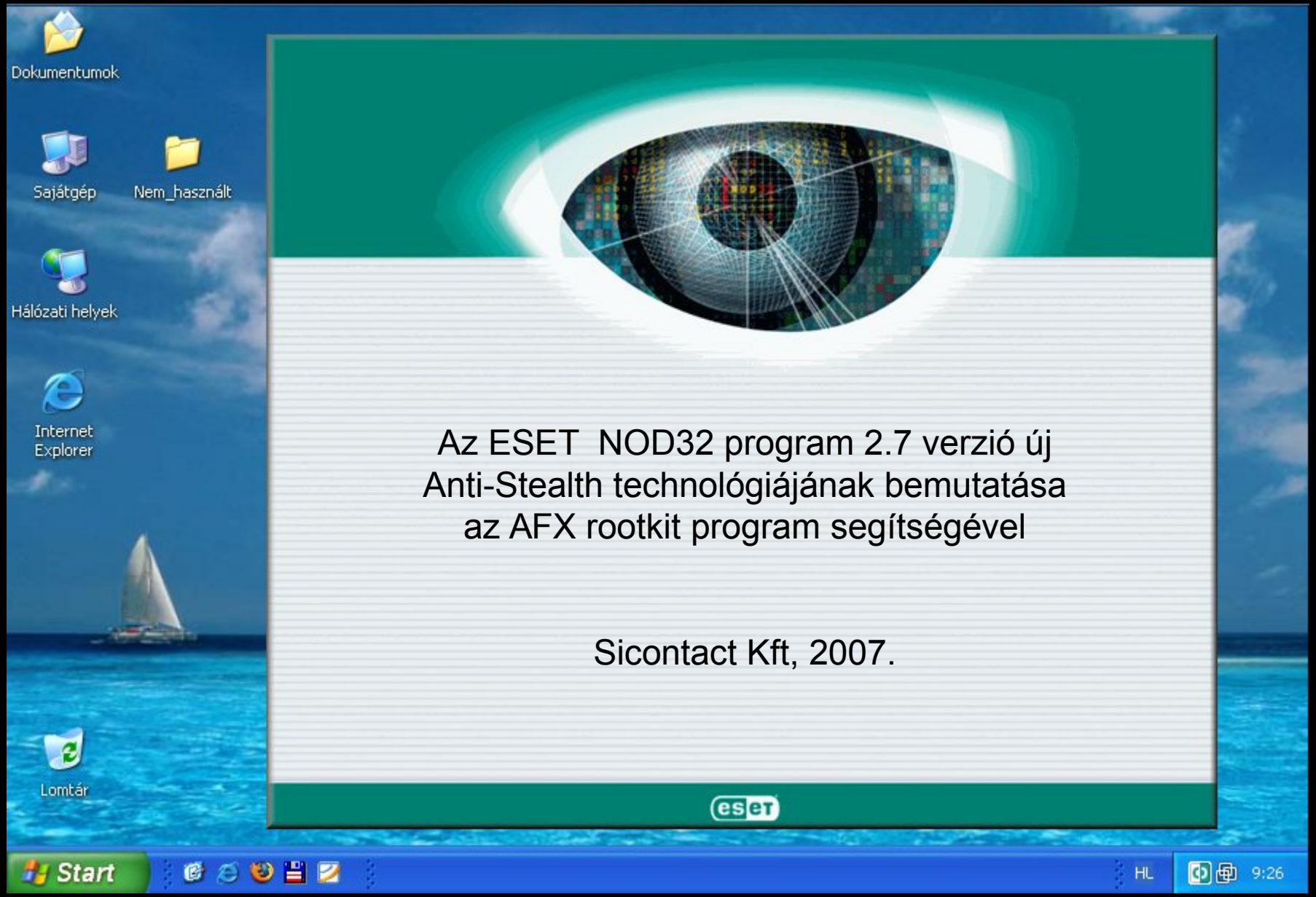

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Az ESET NOD32 program 2.7 verzió új
Anti-Stealth technológiájának bemutatása
az AFX rootkit program segítségével
Sicontact Kft, 2007.
eset
Start
HL
9:26

Előadás vázlat

Telepítjük a NOD32 2.7-es változatát
Normál körülmények között a valósidejű védelem már a 2.5-ös verzió óta képes észlelni a rootkiteket, még mielőtt azok települhetnének.

Kikapcsoljuk a valósidejű védelmet, majd feltelepítünk egy rootkitet, melynek segítségével különféle állományokat rejtünk el.

Lefuttatjuk a NOD32 kézzel indítható víruskeresőjét az Anti-Stealth funkció nélkül, és megnézzük látja-e a rootkitet.

A NOD32 nem veszi észre a már feltelepült rootkitet, és az általa elrejtett fájlokat sem látja.

Visszakapcsoljuk az Anti-Stealth funkciót az aktív rootkites környezetben.

Újból elindítunk egy kézi víruskeresést a rendszeren.

A NOD32 most már megtalálja a rootkitet, valamint minden általa elrejtett állományt, és sikeresen képes tőlük megtisztítani a rendszert.

Fontos megjegyzések

Amit ebben a bemutatóban láthatunk, az a NOD32 2.7 verziójában debütáló új Anti-Stealth technológia. Demonstrálni szeretnénk, hogy a NOD32 már aktív rootkitek ellen is hatékony védelmet nyújt.

Rootkitnek az Interneten szabadon elérhető AFX Rootkit 2005 nevű csomagot töltöttük le, és azzel végeztük a kísérletet.

Az AFX igen elterjedt rootkit - köszönhetően a szabadon hozzáférhető nyílt forráskódjának. Az AFX a "KERNEL32.DLL" függvénykönyvtár átirányításával és foltozásával (kernel32.dll hooking and patching) manipulálja a rendszert.

Ezt a tesztet egy biztonsági szakértő hajtotta végre, szigorúan ellenőrzött körülmények között. Bár hiszünk benne, hogy a NOD32 2.7 a lehetséges legjobb védelmet kínálja a különféle digitális fenyegetések ellen, mégis határozattan azt tanácsoljuk, hogy a kísérletet semmiképpen ne próbálják ki otthoni körülmények között!

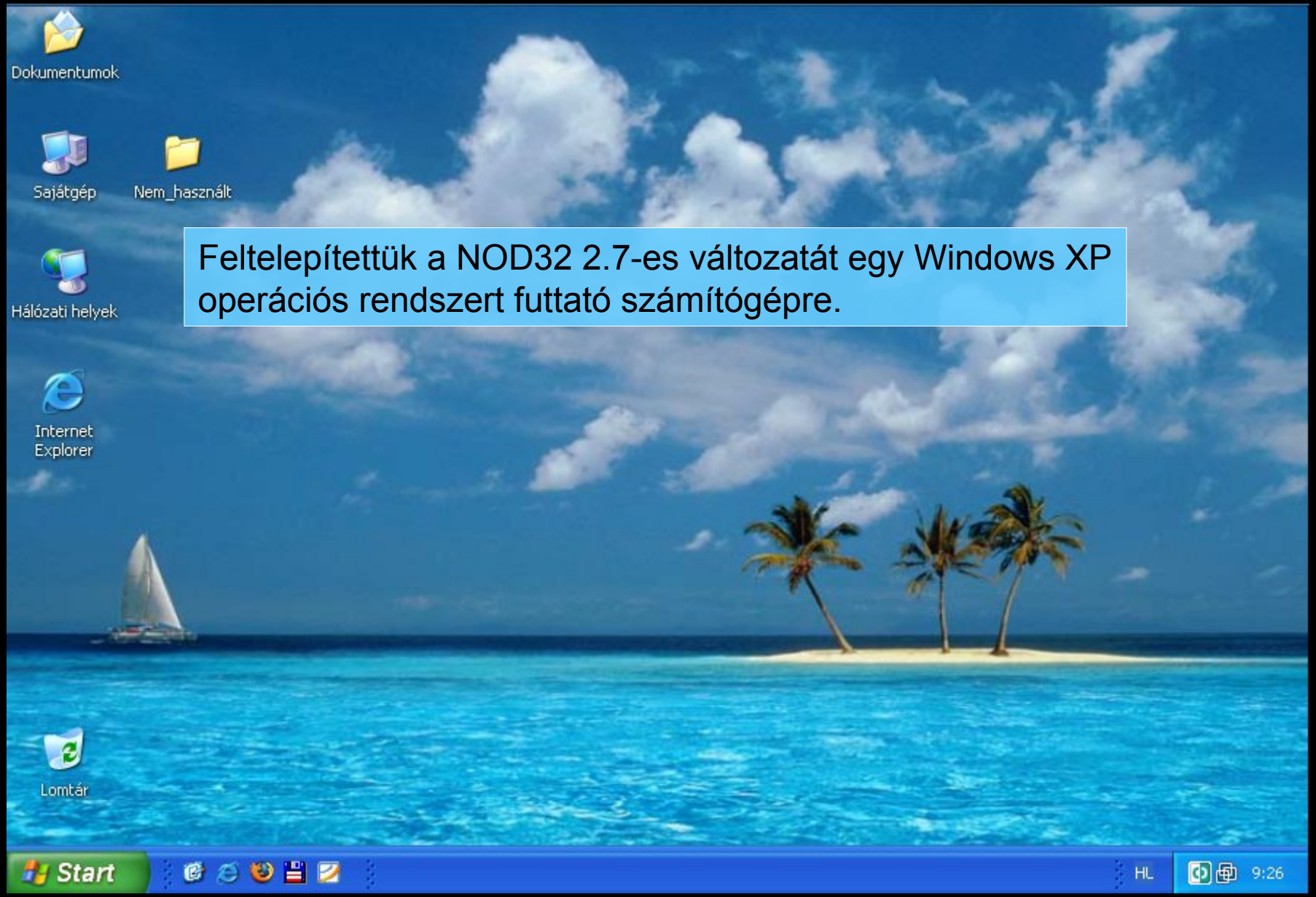
A használt állományok:

"root.exe„	- Az AFX főprogramja
"hook.dll„	- Az AFX telepítése után hozza létre ezt a dinamikus könyvtár fájlt

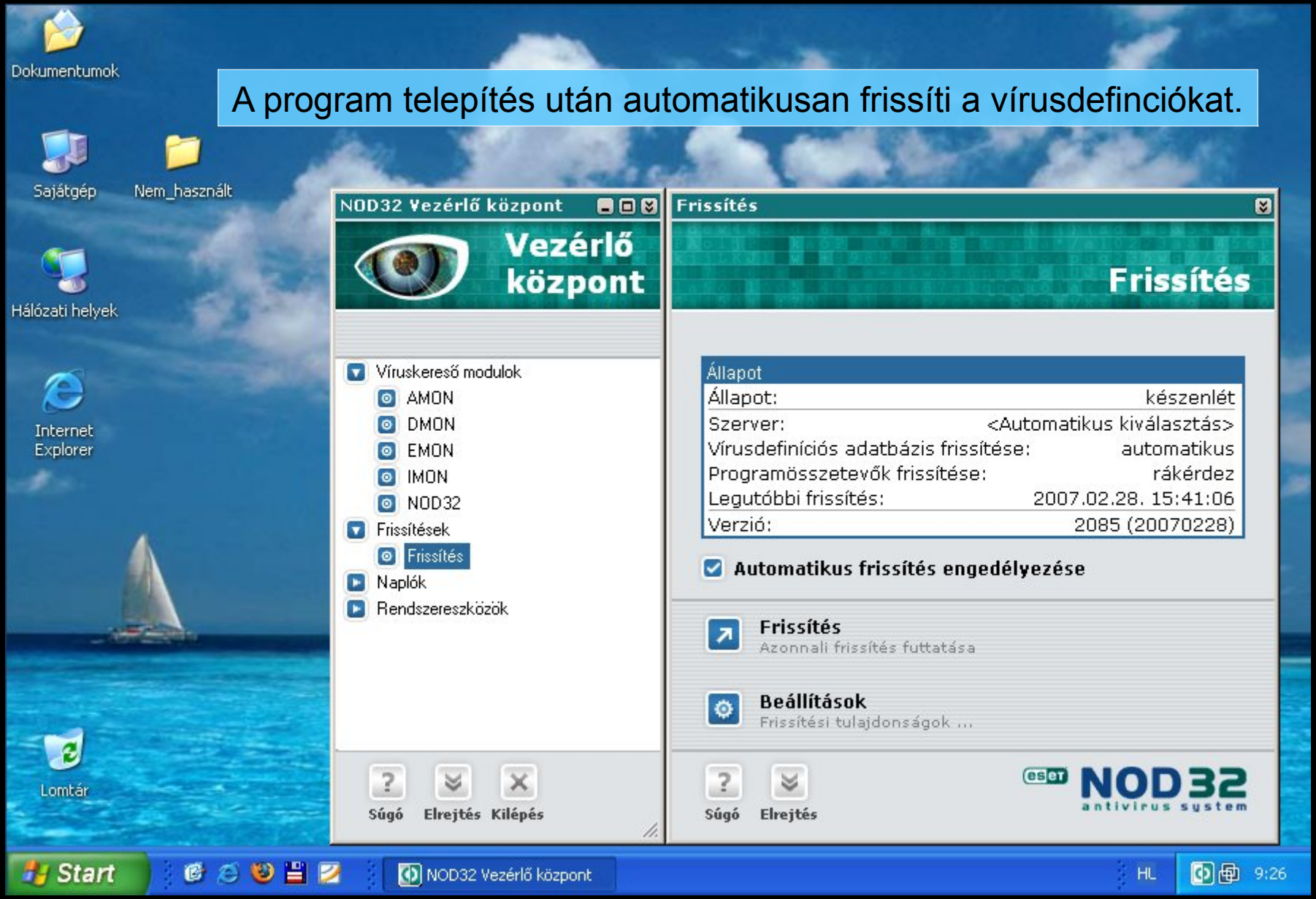
A rootkiteket leggyakrabban pontosan arra használják, hogy segítségükkel különféle eljárásokat, program állományokat álcázzanak.

eset

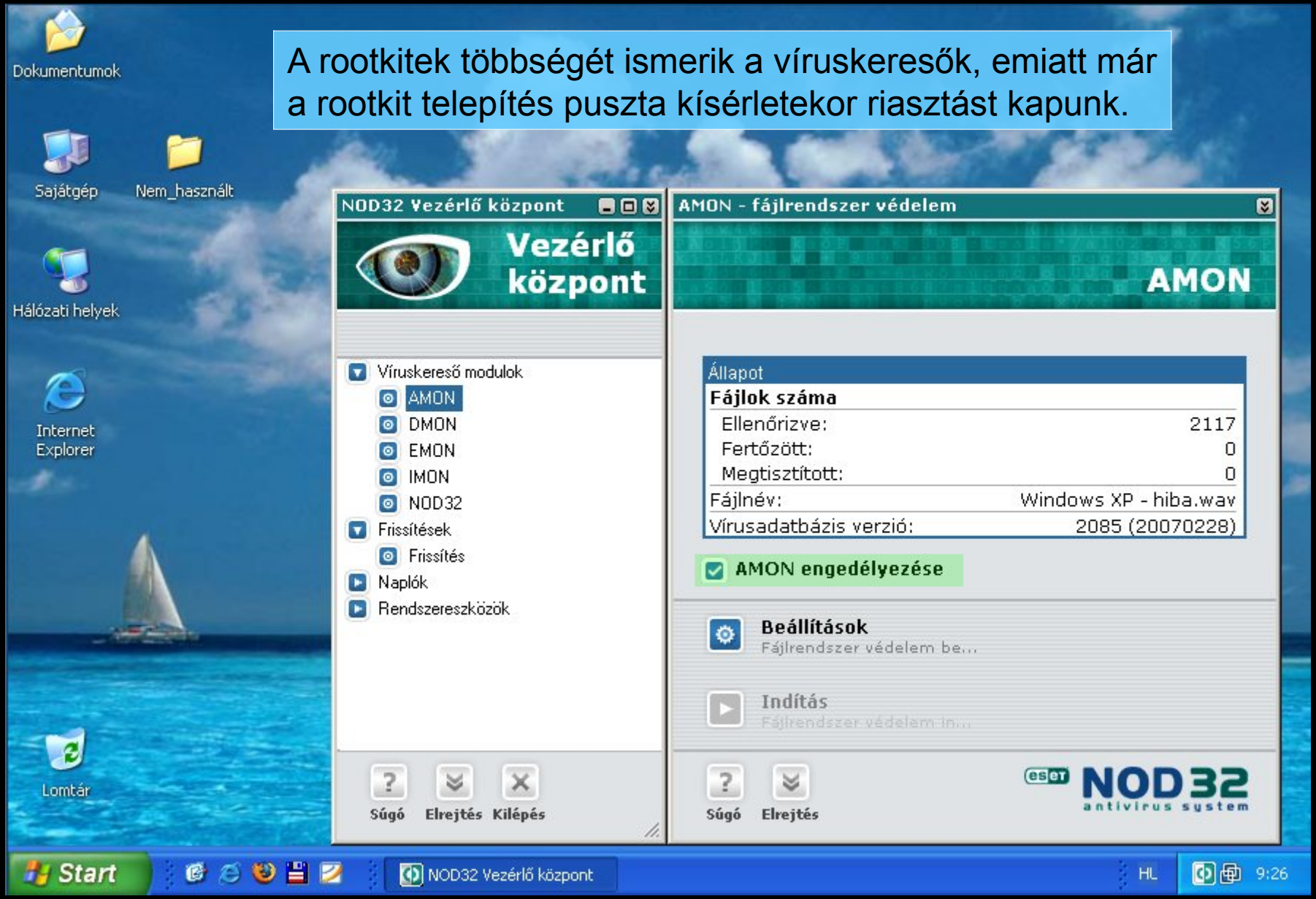
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Start
HL
9:26

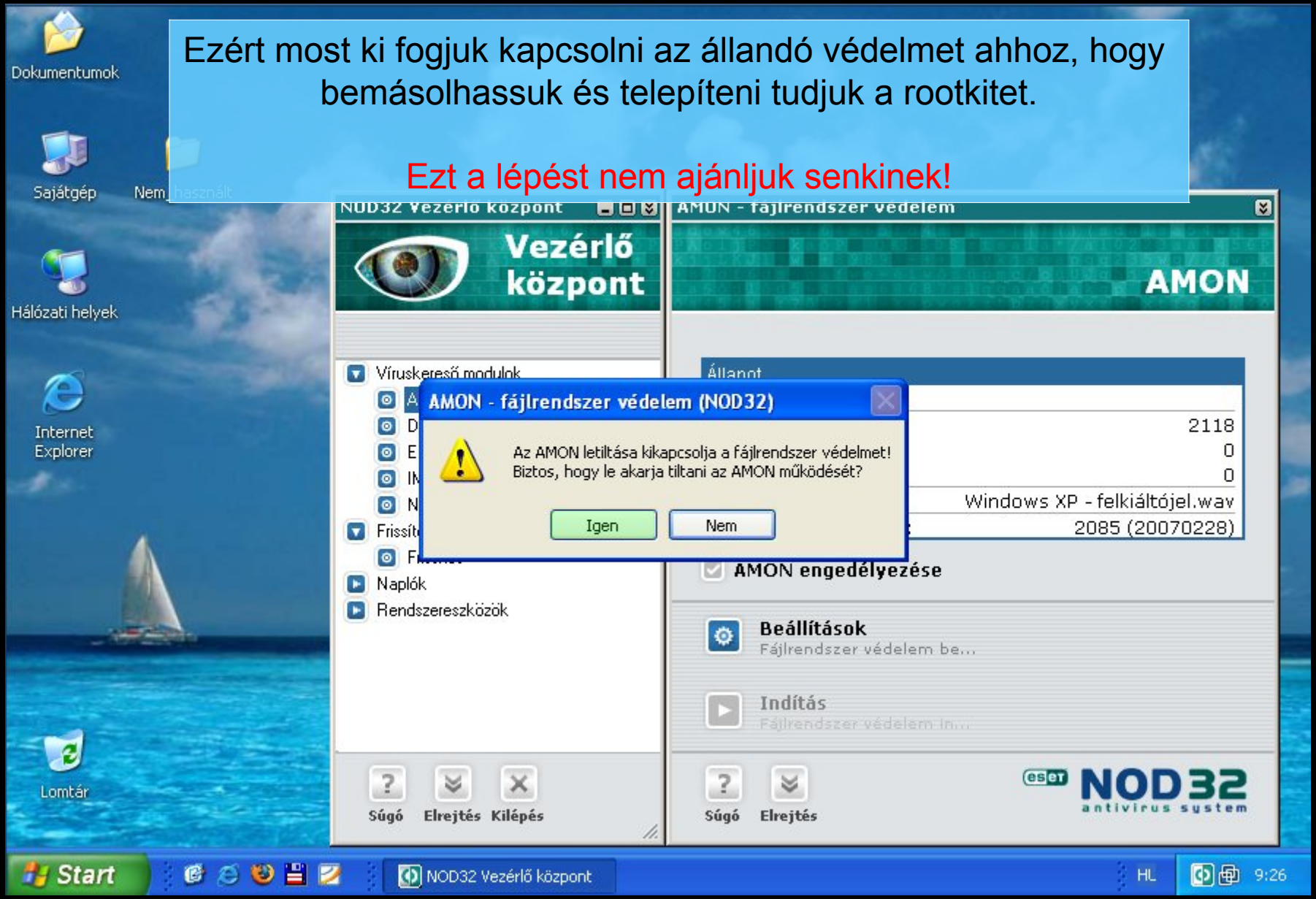


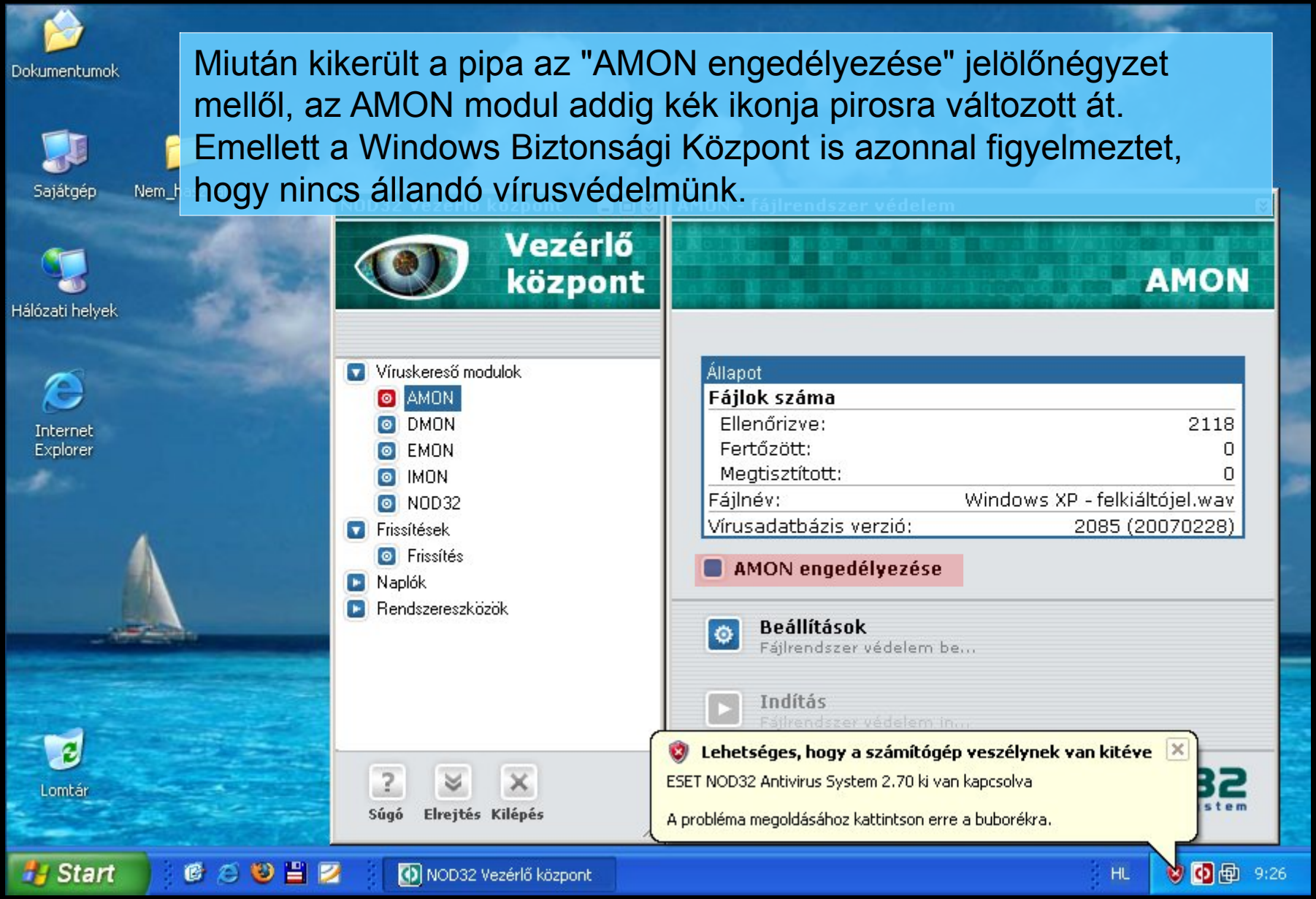
Feltelepítettük a NOD32 2.7-es változatát egy Windows XP operációs rendszert futtató számítógépre.

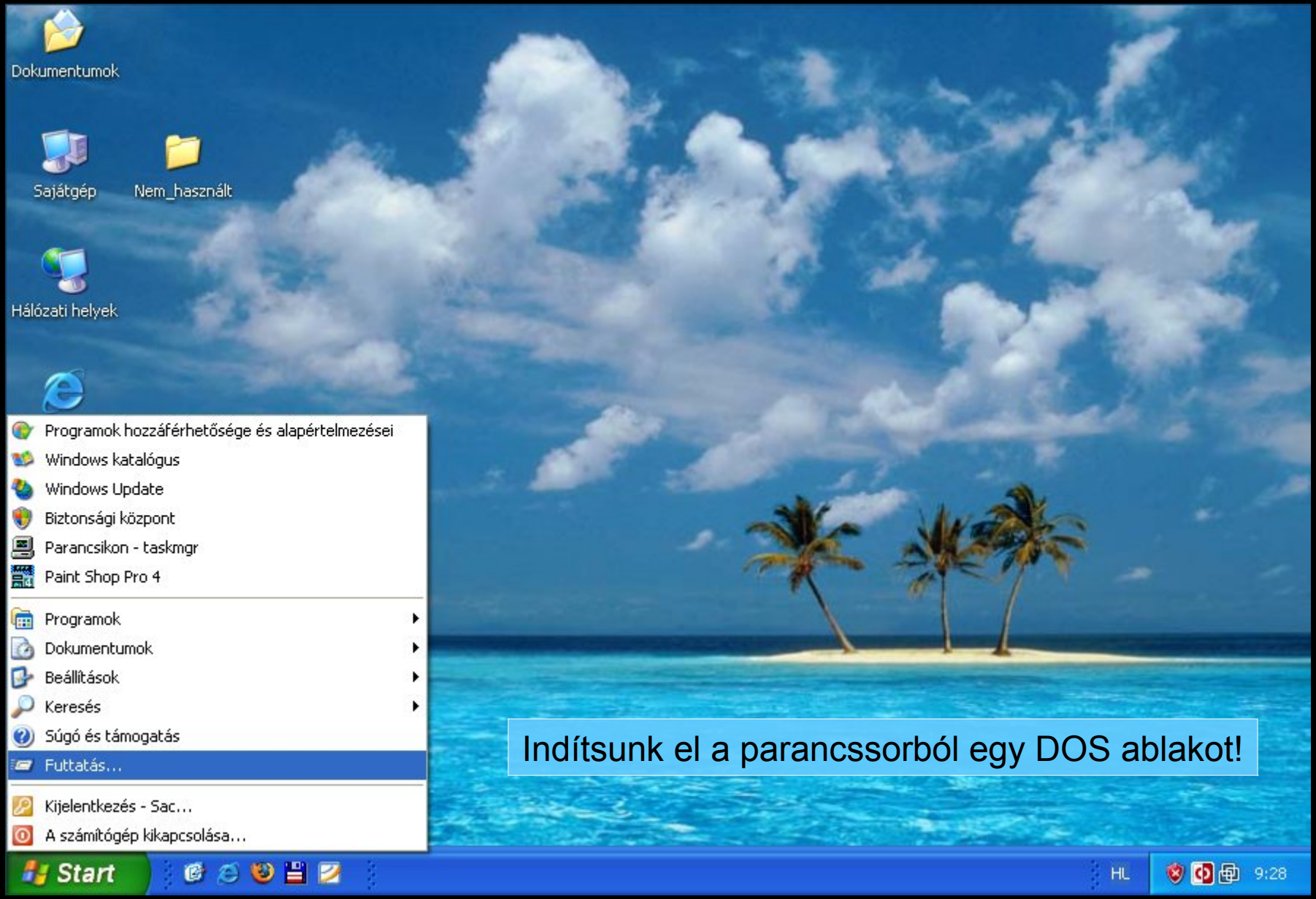

A program telepítés után automatikusan frissíti a vírusdefinciókat.
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Súgó
Elrejtés
Kilépés
Frissítés
Frissítés
Állapot
Állapot: készenlét
Szerver: <Automatikus kiválasztás>
Vírusdefiníciós adatbázis frissítése: automatikus
Programösszetevők frissítése: rákérdez
Legutóbbi frissítés: 2007.02.28. 15:41:06
Verzió: 2085 (20070228)
Automatikus frissítés engedélyezése
Frissítés
Azonnali frissítés futtatása
Beállítások
Frissítési tulajdonságok ...
Súgó
Elrejtés
eset NOD32 antivirus system
Start
NOD32 Vezérlő központ
HL
9:26

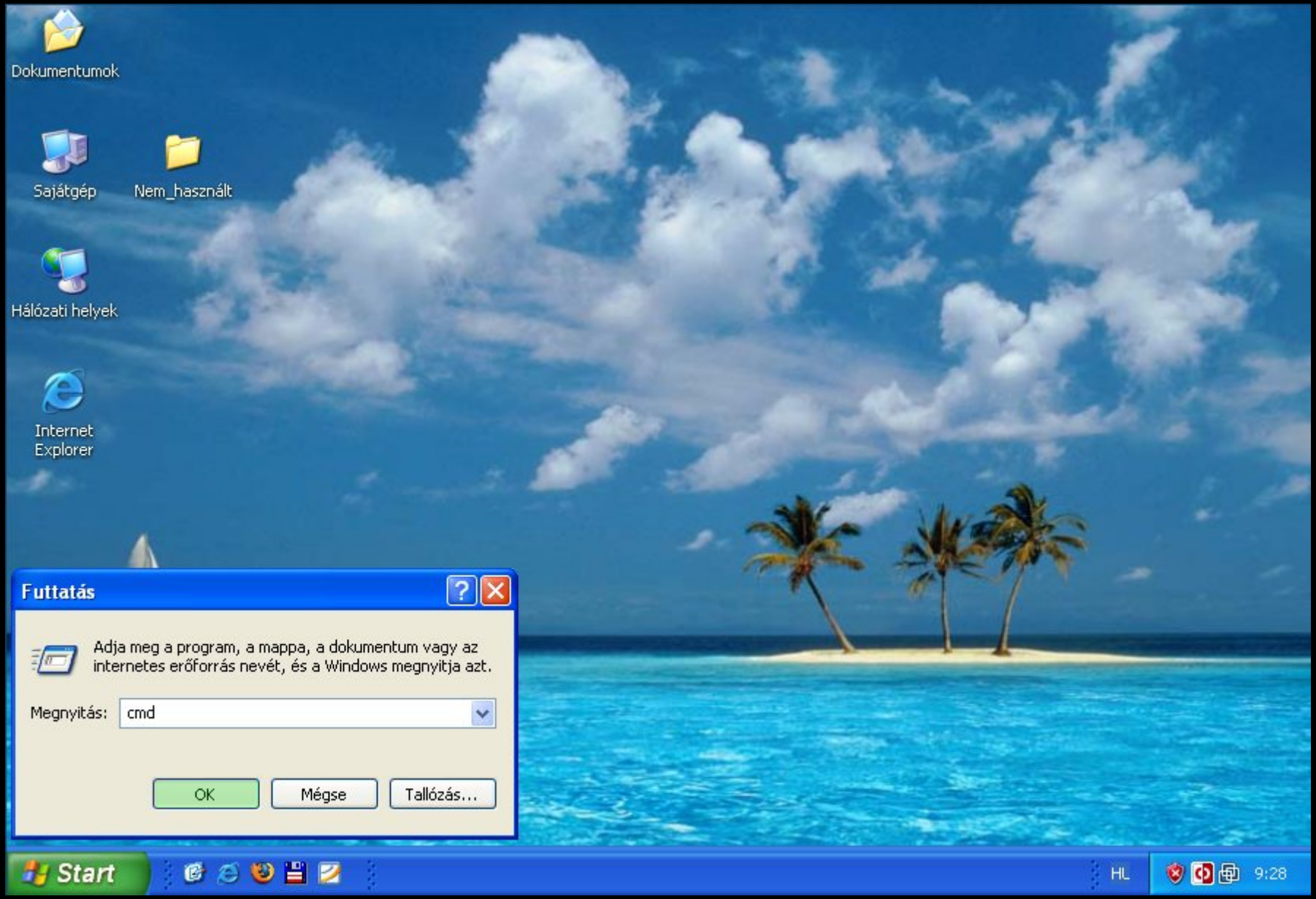
A rootkitek többségét ismerik a víruskeresők, emiatt már a rootkit telepítés puszta kísérletekor riasztást kapunk.

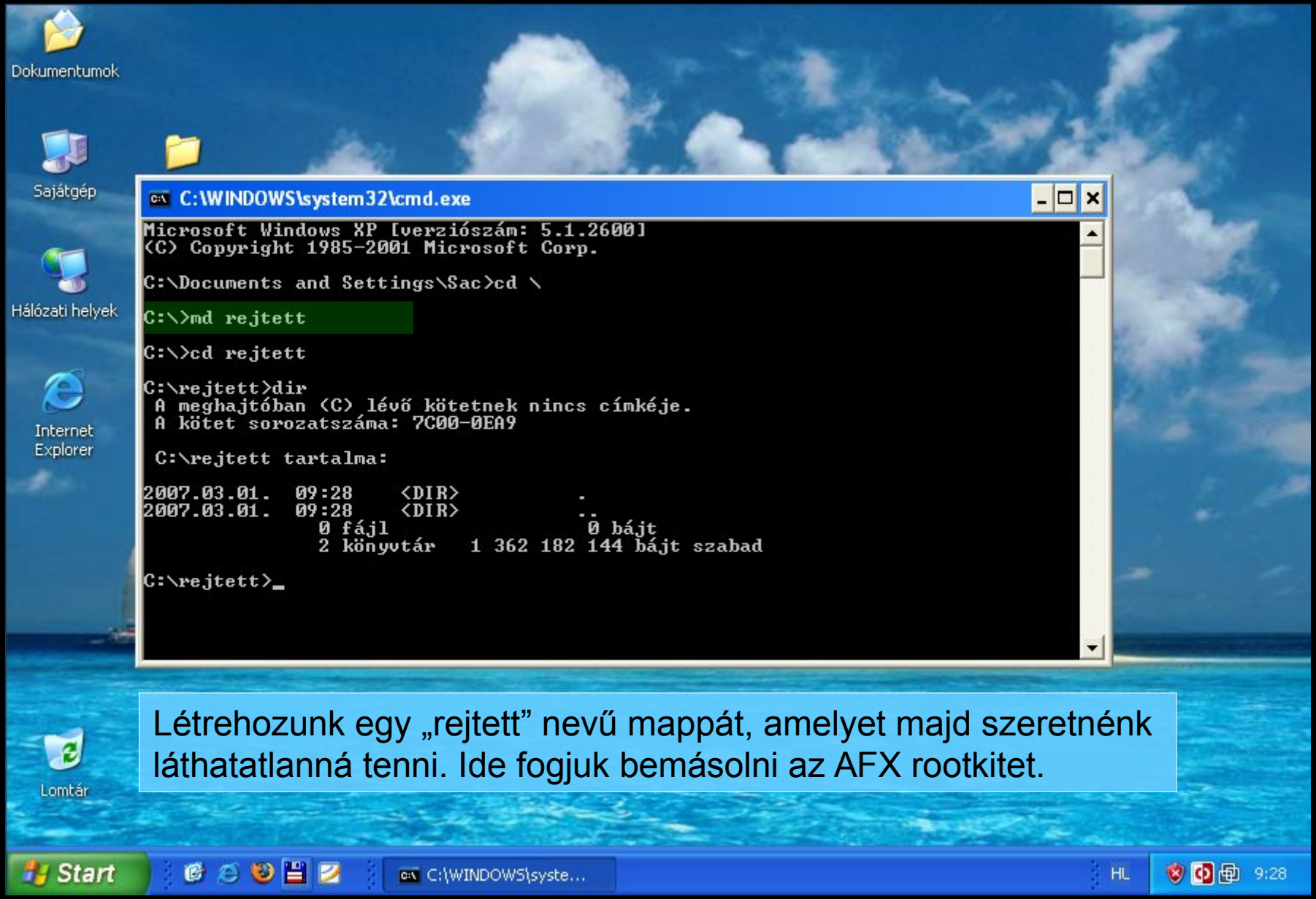



Ezért most ki fogjuk kapcsolni az állandó védelmet ahhoz, hogy bemásolhassuk és telepíteni tudjuk a rootkitet.
Ezt a lépést nem ajánljuk senkinek!
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
Frissítés
Naplók
Rendszereszközök
Súgó
Elrejtés
Kilépés
AMON - fájlrendszer védelem
AMON
Állapot
2118
0
0
Windows XP - felkiáltójel.wav
2085 (20070228)
AMON engedélyezése
Beállítások
Fájlrendszer védelem be...
Indítás
Fájlrendszer védelem in...
Súgó
Elrejtés
eset NOD32 antivirus system
AMON - fájlrendszer védelem (NOD32)
Az AMON letiltása kikapcsolja a fájlrendszer védelmet!
Biztos, hogy le akarja tiltani az AMON működését?
Igen
Nem
Start
NOD32 Vezérlő központ
HL
9:26

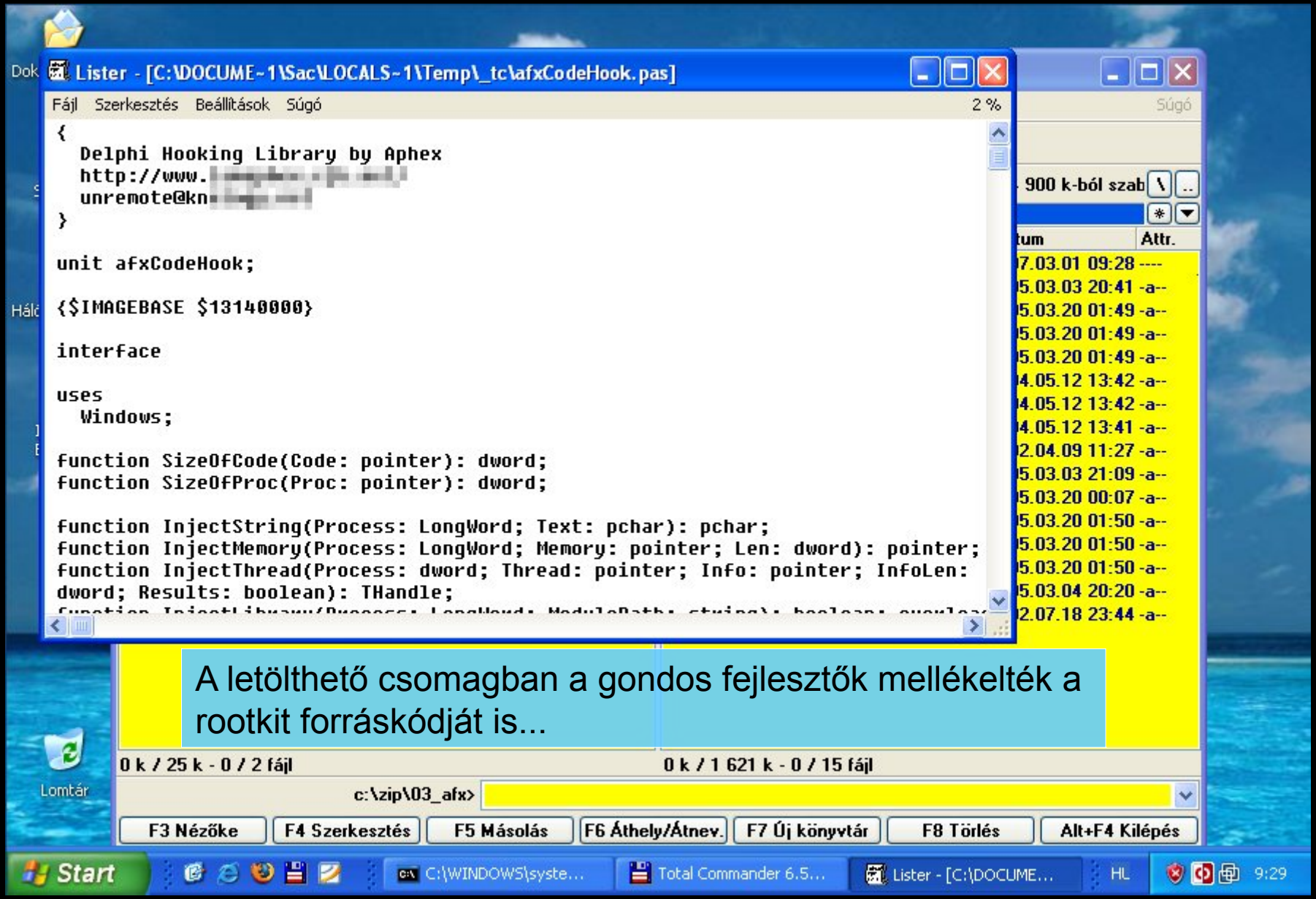

Miután kikerült a pipa az "AMON engedélyezése" jelölőnégyzet mellől, az AMON modul addig kék ikonja pirosra változott át. Emellett a Windows Biztonsági Központ is azonnal figyelmeztet, hogy nincs állandó vírusvédelmünk.
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Vezérlő központ
AMON
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Állapot
Fájlok száma
Ellenőrizve: 2118
Fertőzött: 0
Megtisztított: 0
Fájlnév: Windows XP - felkiáltójel.wav
Vírusadatbázis verzió: 2085 (20070228)
AMON engedélyezése
Beállítások
Fájlrendszer védelem be...
Indítás
Súgó
Elrejtés
Kilépés
Lehetséges, hogy a számítógép veszélynek van kitéve
ESET NOD32 Antivirus System 2.70 ki van kapcsolva
A probléma megoldásához kattintson erre a buborékra.
Start
NOD32 Vezérlő központ
HL
9:26

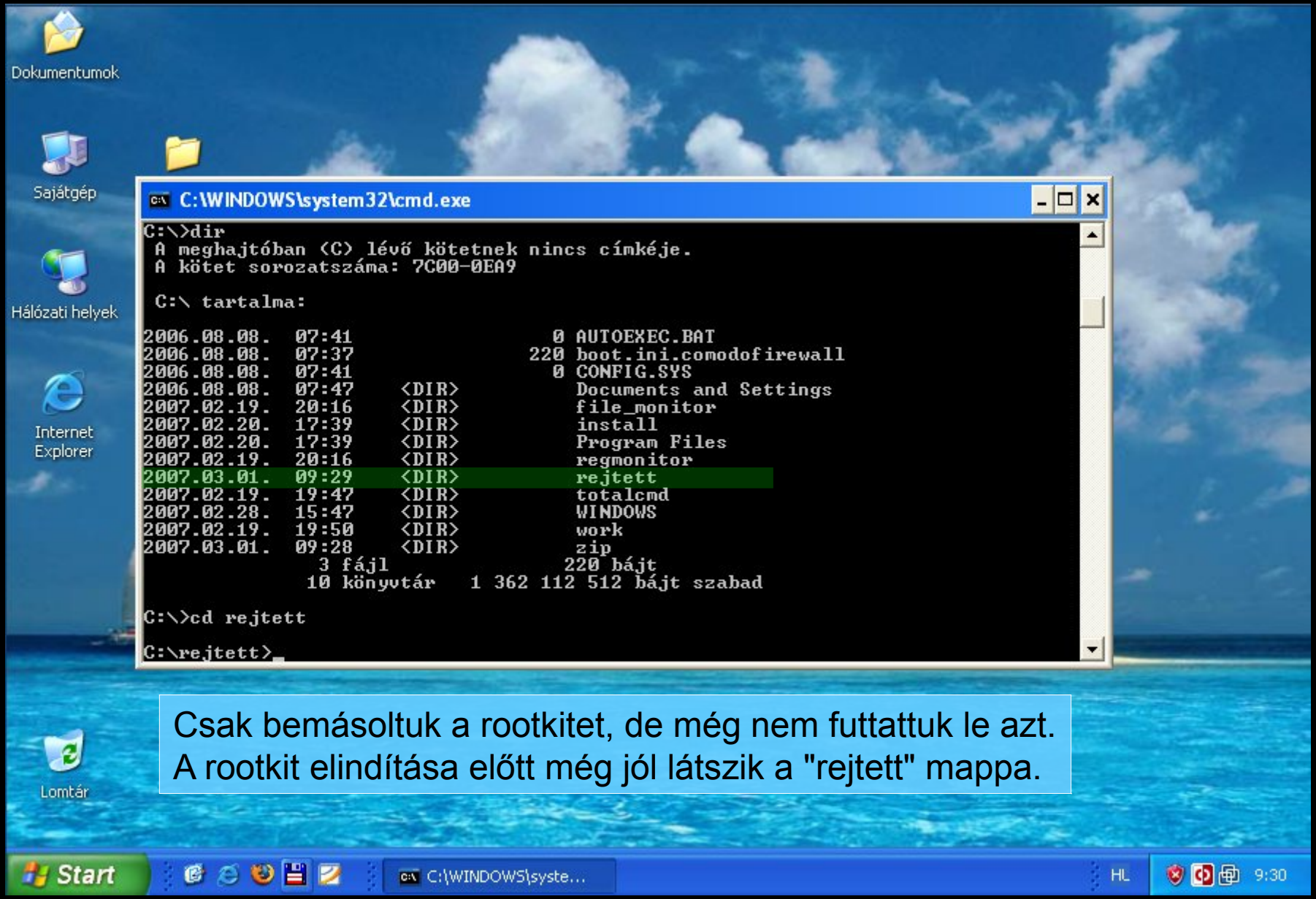

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Programok hozzáférhetősége és alapértelmezései
Windows katalógus
Windows Update
Biztonsági központ
Parancsikon - taskmgr
Paint Shop Pro 4
Programok
Dokumentumok
Beállítások
Keresés
Súgó és támogatás
Futtatás...
Kijelentkezés - Sac...
A számítógép kikapcsolása...
Start
HL
9:28
Indítsunk el a parancssorból egy DOS ablakot!

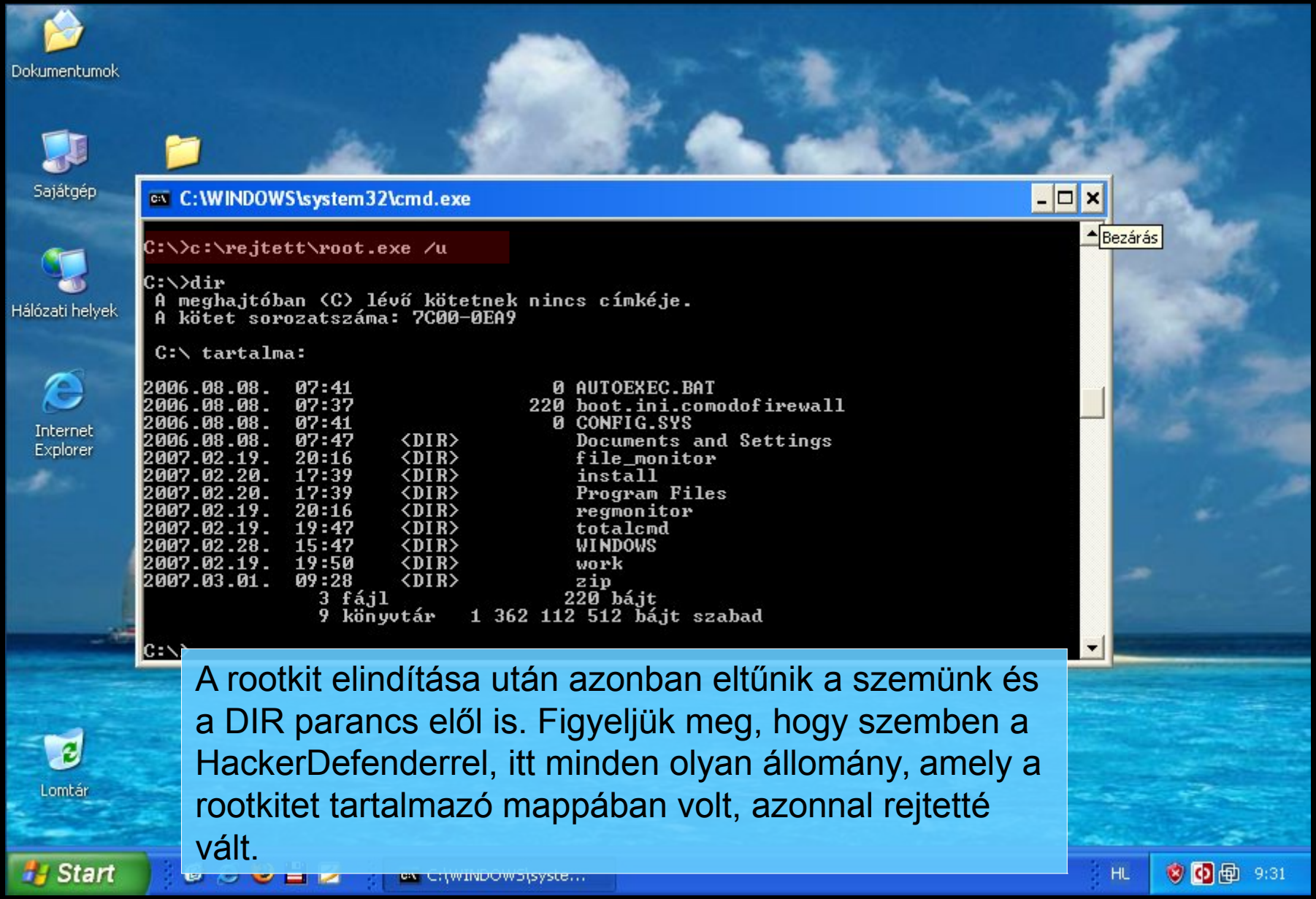

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Futtatás
Adja meg a program, a mappa, a dokumentum vagy az internetes erőforrás nevét, és a Windows megnyitja azt.
Megnyitás:
cmd
OK
Mégse
Tallózás...
Start
HL
9:28

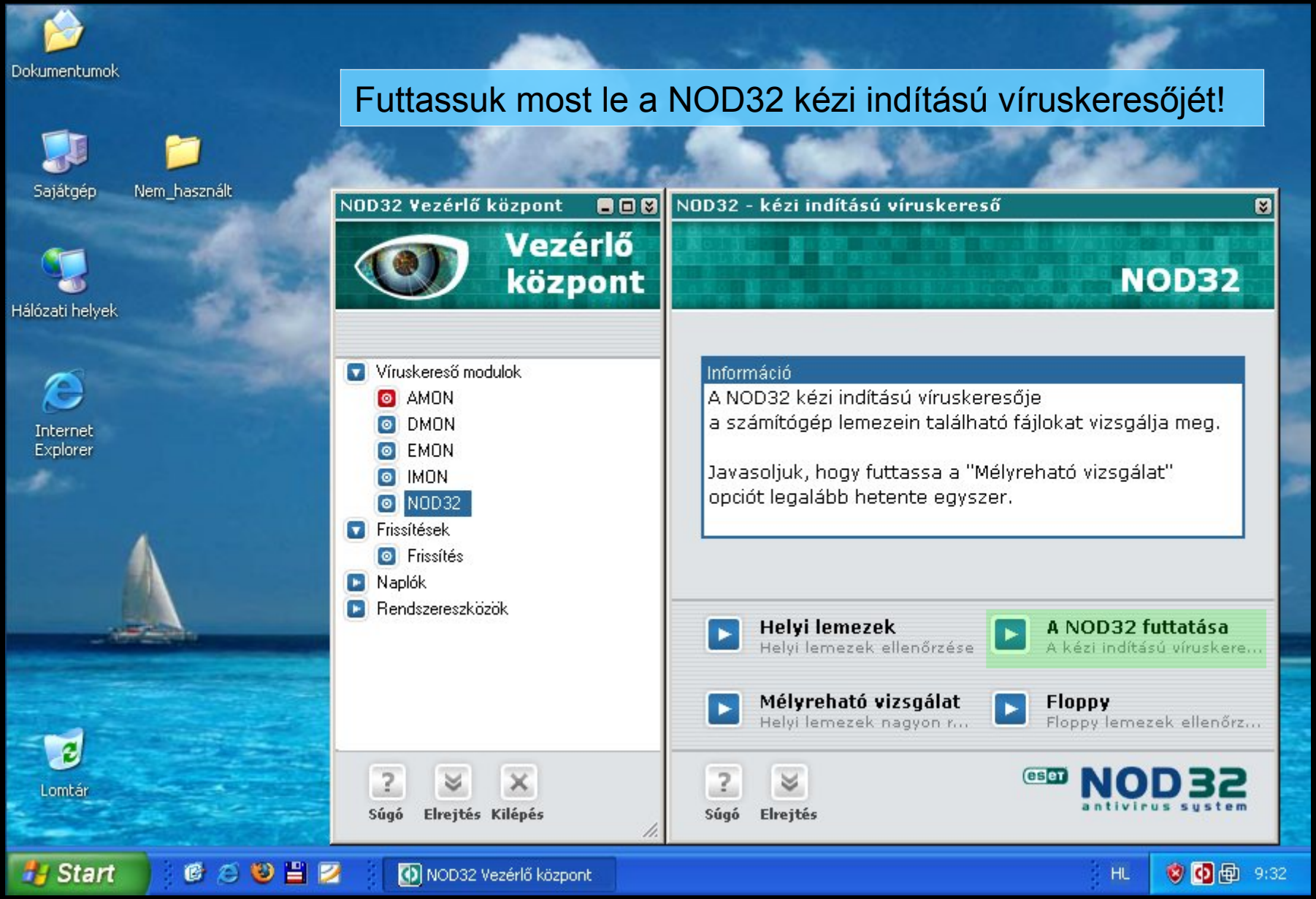


Létrehozunk egy „rejtett” nevű mappát, amelyet majd szeretnénk láthatatlanná tenni. Ide fogjuk bemásolni az AFX rootkitet.

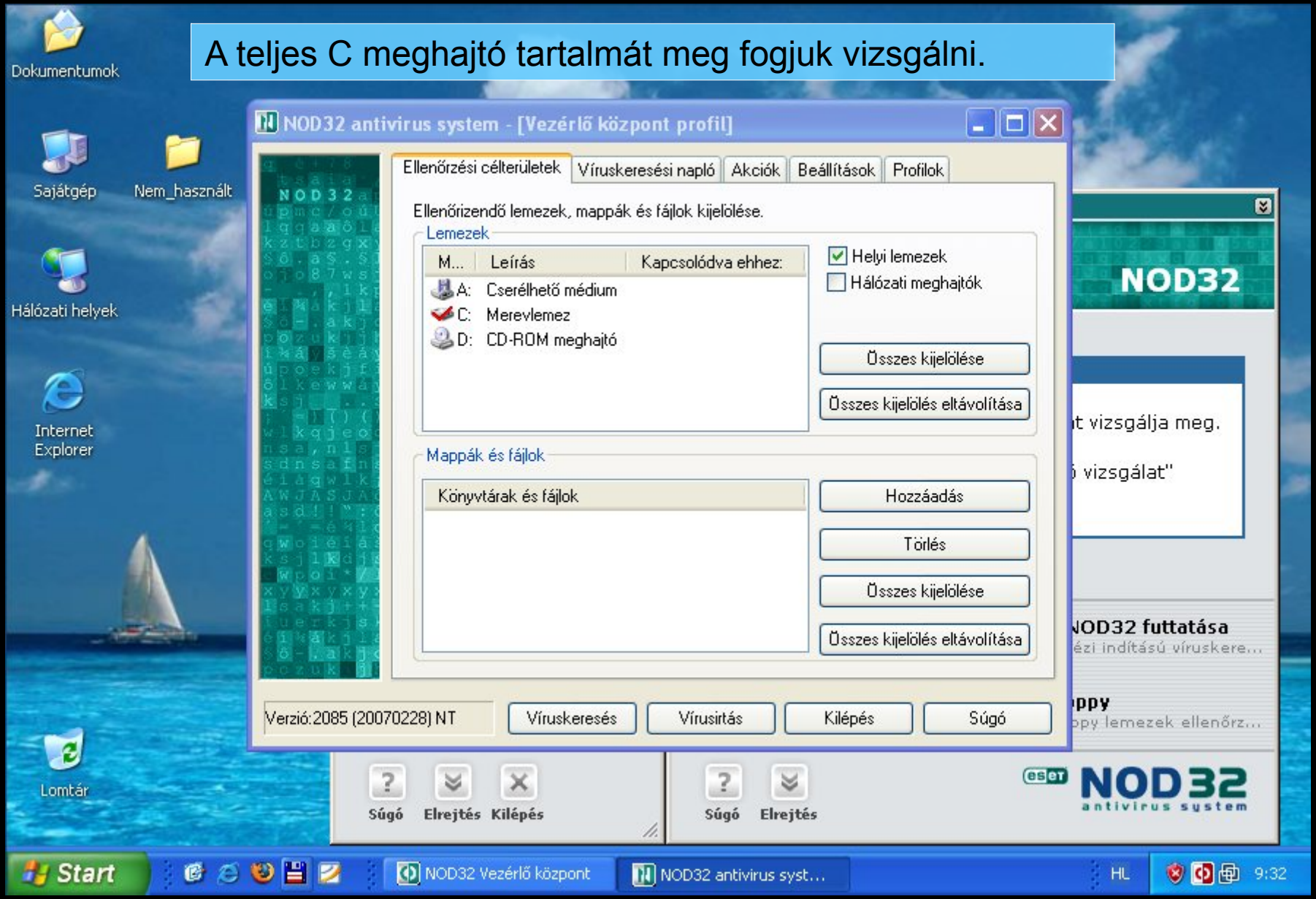

Lister - [C:\DOCUME~1\Sac\LOCALS~1\Temp_tc\afxCodeHook.pas]
Fájl Szerkesztés Beállítások Súgó 2 %
{
Delphi Hooking Library by Aphex
http://www.
unremote@kn
}
unit afxCodeHook;
{$IMAGEBASE $13140000}
interface
uses
Windows;
function SizeOfCode(Code: pointer): dword;
function SizeOfProc(Proc: pointer): dword;
function InjectString(Process: LongWord; Text: pchar): pchar;
function InjectMemory(Process: LongWord; Memory: pointer; Len: dword): pointer;
function InjectThread(Process: dword; Thread: pointer; Info: pointer; InfoLen:
dword; Results: boolean): THandle;
A letölthető csomagban a gondos fejlesztők mellékelték a rootkit forráskódját is...
0 k / 25 k - 0 / 2 fájl
0 k / 1 621 k - 0 / 15 fájl
c:\zip\03_afx>
F3 Nézőke
F4 Szerkesztés
F5 Másolás
F6 Áthely/Átnev.
F7 Új könyvtár
F8 Törlés
Alt+F4 Kilépés
Start
Total Commander 6.5...
Lister - [C:\DOCUME...
9:29


Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
C:\WINDOWS\system32\cmd.exe
C:\>dir
A meghajtóban (C) lévő kötetnek nincs címkéje.
A kötet sorozatszáma: 7C00-0EA9
C:\ tartalma:
2006.08.08. 07:41 0 AUTOEXEC.BAT
2006.08.08. 07:37 220 boot.ini.comodofirewall
2006.08.08. 07:41 0 CONFIG.SYS
2006.08.08. 07:47 <DIR> Documents and Settings
2007.02.19. 20:16 <DIR> file_monitor
2007.02.20. 17:39 <DIR> install
2007.02.20. 17:39 <DIR> Program Files
2007.02.19. 20:16 <DIR> regmonitor
2007.03.01. 09:29 <DIR> rejtett
2007.02.19. 19:47 <DIR> totalcmd
2007.02.28. 15:47 <DIR> WINDOWS
2007.02.19. 19:50 <DIR> work
2007.03.01. 09:28 <DIR> zip
3 fájl 220 bájt
10 könyvtár 1 362 112 512 bájt szabad
C:\>cd rejtett
C:\rejtett>
Csak bemásoltuk a rootkitet, de még nem futtattuk le azt.
A rootkit elindítása előtt még jól látszik a "rejtett" mappa.
Start
C:\WINDOWS\syste...
HL
9:30

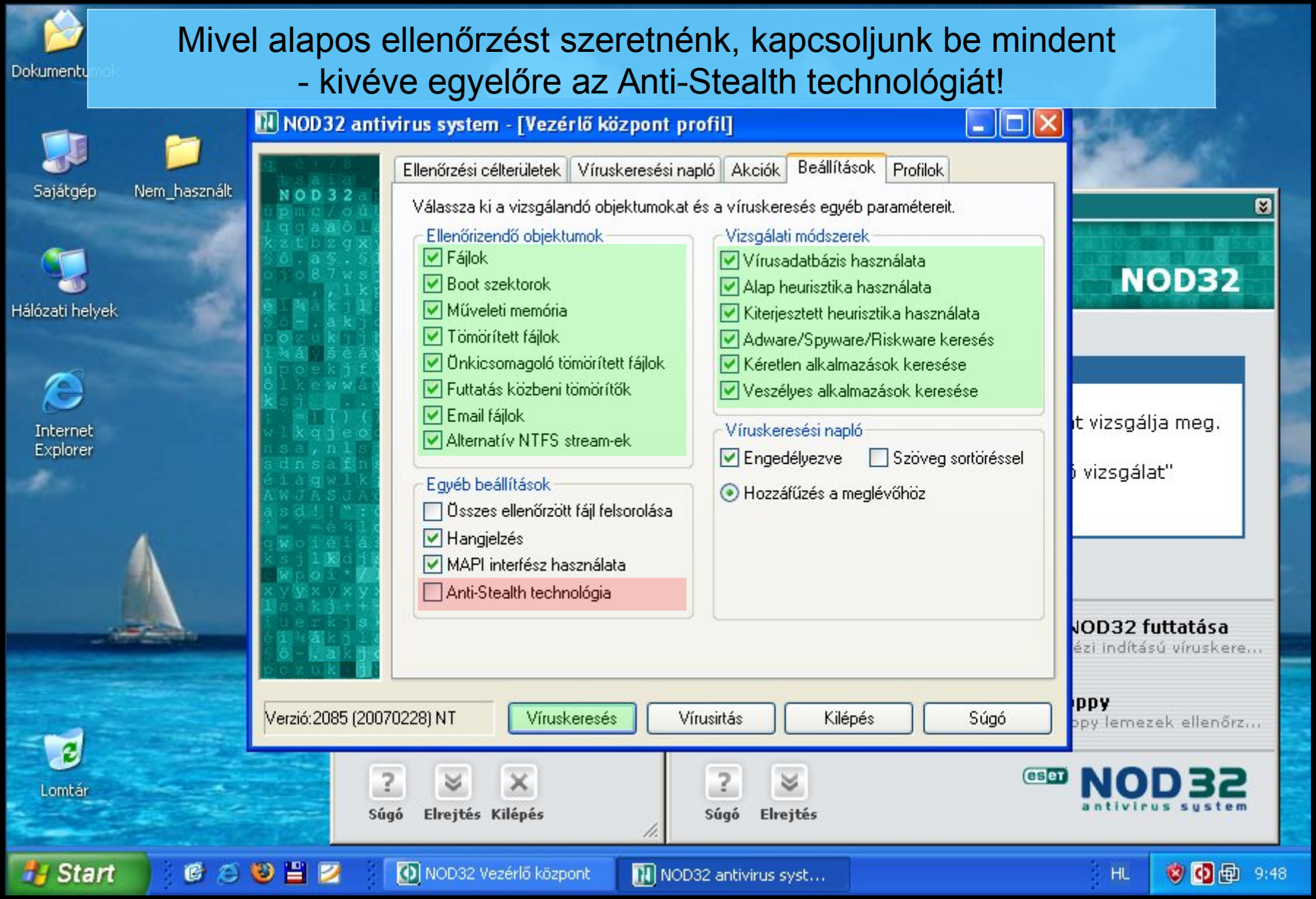

Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
C:\WINDOWS\system32\cmd.exe
Bezárás
C:\>c:\rejtett\root.exe /u
C:\>dir
A meghajtóban (C) lévő kötetnek nincs címkéje.
A kötet sorozatszáma: 7C00-0EA9
C:\ tartalma:
2006.08.08. 07:41 0 AUTOEXEC.BAT
2006.08.08. 07:37 220 boot.ini.comodofirewall
2006.08.08. 07:41 0 CONFIG.SYS
2006.08.08. 07:47 <DIR> Documents and Settings
2007.02.19. 20:16 <DIR> file_monitor
2007.02.20. 17:39 <DIR> install
2007.02.20. 17:39 <DIR> Program Files
2007.02.19. 20:16 <DIR> regmonitor
2007.02.19. 19:47 <DIR> totalcmd
2007.02.28. 15:47 <DIR> WINDOWS
2007.02.19. 19:50 <DIR> work
2007.03.01. 09:28 <DIR> zip
3 fájl 220 bájt
9 könyvtár 1 362 112 512 bájt szabad
C:\
A rootkit elindítása után azonban eltűnik a szemünk és a DIR parancs elől is. Figyeljük meg, hogy szemben a HackerDefenderrel, itt minden olyan állomány, amely a rootkitet tartalmazó mappában volt, azonnal rejtetté vált.
Start
HL
9:31

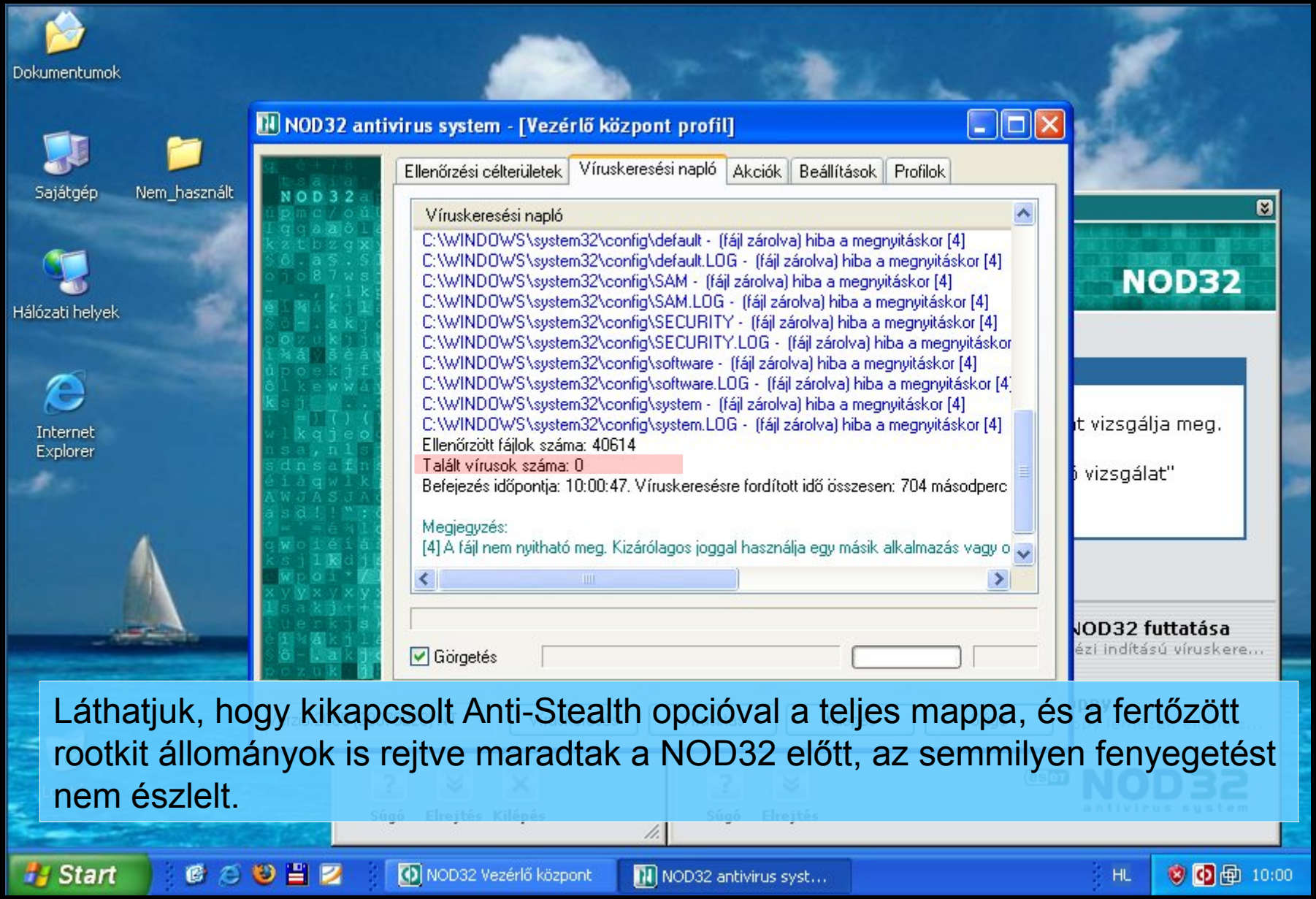

Futtassuk most le a NOD32 kézi indítású víruskeresőjét!
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Súgó
Elrejtés
Kilépés
NOD32 - kézi indítású víruskereső
NOD32
Információ
A NOD32 kézi indítású víruskeresője
a számítógép lemezein található fájlokat vizsgálja meg.
Javasoljuk, hogy futtassa a "Mélyreható vizsgálat"
opciót legalább hetente egyszer.
Helyi lemezek
Helyi lemezek ellenőrzése
A NOD32 futtatása
A kézi indítású víruskere...
Mélyreható vizsgálat
Helyi lemezek nagyon r...
Floppy
Floppy lemezek ellenőrz...
Súgó
Elrejtés
eset NOD32 antivirus system
Start
NOD32 Vezérlő központ
HL
9:32

A teljes C meghajtó tartalmát meg fogjuk vizsgálni.

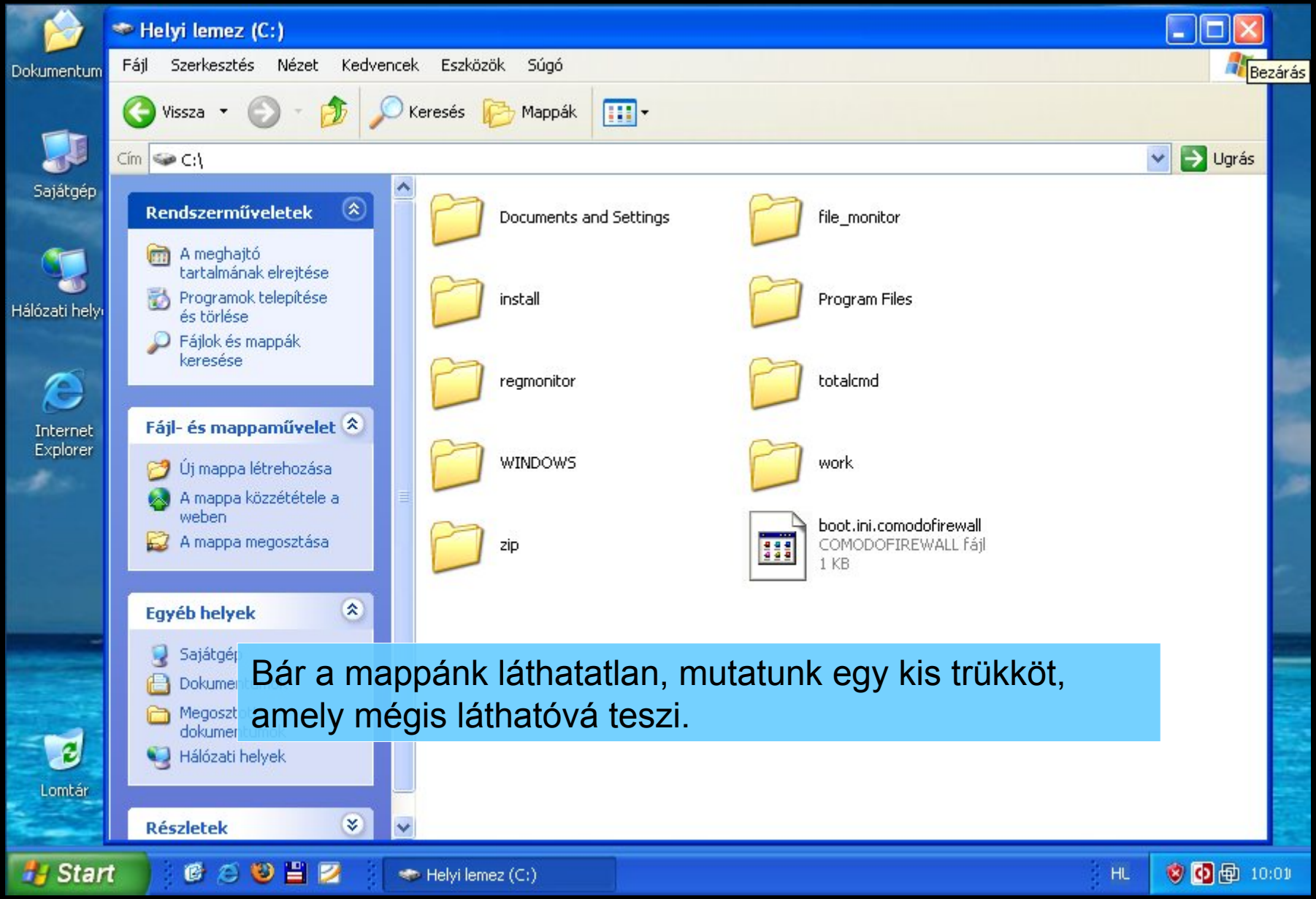


Mivel alapos ellenőrzést szeretnénk, kapcsoljunk be mindent
- kivéve egyelőre az Anti-Stealth technológiát!

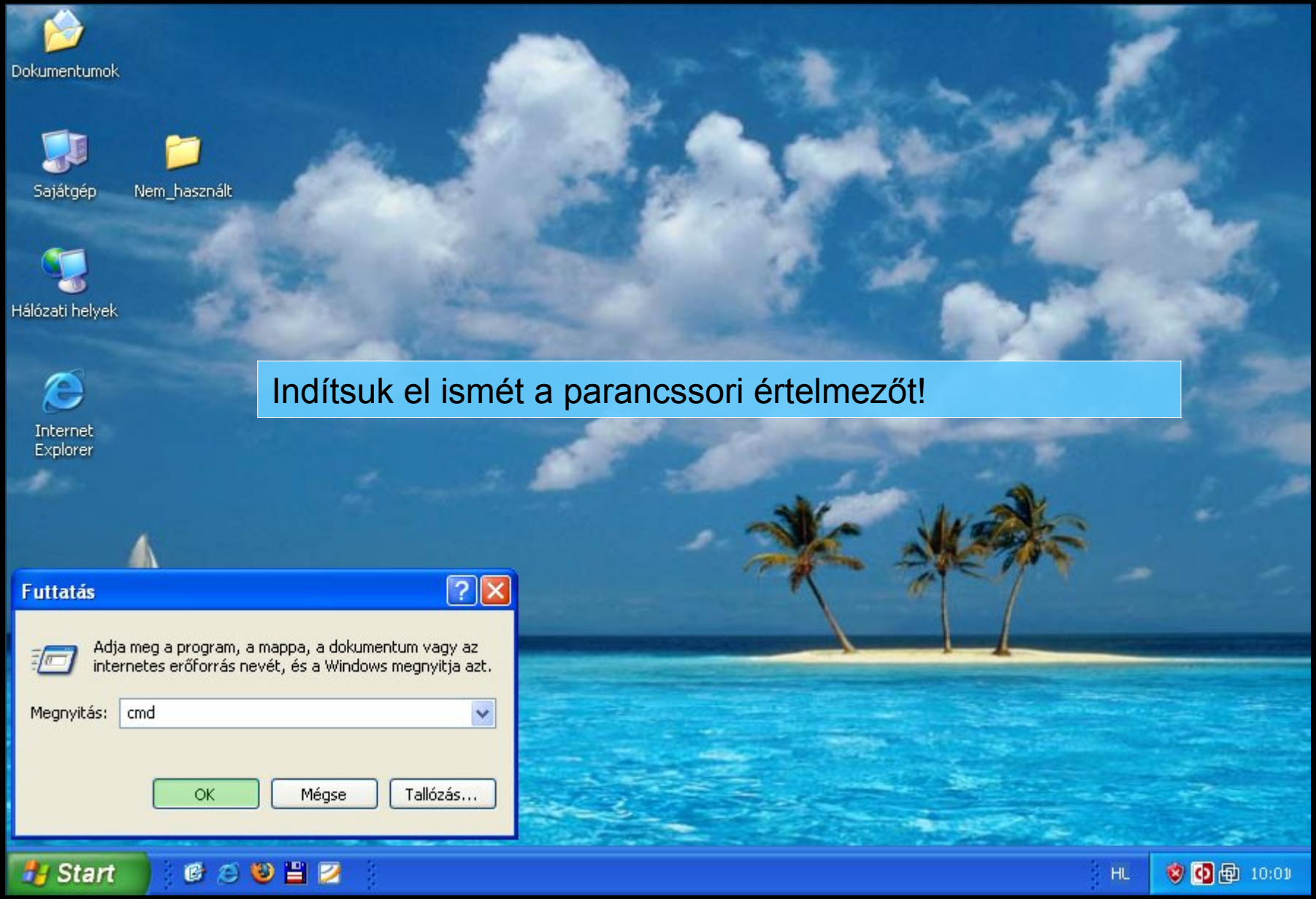


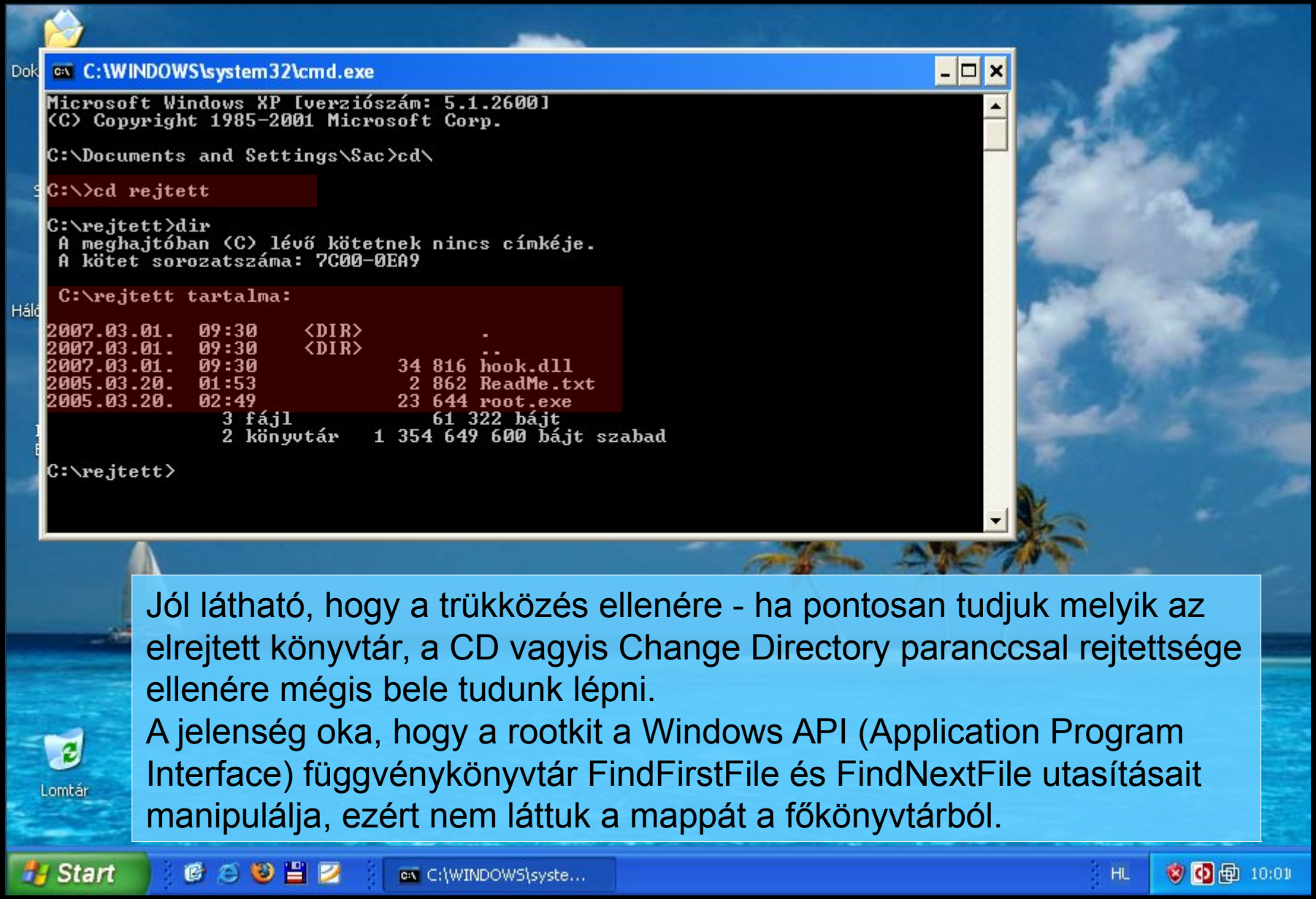


Láthatjuk, hogy kikapcsolt Anti-Stealth opcióval a teljes mappa, és a fertőzött rootkit állományok is rejtve maradtak a NOD32 előtt, az semmilyen fenyegetést nem észlelt.

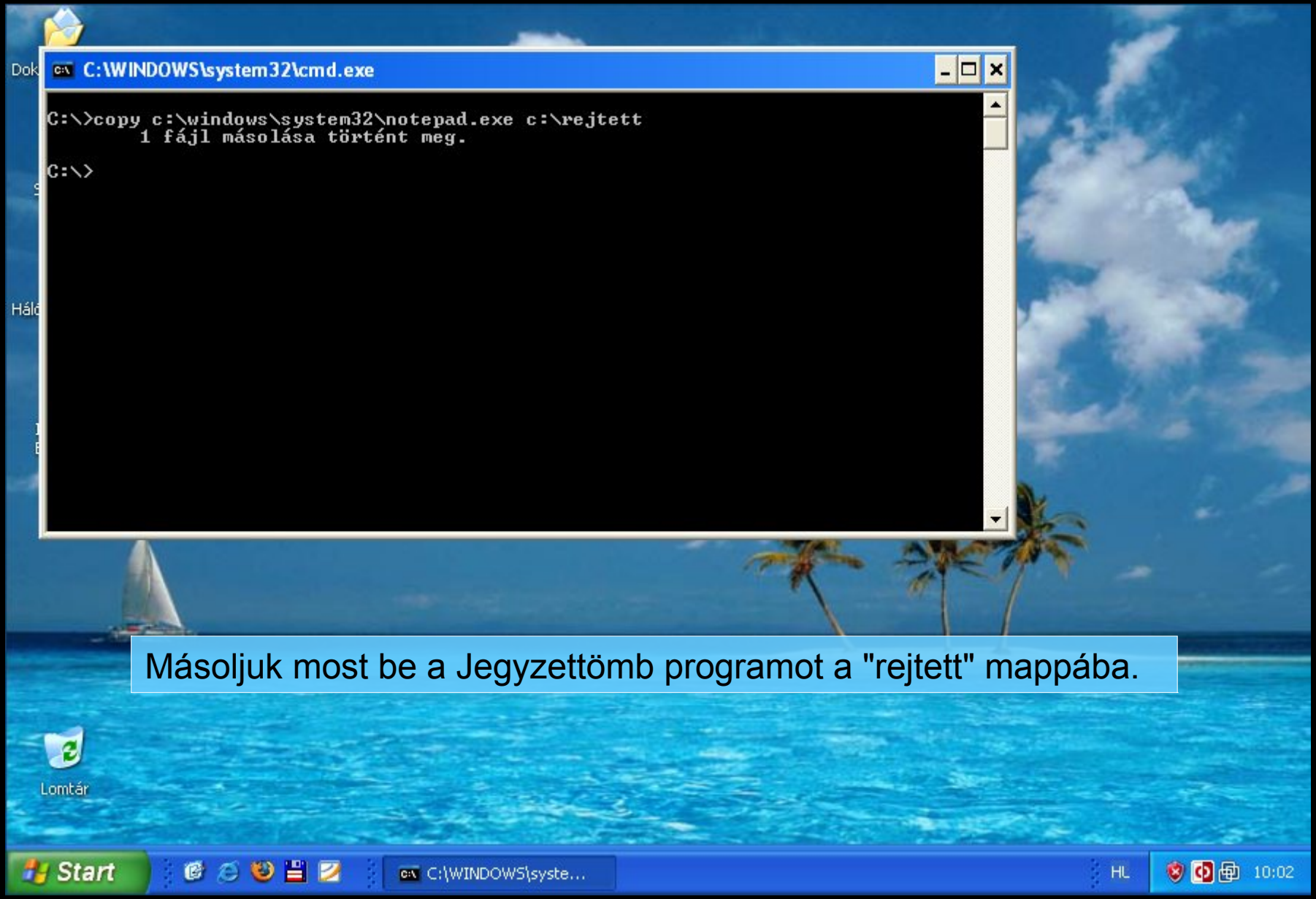


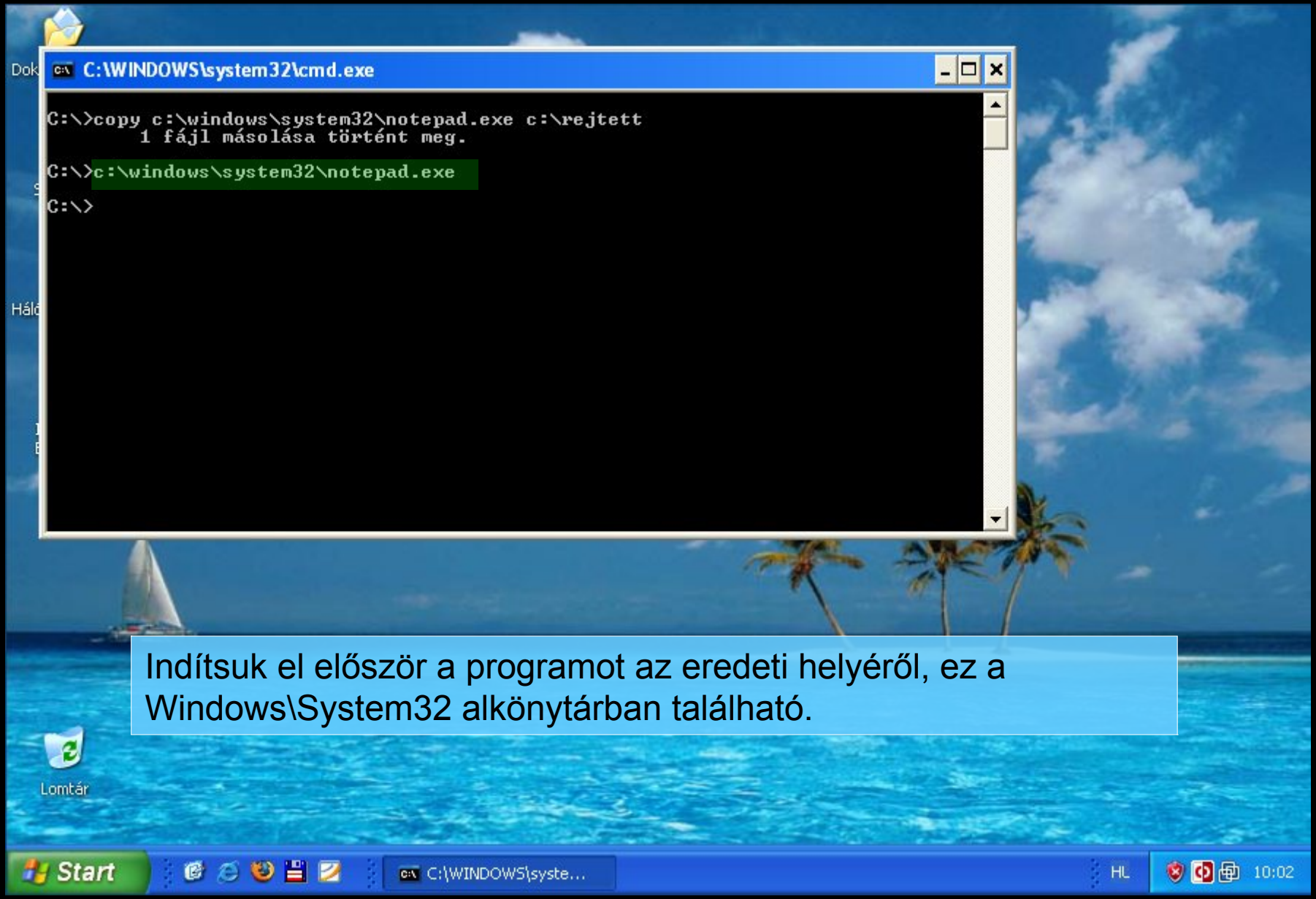
Bár a mappánk láthatatlan, mutatunk egy kis trükköt, amely mégis láthatóvá teszi.

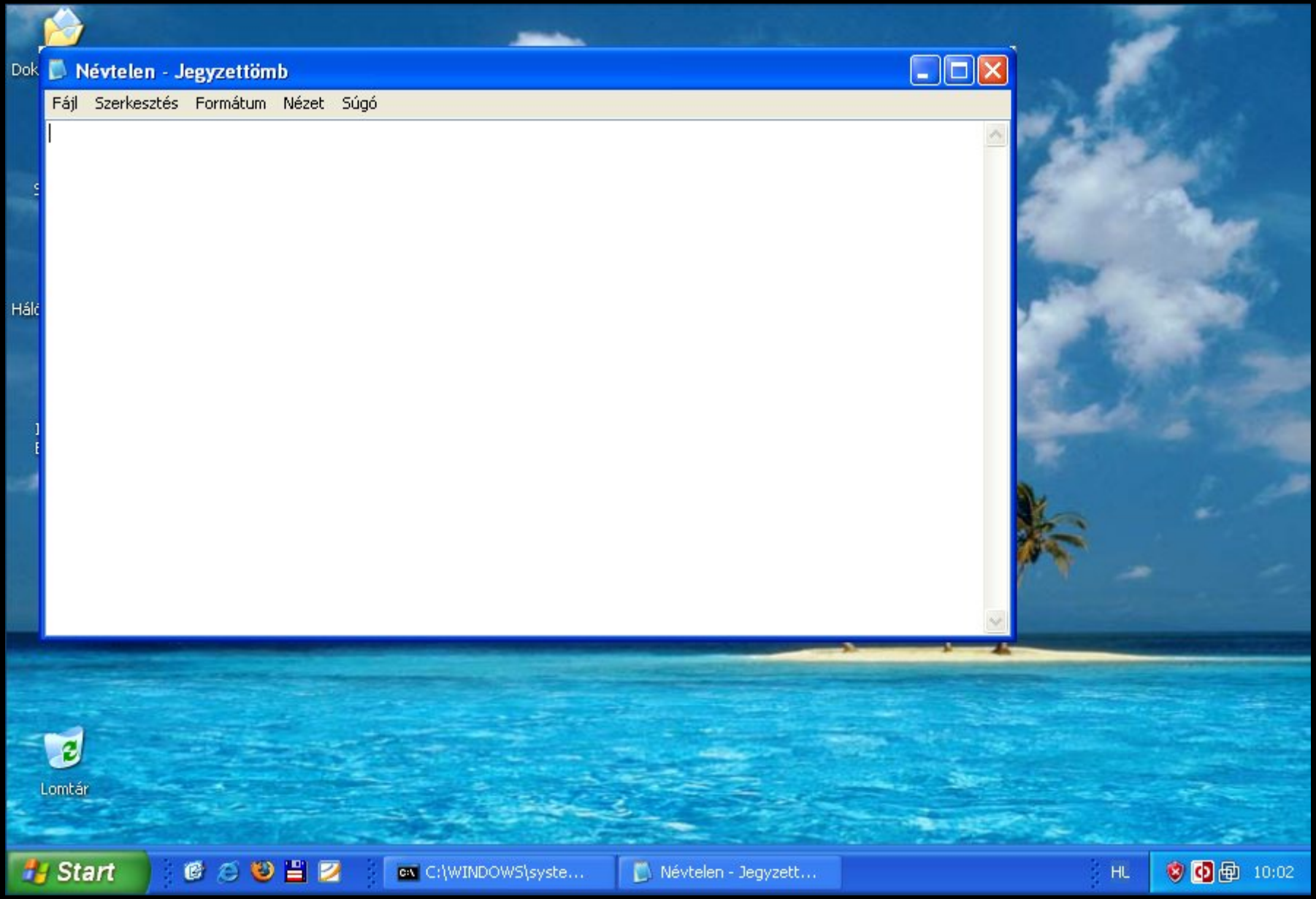

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Indítsuk el ismét a parancssori értelmezőt!
Futtatás
Adja meg a program, a mappa, a dokumentum vagy az internetes erőforrás nevét, és a Windows megnyitja azt.
Megnyitás:
cmd
OK
Mégse
Tallózás...
Start
HL
10:01

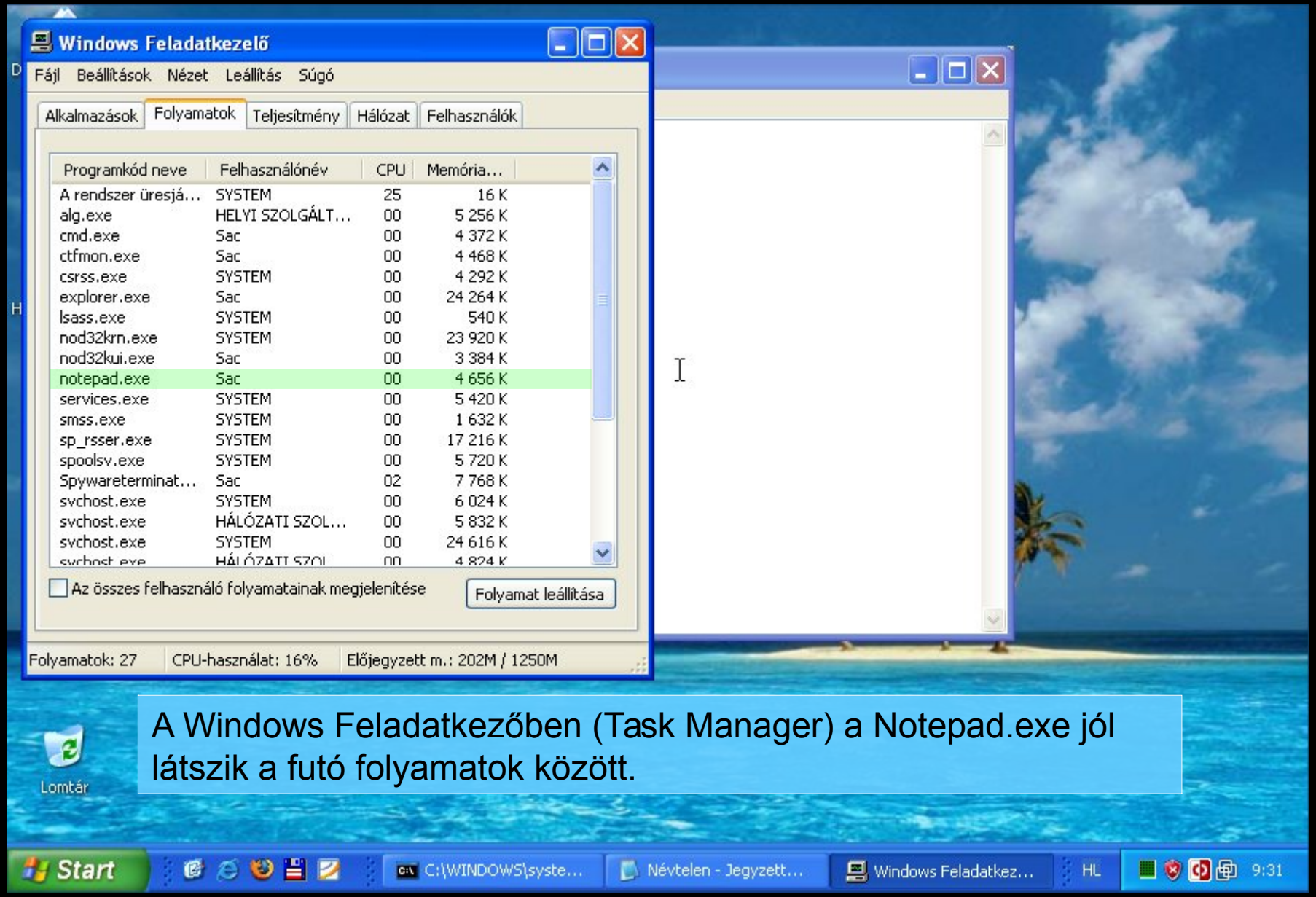


Jól látható, hogy a trükközés ellenére - ha pontosan tudjuk melyik az elrejtett könyvtár, a CD vagyis Change Directory paranccsal rejtettsége ellenére mégis bele tudunk lépni.
A jelenség oka, hogy a rootkit a Windows API (Application Program Interface) függvénykönyvtár FindFirstFile és FindNextFile utasításait manipulálja, ezért nem láttuk a mappát a főkönyvtárból.

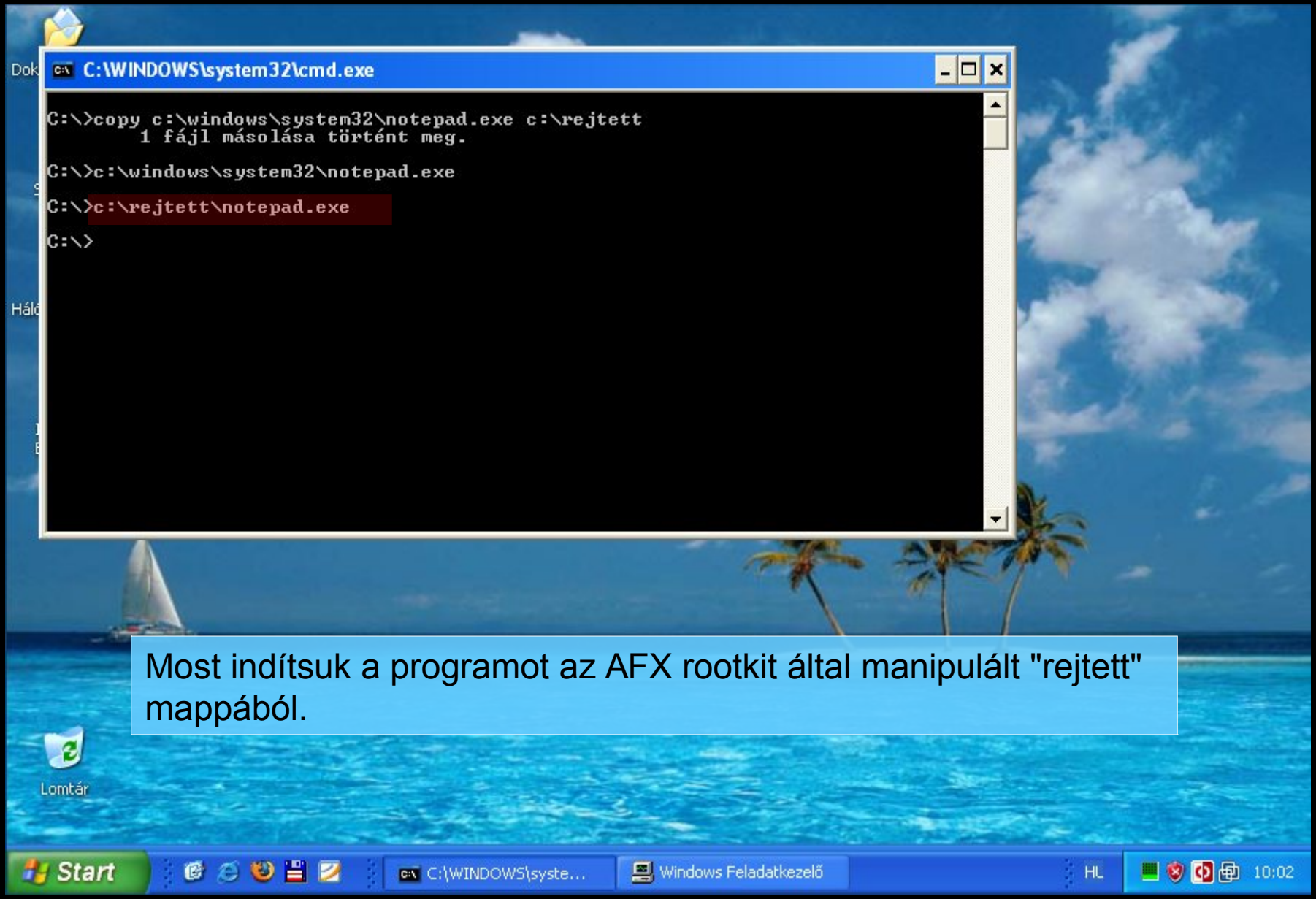

C:\WINDOWS\system32\cmd.exe
C:\>copy c:\windows\system32\notepad.exe c:\rejtett
1 fájl másolása történt meg.
C:\>
Másoljuk most be a Jegyzettömb programot a "rejtett" mappába.
Lomtár
Start
C:\WINDOWS\syste...
HL
10:02

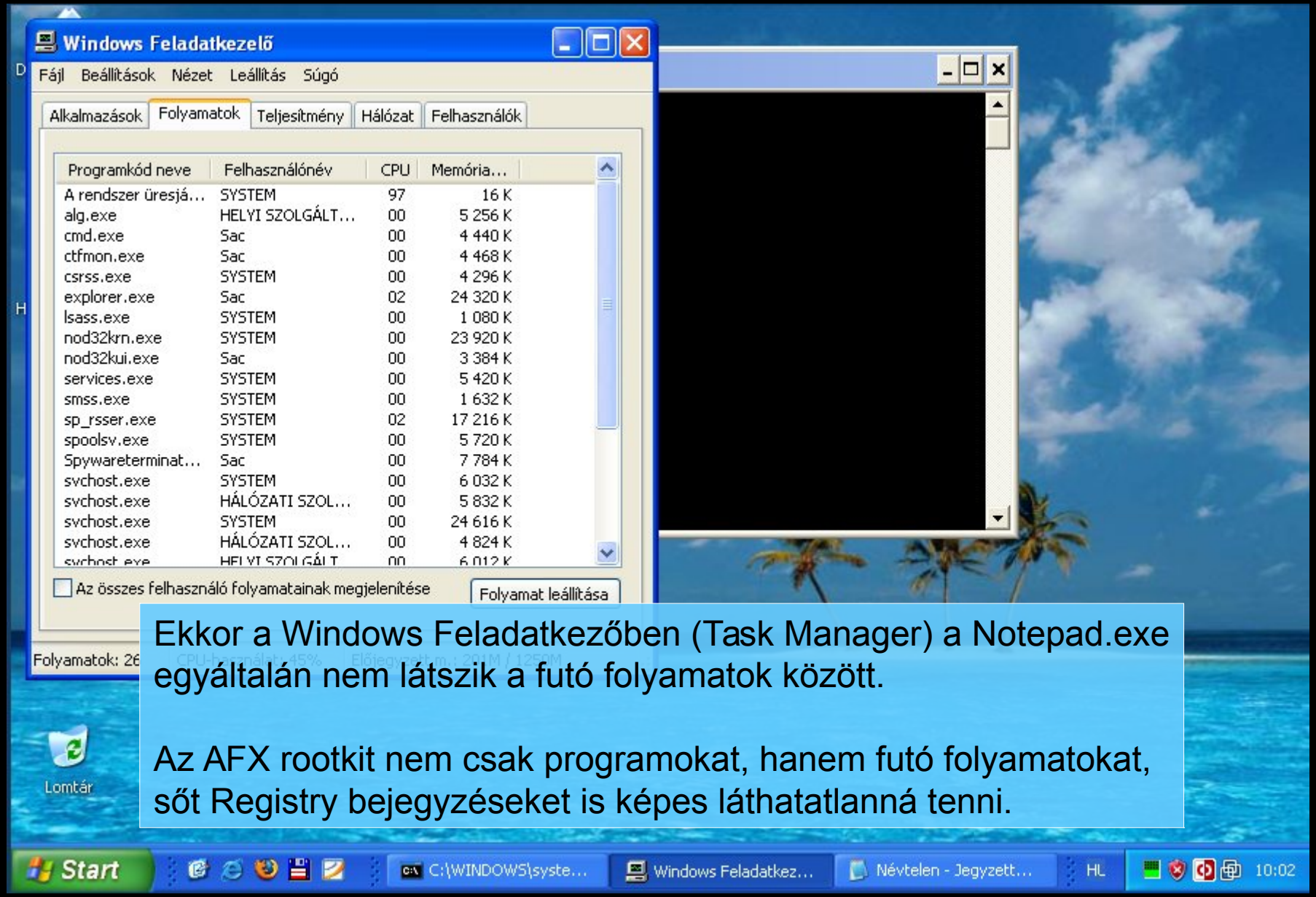

C:\WINDOWS\system32\cmd.exe
C:\>copy c:\windows\system32\notepad.exe c:\rejtett
1 fájl másolása történt meg.
C:\>c:\windows\system32\notepad.exe
C:\>
Indítsuk el először a programot az eredeti helyéről, ez a Windows\System32 alkönytárban található.
Lomtár
Start
C:\WINDOWS\syste...
HL
10:02


Névtelen - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó
Lomtár
Start
C:\WINDOWS\syste...
Névtelen - Jegyzett...
HL
10:02



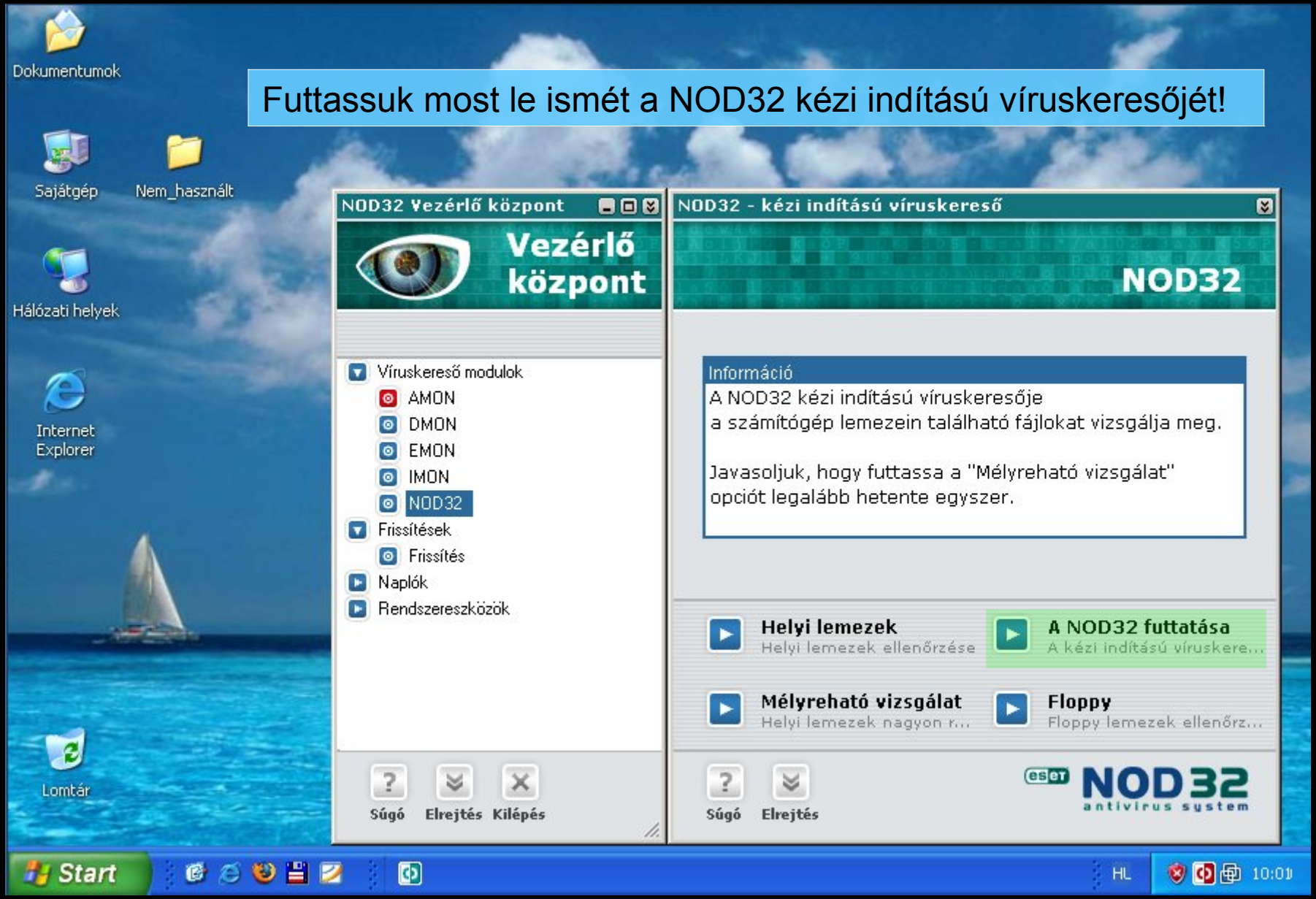
A Windows Feladatkezőben (Task Manager) a Notepad.exe jól látszik a futó folyamatok között.

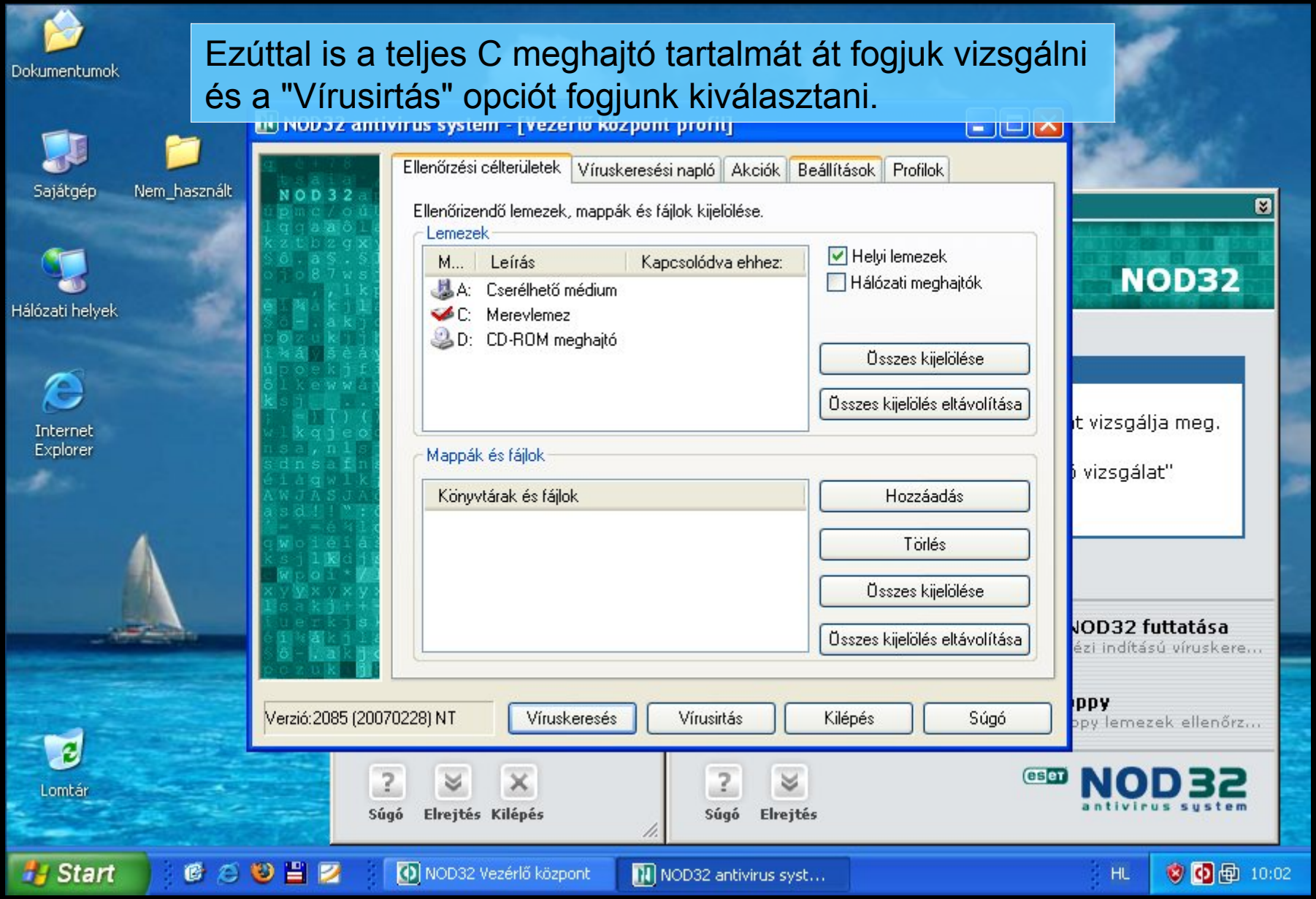

C:\WINDOWS\system32\cmd.exe
C:\>copy c:\windows\system32\notepad.exe c:\rejtett
1 fájl másolása történt meg.
C:\>c:\windows\system32\notepad.exe
C:\>c:\rejtett\notepad.exe
C:\>
Most indítsuk a programot az AFX rootkit által manipulált "rejtett" mappából.
Lomtár
Start
C:\WINDOWS\syste...
Windows Feladatkezelő
HL
10:02



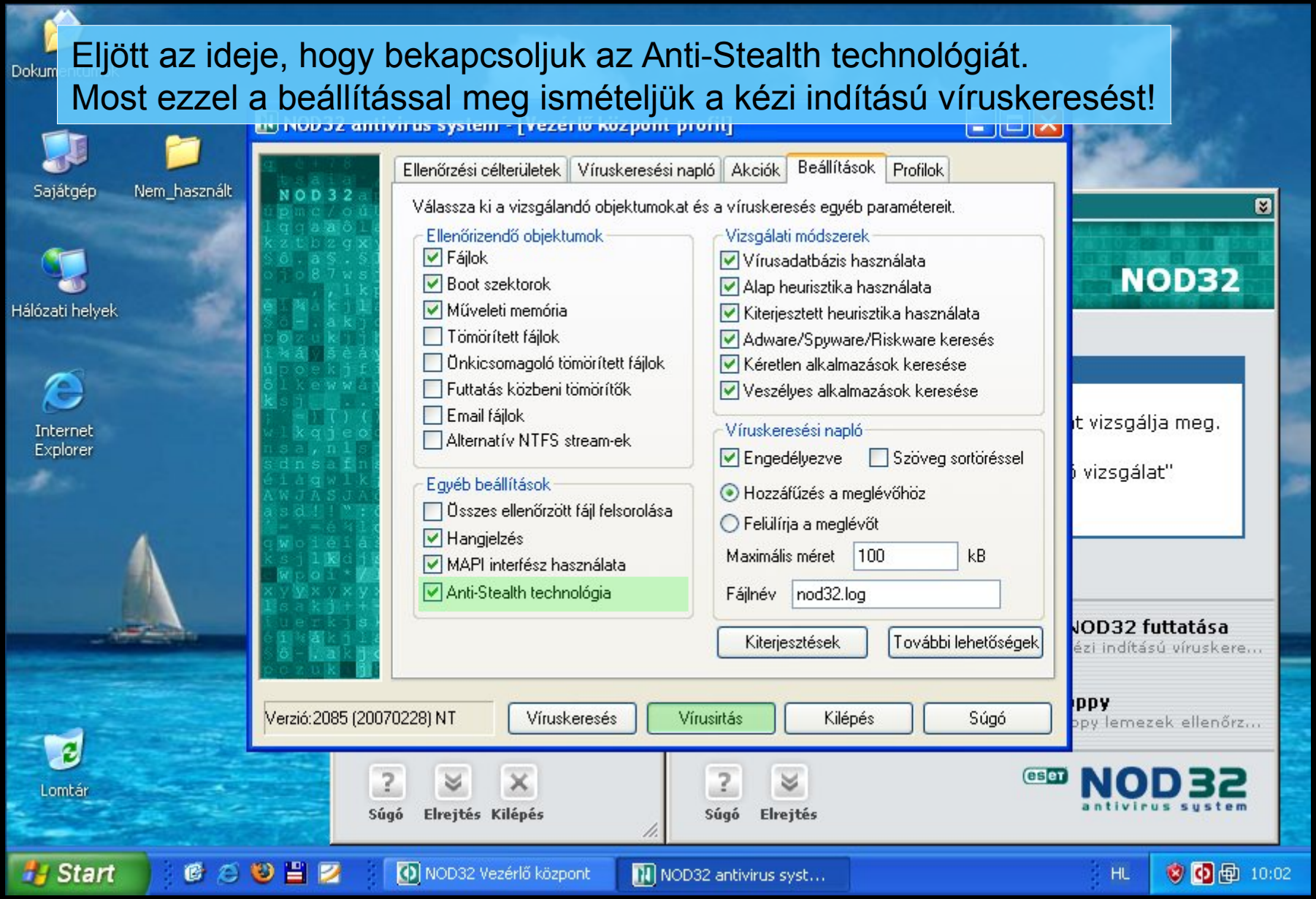
Ekkor a Windows Feladatkezőben (Task Manager) a Notepad.exe egyáltalán nem látszik a futó folyamatok között.

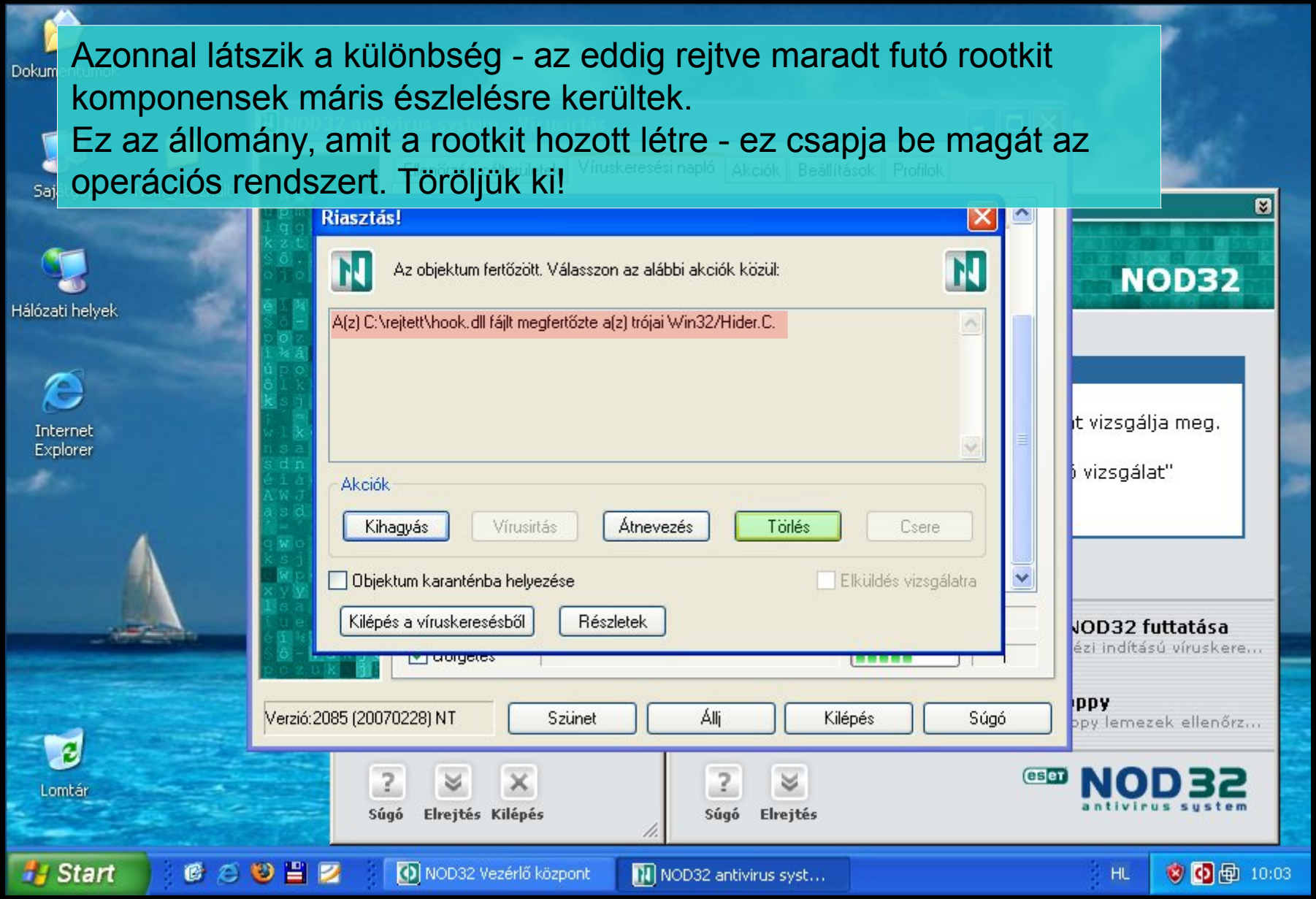
Az AFX rootkit nem csak programokat, hanem futó folyamatokat, sőt Registry bejegyzéseket is képes láthatatlanná tenni.

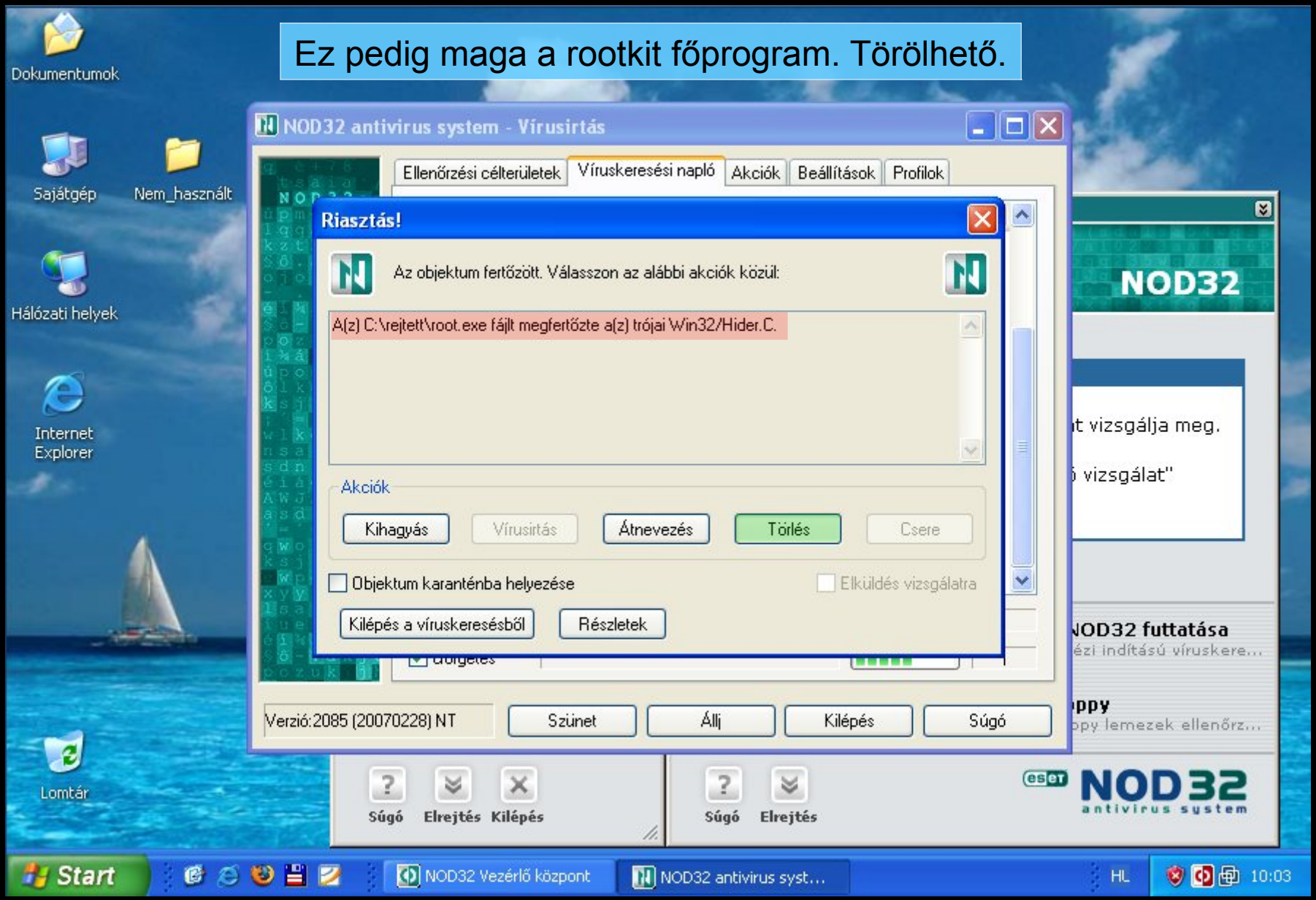

Futtassuk most le ismét a NOD32 kézi indítású víruskeresőjét!
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Súgó
Elrejtés
Kilépés
NOD32 - kézi indítású víruskereső
NOD32
Információ
A NOD32 kézi indítású víruskeresője
a számítógép lemezein található fájlokat vizsgálja meg.
Javasoljuk, hogy futtassa a "Mélyreható vizsgálat"
opciót legalább hetente egyszer.
Helyi lemezek
Helyi lemezek ellenőrzése
A NOD32 futtatása
A kézi indítású víruskere...
Mélyreható vizsgálat
Helyi lemezek nagyon r...
Floppy
Floppy lemezek ellenőrz...
Súgó
Elrejtés
eset NOD32 antivirus system
Start
HL
10:01

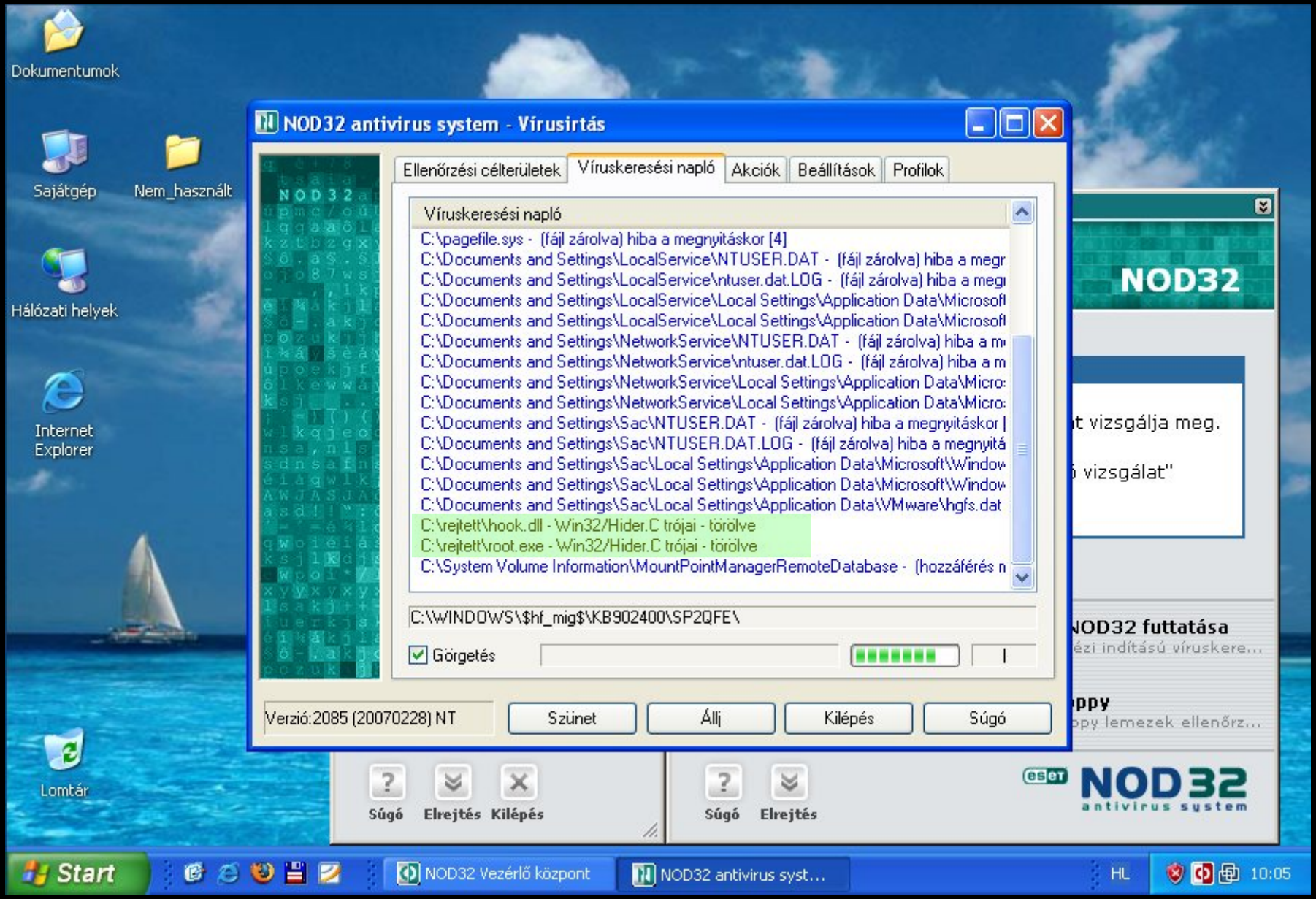

Ezúttal is a teljes C meghajtó tartalmát át fogjuk vizsgálni és a "Vírusirtás" opciót fogjunk kiválasztani.
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - [Vezérlő központ profil]
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Ellenőrizendő lemezek, mappák és fájlok kijelölése.
Lemezek
M...
Leírás
Kapcsolódva ehhez:
A: Cserélhető médium
C: Merevlemez
D: CD-ROM meghajtó
Helyi lemezek
Hálózati meghajtók
Összes kijelölése
Összes kijelölés eltávolítása
Mappák és fájlok
Könyvtárak és fájlok
Hozzáadás
Törlés
Összes kijelölése
Összes kijelölés eltávolítása
Verzió:2085 (20070228) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
NOD32
Súgó
Elrejtés
Kilépés
Súgó
Elrejtés
eset NOD32 antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:02

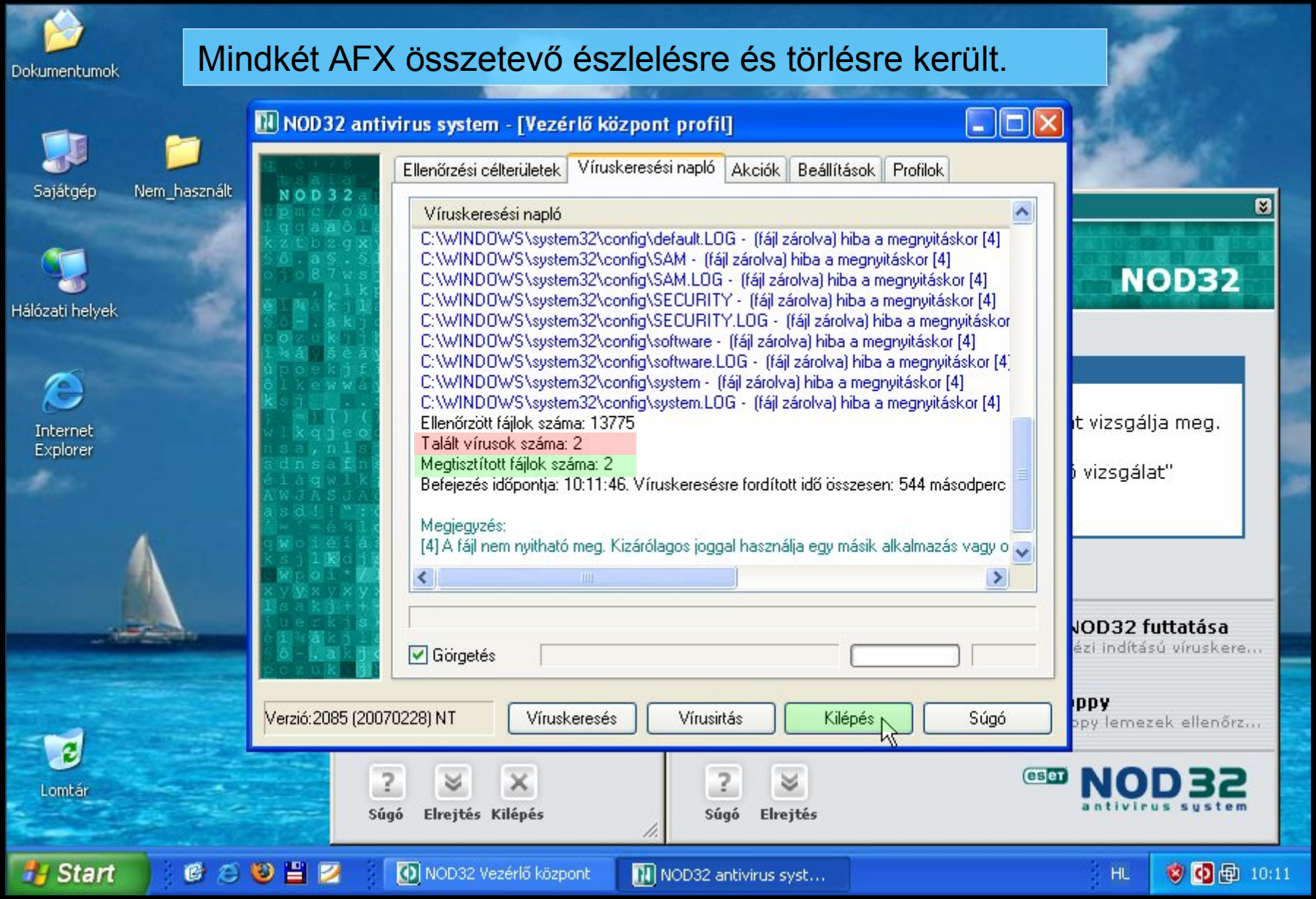
Eljött az ideje, hogy bekapcsoljuk az Anti-Stealth technológiát.
Most ezzel a beállítással meg ismételjük a kézi indítású víruskeresést!

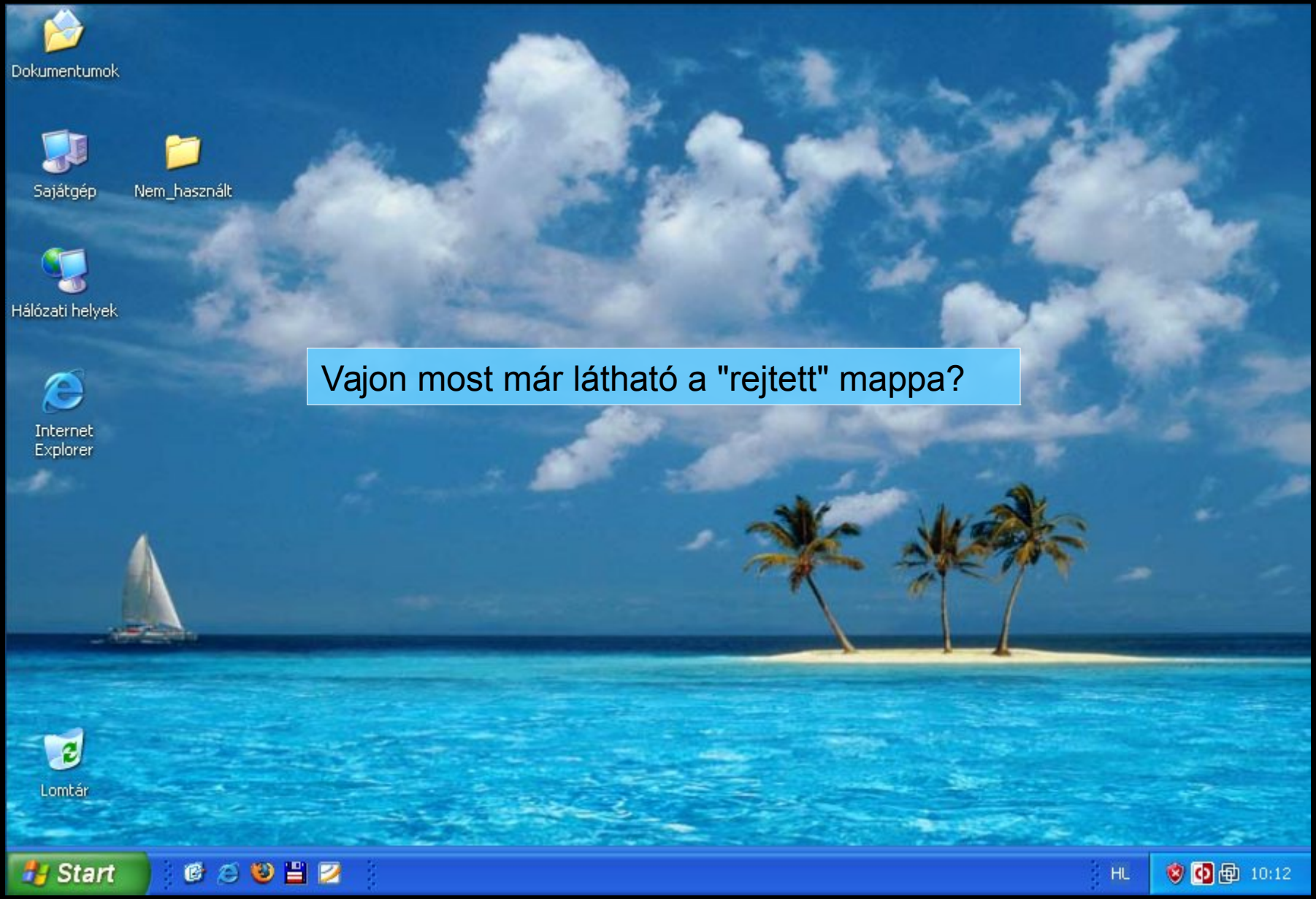


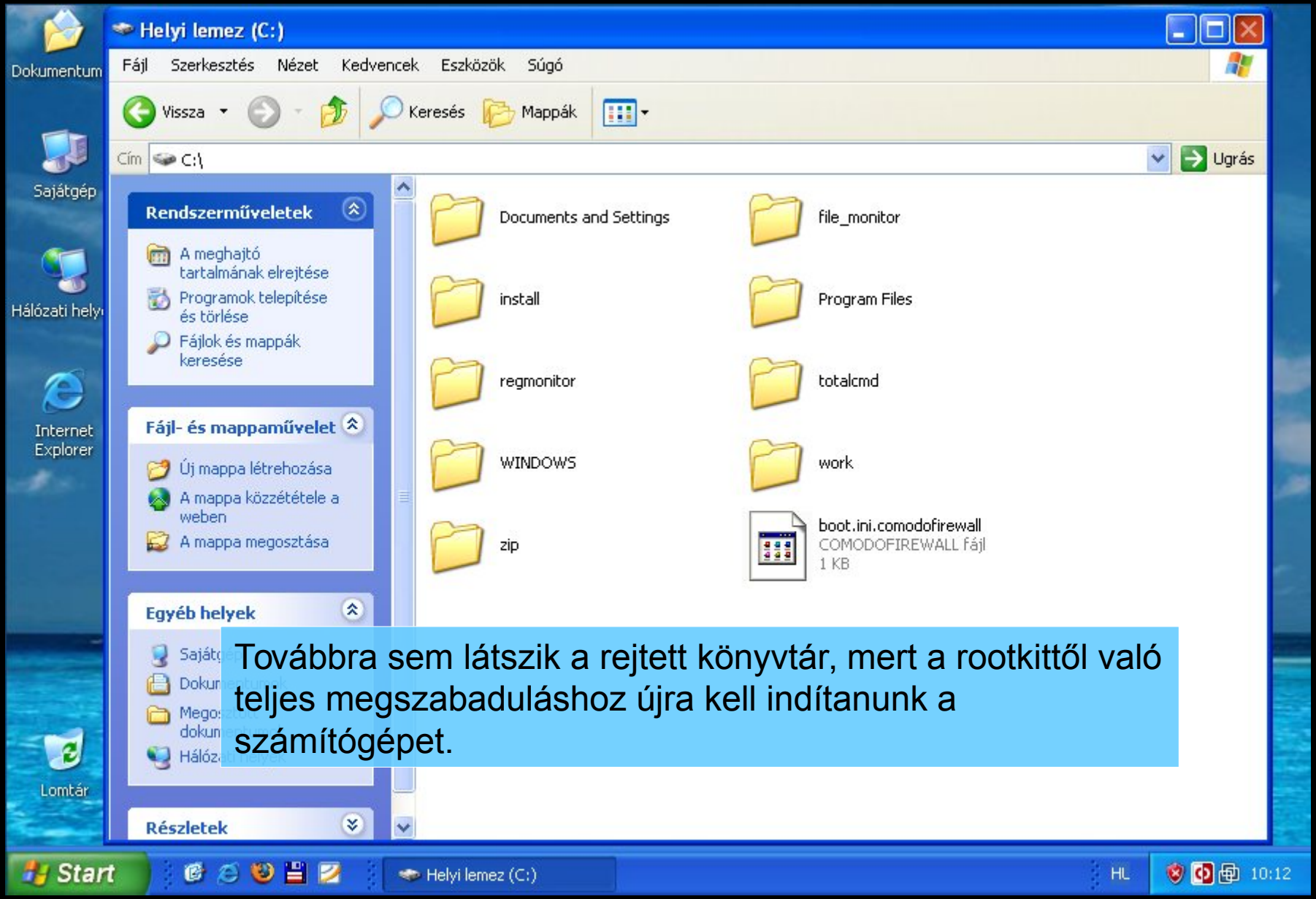

Azonnal látszik a különbség - az eddig rejtve maradt futó rootkit komponensek máris észlelésre kerültek.
Ez az állomány, amit a rootkit hozott létre - ez csapja be magát az operációs rendszert. Töröljük ki!
Riasztás!
Az objektum fertőzött. Válasszon az alábbi akciók közül:
A(z) C:\rejtett\hook.dll fájlt megfertőzte a(z) trójai Win32/Hider.C.
Akciók
Kihagyás
Vírusirtás
Átnevezés
Törlés
Csere
Objektum karanténba helyezése
Elküldés vizsgálatra
Kilépés a víruskeresésből
Részletek
Verzió:2085 (20070228) NT
Szünet
Állj
Kilépés
Súgó
NOD32
Súgó
Elrejtés
Kilépés
Súgó
Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:03


Ez pedig maga a rootkit főprogram. Törölhető.
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - Vírusirtás
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Riasztás!
Az objektum fertőzött. Válasszon az alábbi akciók közül:
A(z) C:\rejtett\root.exe fájlt megfertőzte a(z) trójai Win32/Hider.C.
Akciók
Kihagyás
Vírusirtás
Átnevezés
Törlés
Csere
Objektum karanténba helyezése
Elküldés vizsgálatra
Kilépés a víruskeresésből
Részletek
Verzió:2085 (20070228) NT
Szünet
Állj
Kilépés
Súgó
NOD32
Súgó
Elrejtés
Kilépés
Súgó
Elrejtés
eset NOD32 antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:03

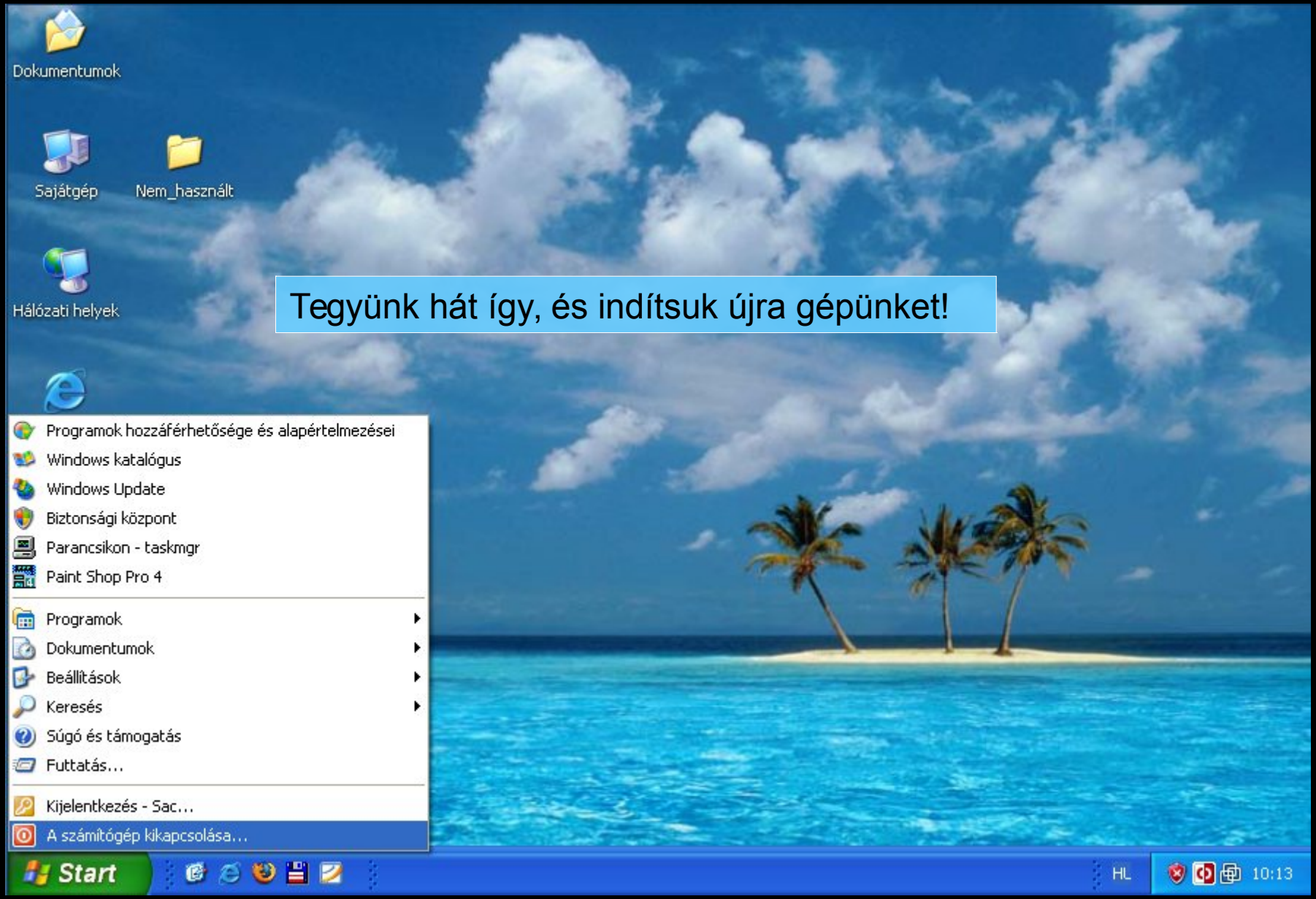

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - Vírusirtás
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Víruskeresési napló
C:\pagefile.sys - (fájl zárolva) hiba a megnyitáskor [4]
C:\Documents and Settings\LocalService\NTUSER.DAT - (fájl zárolva) hiba a megr
C:\Documents and Settings\LocalService\ntuser.dat.LOG - (fájl zárolva) hiba a megı
C:\Documents and Settings\LocalService\Local Settings\Application Data\Microsofl
C:\Documents and Settings\LocalService\Local Settings\Application Data\Microsofl
C:\Documents and Settings\NetworkService\NTUSER.DAT - (fájl zárolva) hiba a m
C:\Documents and Settings\NetworkService\ntuser.dat.LOG - (fájl zárolva) hiba a m
C:\Documents and Settings\NetworkService\Local Settings\Application Data\Micro:
C:\Documents and Settings\NetworkService\Local Settings\Application Data\Micro:
C:\Documents and Settings\Sac\NTUSER.DAT - (fájl zárolva) hiba a megnyitáskor |
C:\Documents and Settings\Sac\NTUSER.DAT.LOG - (fájl zárolva) hiba a megnyitá
C:\Documents and Settings\Sac\Local Settings\Application Data\Microsoft\Windov
C:\Documents and Settings\Sac\Local Settings\Application Data\Microsoft\Windov
C:\Documents and Settings\Sac\Local Settings\Application Data\VMware\hgfs.dat
C:\rejtett\hook.dll - Win32/Hider.C trójai - törölve
C:\rejtett\root.exe - Win32/Hider.C trójai - törölve
C:\System Volume Information\MountPointManagerRemoteDatabase - (hozzáférés n
C:\WINDOWS\hf_mig\KB902400\SP2QFE\
Görgetés
Verzió:2085 (20070228) NT
Szünet
Állj
Kilépés
Súgó
NOD32
t vizsgálja meg.
vizsgálat"
NOD32 futtatása
ézi indítású víruskere...
ppy
ppy lemezek ellenőrz...
Súgó
Elrejtés
Kilépés
Súgó
Elrejtés
eset NOD32 antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:05

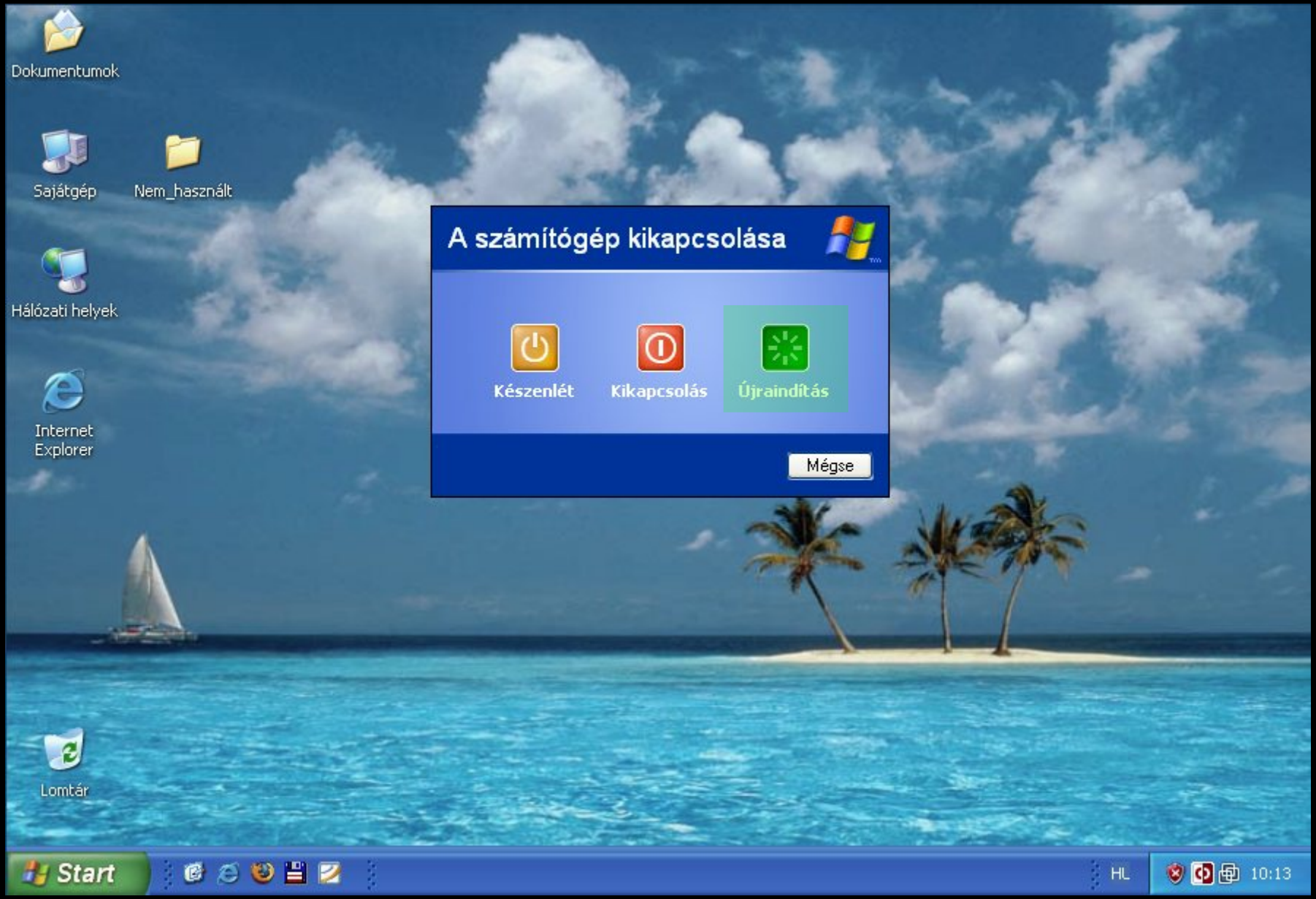

Mindkét AFX összetevő észlelésre és törlésre került.
NOD32 antivirus system - [Vezérlő központ profil]
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Víruskeresési napló
C:\WINDOWS\system32\config\default.LOG - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SAM - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SAM.LOG - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SECURITY - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SECURITY.LOG - (fájl zárolva) hiba a megnyitáskor
C:\WINDOWS\system32\config\software - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\software.LOG - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\system - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\system.LOG - (fájl zárolva) hiba a megnyitáskor [4]
Ellenőrzött fájlok száma: 13775
Talált vírusok száma: 2
Megtisztított fájlok száma: 2
Befejezés időpontja: 10:11:46. Víruskeresésre fordított idő összesen: 544 másodperc
Megjegyzés:
[4] A fájl nem nyitható meg. Kizárólagos joggal használja egy másik alkalmazás vagy o
Görgetés
Verzió:2085 (20070228) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32
Súgó
Elrejtés
Kilépés
Súgó
Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:11


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Vajon most már látható a "rejtett" mappa?
Lomtár
Start
HL
10:12



Továbbra sem látszik a rejtett könyvtár, mert a rootkittől való teljes megszabaduláshoz újra kell indítanunk a számítógépet.

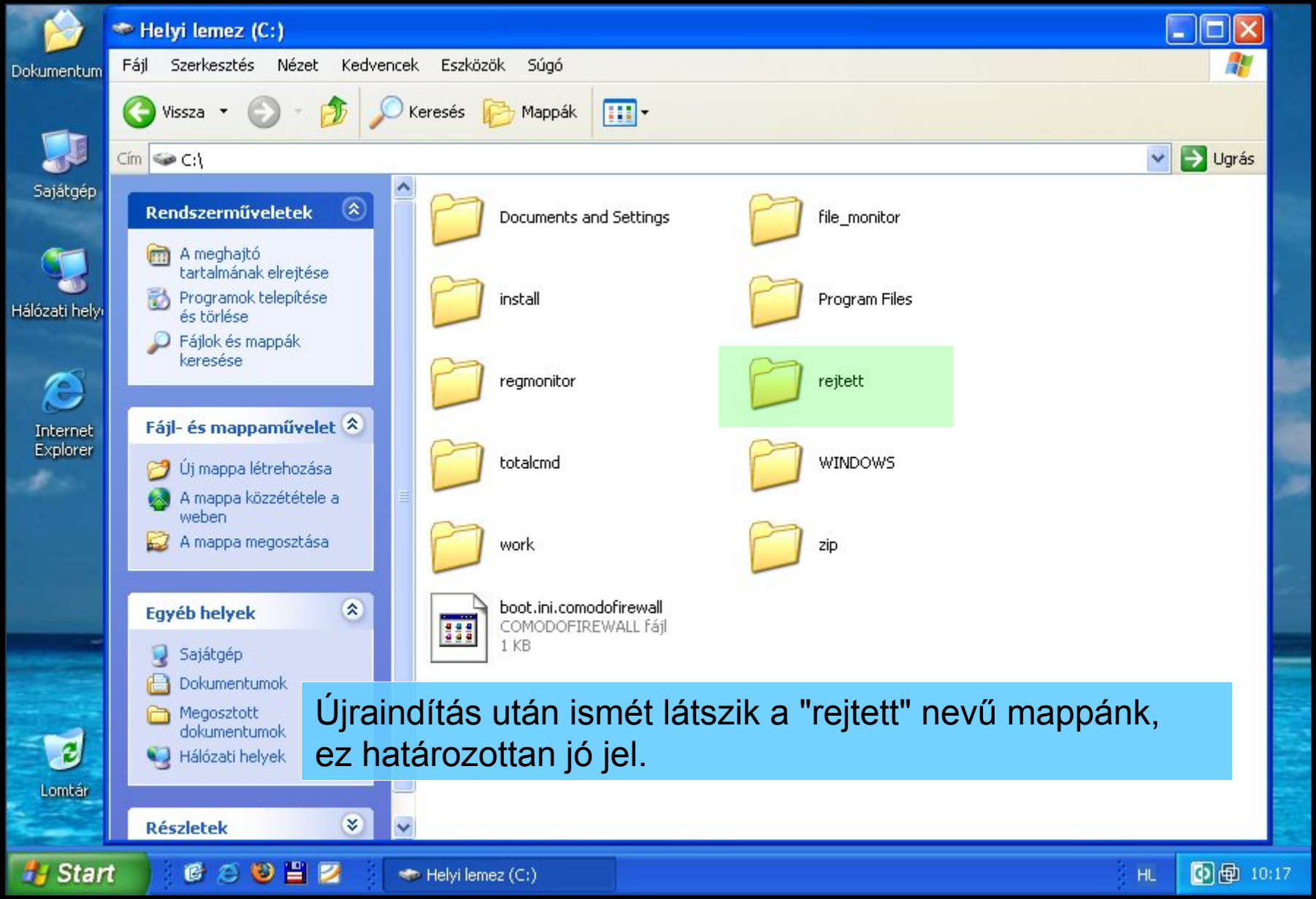

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Tegyünk hát így, és indítsuk újra gépünket!
Programok hozzáférhetősége és alapértelmezései
Windows katalógus
Windows Update
Biztonsági központ
Parancsikon - taskmgr
Paint Shop Pro 4
Programok
Dokumentumok
Beállítások
Keresés
Súgó és támogatás
Futtatás...
Kijelentkezés - Sac...
A számítógép kikapcsolása...
Start
HL
10:13


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
A számítógép kikapcsolása
Készenlét
Kikapcsolás
Újraindítás
Mégse
Start
HL
10:13

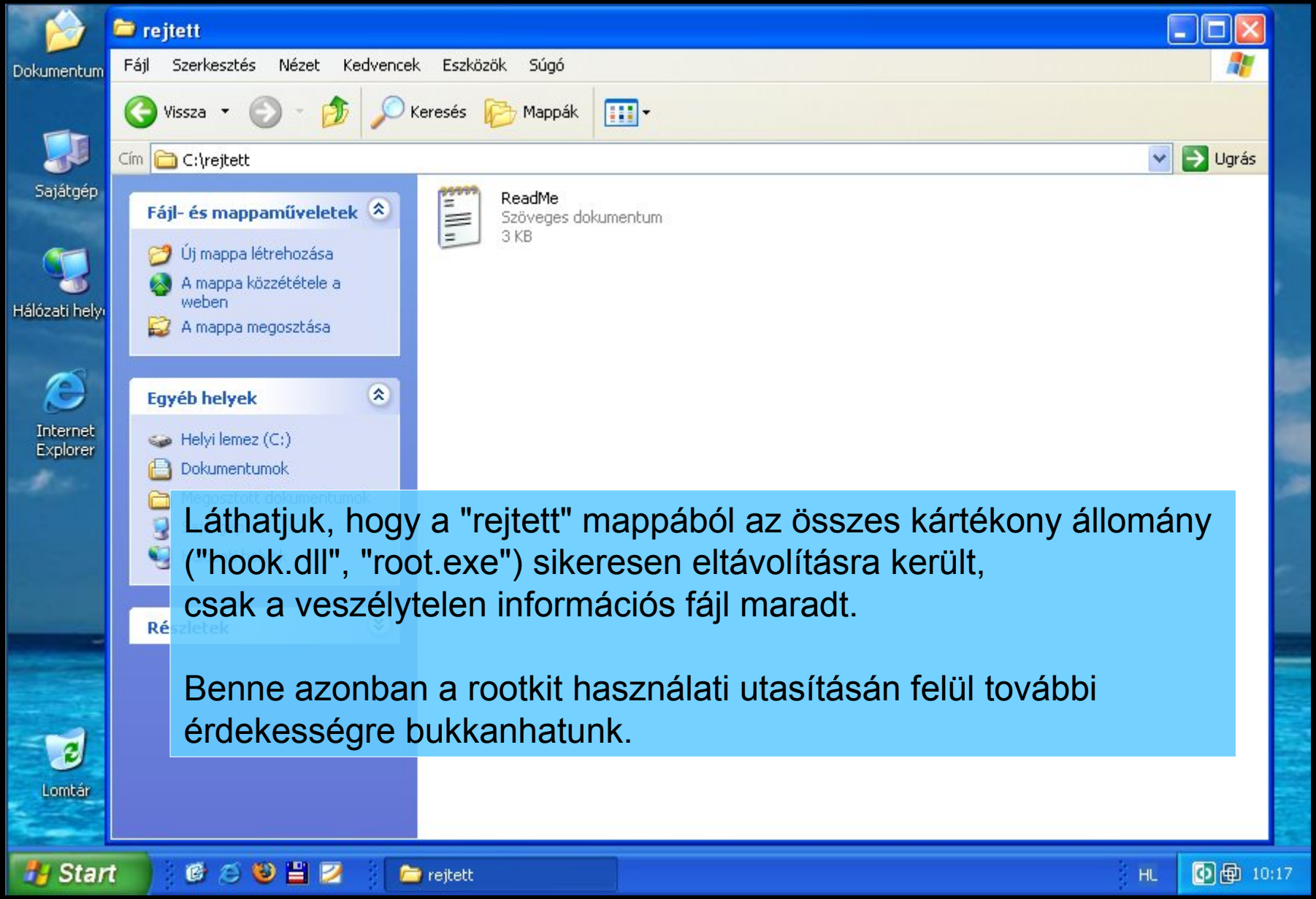
Kijelentkezés...


Microsoft®
Windows®xp
Copyright © Microsoft Corporation
Microsoft

Üdvözöljük

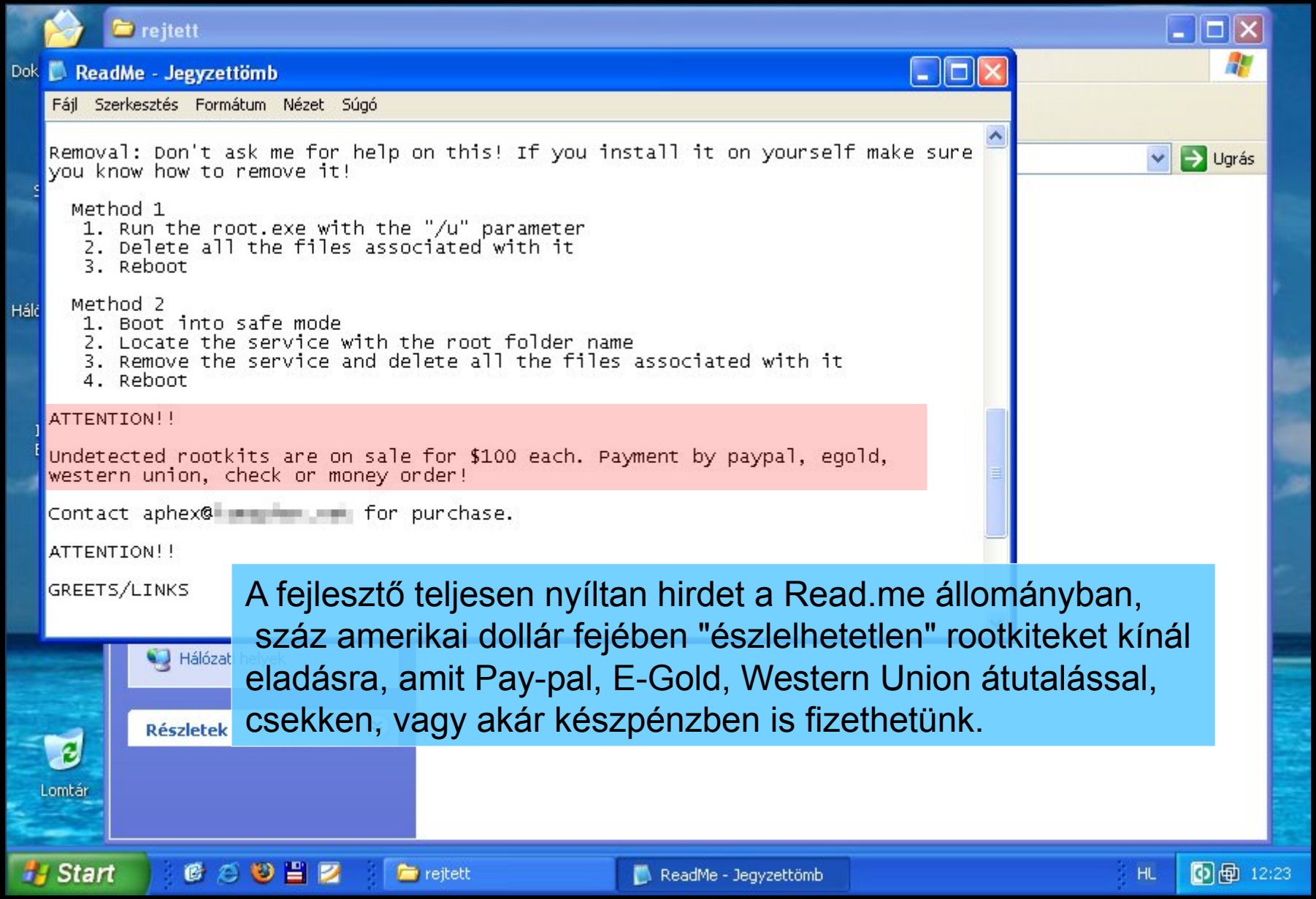


Újraindítás után ismét látszik a "rejtett" nevű mappánk, ez határozottan jó jel.

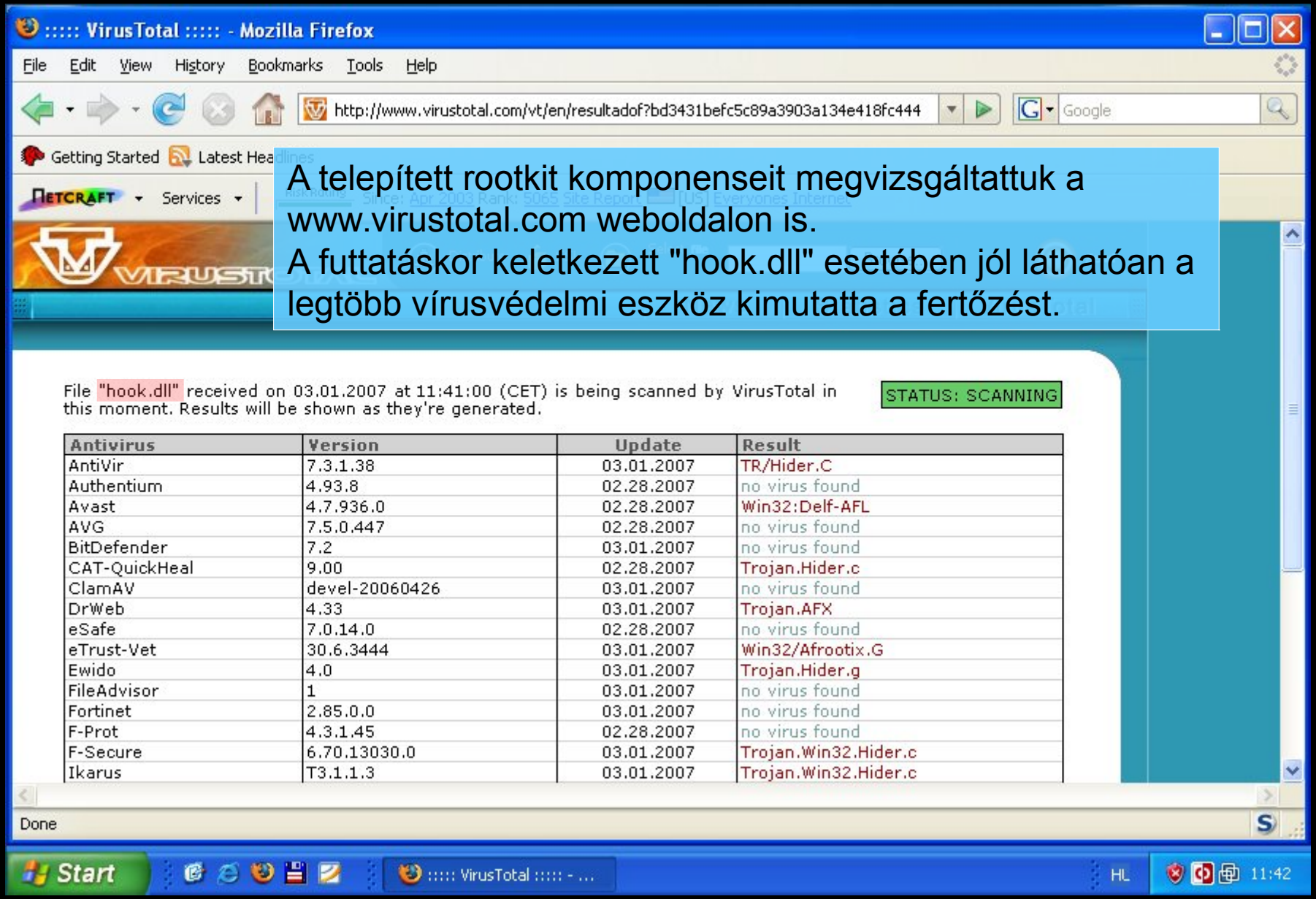


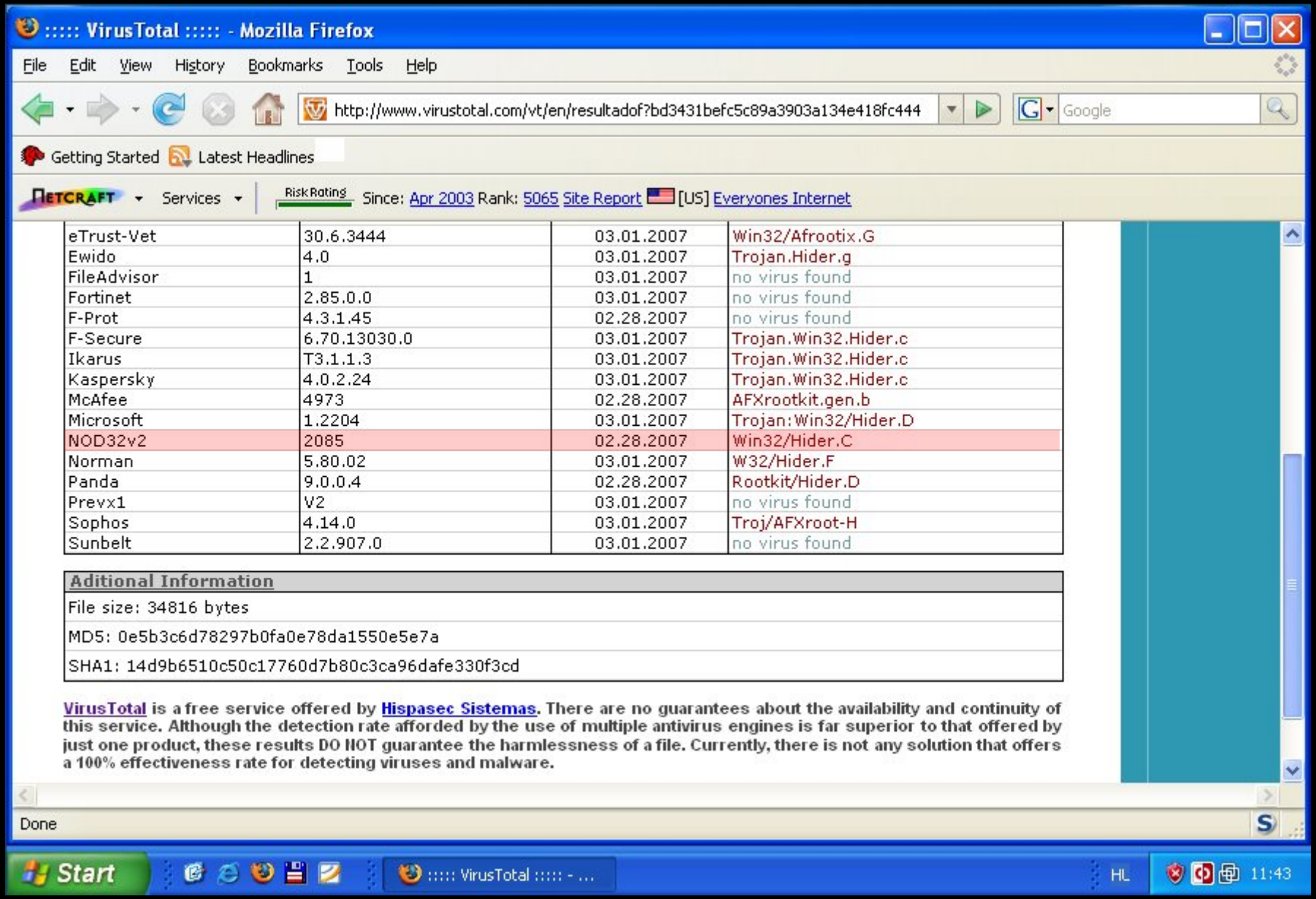
Láthatjuk, hogy a "rejtett" mappából az összes kártékony állomány ("hook.dll", "root.exe") sikeresen eltávolításra került,
csak a veszélytelen információs fájl maradt.

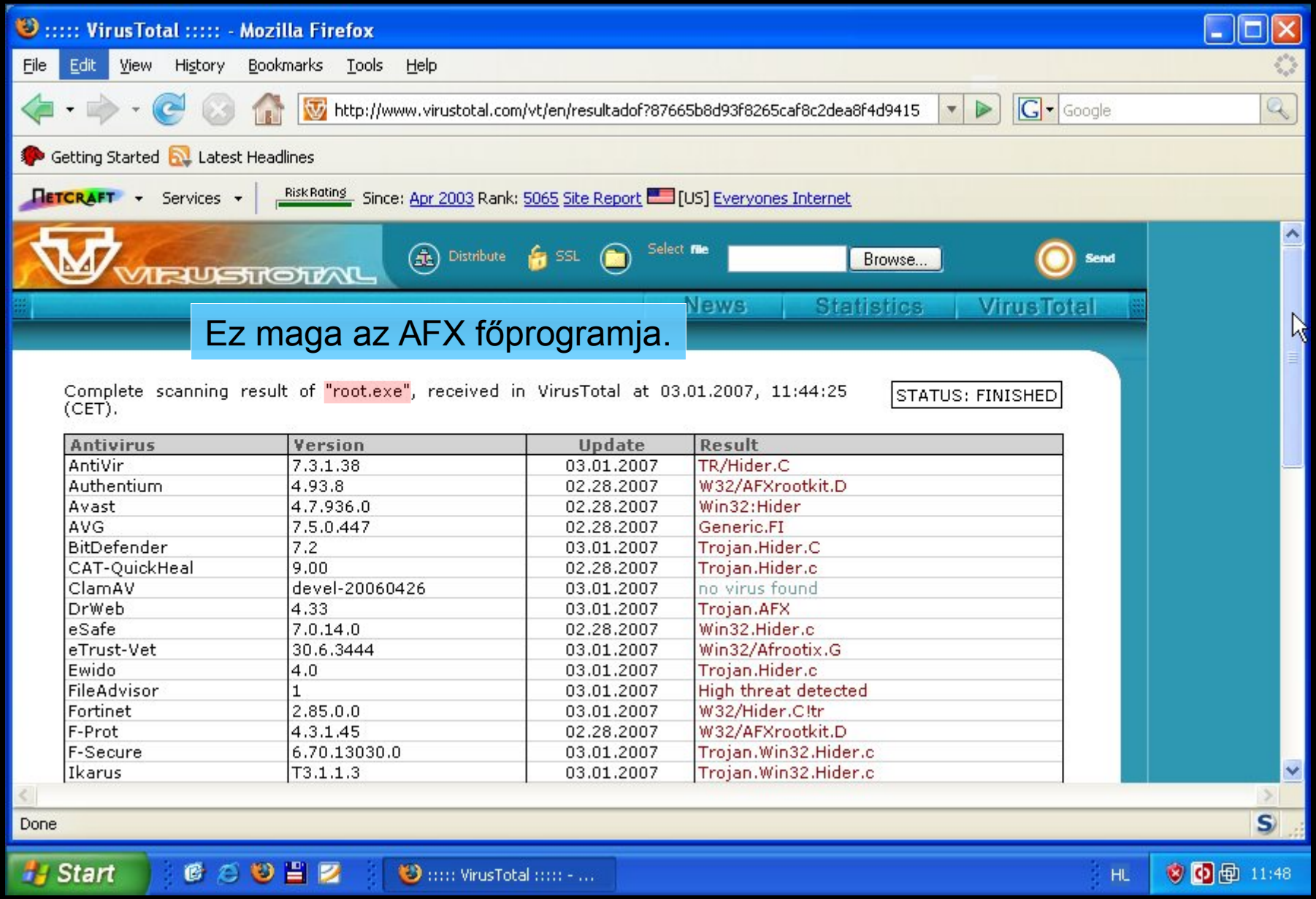
Benne azonban a rootkit használati utasításán felül további érdekességre bukkanhatunk.

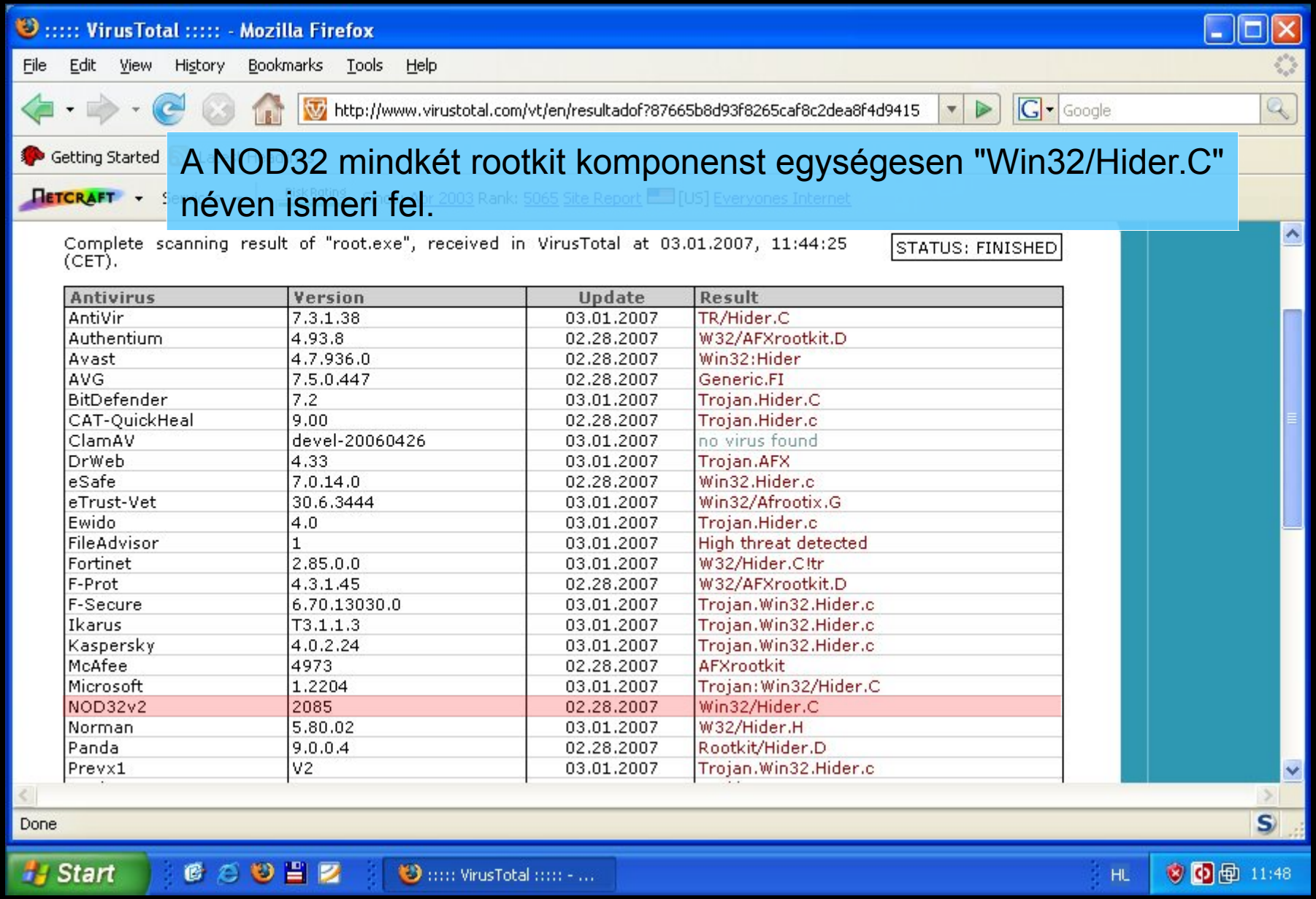


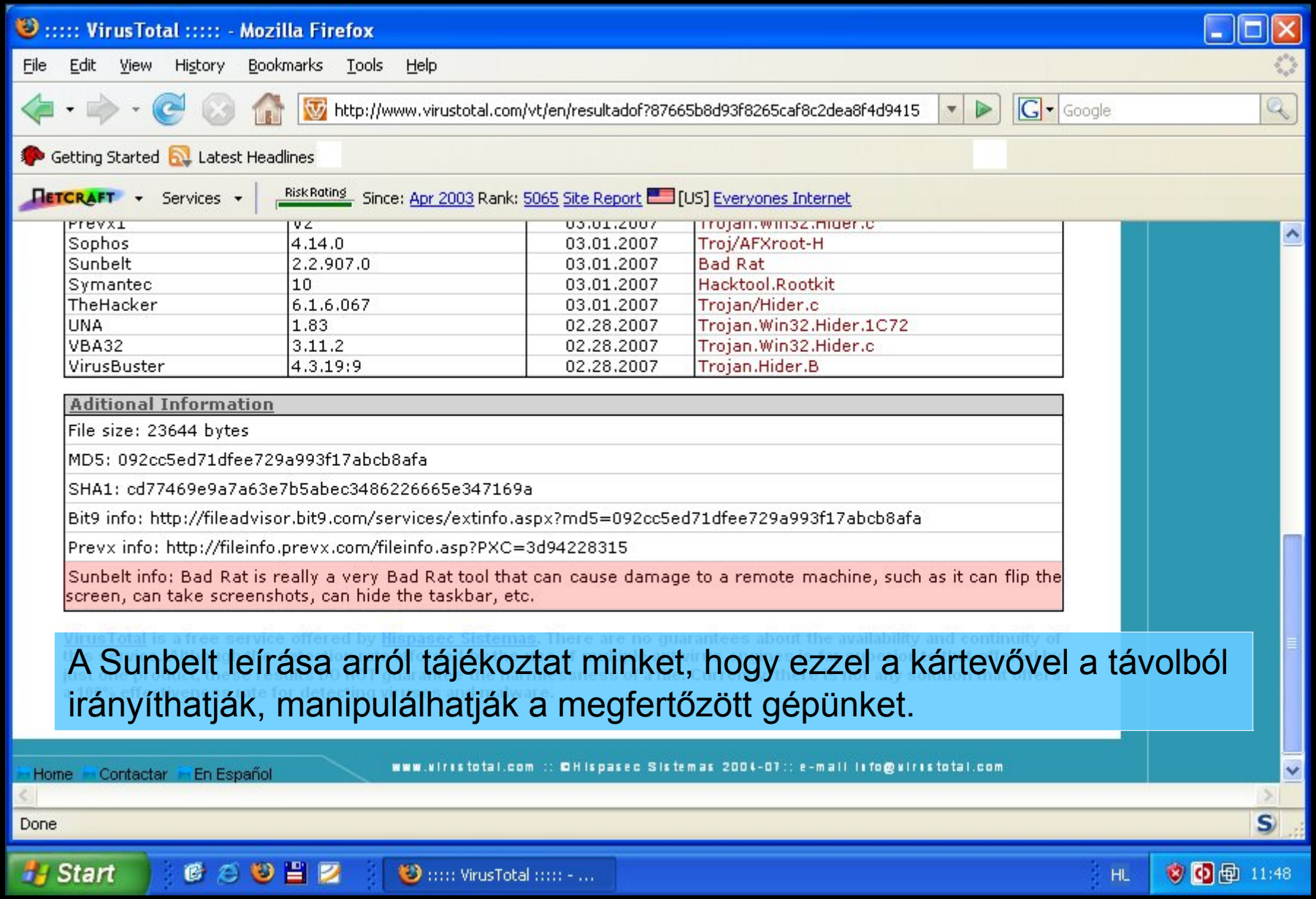
A fejlesztő teljesen nyíltan hirdet a Read.me állományban, száz amerikai dollár fejében "észlelhetetlen" rootkiteket kínál eladásra, amit Pay-pal, E-Gold, Western Union átutalással, csekken, vagy akár készpénzben is fizethetünk.


::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?bd3431befc5c89a3903a134e418fc444
Google
Getting Started
NETCRAFT
Services
A telepített rootkit komponenseit megvizsgáltattuk a www.virustotal.com weboldalon is.
A futtatáskor keletkezett "hook.dll" esetében jól láthatóan a legtöbb vírusvédelmi eszköz kimutatta a fertőzést.
File "hook.dll" received on 03.01.2007 at 11:41:00 (CET) is being scanned by VirusTotal in this moment. Results will be shown as they're generated.
STATUS: SCANNING
Antivirus | Version | Update | Result
AntiVir | 7.3.1.38 | 03.01.2007 | TR/Hider.C
Authentium | 4.93.8 | 02.28.2007 | no virus found
Avast | 4.7.936.0 | 02.28.2007 | Win32:Delf-AFL
AVG | 7.5.0.447 | 02.28.2007 | no virus found
BitDefender | 7.2 | 03.01.2007 | no virus found
CAT-QuickHeal | 9.00 | 02.28.2007 | Trojan.Hider.c
ClamAV | devel-20060426 | 03.01.2007 | no virus found
DrWeb | 4.33 | 03.01.2007 | Trojan.AFX
eSafe | 7.0.14.0 | 02.28.2007 | no virus found
eTrust-Vet | 30.6.3444 | 03.01.2007 | Win32/Afrootix.G
Ewido | 4.0 | 03.01.2007 | Trojan.Hider.g
FileAdvisor | 1 | 03.01.2007 | no virus found
Fortinet | 2.85.0.0 | 03.01.2007 | no virus found
F-Prot | 4.3.1.45 | 02.28.2007 | no virus found
F-Secure | 6.70.13030.0 | 03.01.2007 | Trojan.Win32.Hider.c
Ikarus | T3.1.1.3 | 03.01.2007 | Trojan.Win32.Hider.c
Done
Start
::::: VirusTotal ::::: - ...
HL
11:42

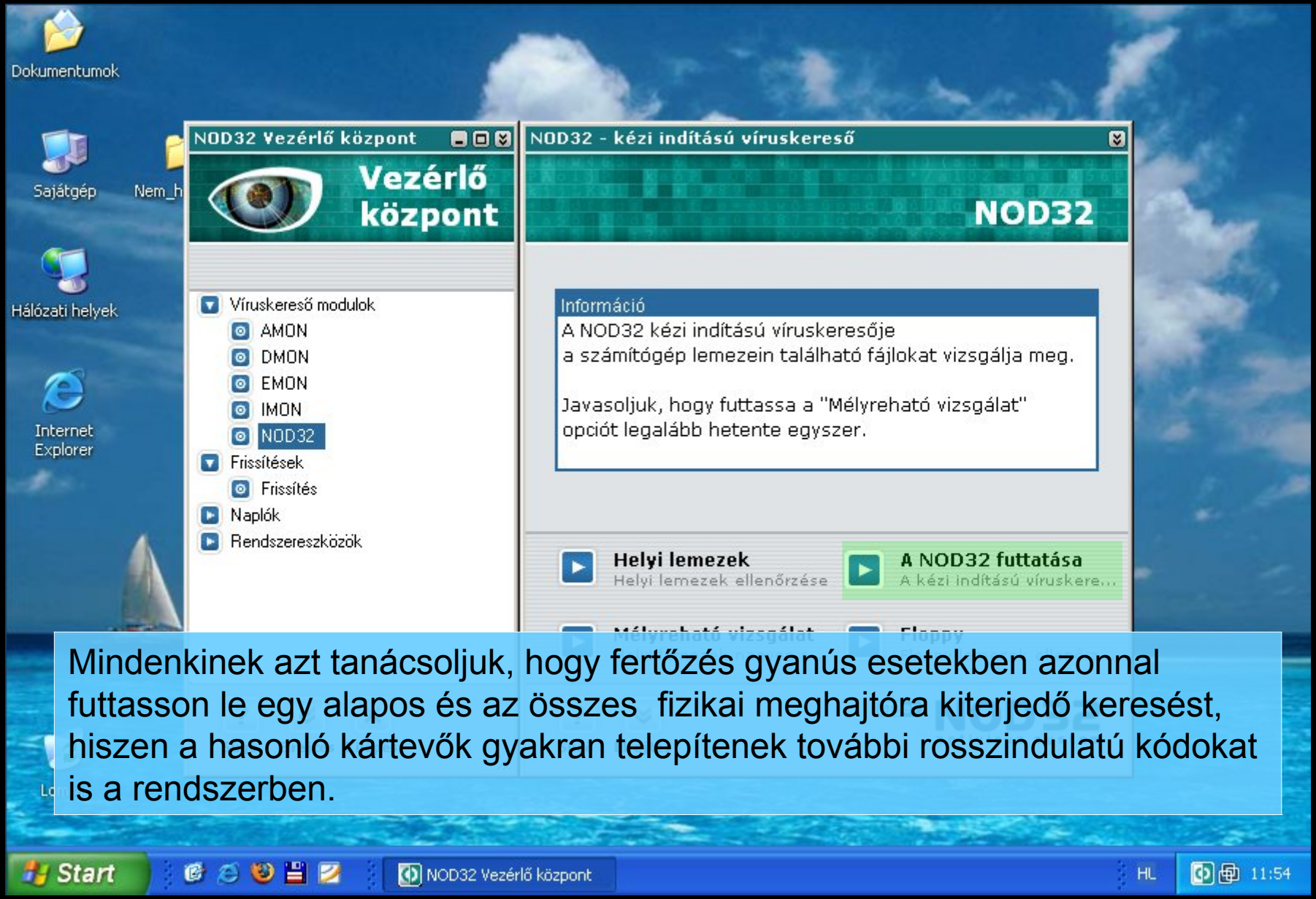

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?bd3431befc5c89a3903a134e418fc444
Google
Getting Started
Latest Headlines
NETCRAFT
Services
Risk Rating
Since: Apr 2003 Rank: 5065 Site Report
[US] Everyones Internet
eTrust-Vet 30.6.3444 03.01.2007 Win32/Afrootix.G
Ewido 4.0 03.01.2007 Trojan.Hider.g
FileAdvisor 1 03.01.2007 no virus found
Fortinet 2.85.0.0 03.01.2007 no virus found
F-Prot 4.3.1.45 02.28.2007 no virus found
F-Secure 6.70.13030.0 03.01.2007 Trojan.Win32.Hider.c
Ikarus T3.1.1.3 03.01.2007 Trojan.Win32.Hider.c
Kaspersky 4.0.2.24 03.01.2007 Trojan.Win32.Hider.c
McAfee 4973 02.28.2007 AFXrootkit.gen.b
Microsoft 1.2204 03.01.2007 Trojan:Win32/Hider.D
NOD32v2 2085 02.28.2007 Win32/Hider.C
Norman 5.80.02 03.01.2007 W32/Hider.F
Panda 9.0.0.4 02.28.2007 Rootkit/Hider.D
Prevx1 V2 03.01.2007 no virus found
Sophos 4.14.0 03.01.2007 Troj/AFXroot-H
Sunbelt 2.2.907.0 03.01.2007 no virus found
Aditional Information
File size: 34816 bytes
MD5: 0e5b3c6d78297b0fa0e78da1550e5e7a
SHA1: 14d9b6510c50c17760d7b80c3ca96dafe330f3cd
VirusTotal is a free service offered by Hispasec Sistemas. There are no guarantees about the availability and continuity of this service. Although the detection rate afforded by the use of multiple antivirus engines is far superior to that offered by just one product, these results DO NOT guarantee the harmlessness of a file. Currently, there is not any solution that offers a 100% effectiveness rate for detecting viruses and malware.
Done
Start
::::: VirusTotal ::::: - ...
HL
11:43


::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?87665b8d93f8265caf8c2dea8f4d9415
Getting Started Latest Headlines
NETCRAFT Services Risk Rating Since: Apr 2003 Rank: 5065 Site Report [US] Everyones Internet
VIRUSTOTAL
Distribute SSL Select file Browse... Send
News Statistics VirusTotal
Ez maga az AFX főprogramja.
Complete scanning result of "root.exe", received in VirusTotal at 03.01.2007, 11:44:25 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.38 | 03.01.2007 | TR/Hider.C
Authentium | 4.93.8 | 02.28.2007 | W32/AFXrootkit.D
Avast | 4.7.936.0 | 02.28.2007 | Win32:Hider
AVG | 7.5.0.447 | 02.28.2007 | Generic.FI
BitDefender | 7.2 | 03.01.2007 | Trojan.Hider.C
CAT-QuickHeal | 9.00 | 02.28.2007 | Trojan.Hider.c
ClamAV | devel-20060426 | 03.01.2007 | no virus found
DrWeb | 4.33 | 03.01.2007 | Trojan.AFX
eSafe | 7.0.14.0 | 02.28.2007 | Win32.Hider.c
eTrust-Vet | 30.6.3444 | 03.01.2007 | Win32/Afrootix.G
Ewido | 4.0 | 03.01.2007 | Trojan.Hider.c
FileAdvisor | 1 | 03.01.2007 | High threat detected
Fortinet | 2.85.0.0 | 03.01.2007 | W32/Hider.C!tr
F-Prot | 4.3.1.45 | 02.28.2007 | W32/AFXrootkit.D
F-Secure | 6.70.13030.0 | 03.01.2007 | Trojan.Win32.Hider.c
Ikarus | T3.1.1.3 | 03.01.2007 | Trojan.Win32.Hider.c
Done
Start
::::: VirusTotal ::::: - ...
HL
11:48


::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?87665b8d93f8265caf8c2dea8f4d9415
Google
Getting Started
NETCRAFT
A NOD32 mindkét rootkit komponenst egységesen "Win32/Hider.C" néven ismeri fel.
Complete scanning result of "root.exe", received in VirusTotal at 03.01.2007, 11:44:25 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.38 | 03.01.2007 | TR/Hider.C
Authentium | 4.93.8 | 02.28.2007 | W32/AFXrootkit.D
Avast | 4.7.936.0 | 02.28.2007 | Win32:Hider
AVG | 7.5.0.447 | 02.28.2007 | Generic.FI
BitDefender | 7.2 | 03.01.2007 | Trojan.Hider.C
CAT-QuickHeal | 9.00 | 02.28.2007 | Trojan.Hider.c
ClamAV | devel-20060426 | 03.01.2007 | no virus found
DrWeb | 4.33 | 03.01.2007 | Trojan.AFX
eSafe | 7.0.14.0 | 02.28.2007 | Win32.Hider.c
eTrust-Vet | 30.6.3444 | 03.01.2007 | Win32/Afrootix.G
Ewido | 4.0 | 03.01.2007 | Trojan.Hider.c
FileAdvisor | 1 | 03.01.2007 | High threat detected
Fortinet | 2.85.0.0 | 03.01.2007 | W32/Hider.C!tr
F-Prot | 4.3.1.45 | 02.28.2007 | W32/AFXrootkit.D
F-Secure | 6.70.13030.0 | 03.01.2007 | Trojan.Win32.Hider.c
Ikarus | T3.1.1.3 | 03.01.2007 | Trojan.Win32.Hider.c
Kaspersky | 4.0.2.24 | 03.01.2007 | Trojan.Win32.Hider.c
McAfee | 4973 | 02.28.2007 | AFXrootkit
Microsoft | 1.2204 | 03.01.2007 | Trojan:Win32/Hider.C
NOD32v2 | 2085 | 02.28.2007 | Win32/Hider.C
Norman | 5.80.02 | 03.01.2007 | W32/Hider.H
Panda | 9.0.0.4 | 02.28.2007 | Rootkit/Hider.D
Prevx1 | V2 | 03.01.2007 | Trojan.Win32.Hider.c
Done
Start
::::: VirusTotal ::::: - ...
HL
11:48

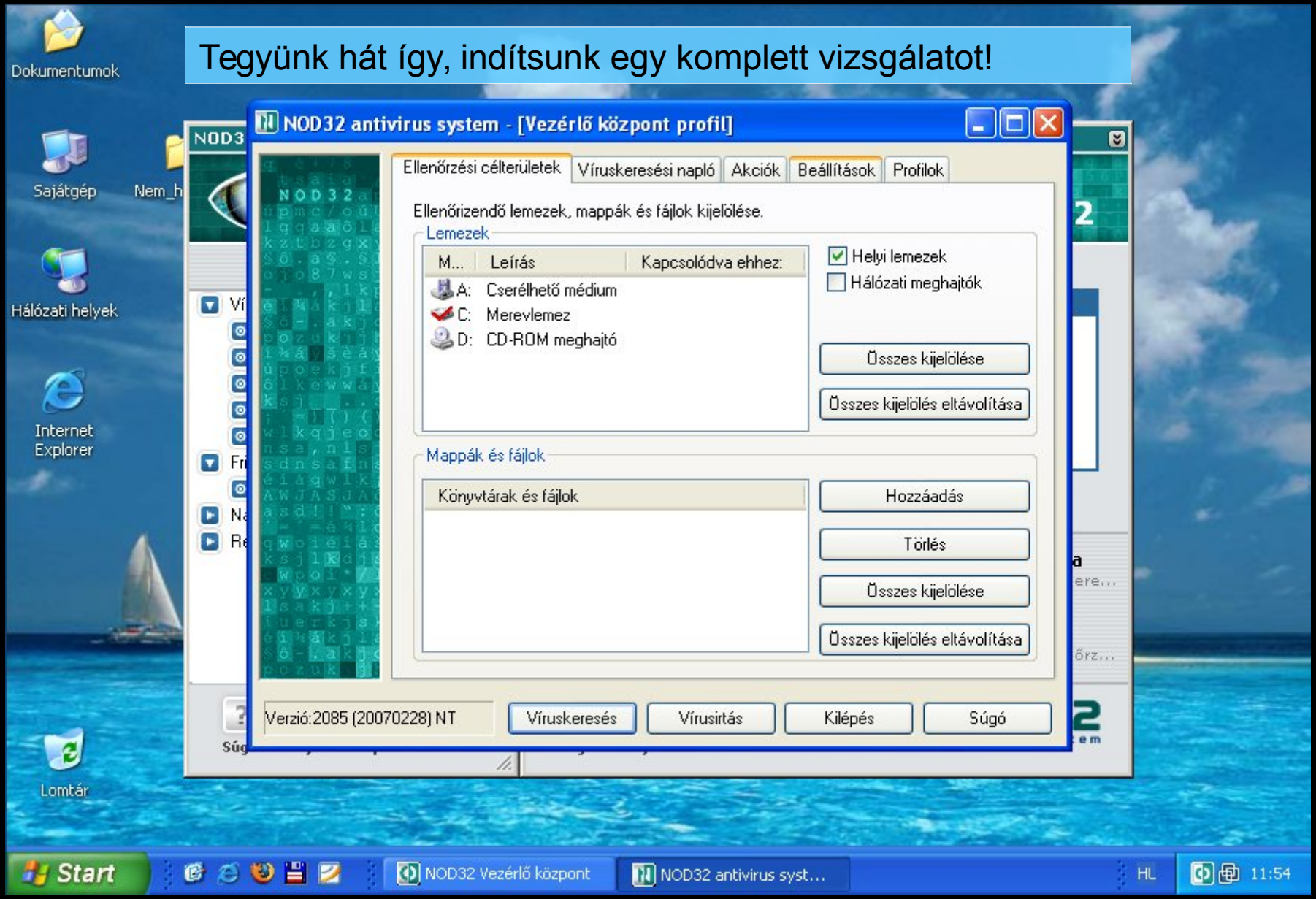


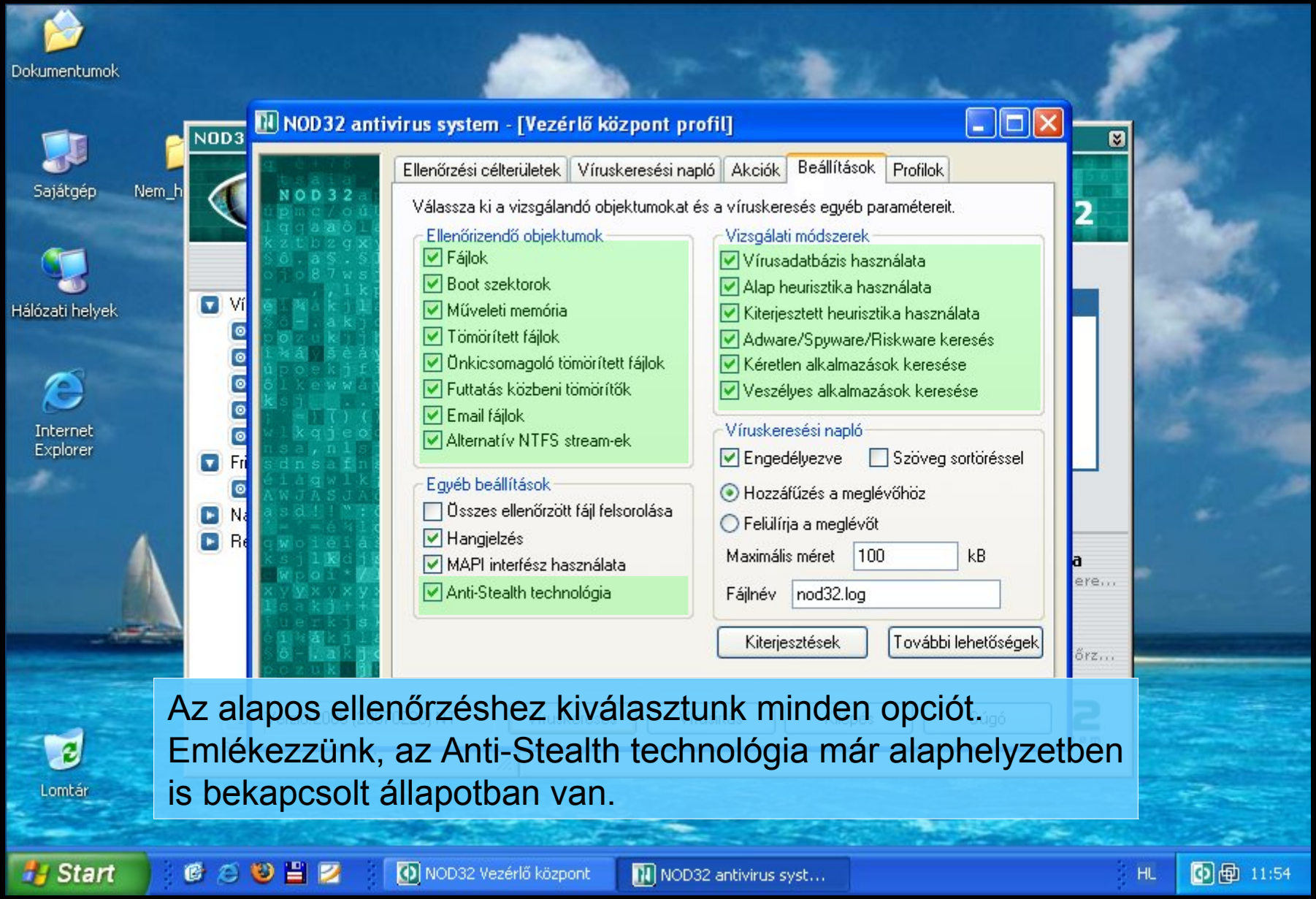
A Sunbelt leírása arról tájékoztat minket, hogy ezzel a kártevővel a távolból irányíthatják, manipulálhatják a megfertőzött gépünket.



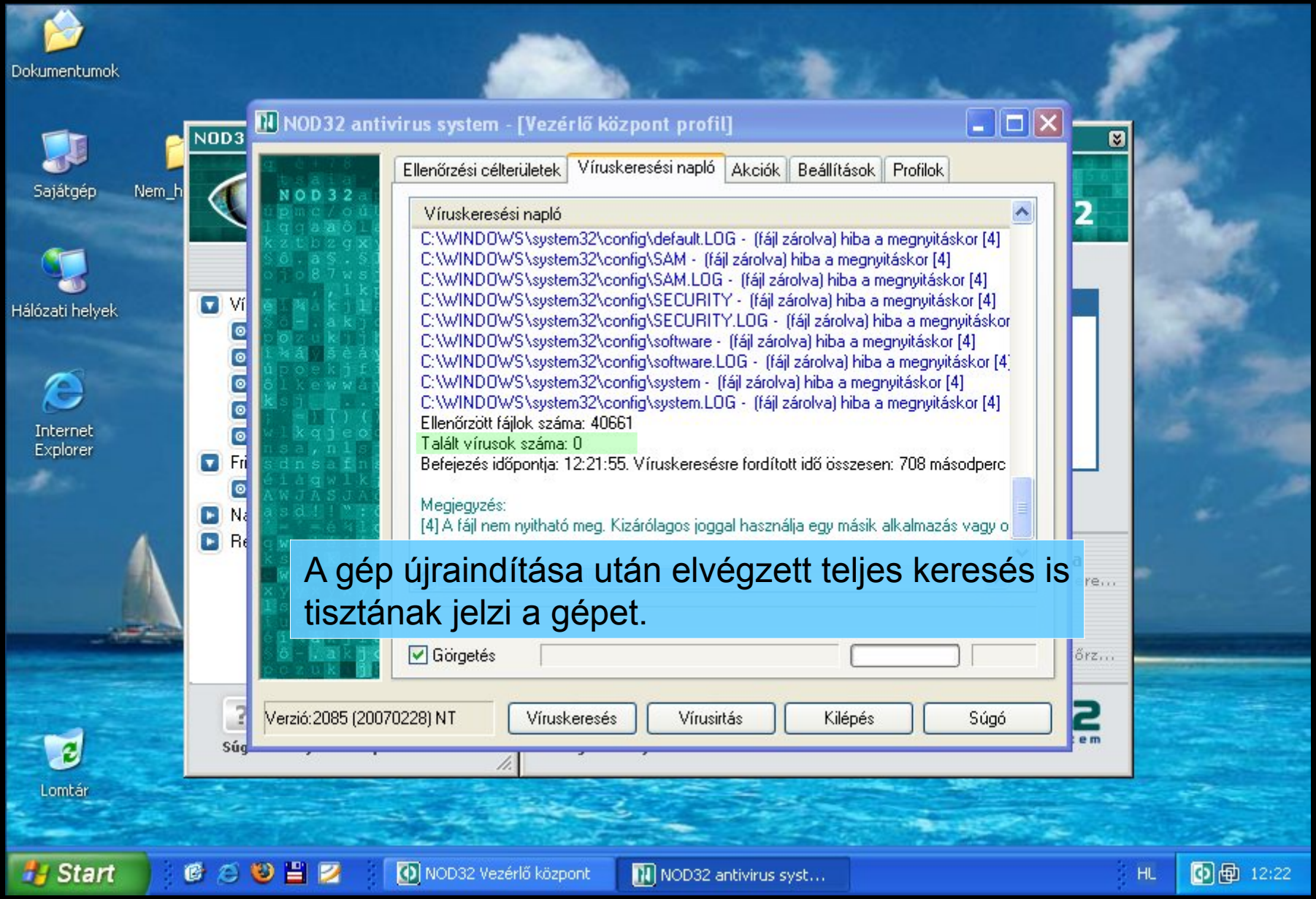
Mindenkinek azt tanácsoljuk, hogy fertőzés gyanús esetekben azonnal futtasson le egy alapos és az összes fizikai meghajtóra kiterjedő keresést, hiszen a hasonló kártevők gyakran telepítenek további rosszindulatú kódokat is a rendszerben.

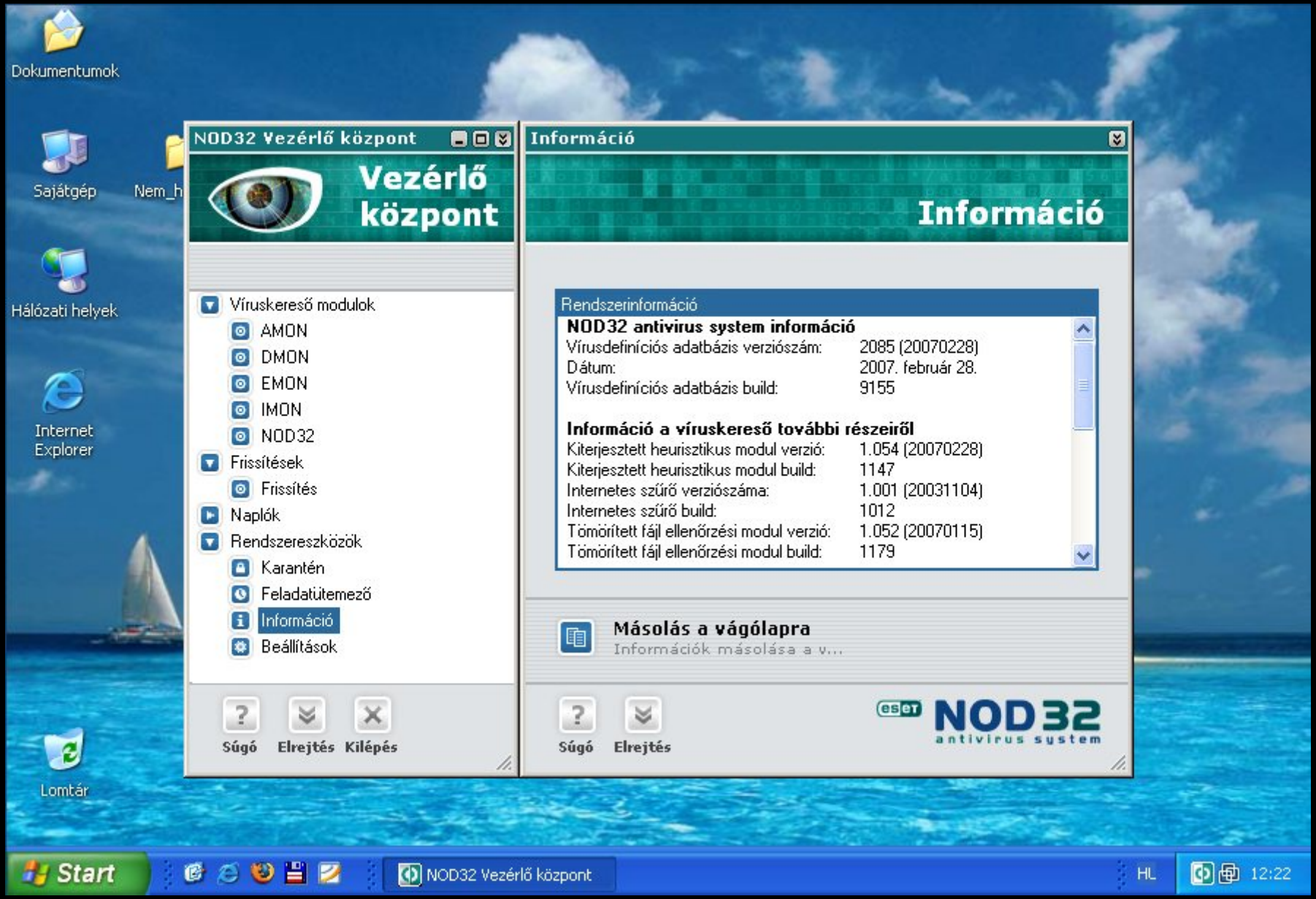
Tegyünk hát így, indítsunk egy komplett vizsgálatot!

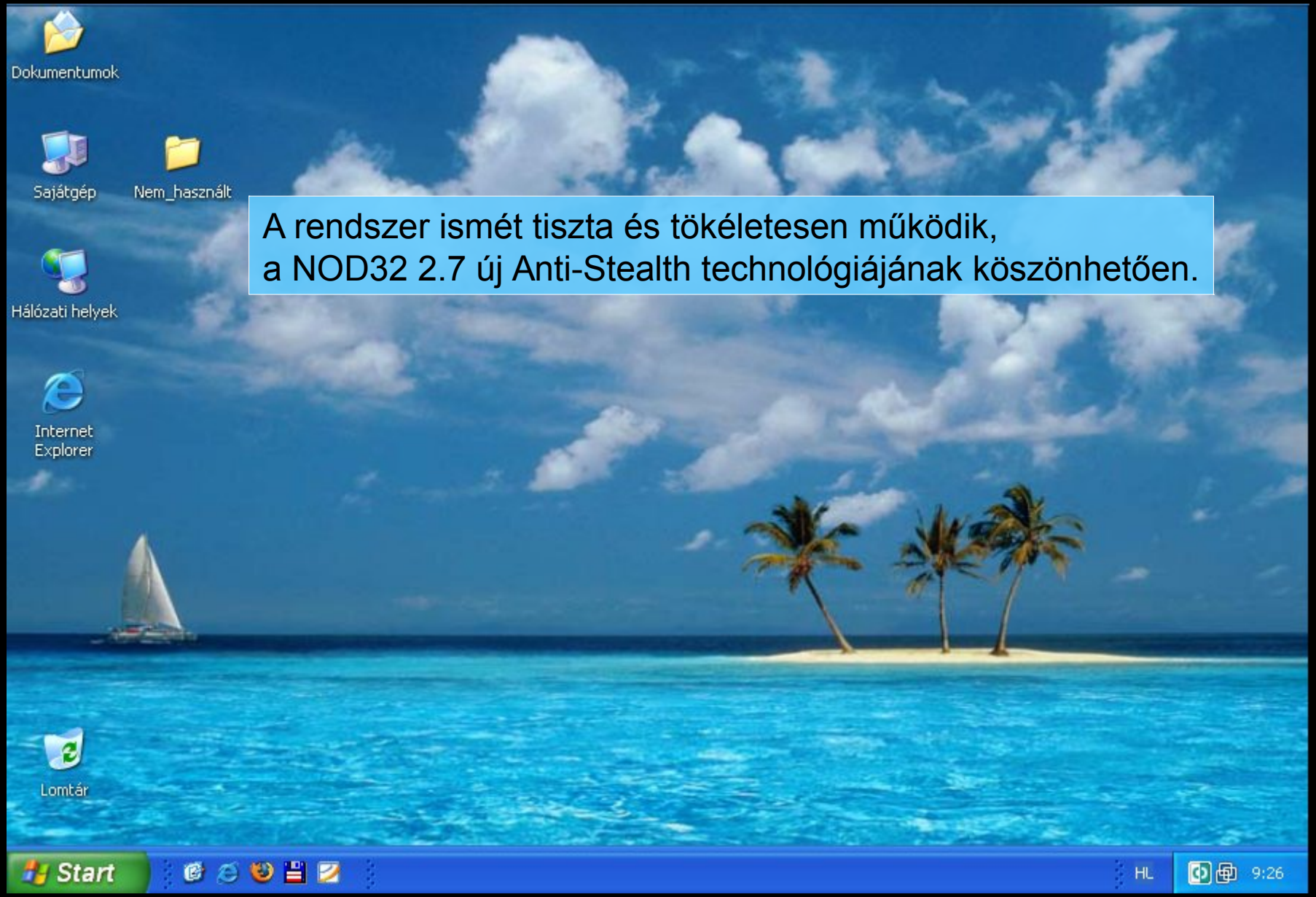


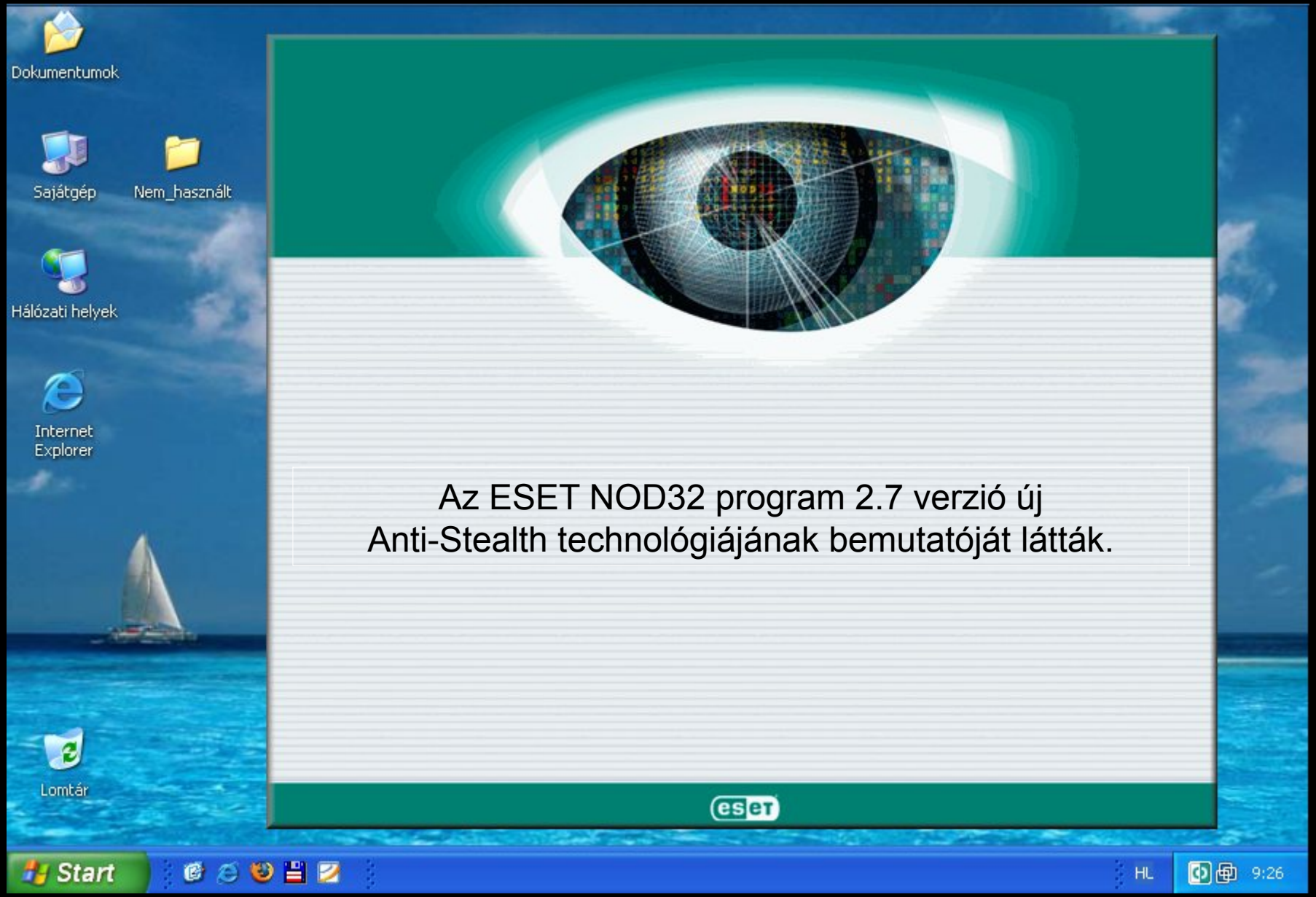


Az alapos ellenőrzéshez kiválasztunk minden opciót. Emlékezzünk, az Anti-Stealth technológia már alaphelyzetben is bekapcsolt állapotban van.


Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - [Vezérlő központ profil]
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Víruskeresési napló
C:\WINDOWS\system32\config\default.LOG - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SAM - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SAM.LOG - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SECURITY - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\SECURITY.LOG - (fájl zárolva) hiba a megnyitáskor
C:\WINDOWS\system32\config\software - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\software.LOG - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\system - (fájl zárolva) hiba a megnyitáskor [4]
C:\WINDOWS\system32\config\system.LOG - (fájl zárolva) hiba a megnyitáskor [4]
Ellenőrzött fájlok száma: 40661
Talált vírusok száma: 0
Befejezés időpontja: 12:21:55. Víruskeresésre fordított idő összesen: 708 másodperc
Megjegyzés:
[4] A fájl nem nyitható meg. Kizárólagos joggal használja egy másik alkalmazás vagy o
Görgetés
Verzió:2085 (20070228) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
A gép újraindítása után elvégzett teljes keresés is tisztának jelzi a gépet.
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HU
12:22


Dokumentumok
Sajátgép
Nem_h
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Karantén
Feladatütemező
Információ
Beállítások
Súgó
Elrejtés
Kilépés
Információ
Információ
Rendszerinformáció
NOD32 antivirus system információ
Vírusdefiníciós adatbázis verziószám: 2085 (20070228)
Dátum: 2007. február 28.
Vírusdefiníciós adatbázis build: 9155
Információ a víruskereső további részeiről
Kiterjesztett heurisztikus modul verzió: 1.054 (20070228)
Kiterjesztett heurisztikus modul build: 1147
Internetes szűrő verziószáma: 1.001 (20031104)
Internetes szűrő build: 1012
Tömörített fájl ellenőrzési modul verzió: 1.052 (20070115)
Tömörített fájl ellenőrzési modul build: 1179
Másolás a vágólapra
Információk másolása a v...
Súgó
Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
HL
12:22


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
A rendszer ismét tiszta és tökéletesen működik,
a NOD32 2.7 új Anti-Stealth technológiájának köszönhetően.
Start
HL
9:26


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Az ESET NOD32 program 2.7 verzió új
Anti-Stealth technológiájának bemutatóját látták.
eset
Start
HL
9:26