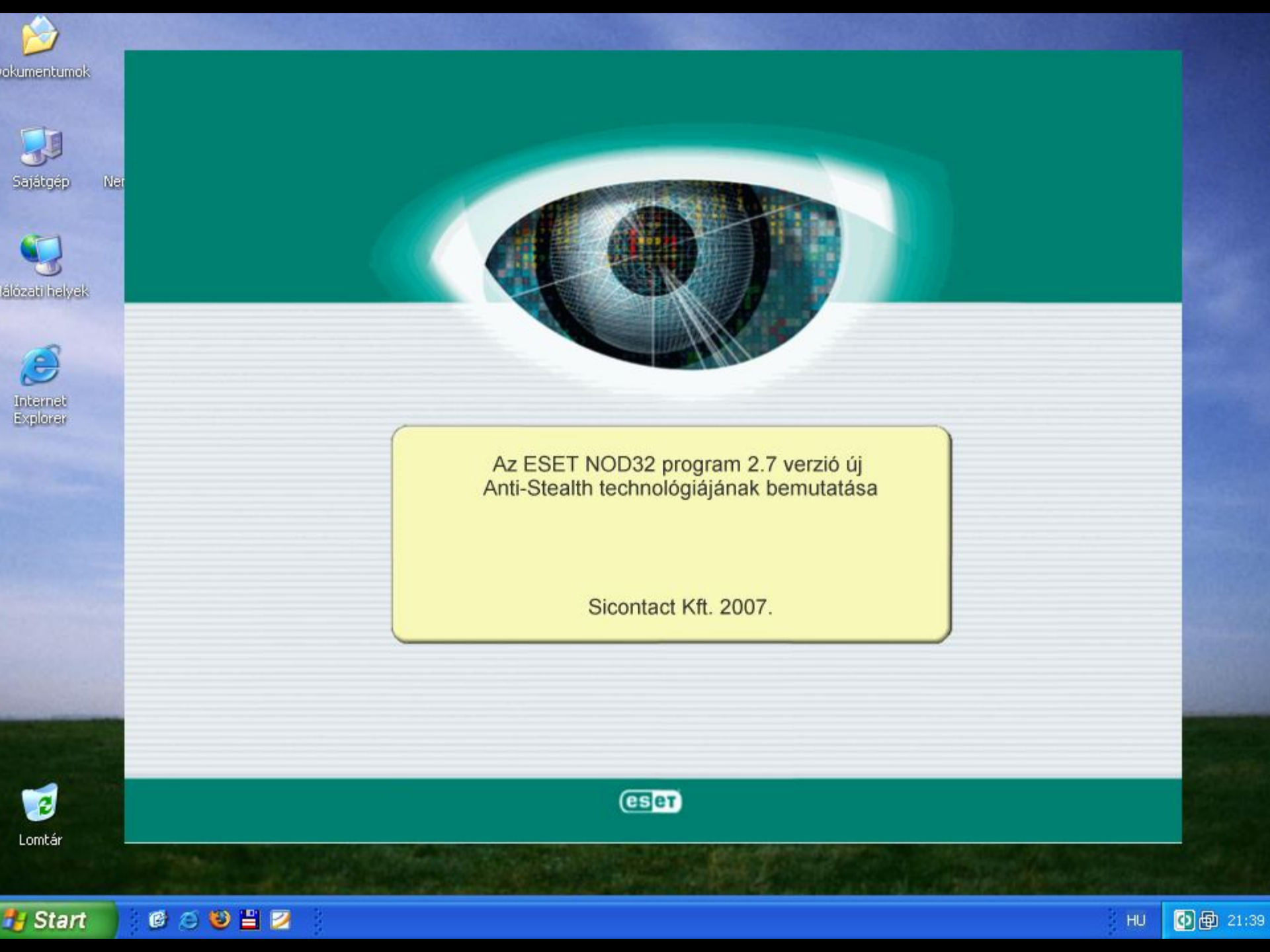

okumentumok
Sajátgép
Ne
lózati helyek
Internet Explorer
Lomtár
Az ESET NOD32 program 2.7 verzió új
Anti-Stealth technológiájának bemutatása
Sicontact Kft. 2007.
eset
Start
HU
21:39

Bemutató 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 HackerDefender nevű készlet 1.0.0 revisited csomagját töltöttük le, és azzel végeztük a kísérletet.

A HackerDefender az egyik leginkább elterjedt rootkit - köszönhetően a szabadon hozzáférhető nyílt forráskódnak, de már létezik belőle kereskedelmi változat is. A HackerDefender az "NTDLL.DLL" függvénykönyvtár foltozásával (ntdll.dll 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:

"bdcli100.exe„	- A HackerDefender hátsó ajtó (backdoor) kliense*
"hxdef100.exe„	- A Hacker Defender főprogramja
"hxdOFena.exe"	- A Hacker Defender főprogram módosított változata
"rdrbs100.exe„	- A Hacker Defender port átirányító programja*

**Példánkban a hátsóajtót és a port átirányítást nem használtuk ki, de ezek a komponensek is automatikusan elrejtésre kerültek a rootkit használata során. A rootkiteket leggyakrabban pontosan arra használják, hogy segítségükkel különféle eljárásokat, program állományokat álcázzanak.*

eset

Sajátgép

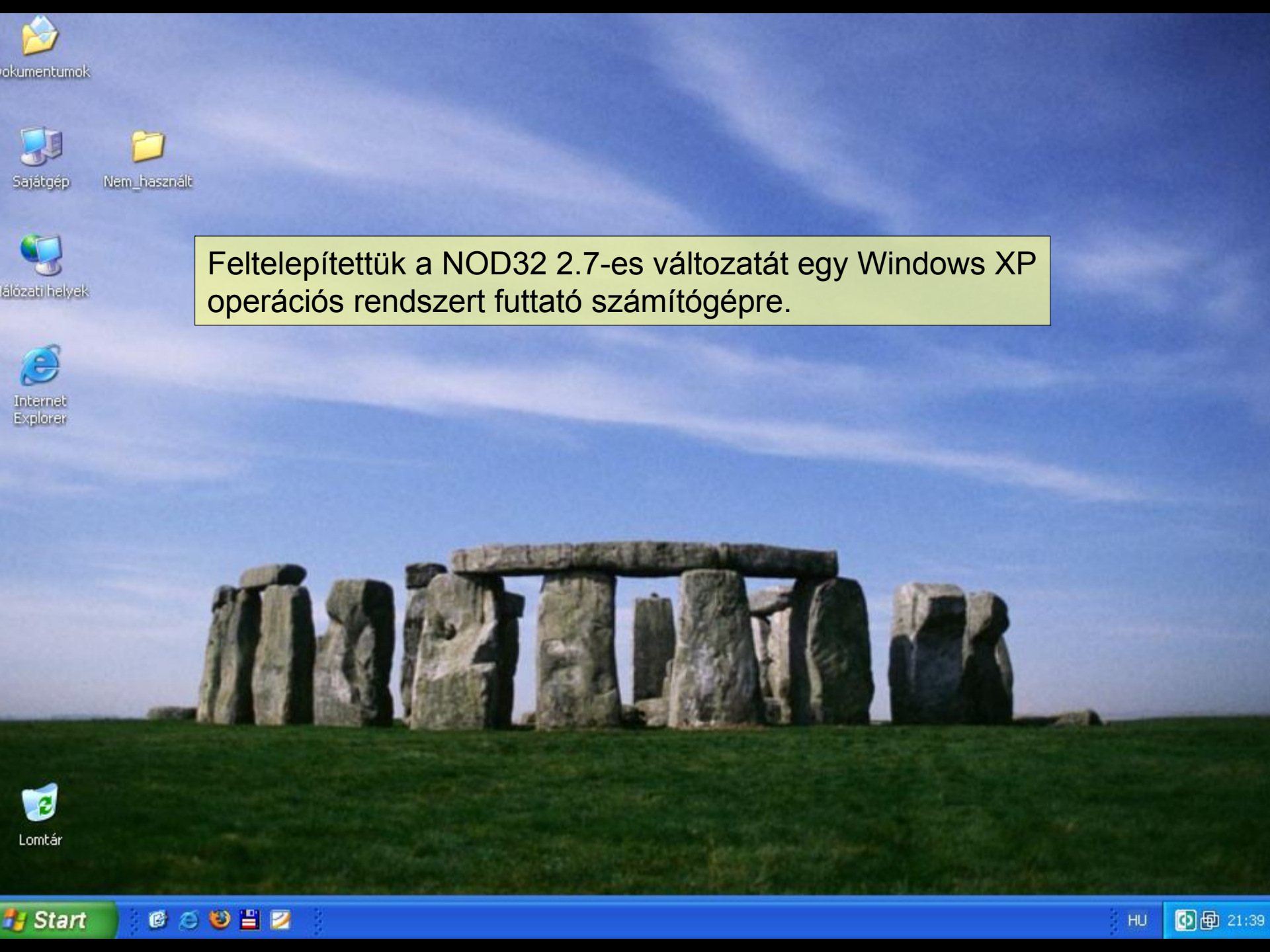
Internet Explorer

Lomtár

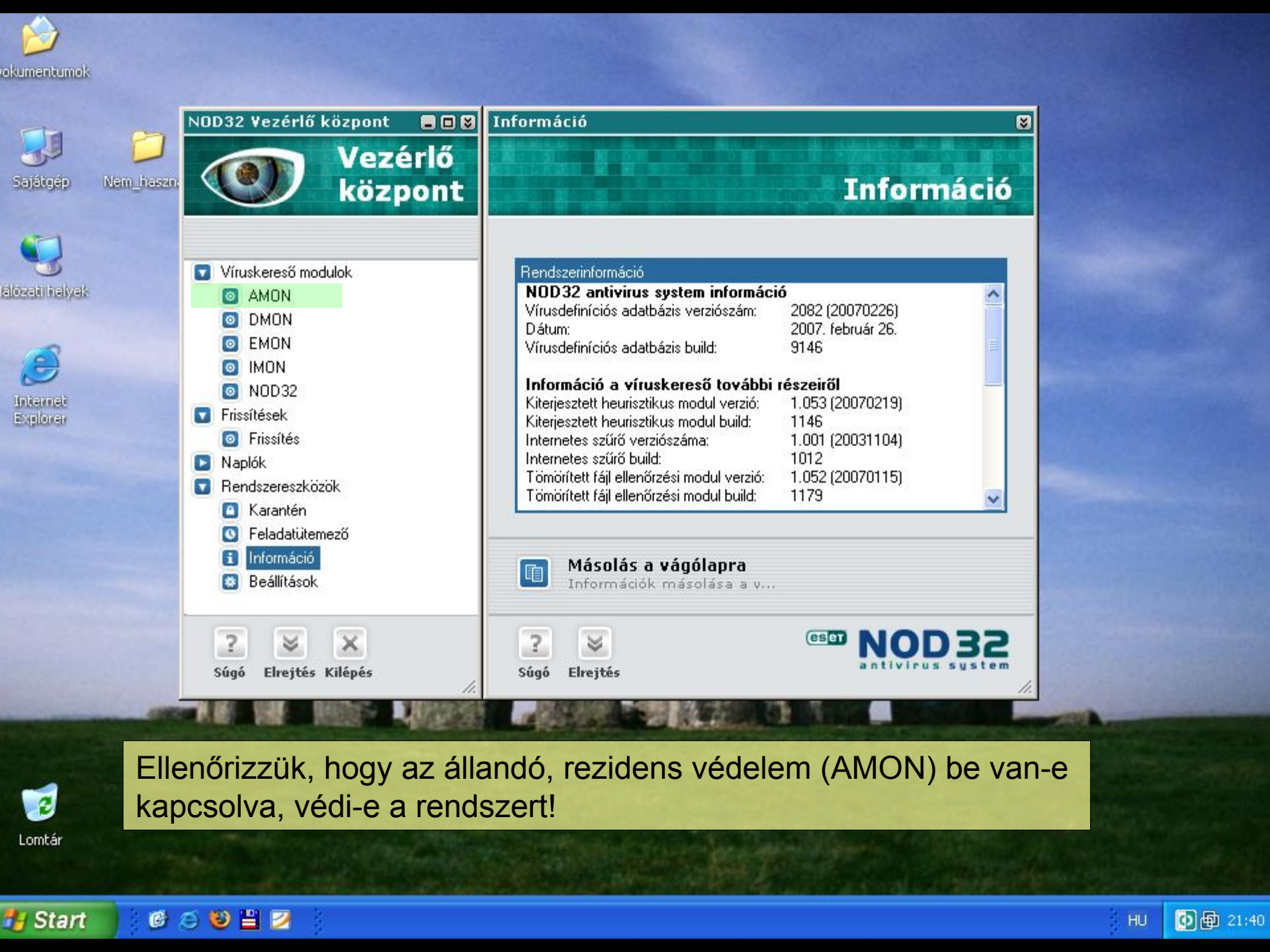
Start

HU

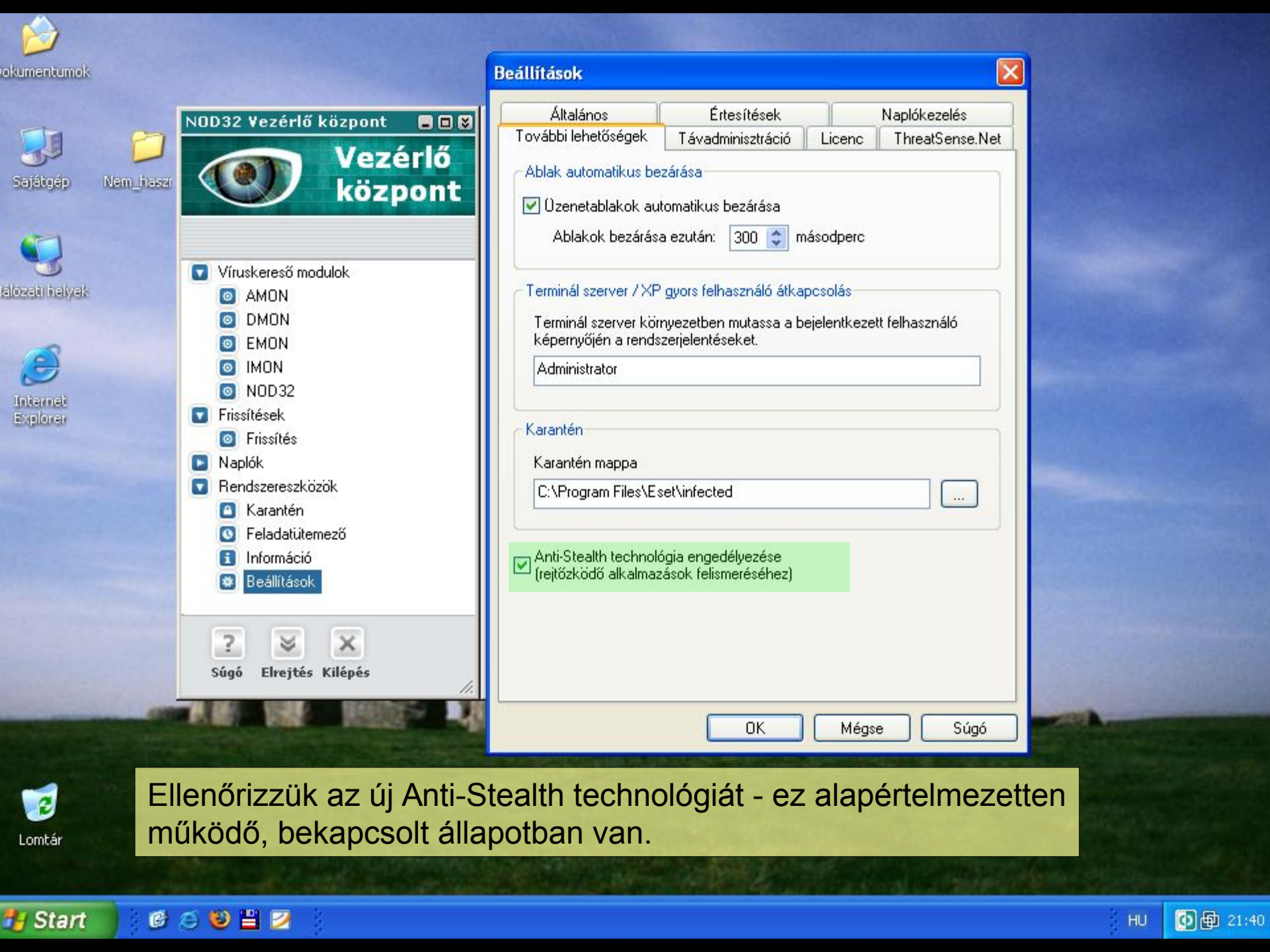
21:39



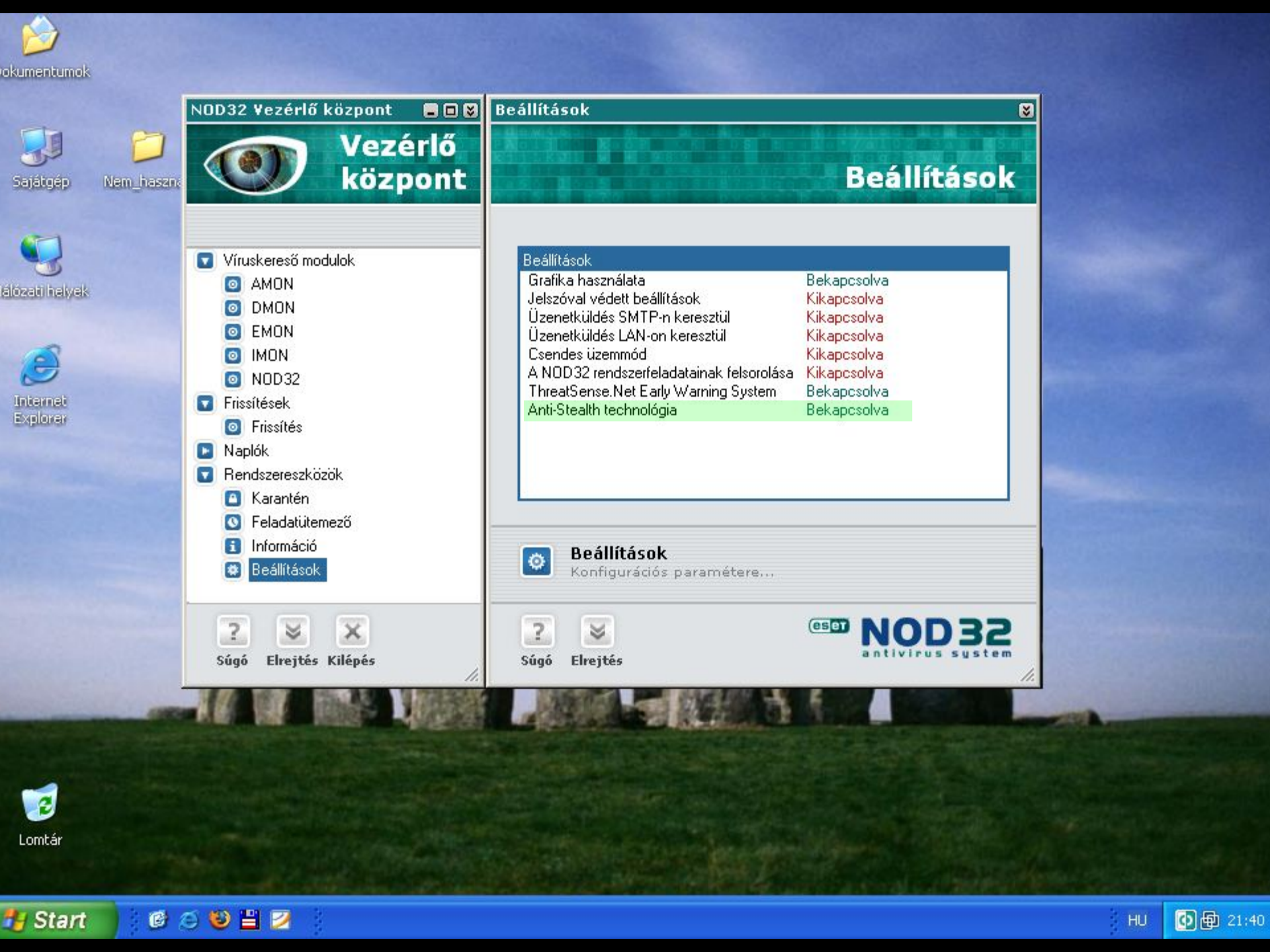
Feltelepítettük a NOD32 2.7-es változatát egy Windows XP operációs rendszert futtató számítógépre.

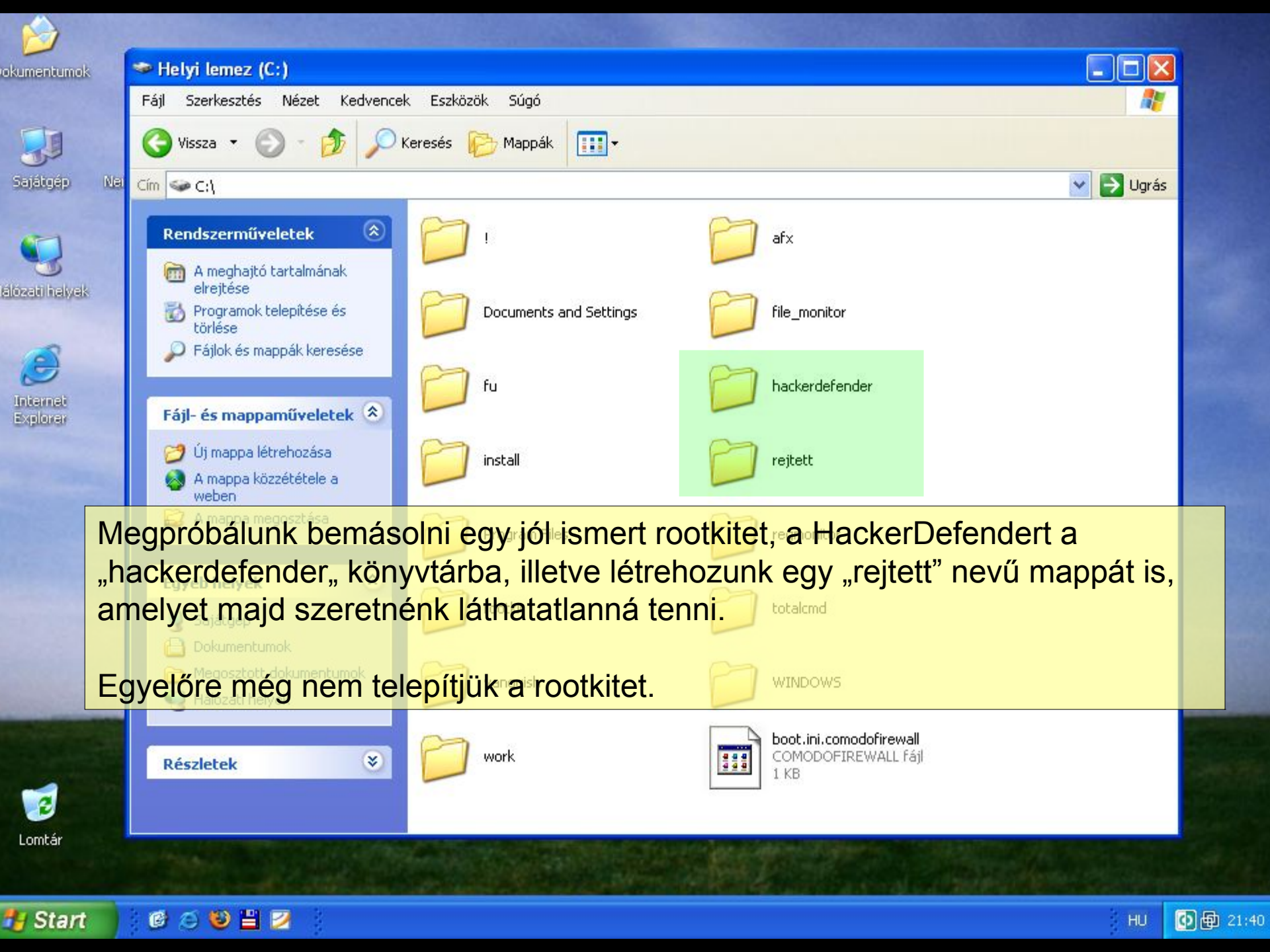


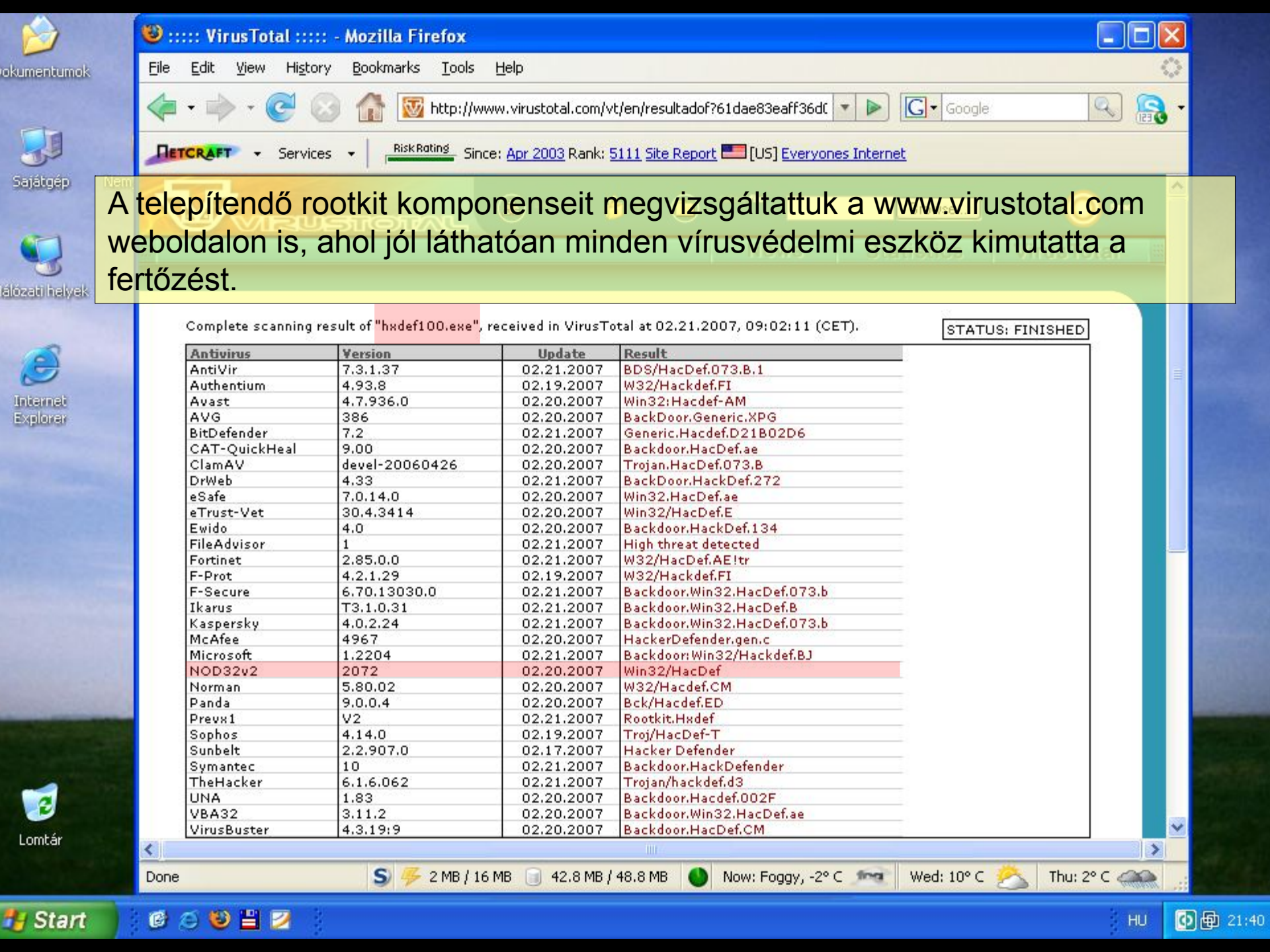
Ellenőrizzük, hogy az állandó, rezidens védelem (AMON) be van-e kapcsolva, védi-e a rendszert!

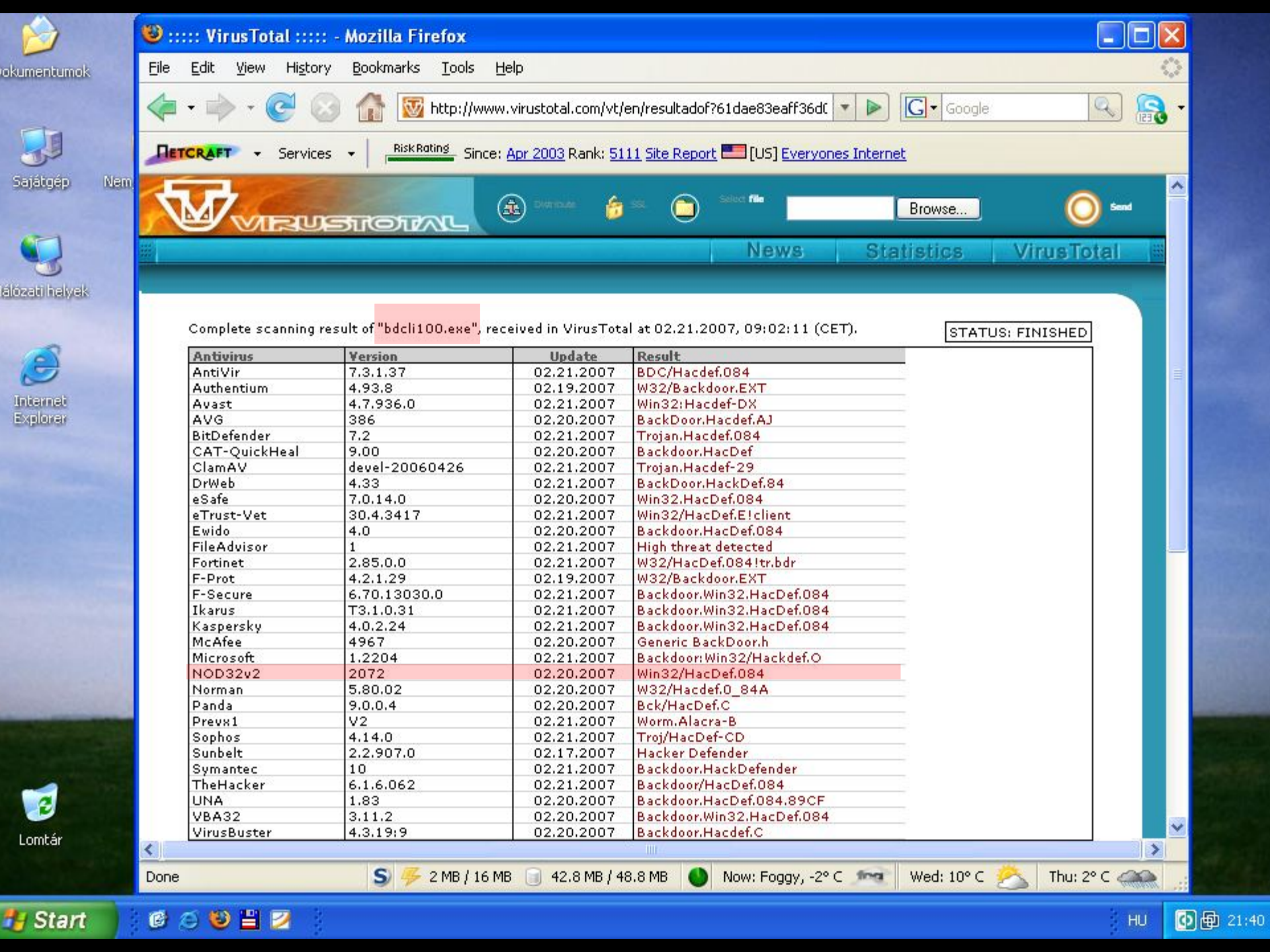


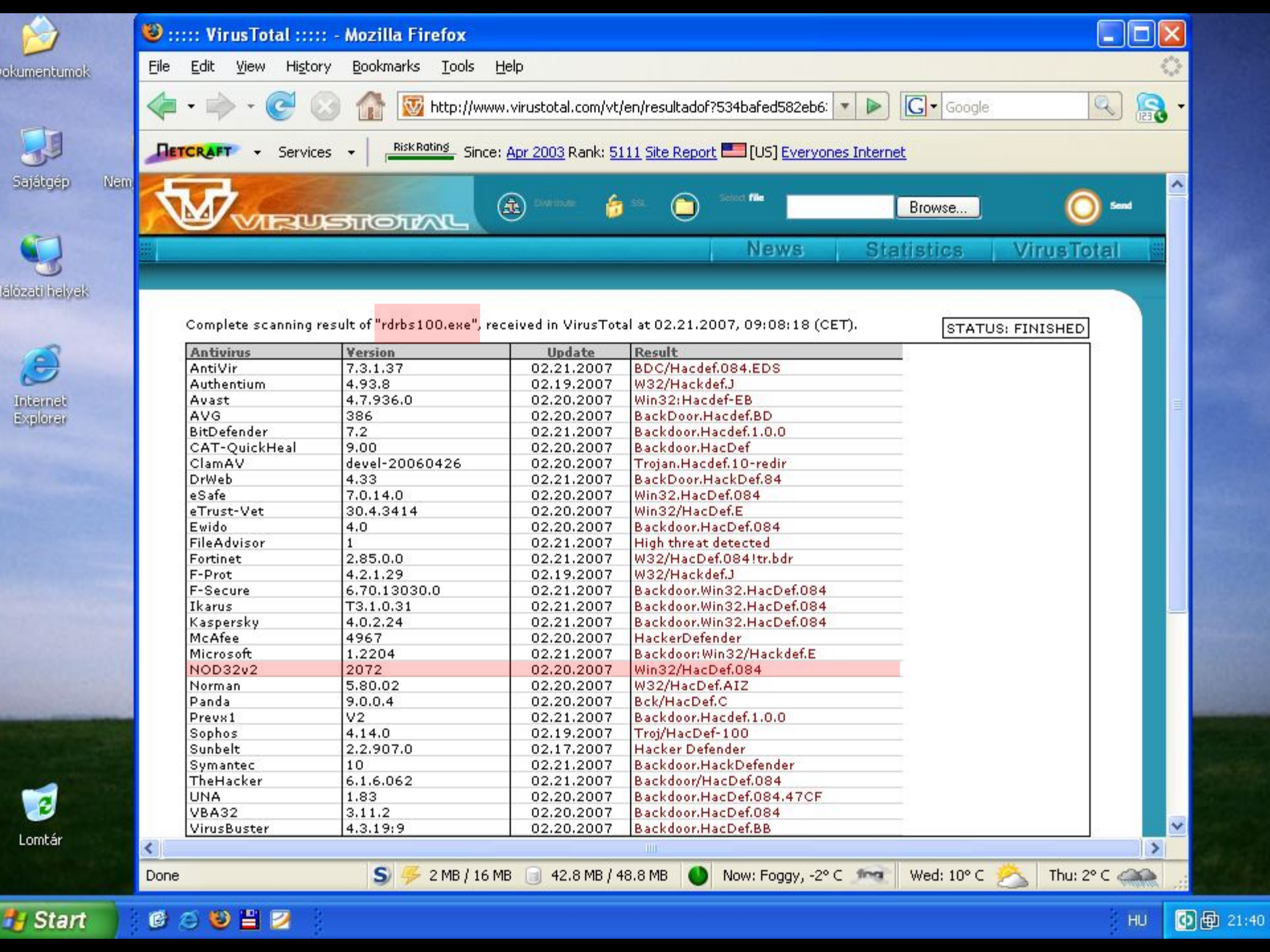
Ellenőrizzük az új Anti-Stealth technológiát - ez alapértelmezetten működő, bekapcsolt állapotban van.

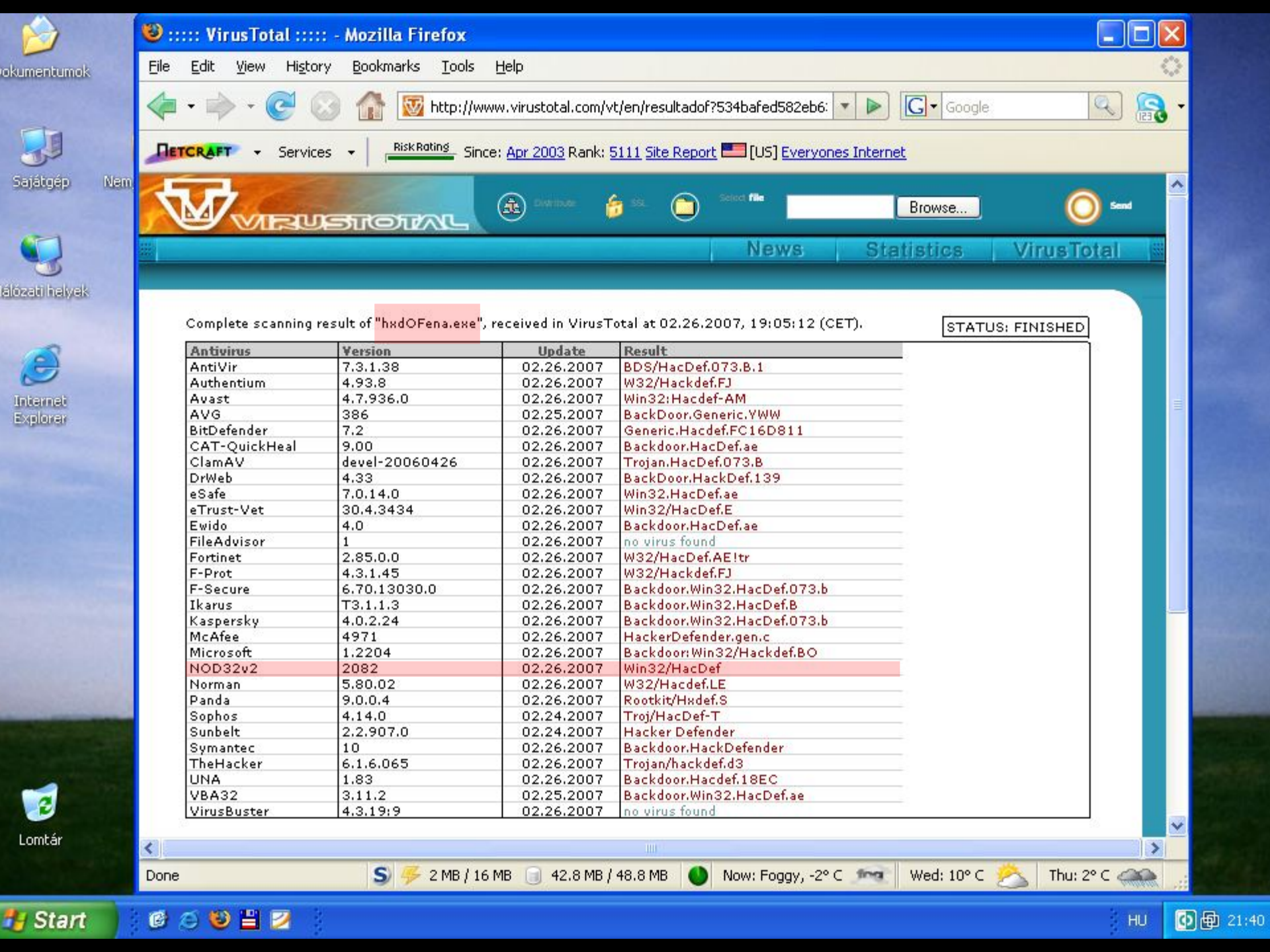

NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Karantén
Feladatütemező
Információ
Beállítások
Súgó
Elrejtés
Kilépés
Beállítások
Beállítások
Beállítások
Grafika használata Bekapcsolva
Jelszóval védett beállítások Kikapcsolva
Üzenetküldés SMTP-n keresztül Kikapcsolva
Üzenetküldés LAN-on keresztül Kikapcsolva
Csendes üzemmód Kikapcsolva
A NOD32 rendszerfeladatainak felsorolása Kikapcsolva
ThreatSense.Net Early Warning System Bekapcsolva
Anti-Stealth technológia Bekapcsolva
Beállítások
Konfigurációs paramétere...
Súgó
Elrejtés
eset NOD32 antivirus system
Sajátgép
Internet Explorer
Lomtár
Start
HU
21:40

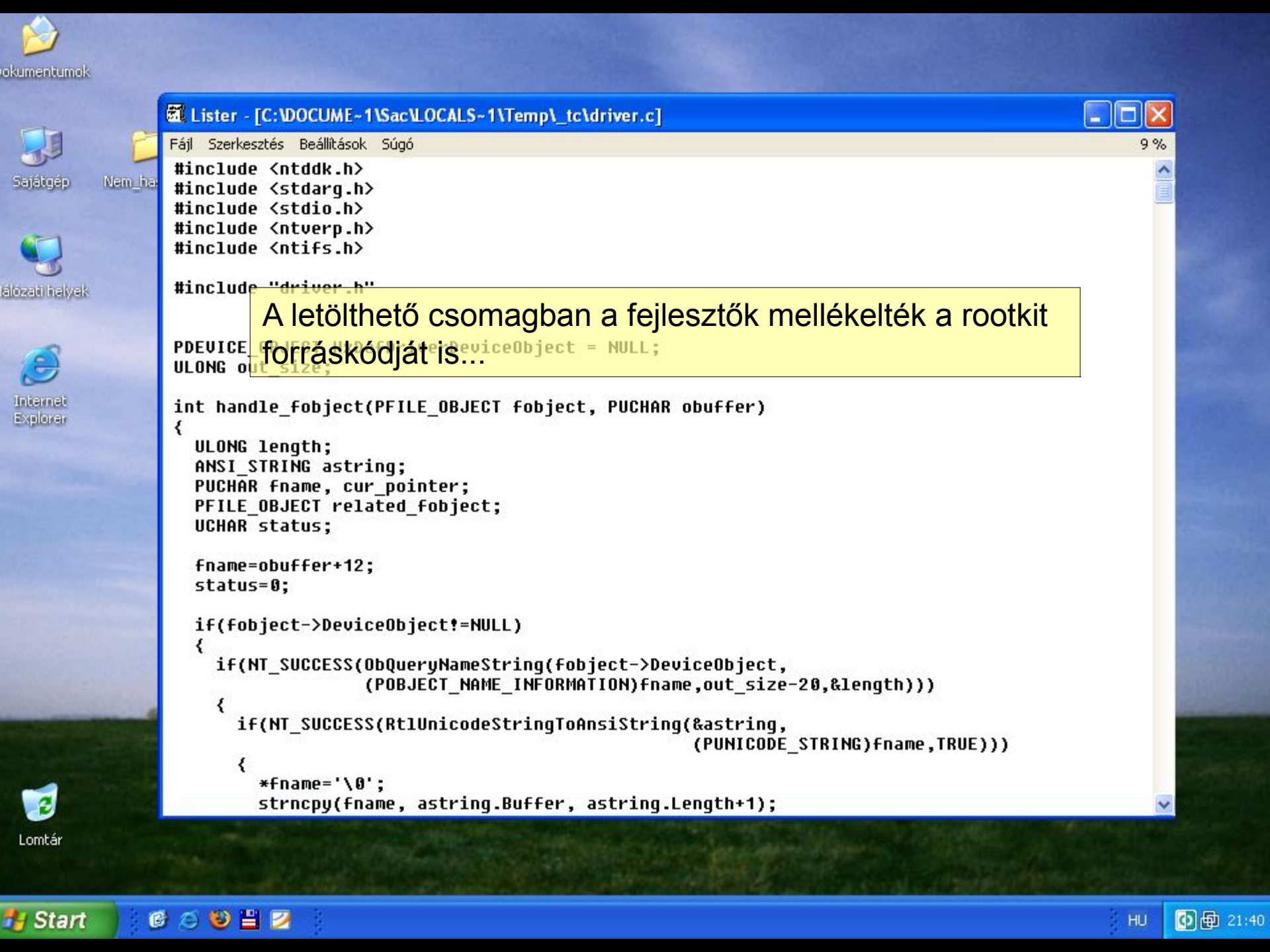

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza Keresés Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaműveletek
Új mappa létrehozása
A mappa közzététele a weben
Részletek
!
afx
Documents and Settings
file_monitor
fu
hackerdefender
install
rejtett
totalcmd
WINDOWS
work
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
Megpróbálunk bemásolni egy jól ismert rootkitet, a HackerDefendert a „hackerdefender„ könyvtárba, illetve létrehozunk egy „rejtett” nevű mappát is, amelyet majd szeretnénk láthatatlanná tenni.
Egyelőre még nem telepítjük a rootkitet.
Sajátgép
Internet Explorer
Lomtár
Start
HU
21:40

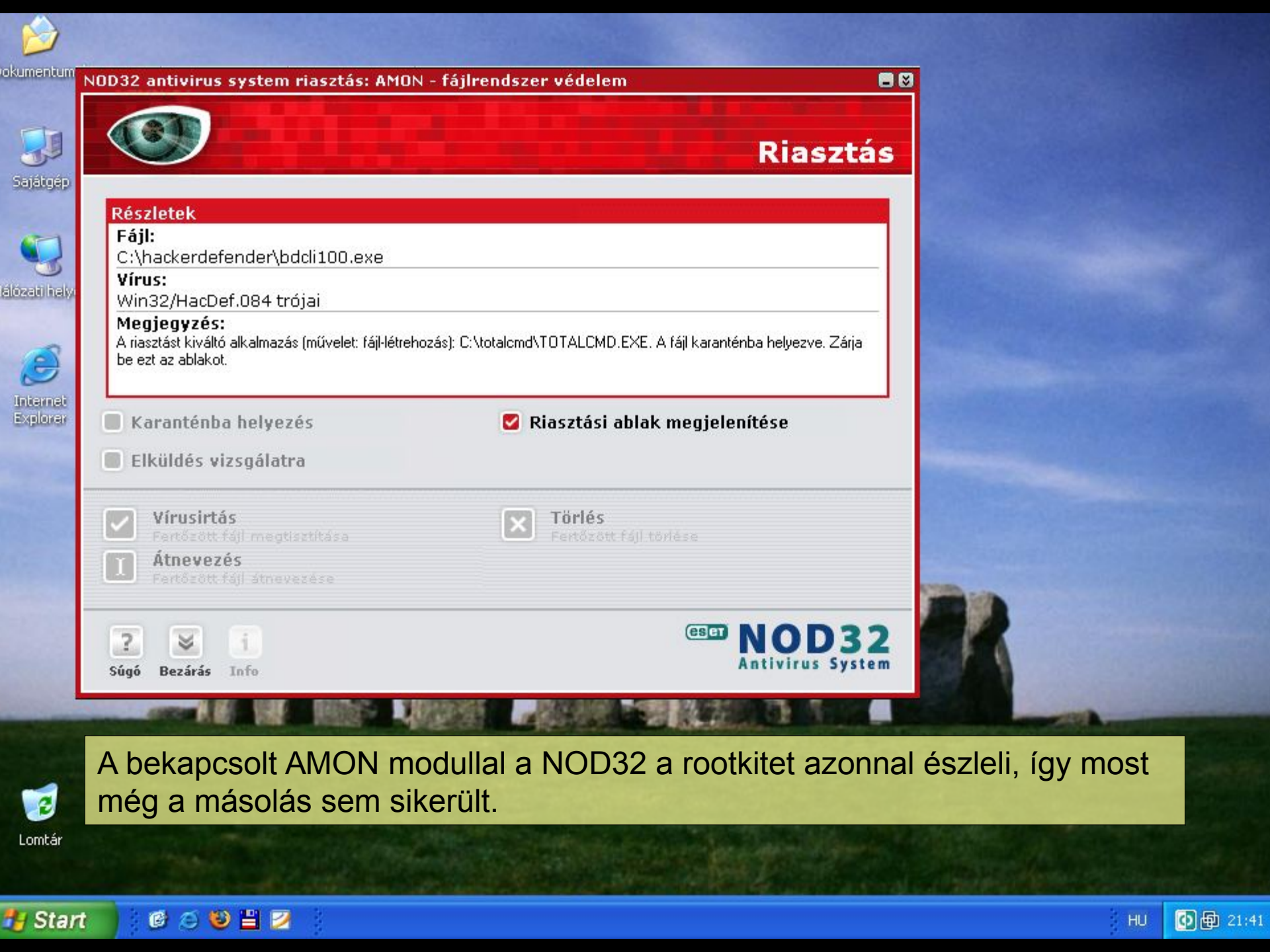

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?61dae83eaff36d(
Google
NETCRAFT Services Risk Rating Since: Apr 2003 Rank: 5111 Site Report [US] Everyones Internet
A telepítendő rootkit komponenseit megvizsgáltattuk a www.virustotal.com weboldalon is, ahol jól láthatóan minden vírusvédelmi eszköz kimutatta a fertőzést.
Complete scanning result of "hxdef100.exe", received in VirusTotal at 02.21.2007, 09:02:11 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.37 | 02.21.2007 | BDS/HacDef.073.B.1
Authentium | 4.93.8 | 02.19.2007 | W32/Hackdef.FI
Avast | 4.7.936.0 | 02.20.2007 | Win32:Hacdef-AM
AVG | 386 | 02.20.2007 | BackDoor.Generic.XPG
BitDefender | 7.2 | 02.21.2007 | Generic.Hacdef.D21B02D6
CAT-QuickHeal | 9.00 | 02.20.2007 | Backdoor.HacDef.ae
ClamAV | devel-20060426 | 02.20.2007 | Trojan.HacDef.073.B
DrWeb | 4.33 | 02.21.2007 | BackDoor.HackDef.272
eSafe | 7.0.14.0 | 02.20.2007 | Win32.HacDef.ae
eTrust-Vet | 30.4.3414 | 02.20.2007 | Win32/HacDef.E
Ewido | 4.0 | 02.20.2007 | Backdoor.HackDef.134
FileAdvisor | 1 | 02.21.2007 | High threat detected
Fortinet | 2.85.0.0 | 02.21.2007 | W32/HacDef.AE!tr
F-Prot | 4.2.1.29 | 02.19.2007 | W32/Hackdef.FI
F-Secure | 6.70.13030.0 | 02.21.2007 | Backdoor.Win32.HacDef.073.b
Ikarus | T3.1.0.31 | 02.21.2007 | Backdoor.Win32.HacDef.B
Kaspersky | 4.0.2.24 | 02.21.2007 | Backdoor.Win32.HacDef.073.b
McAfee | 4967 | 02.20.2007 | HackerDefender.gen.c
Microsoft | 1.2204 | 02.21.2007 | Backdoor:Win32/Hackdef.BJ
NOD32v2 | 2072 | 02.20.2007 | Win32/HacDef
Norman | 5.80.02 | 02.20.2007 | W32/Hacdef.CM
Panda | 9.0.0.4 | 02.20.2007 | Bck/Hacdef.ED
Prevx1 | V2 | 02.21.2007 | Rootkit.Hxdef
Sophos | 4.14.0 | 02.19.2007 | Troj/HacDef-T
Sunbelt | 2.2.907.0 | 02.17.2007 | Hacker Defender
Symantec | 10 | 02.21.2007 | Backdoor.HackDefender
TheHacker | 6.1.6.062 | 02.21.2007 | Trojan/hackdef.d3
UNA | 1.83 | 02.20.2007 | Backdoor.Hacdef.002F
VBA32 | 3.11.2 | 02.20.2007 | Backdoor.Win32.HacDef.ae
VirusBuster | 4.3.19:9 | 02.20.2007 | Backdoor.HacDef.CM
Done
2 MB / 16 MB
42.8 MB / 48.8 MB
Now: Foggy, -2° C
Wed: 10° C
Thu: 2° C
Start
HU
21:40


::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?61dae83eaff36d(
Google
NETCRAFT Services Risk Rating Since: Apr 2003 Rank: 5111 Site Report [US] Everyones Internet
VIRUSTOTAL
Browse...
News Statistics VirusTotal
Complete scanning result of "bdcli100.exe", received in VirusTotal at 02.21.2007, 09:02:11 (CET).
STATUS: FINISHED
Antivirus Version Update Result
AntiVir 7.3.1.37 02.21.2007 BDC/Hacdef.084
Authentium 4.93.8 02.19.2007 W32/Backdoor.EXT
Avast 4.7.936.0 02.21.2007 Win32:Hacdef-DX
AVG 386 02.20.2007 BackDoor.Hacdef.AJ
BitDefender 7.2 02.21.2007 Trojan.Hacdef.084
CAT-QuickHeal 9.00 02.20.2007 Backdoor.HacDef
ClamAV devel-20060426 02.21.2007 Trojan.Hacdef-29
DrWeb 4.33 02.21.2007 BackDoor.HackDef.84
eSafe 7.0.14.0 02.20.2007 Win32.HacDef.084
eTrust-Vet 30.4.3417 02.21.2007 Win32/HacDef.E!client
Ewido 4.0 02.20.2007 Backdoor.HacDef.084
FileAdvisor 1 02.21.2007 High threat detected
Fortinet 2.85.0.0 02.21.2007 W32/HacDef.084!tr.bdr
F-Prot 4.2.1.29 02.19.2007 W32/Backdoor.EXT
F-Secure 6.70.13030.0 02.21.2007 Backdoor.Win32.HacDef.084
Ikarus T3.1.0.31 02.21.2007 Backdoor.Win32.HacDef.084
Kaspersky 4.0.2.24 02.21.2007 Backdoor.Win32.HacDef.084
McAfee 4967 02.20.2007 Generic BackDoor.h
Microsoft 1.2204 02.21.2007 Backdoor:Win32/Hackdef.O
NOD32v2 2072 02.20.2007 Win32/HacDef.084
Norman 5.80.02 02.20.2007 W32/Hacdef.0_84A
Panda 9.0.0.4 02.20.2007 Bck/HacDef.C
Prevx1 V2 02.21.2007 Worm.Alacra-B
Sophos 4.14.0 02.21.2007 Troj/HacDef-CD
Sunbelt 2.2.907.0 02.17.2007 Hacker Defender
Symantec 10 02.21.2007 Backdoor.HackDefender
TheHacker 6.1.6.062 02.21.2007 Backdoor/HacDef.084
UNA 1.83 02.20.2007 Backdoor.HacDef.084.89CF
VBA32 3.11.2 02.20.2007 Backdoor.Win32.HacDef.084
VirusBuster 4.3.19:9 02.20.2007 Backdoor.Hacdef.C
Done
2 MB / 16 MB
42.8 MB / 48.8 MB
Now: Foggy, -2° C
Wed: 10° C
Thu: 2° C
Start
HU
21:40
Sajátgép
Internet Explorer
Lomtár

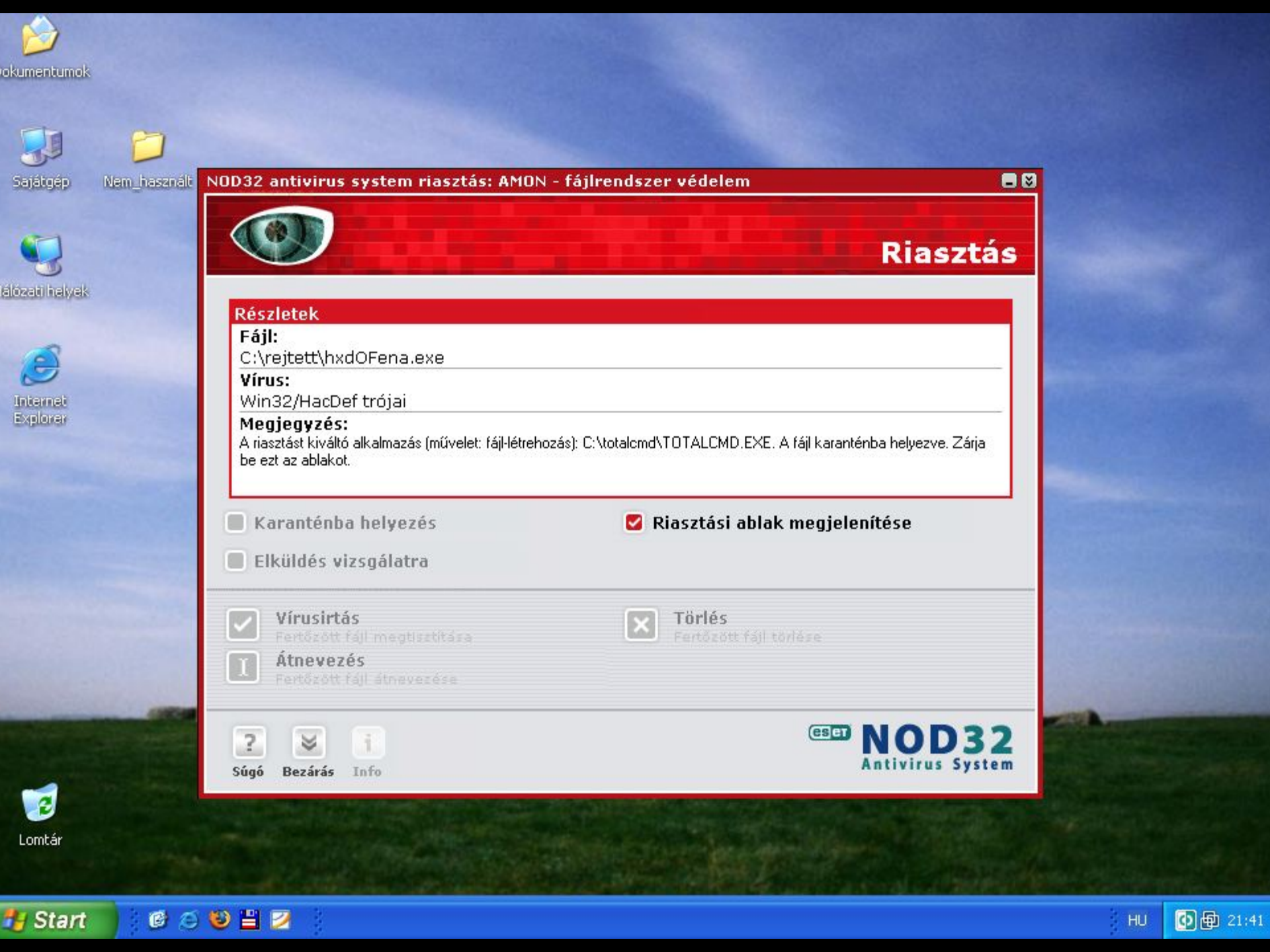

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?534bafed582eb6:
Google
NETCRAFT Services Risk Rating Since: Apr 2003 Rank: 5111 Site Report [US] Everyones Internet
VIRUSTOTAL
Browse...
News Statistics VirusTotal
Complete scanning result of "rdrbs100.exe", received in VirusTotal at 02.21.2007, 09:08:18 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.37 | 02.21.2007 | BDC/Hacdef.084.EDS
Authentium | 4.93.8 | 02.19.2007 | W32/Hackdef.J
Avast | 4.7.936.0 | 02.20.2007 | Win32:Hacdef-EB
AVG | 386 | 02.20.2007 | BackDoor.Hacdef.BD
BitDefender | 7.2 | 02.21.2007 | Backdoor.Hacdef.1.0.0
CAT-QuickHeal | 9.00 | 02.20.2007 | Backdoor.HacDef
ClamAV | devel-20060426 | 02.20.2007 | Trojan.Hacdef.10-redir
DrWeb | 4.33 | 02.21.2007 | BackDoor.HackDef.84
eSafe | 7.0.14.0 | 02.20.2007 | Win32.HacDef.084
eTrust-Vet | 30.4.3414 | 02.20.2007 | Win32/HacDef.E
Ewido | 4.0 | 02.20.2007 | Backdoor.HacDef.084
FileAdvisor | 1 | 02.21.2007 | High threat detected
Fortinet | 2.85.0.0 | 02.21.2007 | W32/HacDef.084!tr.bdr
F-Prot | 4.2.1.29 | 02.19.2007 | W32/Hackdef.J
F-Secure | 6.70.13030.0 | 02.21.2007 | Backdoor.Win32.HacDef.084
Ikarus | T3.1.0.31 | 02.21.2007 | Backdoor.Win32.HacDef.084
Kaspersky | 4.0.2.24 | 02.21.2007 | Backdoor.Win32.HacDef.084
McAfee | 4967 | 02.20.2007 | HackerDefender
Microsoft | 1.2204 | 02.21.2007 | Backdoor:Win32/Hackdef.E
NOD32v2 | 2072 | 02.20.2007 | Win32/HacDef.084
Norman | 5.80.02 | 02.20.2007 | W32/HacDef.AIZ
Panda | 9.0.0.4 | 02.20.2007 | Bck/HacDef.C
Prevx1 | V2 | 02.21.2007 | Backdoor.Hacdef.1.0.0
Sophos | 4.14.0 | 02.19.2007 | Troj/HacDef-100
Sunbelt | 2.2.907.0 | 02.17.2007 | Hacker Defender
Symantec | 10 | 02.21.2007 | Backdoor.HackDefender
TheHacker | 6.1.6.062 | 02.21.2007 | Backdoor/HacDef.084
UNA | 1.83 | 02.20.2007 | Backdoor.HacDef.084.47CF
VBA32 | 3.11.2 | 02.20.2007 | Backdoor.HacDef.084
VirusBuster | 4.3.19:9 | 02.20.2007 | Backdoor.HacDef.BB
Done
2 MB / 16 MB
42.8 MB / 48.8 MB
Now: Foggy, -2° C
Wed: 10° C
Thu: 2° C
Start
HU
21:40
Sajátgép
Internet Explorer
Lomtár

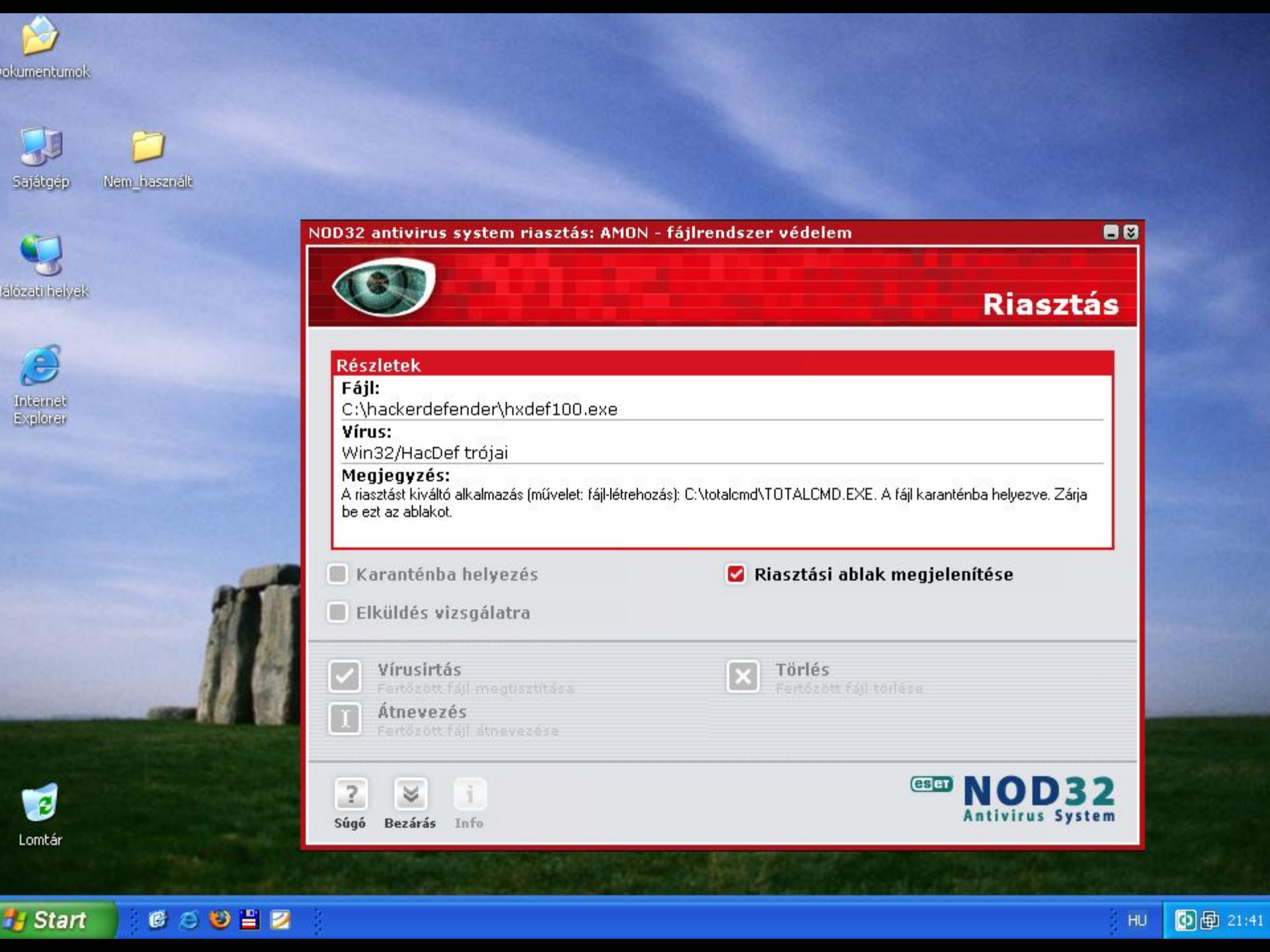

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?534bafed582eb6:
Google
NETCRAFT Services Risk Rating Since: Apr 2003 Rank: 5111 Site Report [US] Everyones Internet
VIRUSTOTAL
Browse...
News Statistics VirusTotal
Complete scanning result of "hxdOFena.exe", received in VirusTotal at 02.26.2007, 19:05:12 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.38 | 02.26.2007 | BDS/HacDef.073.B.1
Authentium | 4.93.8 | 02.26.2007 | W32/Hackdef.FJ
Avast | 4.7.936.0 | 02.26.2007 | Win32:Hacdef-AM
AVG | 386 | 02.25.2007 | BackDoor.Generic.YWW
BitDefender | 7.2 | 02.26.2007 | Generic.Hacdef.FC16D811
CAT-QuickHeal | 9.00 | 02.26.2007 | Backdoor.HacDef.ae
ClamAV | devel-20060426 | 02.26.2007 | Trojan.HacDef.073.B
DrWeb | 4.33 | 02.26.2007 | BackDoor.HackDef.139
eSafe | 7.0.14.0 | 02.26.2007 | Win32.HacDef.ae
eTrust-Vet | 30.4.3434 | 02.26.2007 | Win32/HacDef.E
Ewido | 4.0 | 02.26.2007 | Backdoor.HacDef.ae
FileAdvisor | 1 | 02.26.2007 | no virus found
Fortinet | 2.85.0.0 | 02.26.2007 | W32/HacDef.AE!tr
F-Prot | 4.3.1.45 | 02.26.2007 | W32/Hackdef.FJ
F-Secure | 6.70.13030.0 | 02.26.2007 | Backdoor.Win32.HacDef.073.b
Ikarus | T3.1.1.3 | 02.26.2007 | Backdoor.Win32.HacDef.B
Kaspersky | 4.0.2.24 | 02.26.2007 | Backdoor.Win32.HacDef.073.b
McAfee | 4971 | 02.26.2007 | HackerDefender.gen.c
Microsoft | 1.2204 | 02.26.2007 | Backdoor:Win32/Hackdef.BO
NOD32v2 | 2082 | 02.26.2007 | Win32/HacDef
Norman | 5.80.02 | 02.26.2007 | W32/Hacdef.LE
Panda | 9.0.0.4 | 02.26.2007 | Rootkit/Hxdef.S
Sophos | 4.14.0 | 02.24.2007 | Troj/HacDef-T
Sunbelt | 2.2.907.0 | 02.24.2007 | Hacker Defender
Symantec | 10 | 02.26.2007 | Backdoor.HackDefender
TheHacker | 6.1.6.065 | 02.26.2007 | Trojan/hackdef.d3
UNA | 1.83 | 02.26.2007 | Backdoor.Hacdef.18EC
VBA32 | 3.11.2 | 02.25.2007 | Backdoor.Win32.HacDef.ae
VirusBuster | 4.3.19:9 | 02.26.2007 | no virus found
Done
2 MB / 16 MB
42.8 MB / 48.8 MB
Now: Foggy, -2° C
Wed: 10° C
Thu: 2° C
Start
HU
21:40
Sajátgép
Internet Explorer
Lomtár

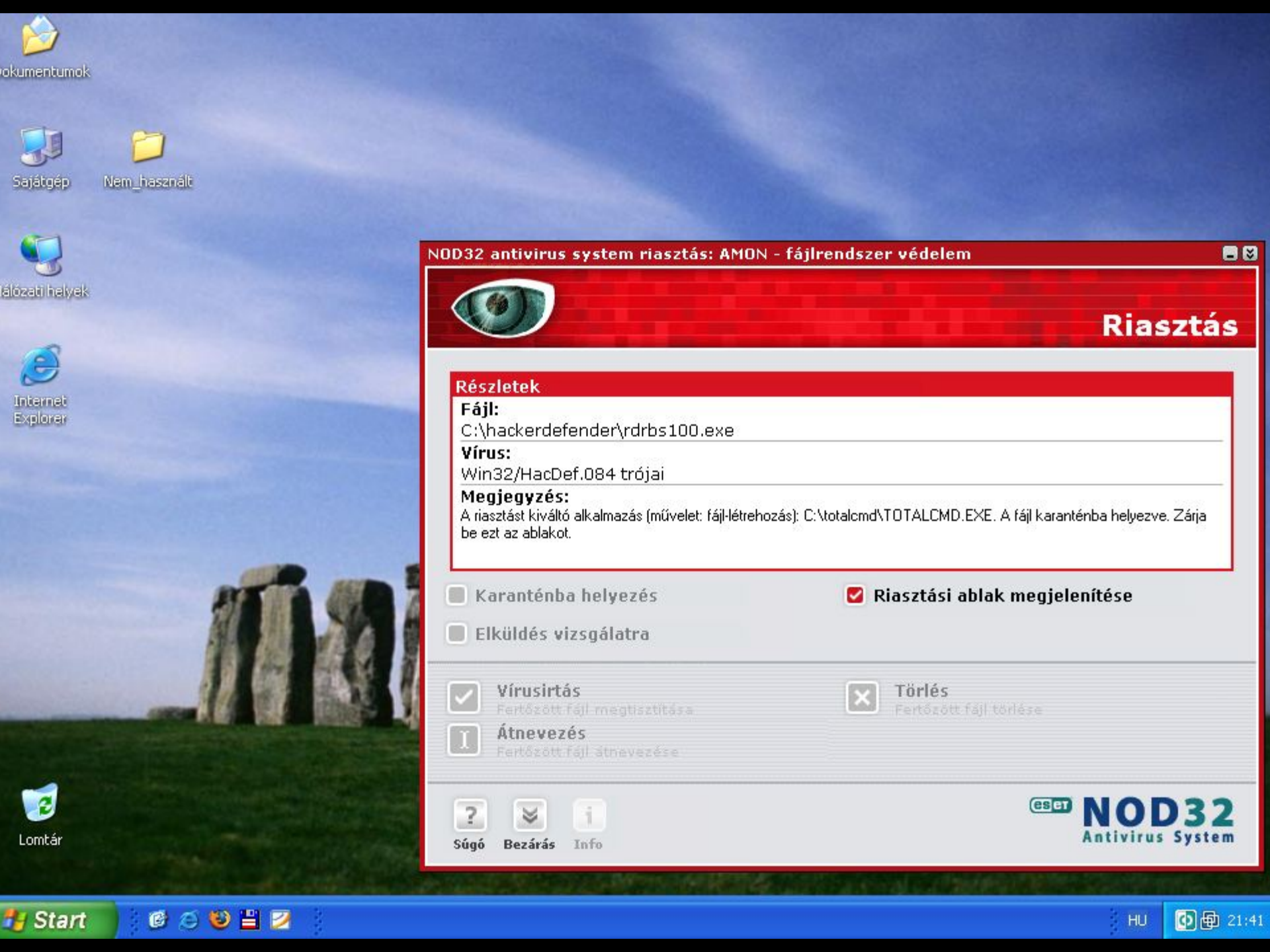

Lister - [C:\DOCUME~1\Sac\LOCALS~1\Temp_tc\driver.c]
Fájl Szerkesztés Beállítások Súgó
9 %
#include <ntddk.h>
#include <stdarg.h>
#include <stdio.h>
#include <ntverp.h>
#include <ntifs.h>
#include "driver.h"
PDEVICE_OBJECT HookedDeviceObject = NULL;
ULONG out_size;
int handle_fobject(PFILE_OBJECT fobject, PUCHAR obuffer)
{
ULONG length;
ANSI_STRING astring;
PUCHAR fname, cur_pointer;
PFILE_OBJECT related_fobject;
UCHAR status;
fname=obuffer+12;
status=0;
if(fobject->DeviceObject!=NULL)
{
if(NT_SUCCESS(ObQueryNameString(fobject->DeviceObject,
(POBJECT_NAME_INFORMATION)fname,out_size-20,&length)))
{
if(NT_SUCCESS(RtlUnicodeStringToAnsiString(&astring,
(PUNICODE_STRING)fname,TRUE)))
{
*fname='\0';
strncpy(fname, astring.Buffer, astring.Length+1);
A letölthető csomagban a fejlesztők mellékelték a rootkit forráskódját is...
Sajátgép
Internet Explorer
Lomtár
Start
HU
21:40

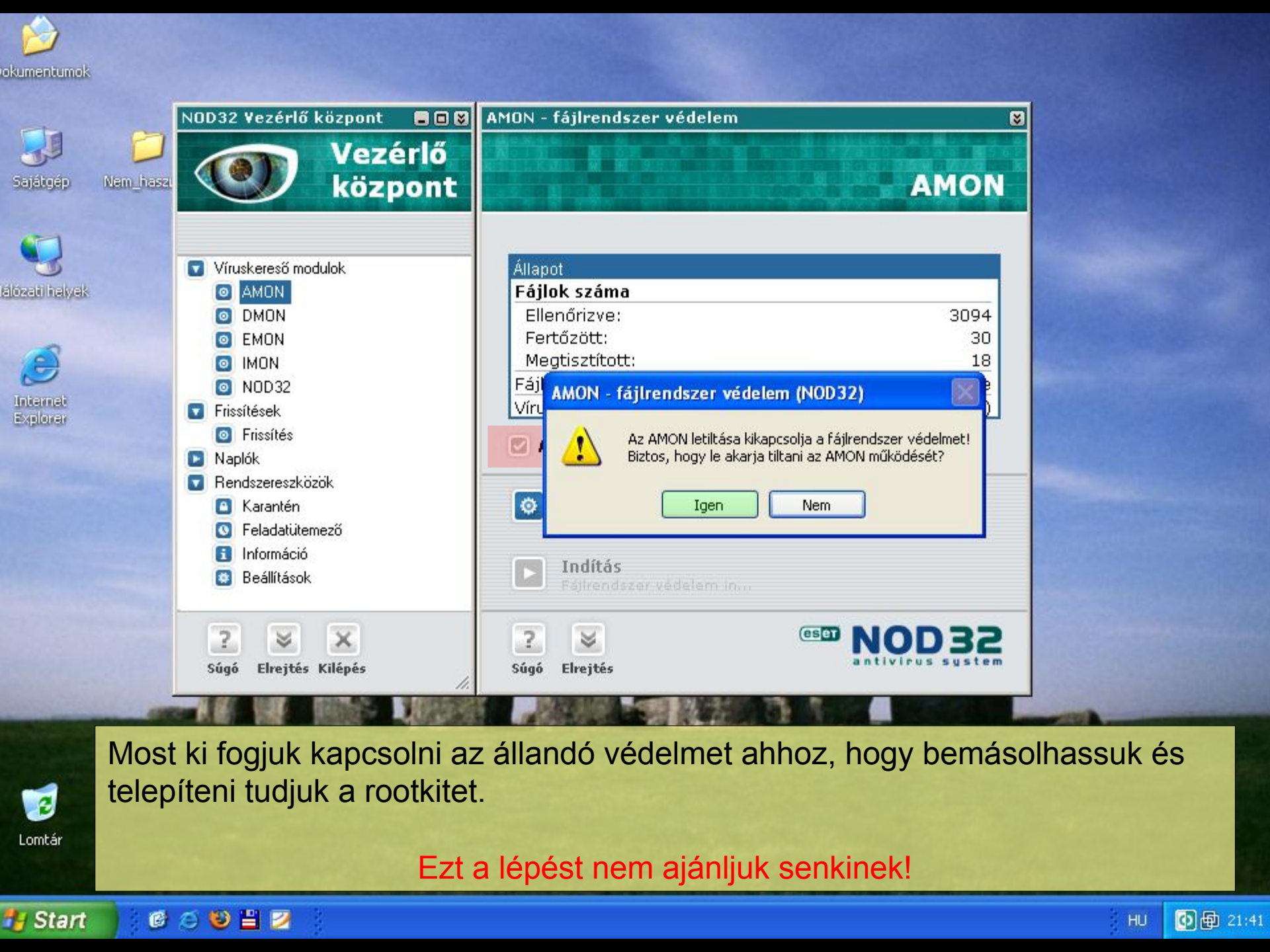


A bekapcsolt AMON modullal a NOD32 a rootkitet azonnal észleli, így most még a másolás sem sikerült.


okumentumok
Sajátgép
Nem_használt
lózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system riasztás: AMON - fájlrendszer védelem
Riasztás
Részletek
Fájl:
C:\rejtett\hxdOFena.exe
Vírus:
Win32/HacDef trójai
Megjegyzés:
A riasztást kiváltó alkalmazás (művelet: fájl-létrehozás): C:\totalcmd\TOTALCMD.EXE. A fájl karanténba helyezve. Zárja be ezt az ablakot.
Karanténba helyezés
Riasztási ablak megjelenítése
Elküldés vizsgálatra
Vírusirtás
Fertőzött fájl megtisztítása
Törlés
Fertőzött fájl törlése
Átnevezés
Fertőzött fájl átnevezése
Súgó
Bezárás
Info
eset NOD32 Antivirus System
Start
HU
21:41


okumentumok
Sajátgép
Nem_használt
lózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system riasztás: AMON - fájlrendszer védelem
Riasztás
Részletek
Fájl:
C:\hackerdefender\hxdef100.exe
Vírus:
Win32/HacDef trójai
Megjegyzés:
A riasztást kiváltó alkalmazás (művelet: fájl-létrehozás): C:\totalcmd\TOTALCMD.EXE. A fájl karanténba helyezve. Zárja be ezt az ablakot.
Karanténba helyezés
Riasztási ablak megjelenítése
Elküldés vizsgálatra
Vírusirtás
Fertőzött fájl megtisztítása
Törlés
Fertőzött fájl törlése
Átnevezés
Fertőzött fájl átnevezése
Súgó
Bezárás
Info
eset NOD32 Antivirus System
Start
HU
21:41


okumentumok
Sajátgép
Nem_használt
lózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system riasztás: AMON - fájlrendszer védelem
Riasztás
Részletek
Fájl:
C:\hackerdefender\rdrbs100.exe
Vírus:
Win32/HacDef.084 trójai
Megjegyzés:
A riasztást kiváltó alkalmazás (művelet: fájl-létrehozás): C:\totalcmd\TOTALCMD.EXE. A fájl karanténba helyezve. Zárja be ezt az ablakot.
Karanténba helyezés
Riasztási ablak megjelenítése
Elküldés vizsgálatra
Vírusirtás
Fertőzött fájl megtisztítása
Törlés
Fertőzött fájl törlése
Átnevezés
Fertőzött fájl átnevezése
Súgó
Bezárás
Info
NOD32
Antivirus System
Start
HU
21:41

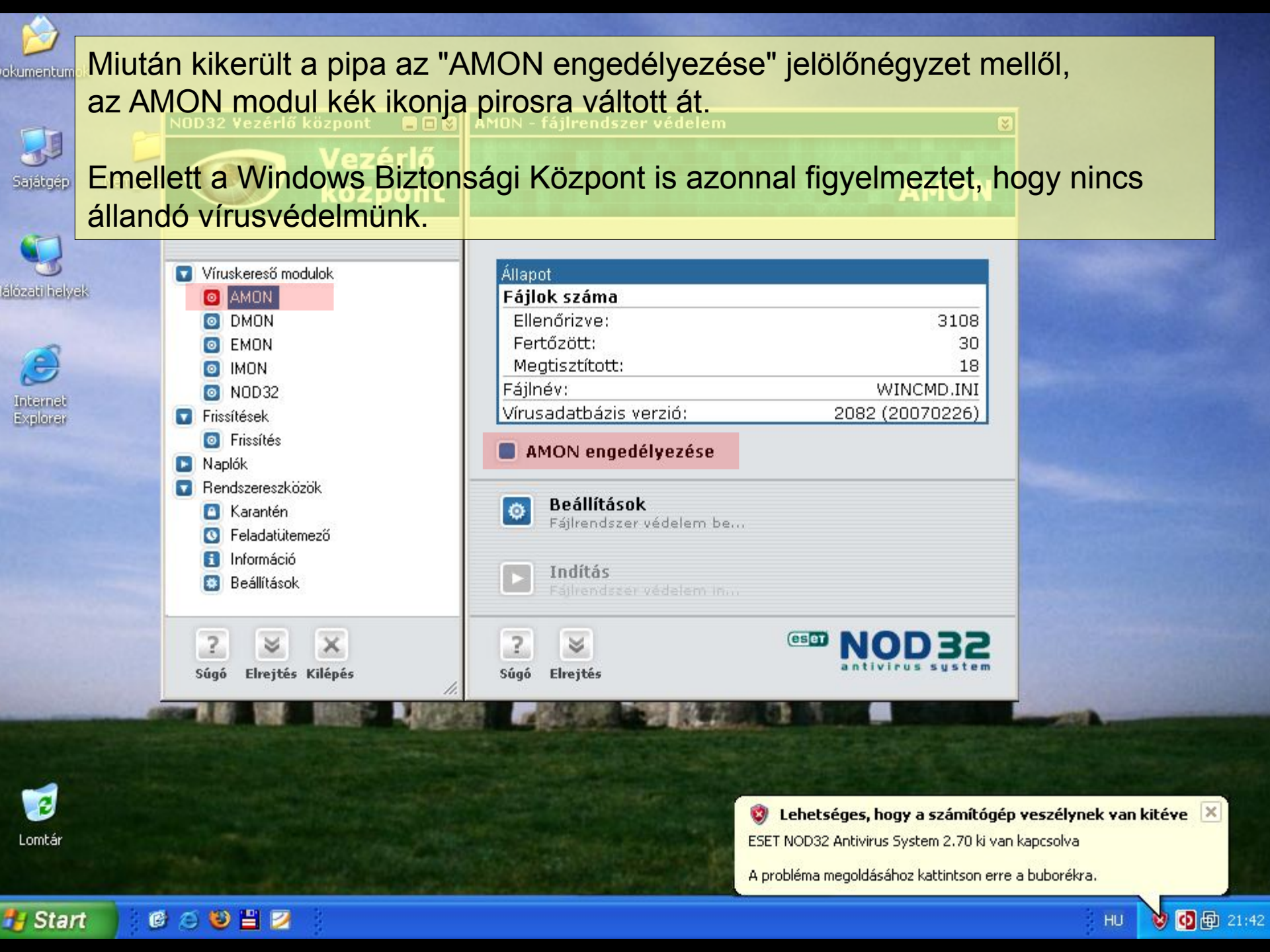


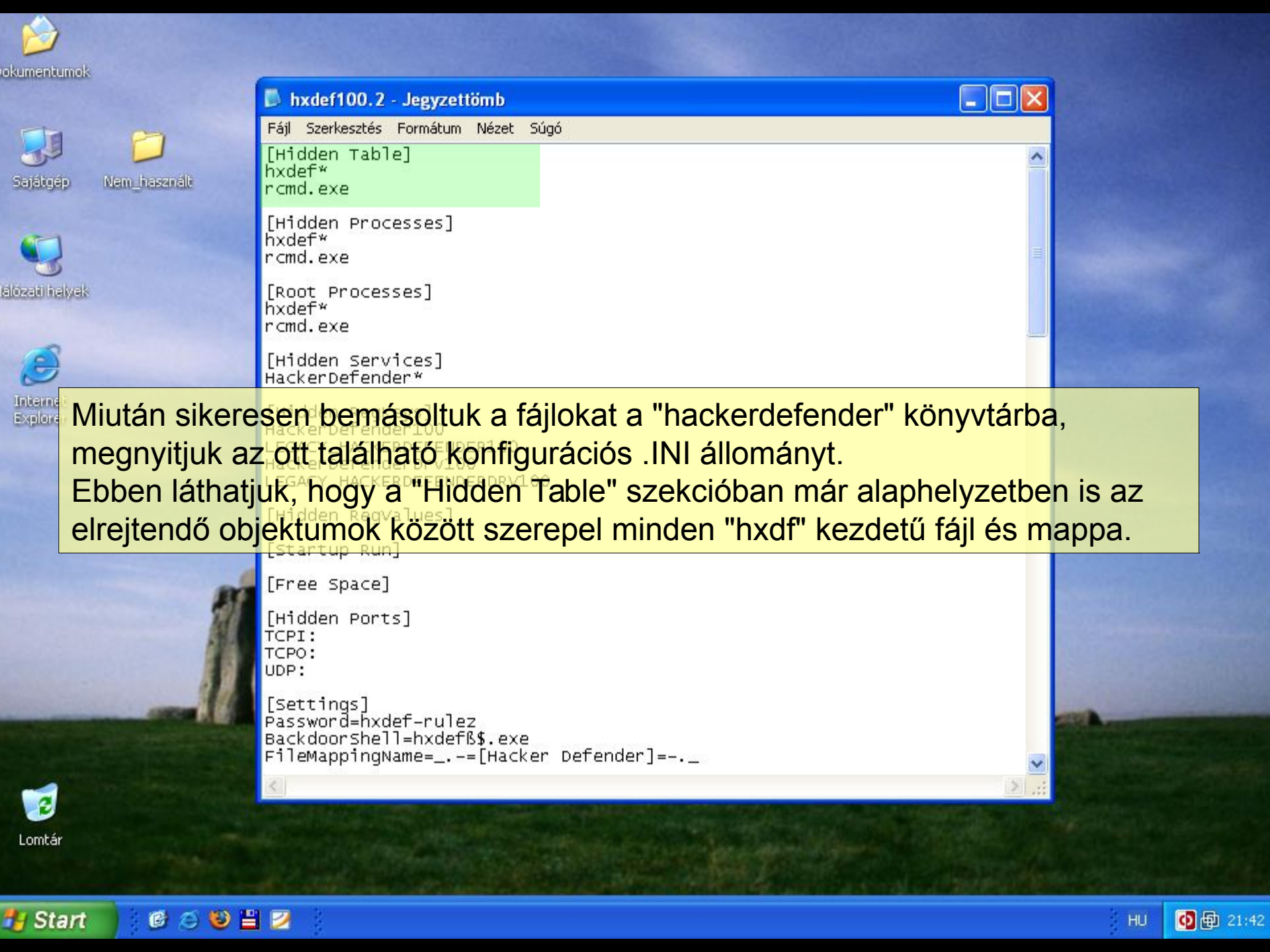
Most ki fogjuk kapcsolni az állandó védelmet ahhoz, hogy bemásolhassuk és telepíteni tudjuk a rootkitet.

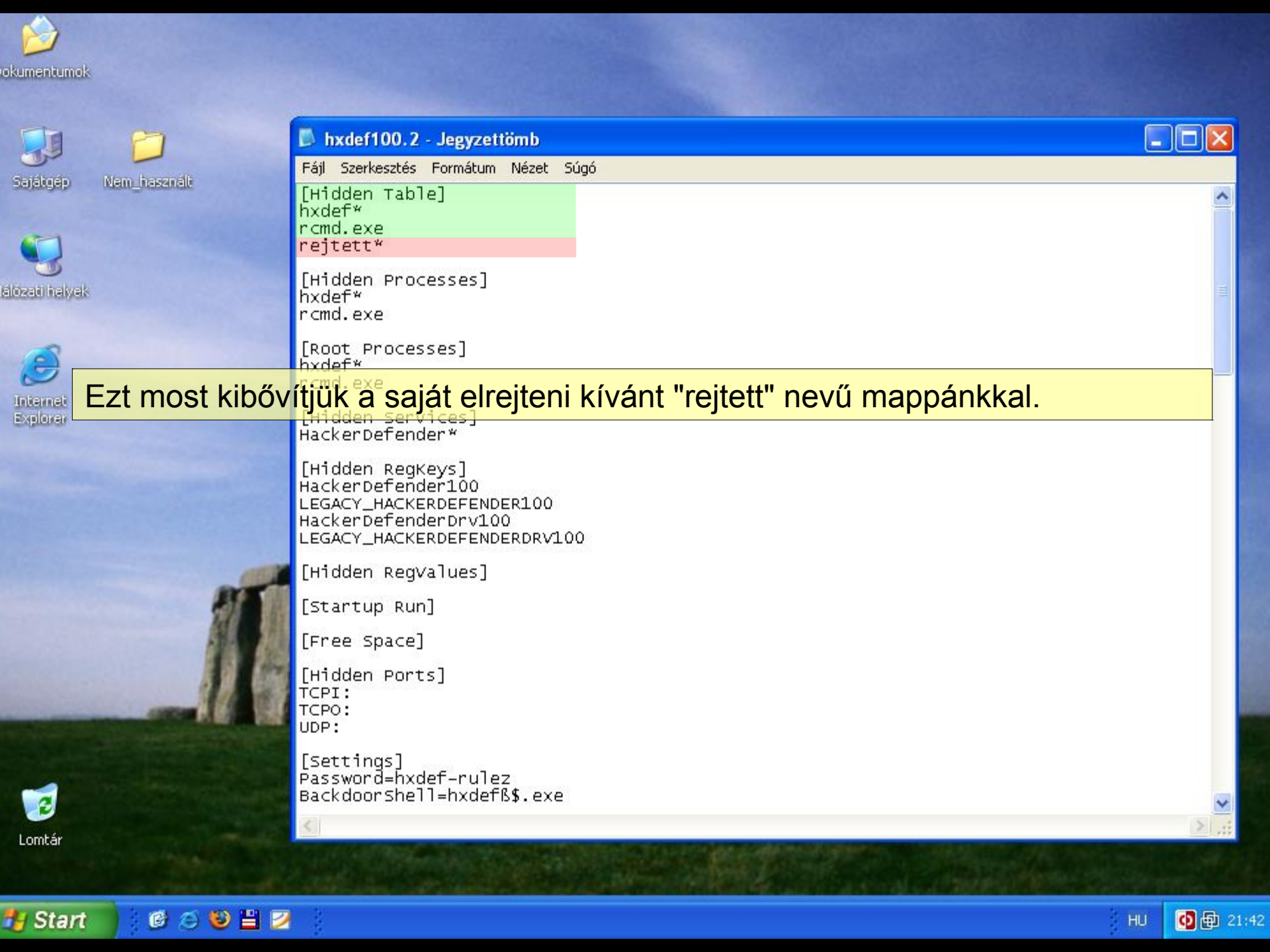
Ezt a lépést nem ajánljuk senkinek!

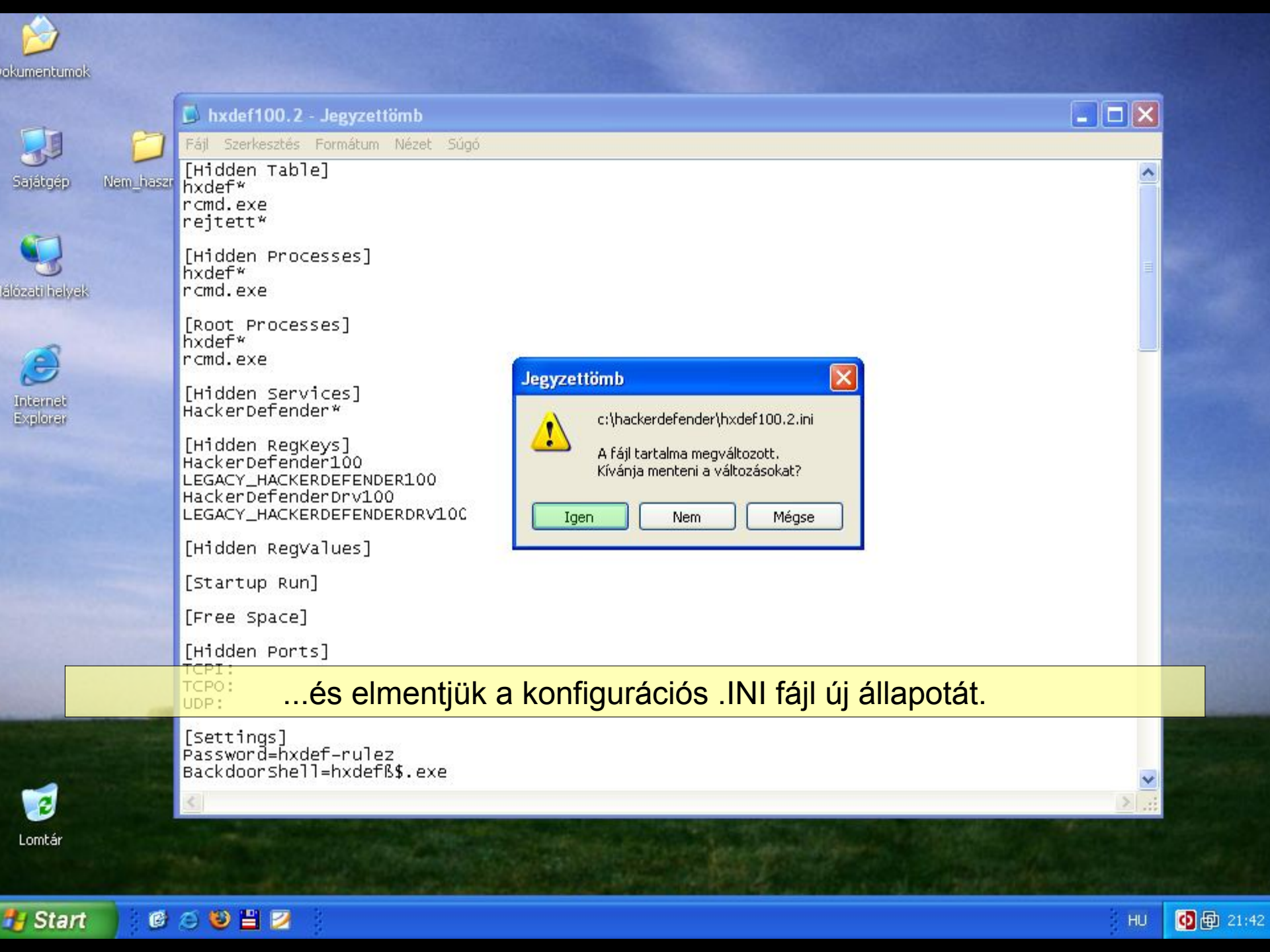
Miután kikerült a pipa az "AMON engedélyezése" jelölőnégyzet mellől, az AMON modul kék ikonja pirosra váltott át.

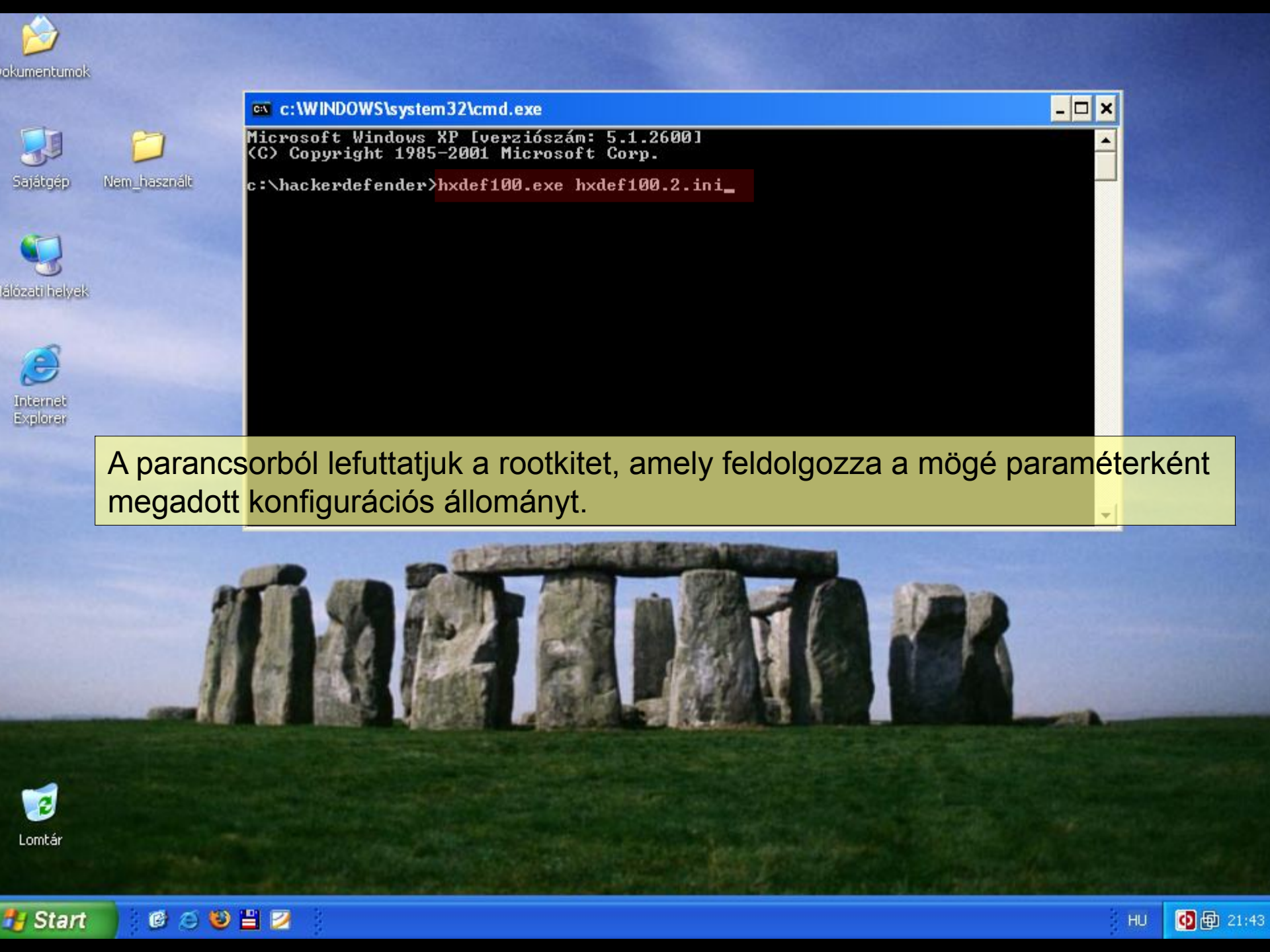
Emellett a Windows Biztonsági Központ is azonnal figyelmeztet, hogy nincs állandó vírusvédelmünk.

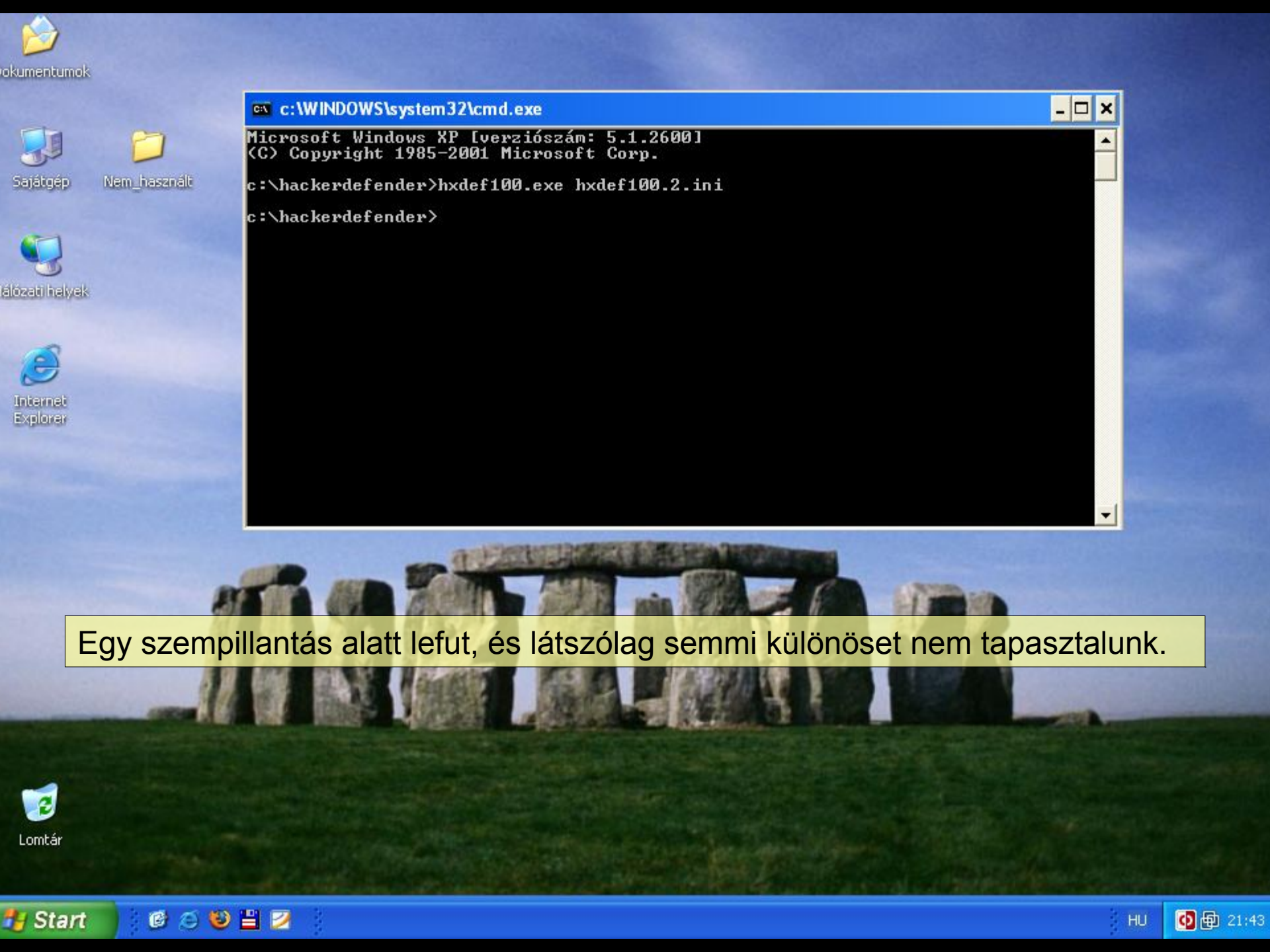


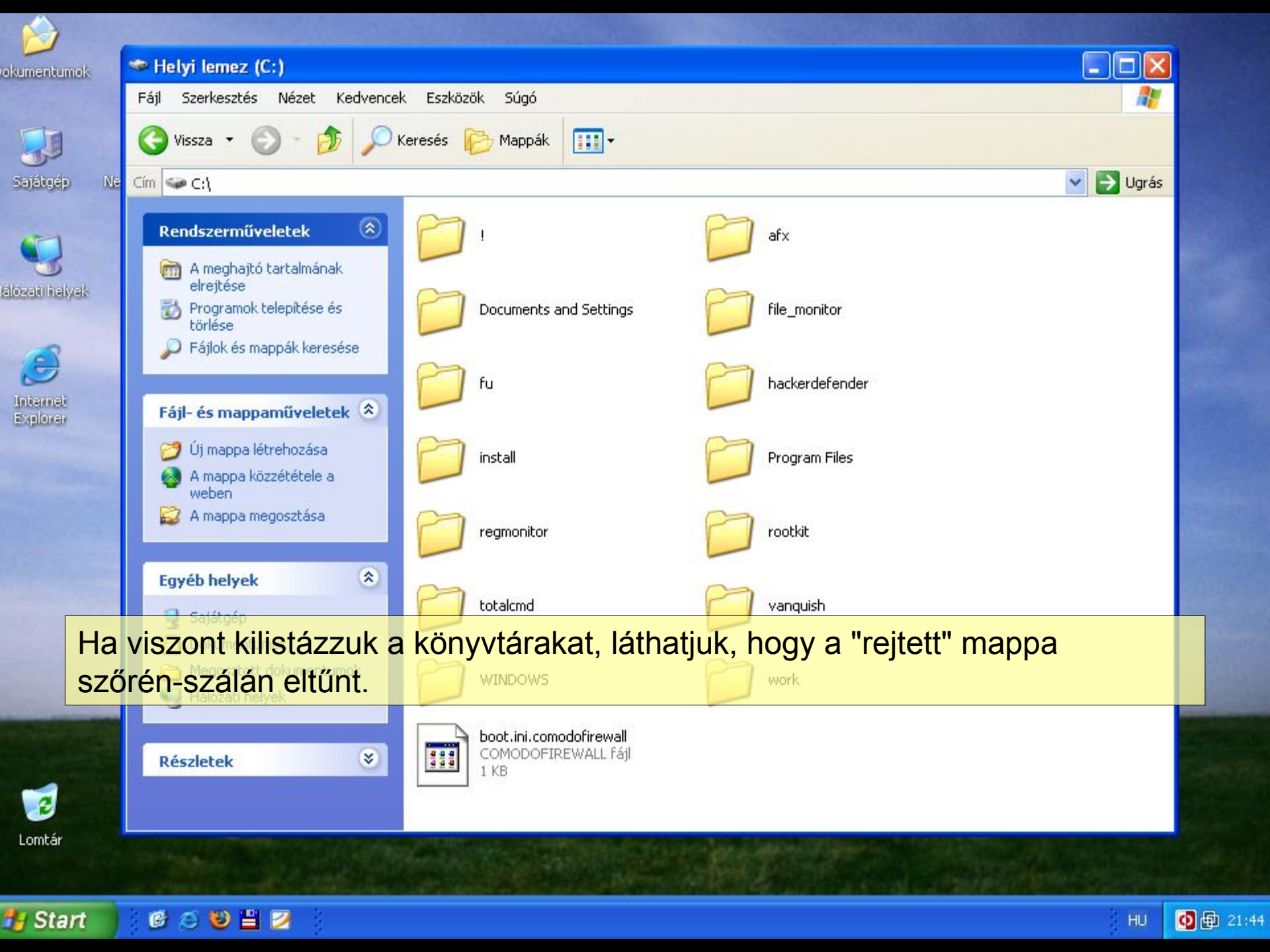

hxdef100.2 - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó
[Hidden Table]
hxdef*
rcmd.exe
[Hidden Processes]
hxdef*
rcmd.exe
[Root Processes]
hxdef*
rcmd.exe
[Hidden Services]
HackerDefender*
[Free Space]
[Hidden Ports]
TCPI:
TCPO:
UDP:
[Settings]
Password=hxdef-rulez
BackdoorShell=hxdefß$.exe
FileMappingName=_.-=[Hacker Defender]=-._
Miután sikeresen bemásoltuk a fájlokat a "hackerdefender" könyvtárba, megnyitjuk az ott található konfigurációs .INI állományt.
Ebben láthatjuk, hogy a "Hidden Table" szekcióban már alaphelyzetben is az elrejtendő objektumok között szerepel minden "hxdf" kezdetű fájl és mappa.
Sajátgép
Nem_használt
Lomtár
Start
HU
21:42


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
hxdef100.2 - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó
[Hidden Table]
hxdef*
rcmd.exe
rejtett*
[Hidden Processes]
hxdef*
rcmd.exe
[Root Processes]
hxdef*
rcmd.exe
[Hidden Services]
HackerDefender*
[Hidden RegKeys]
HackerDefender100
LEGACY_HACKERDEFENDER100
HackerDefenderDrv100
LEGACY_HACKERDEFENDERDRV100
[Hidden RegValues]
[Startup Run]
[Free Space]
[Hidden Ports]
TCPI:
TCPO:
UDP:
[Settings]
Password=hxdef-rulez
BackdoorShell=hxdefß$.exe
Ezt most kibővítjük a saját elrejteni kívánt "rejtett" nevű mappánkkal.
Start
HU
21:42

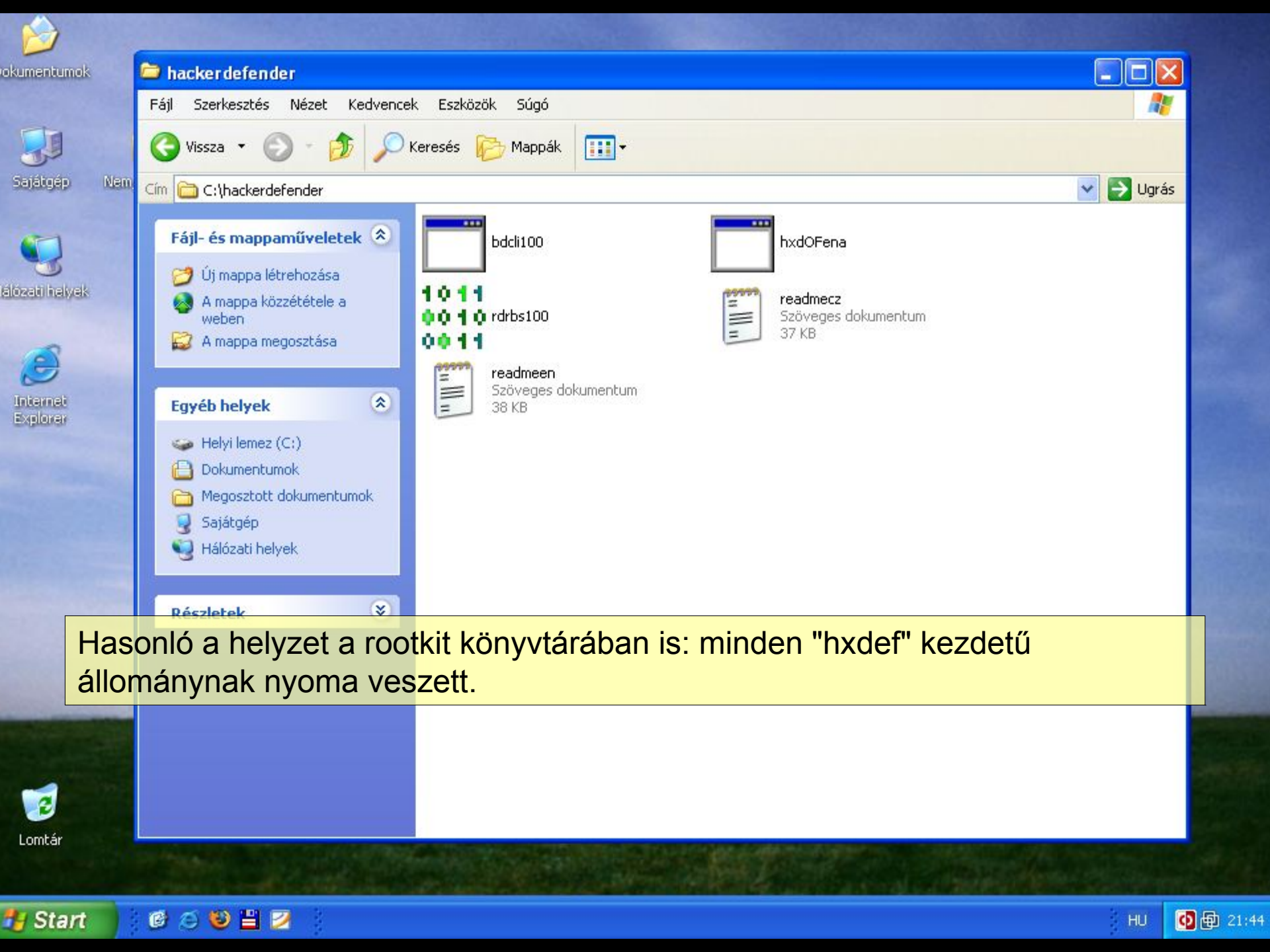

hxdef100.2 - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó
[Hidden Table]
hxdef*
rcmd.exe
rejtett*
[Hidden Processes]
hxdef*
rcmd.exe
[Root Processes]
hxdef*
rcmd.exe
[Hidden Services]
HackerDefender*
[Hidden RegKeys]
HackerDefender100
LEGACY_HACKERDEFENDER100
HackerDefenderDrv100
LEGACY_HACKERDEFENDERDRV10C
[Hidden RegValues]
[Startup Run]
[Free Space]
[Hidden Ports]
TCPI:
TCPO:
UDP:
[Settings]
Password=hxdef-rulez
BackdoorShell=hxdefß$.exe
Jegyzettömb
c:\hackerdefender\hxdef100.2.ini
A fájl tartalma megváltozott.
Kívánja menteni a változásokat?
Igen
Nem
Mégse
...és elmentjük a konfigurációs .INI fájl új állapotát.
Sajátgép
Internet Explorer
Lomtár
Start
HU
21:42


okumentumok
Sajátgép
Nem_használt
lózati helyek
Internet Explorer
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [verziószám: 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
c:\hackerdefender>hxdef100.exe hxdef100.2.ini
A parancsorból lefuttatjuk a rootkitet, amely feldolgozza a mögé paraméterként megadott konfigurációs állományt.
Lomtár
Start
HU
21:43

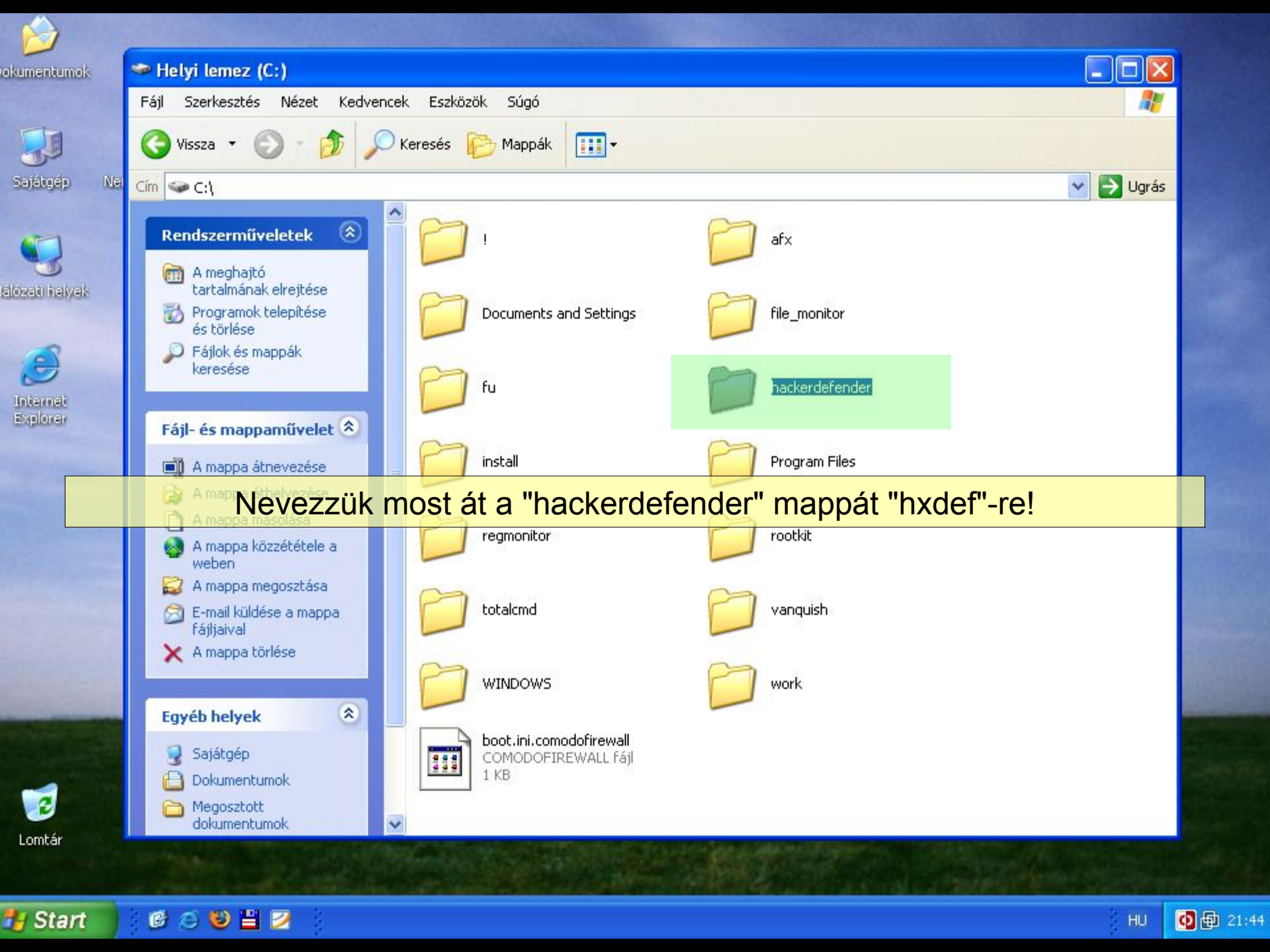

okumentumok
Sajátgép
Nem_használt
lózati helyek
Internet Explorer
Lomtár
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [verziószám: 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
c:\hackerdefender>hxdef100.exe hxdef100.2.ini
c:\hackerdefender>
Egy szempillantás alatt lefut, és látszólag semmi különöset nem tapasztalunk.
Start
HU
21:43

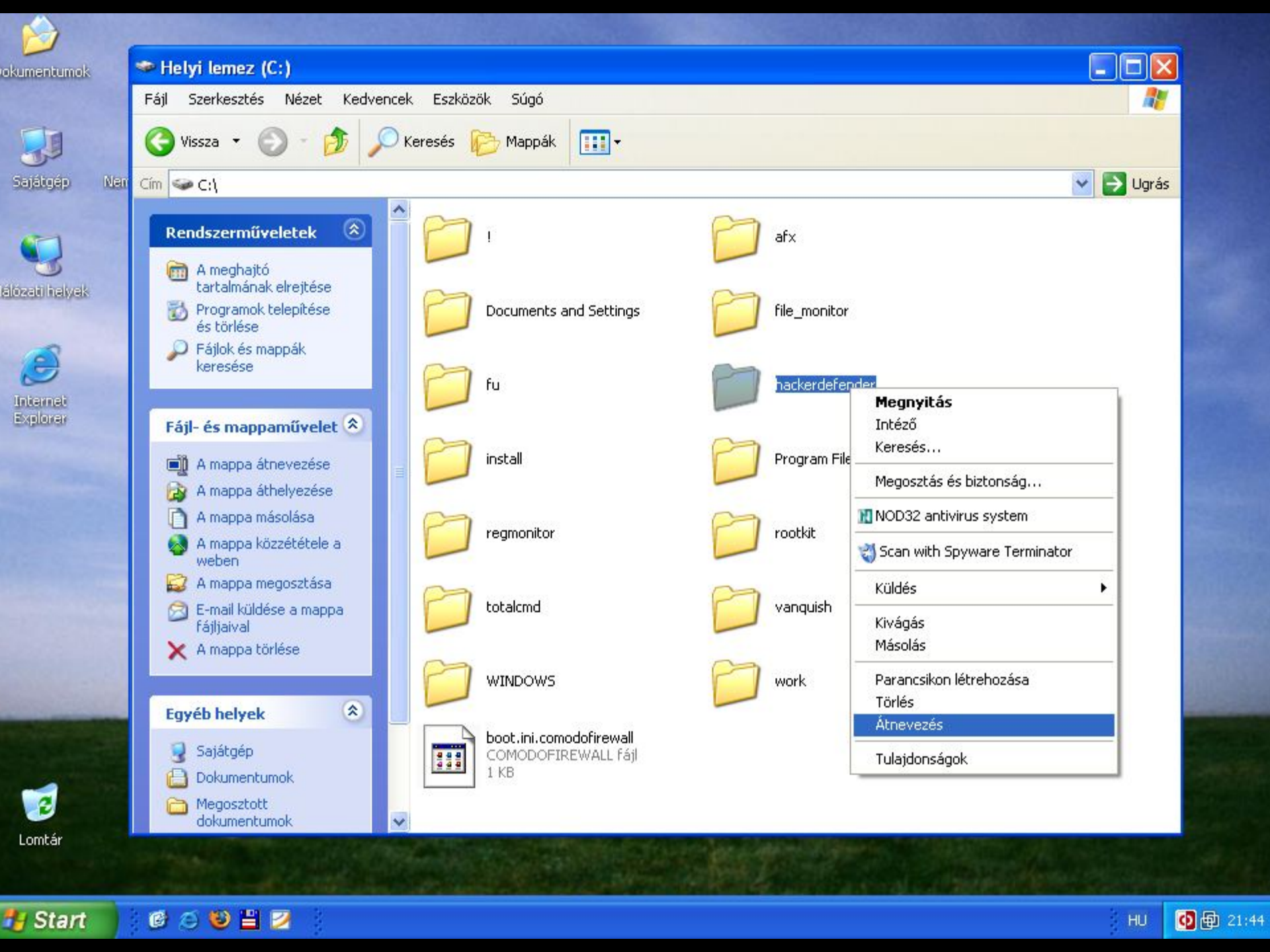


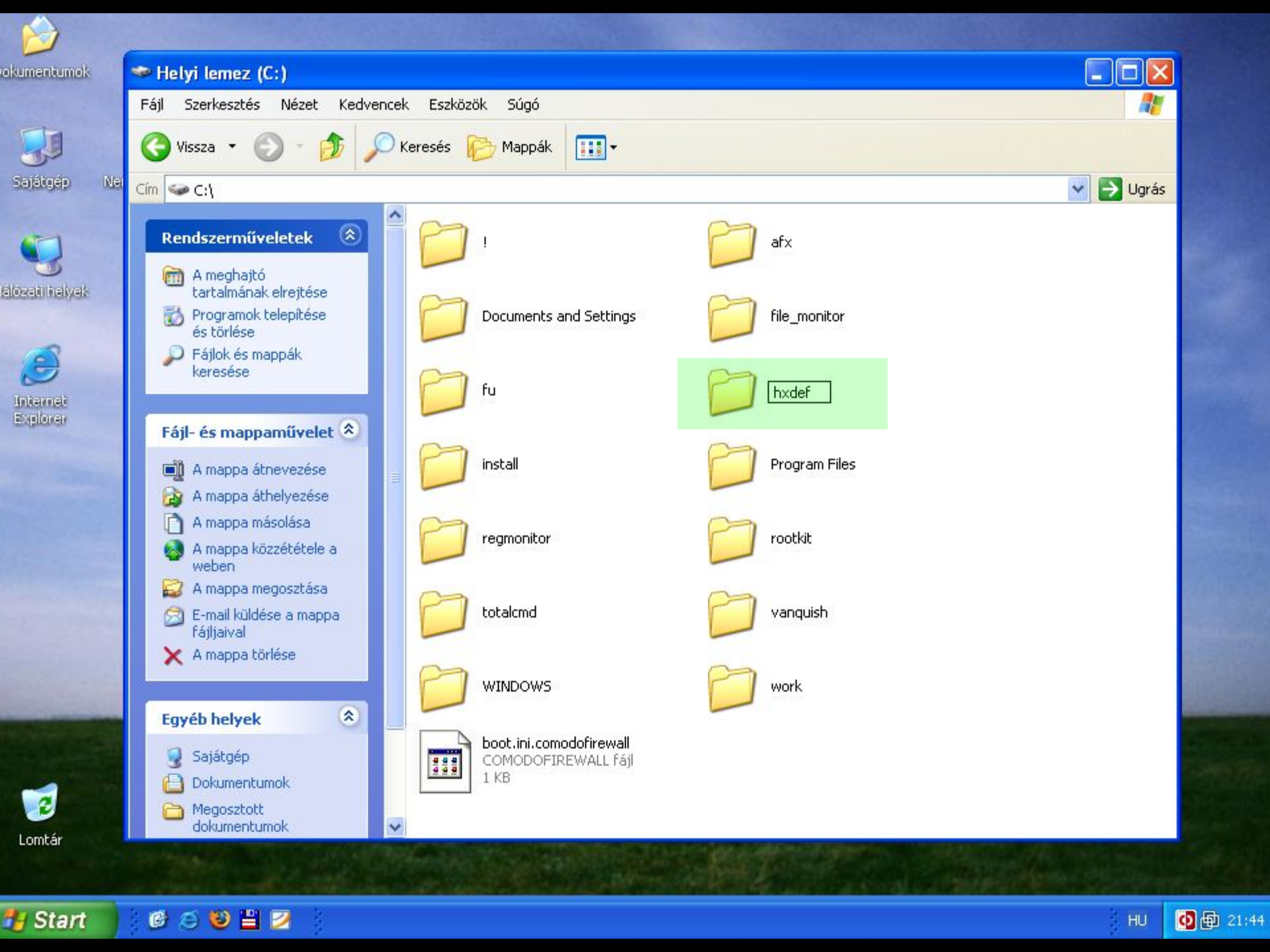
Ha viszont kilistázzuk a könyvtárakat, láthatjuk, hogy a "rejtett" mappa szőrén-szálán eltűnt.

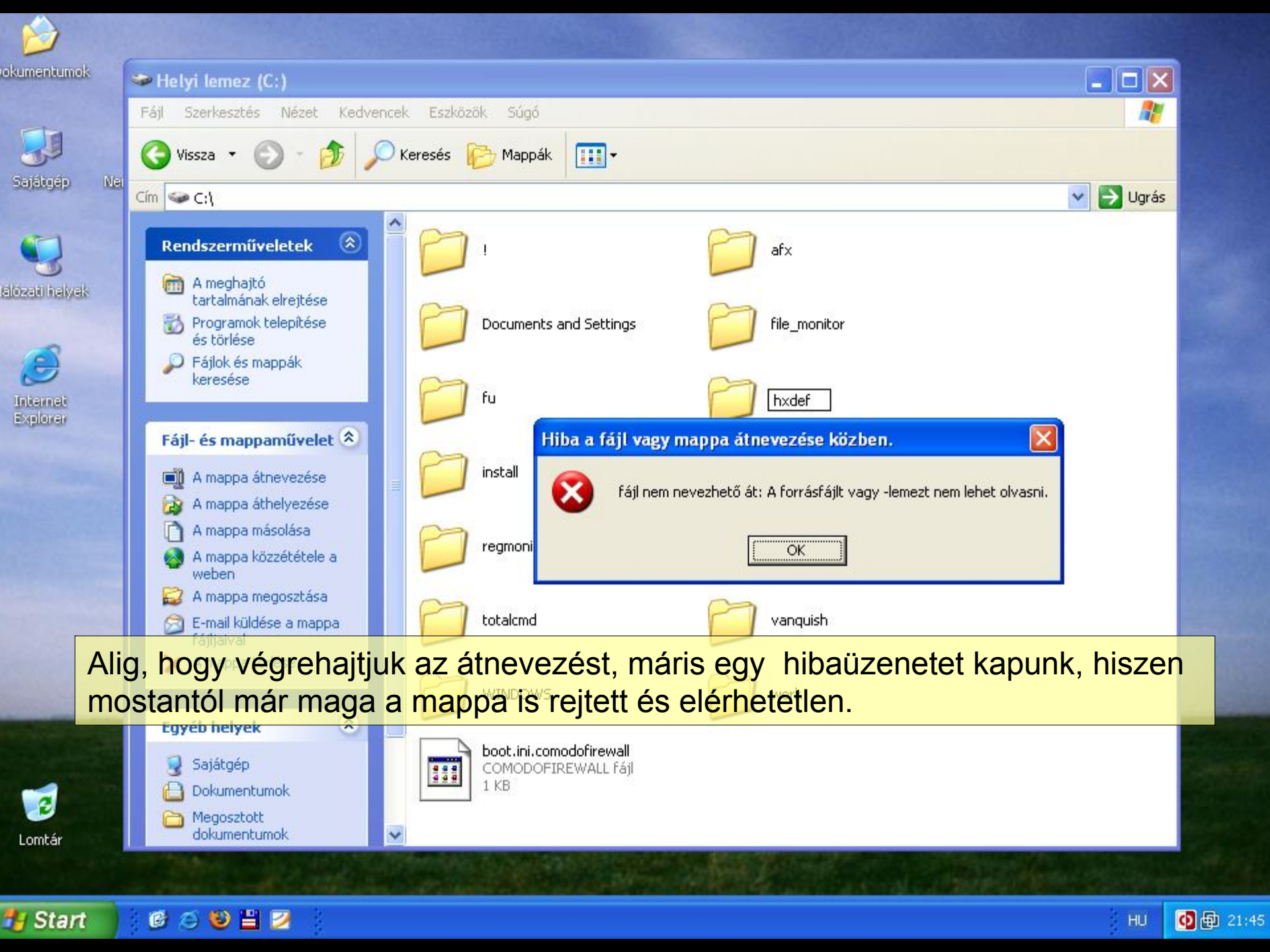


Hasonló a helyzet a rootkit könyvtárában is: minden "hxdef" kezdetű állománynak nyoma veszett.

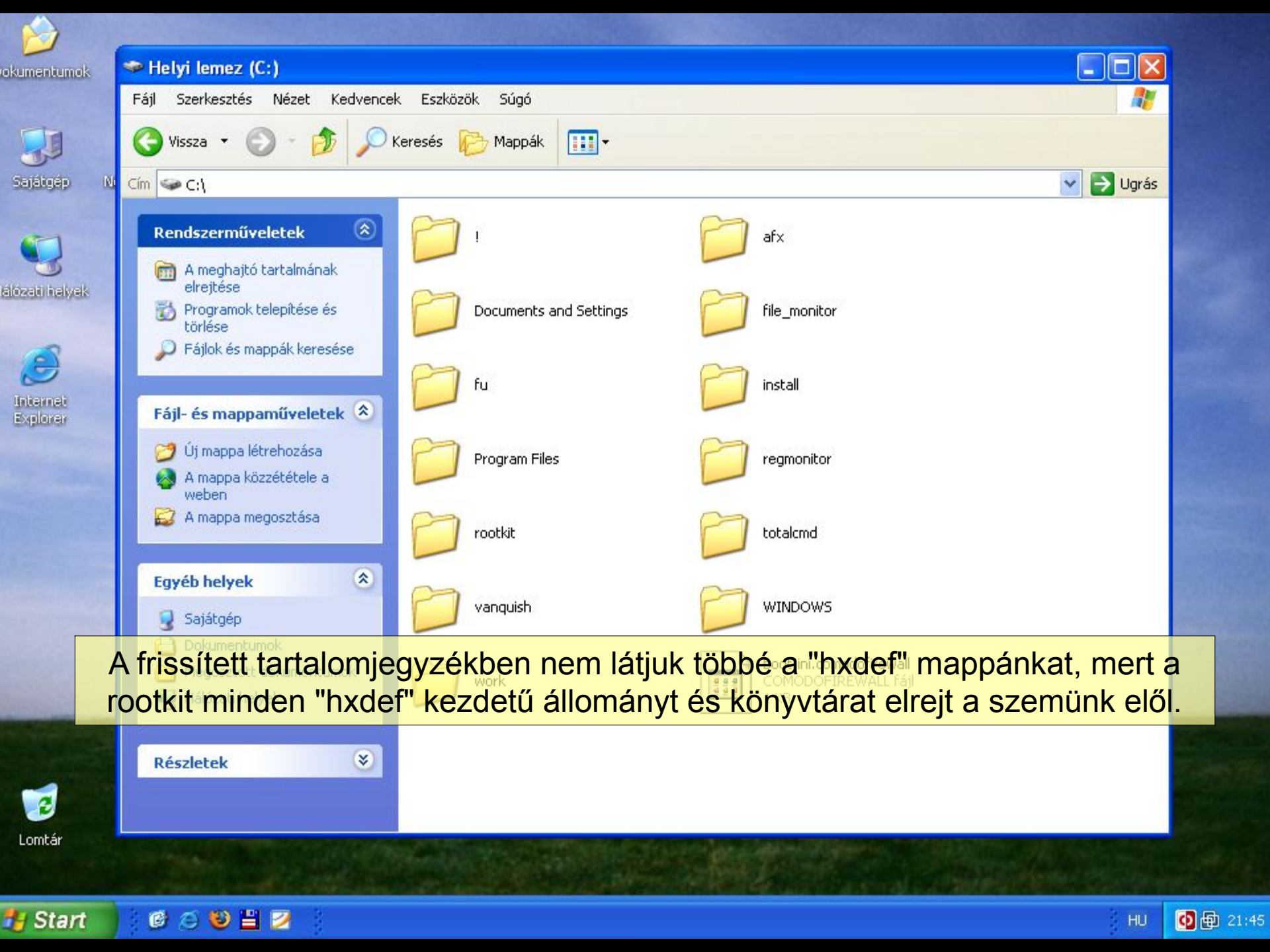

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
A mappa átnevezése
A mappa másolása
A mappa közzététele a weben
A mappa megosztása
E-mail küldése a mappa fájljaival
A mappa törlése
Egyéb helyek
Sajátgép
Dokumentumok
Megosztott dokumentumok
!
afx
Documents and Settings
file_monitor
fu
hackerdefender
install
Program Files
regmonitor
rootkit
totalcmd
vanquish
WINDOWS
work
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
Nevezzük most át a "hackerdefender" mappát "hxdef"-re!
Sajátgép
Internet Explorer
Lomtár
Start
HU
21:44


Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza Keresés Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
A mappa átnevezése
A mappa áthelyezése
A mappa másolása
A mappa közzététele a weben
A mappa megosztása
E-mail küldése a mappa fájljaival
A mappa törlése
Egyéb helyek
Sajátgép
Dokumentumok
Megosztott dokumentumok
!
Documents and Settings
fu
install
regmonitor
totalcmd
WINDOWS
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
afx
file_monitor
hackerdefender
Program File
rootkit
vanquish
work
Megnyitás
Intéző
Keresés...
Megosztás és biztonság...
NOD32 antivirus system
Scan with Spyware Terminator
Küldés
Kivágás
Másolás
Parancsikon létrehozása
Törlés
Átnevezés
Tulajdonságok
Sajátgép
Internet Explorer
Lomtár
Start
HU
21:44

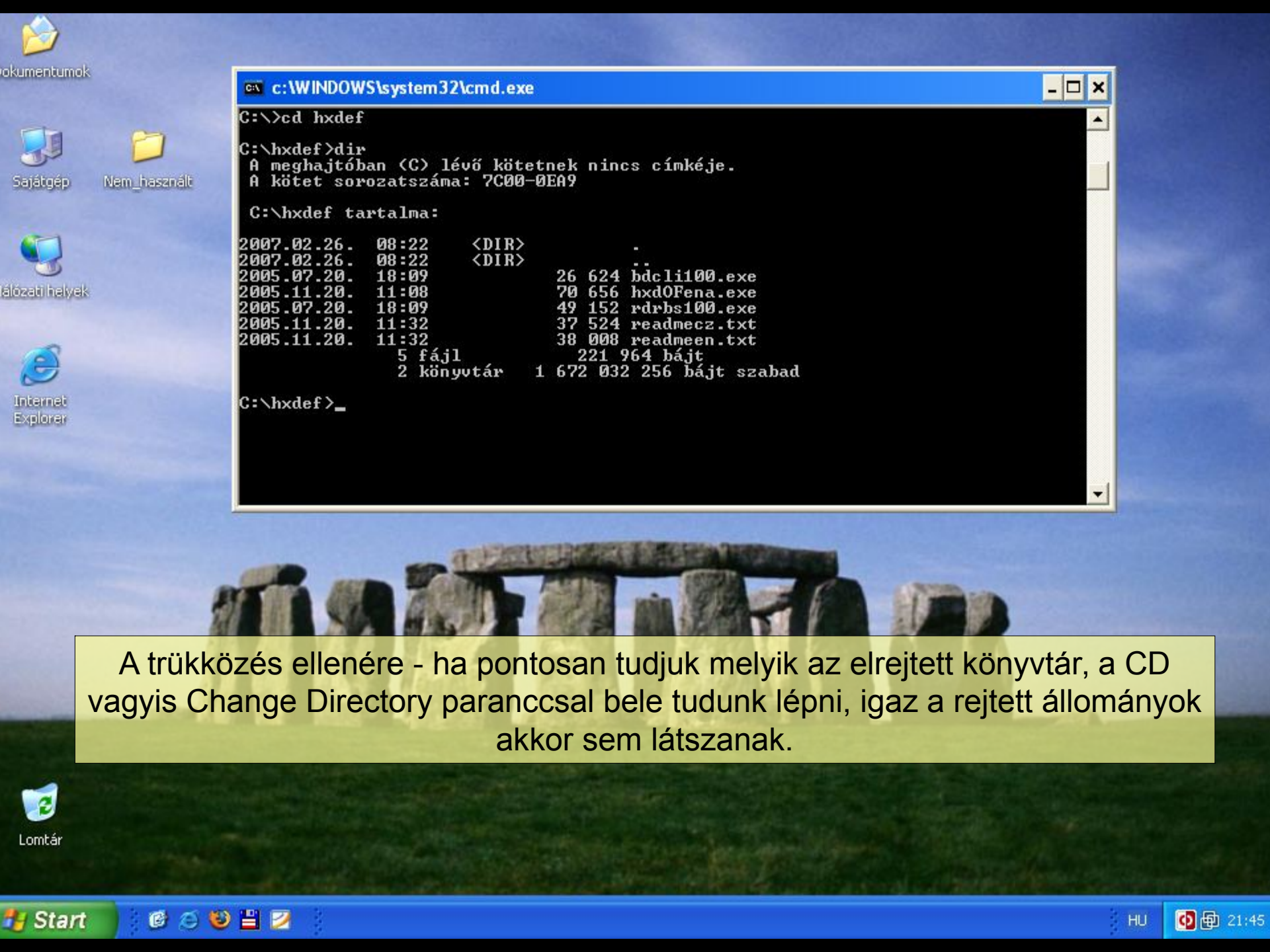

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
A mappa átnevezése
A mappa áthelyezése
A mappa másolása
A mappa közzététele a weben
A mappa megosztása
E-mail küldése a mappa fájljaival
A mappa törlése
Egyéb helyek
Sajátgép
Dokumentumok
Megosztott dokumentumok
!
afx
Documents and Settings
file_monitor
fu
hxdef
install
Program Files
regmonitor
rootkit
totalcmd
vanquish
WINDOWS
work
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
Sajátgép
Internet Explorer
Lomtár
Start
HU
21:44



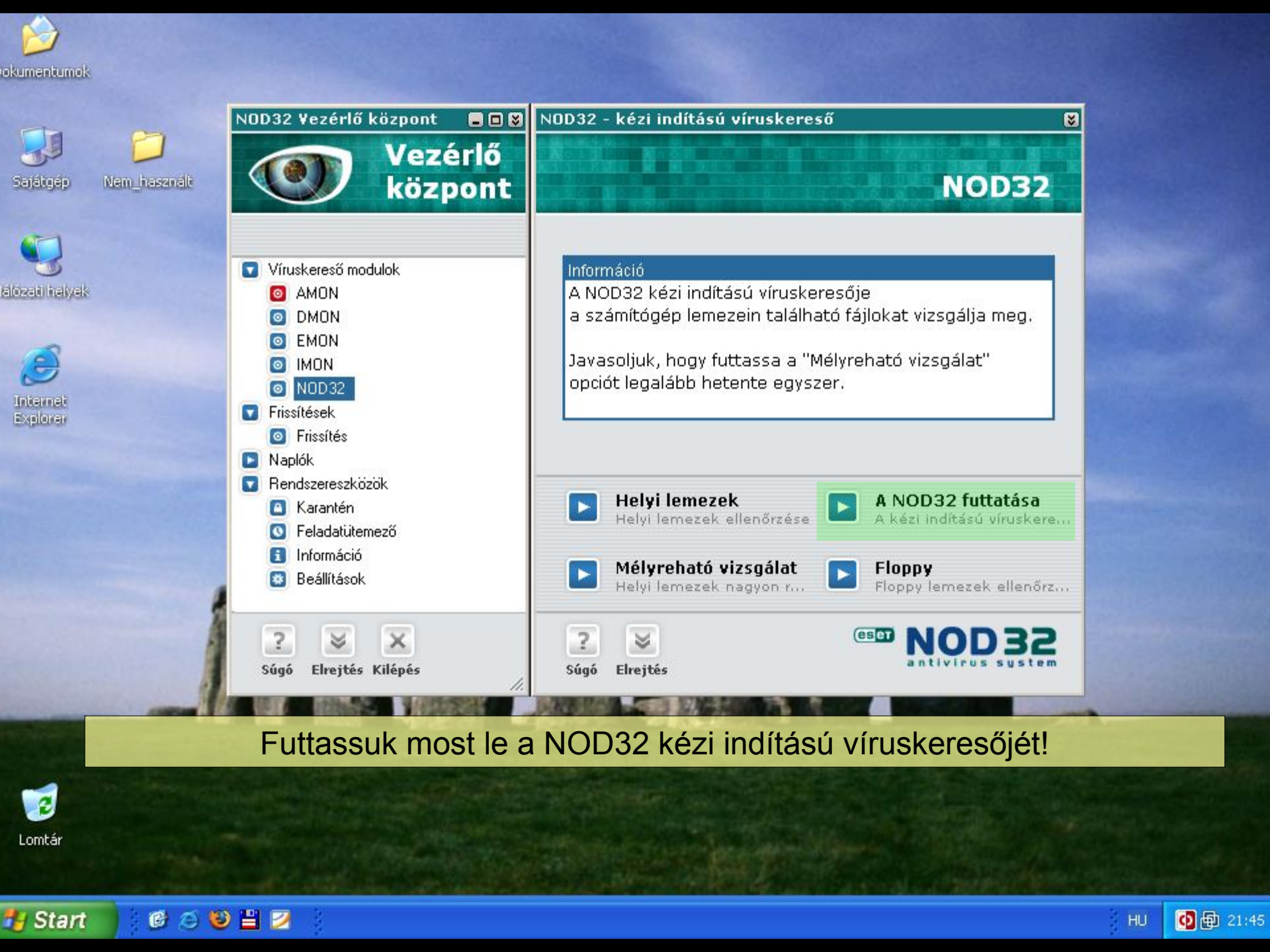
Alig, hogy végrehajtjuk az átnevezést, máris egy hibaüzenetet kapunk, hiszen mostantól már maga a mappa is rejtett és elérhetetlen.



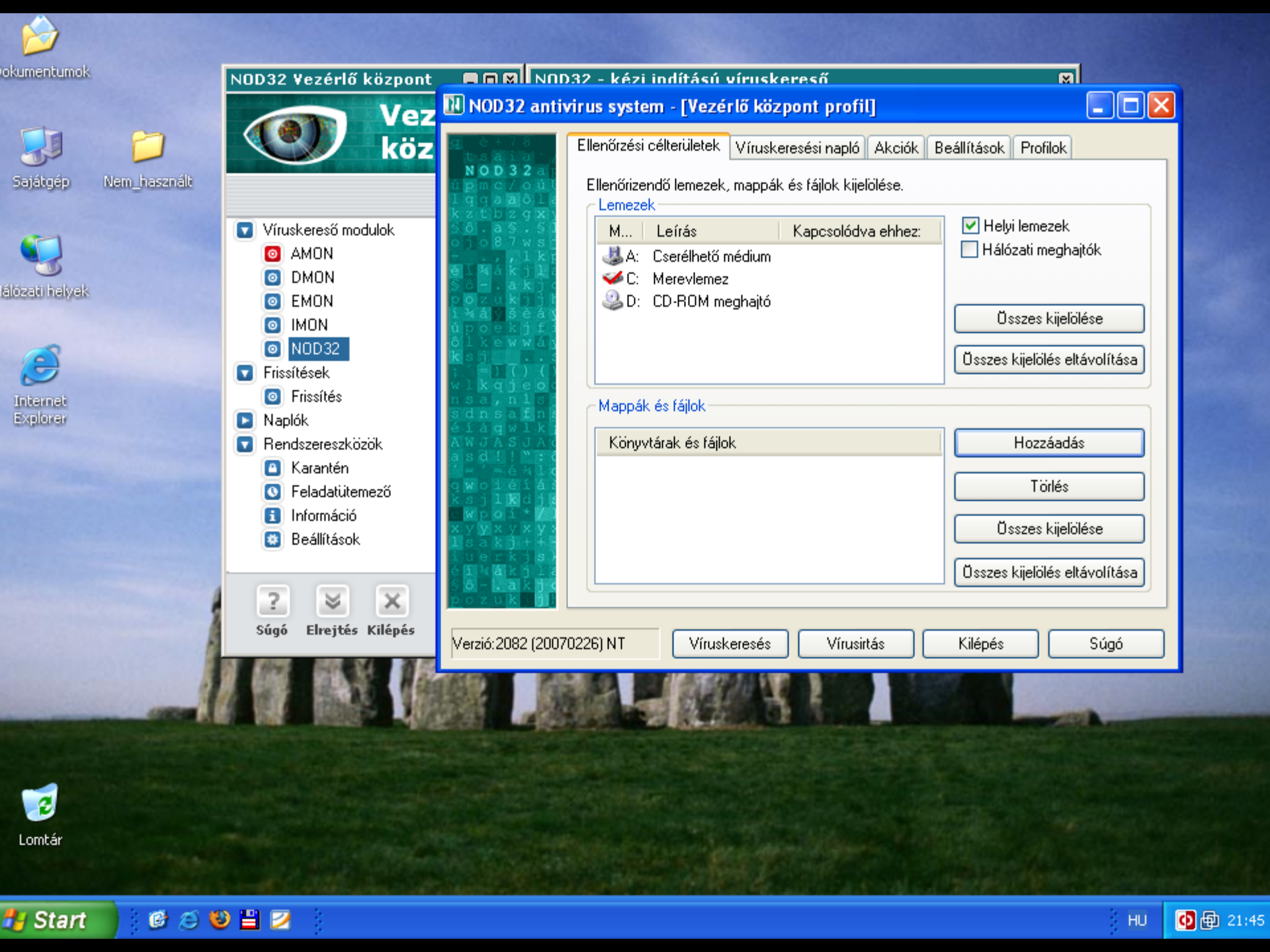
A frissített tartalomjegyzékben nem látjuk többé a "hxdef" mappánkat, mert a rootkit minden "hxdef" kezdetű állományt és könyvtárat elrejt a szemünk elől.

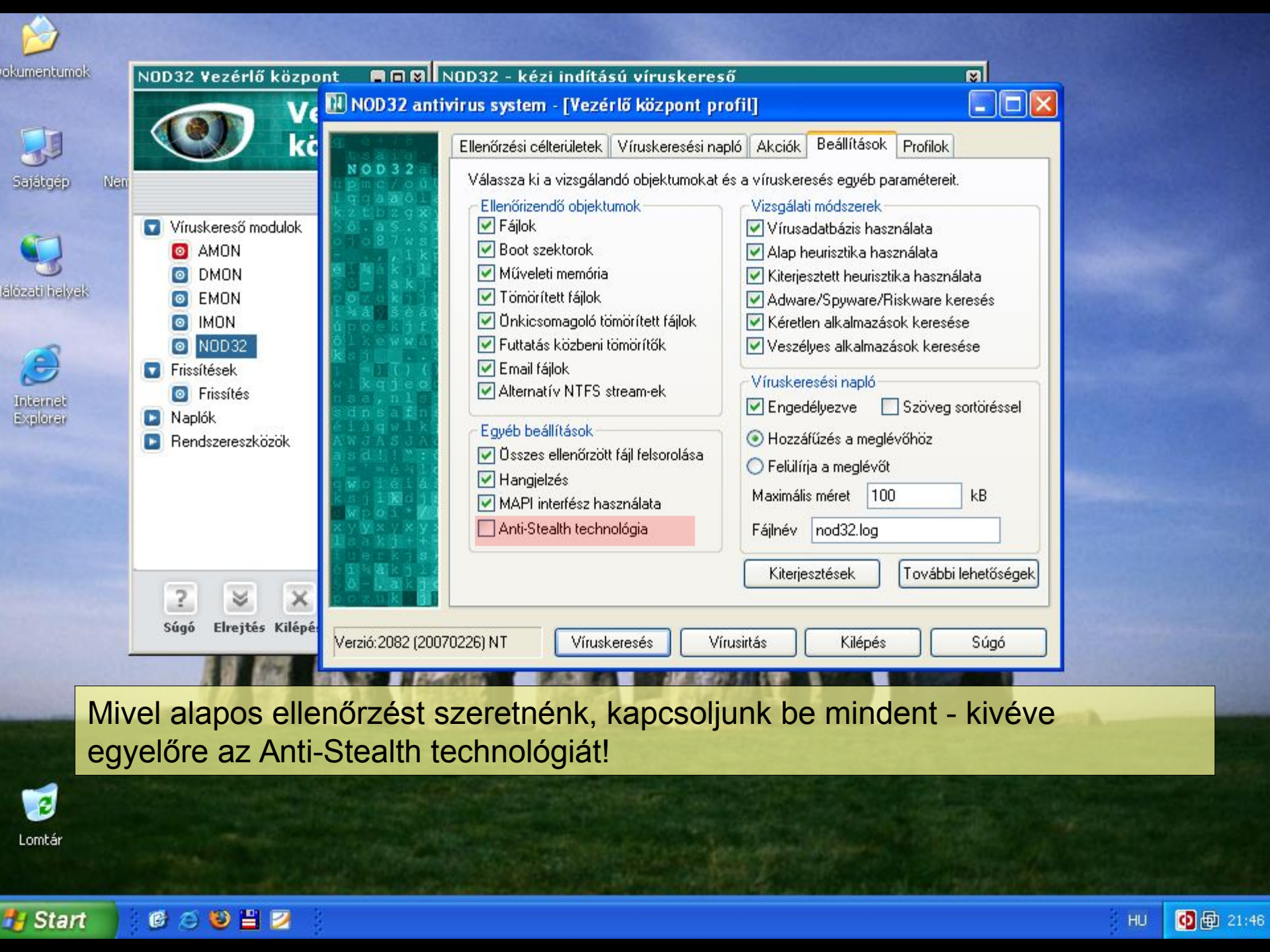


A trükközés ellenére - ha pontosan tudjuk melyik az elrejtett könyvtár, a CD vagyis Change Directory paranccsal bele tudunk lépni, igaz a rejtett állományok akkor sem látszanak.

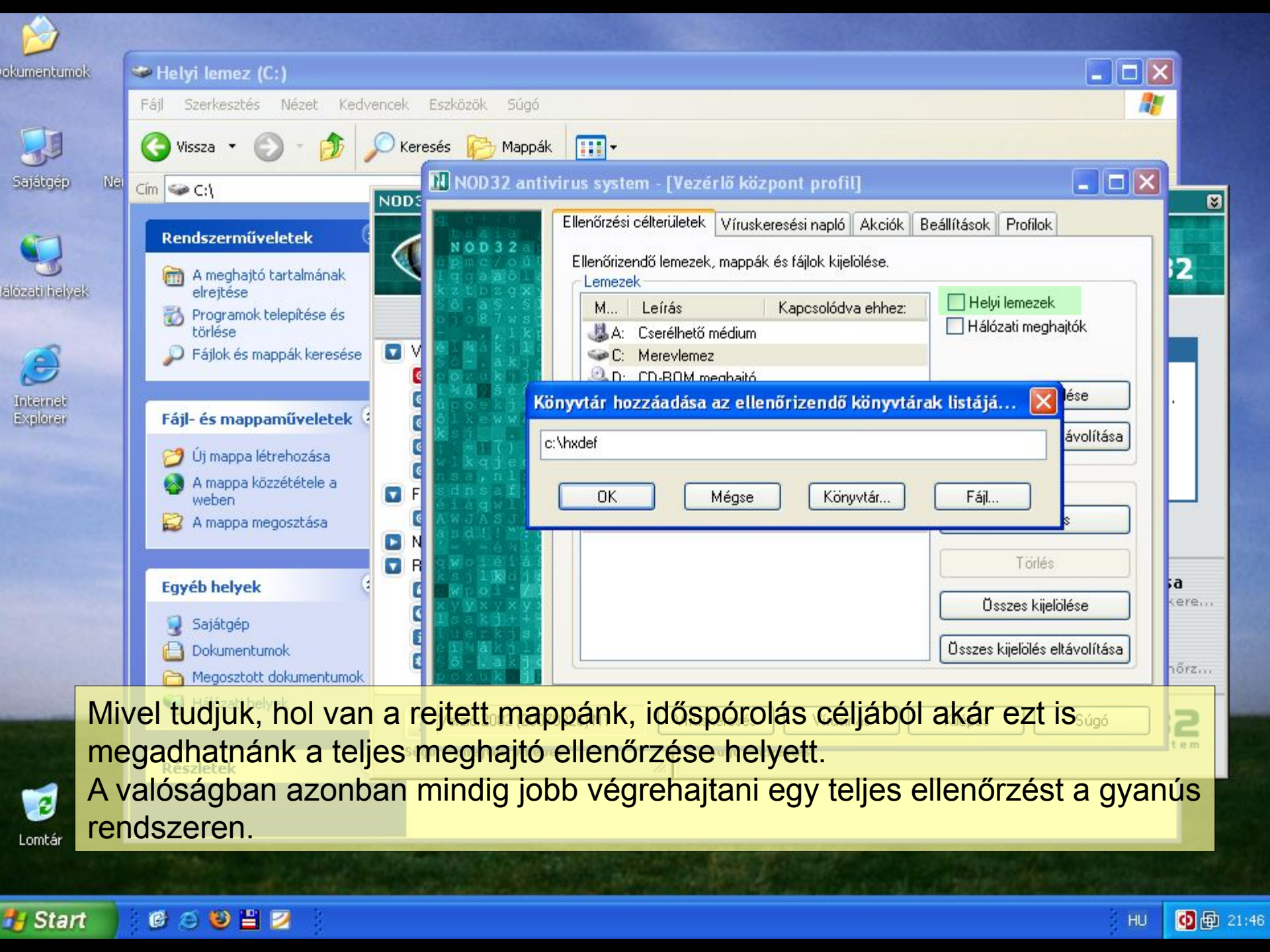


Futtassuk most le a NOD32 kézi indítású víruskeresőjét!

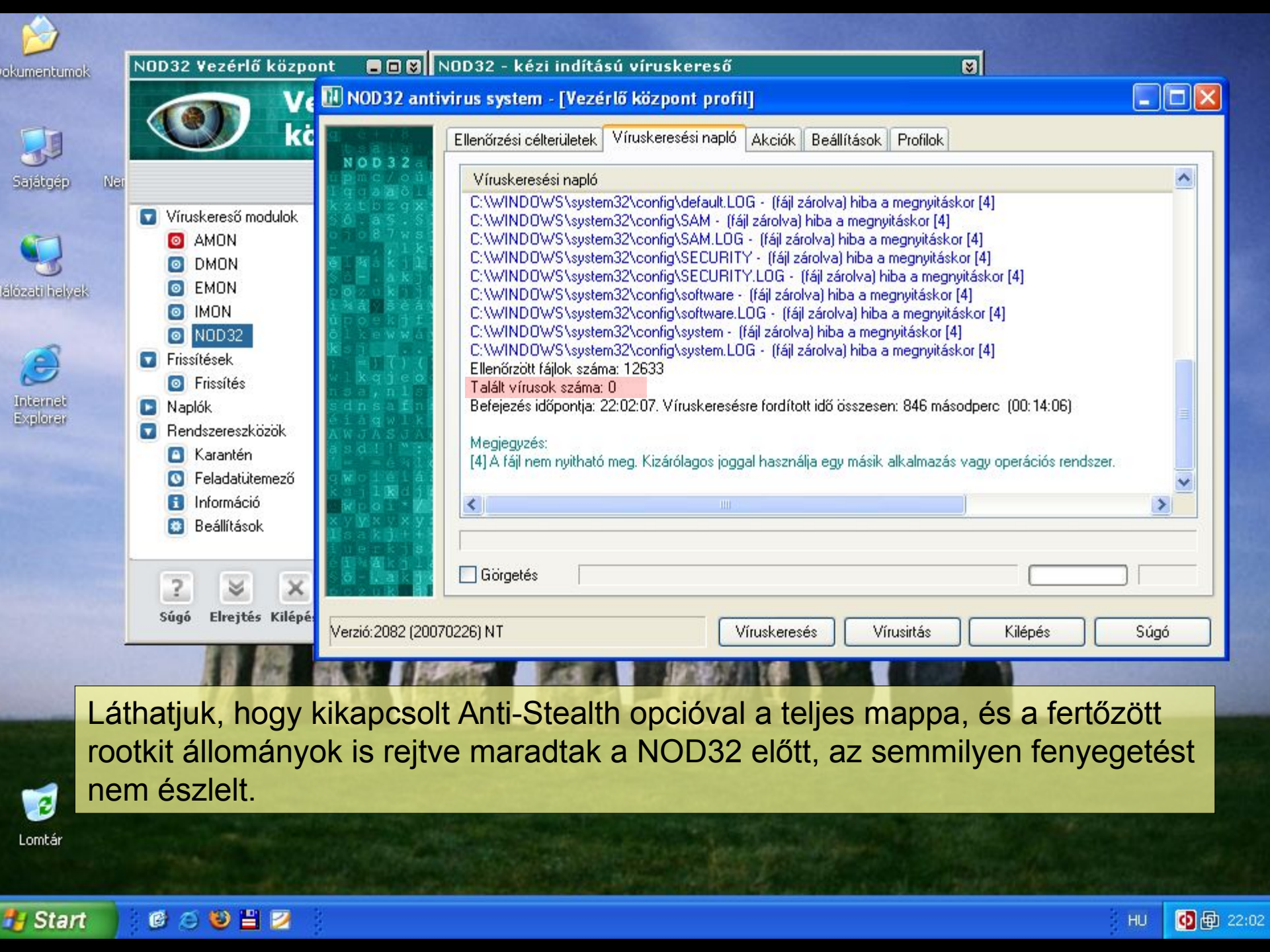

NOD32 Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Karantén
Feladatütemező
Információ
Beállítások
Súgó
Elrejtés
Kilépés
NOD32 antivirus system - [Vezérlő központ profil]
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
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:2082 (20070226) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
Sajátgép
Nem_használt
Internet Explorer
Lomtár
Start
HU
21:45



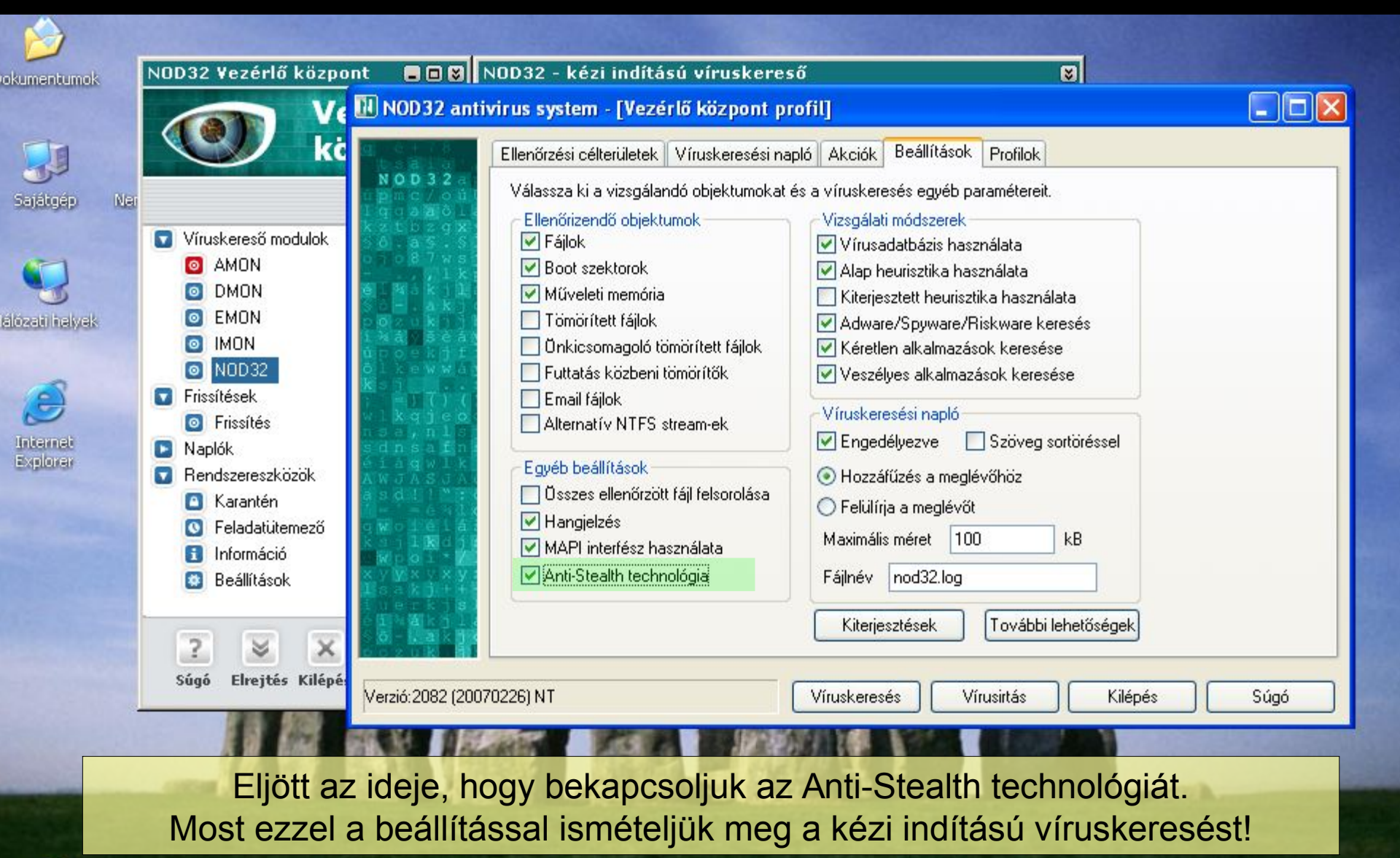
Mivel alapos ellenőrzést szeretnénk, kapcsoljunk be mindent - kivéve egyelőre az Anti-Stealth technológiát!



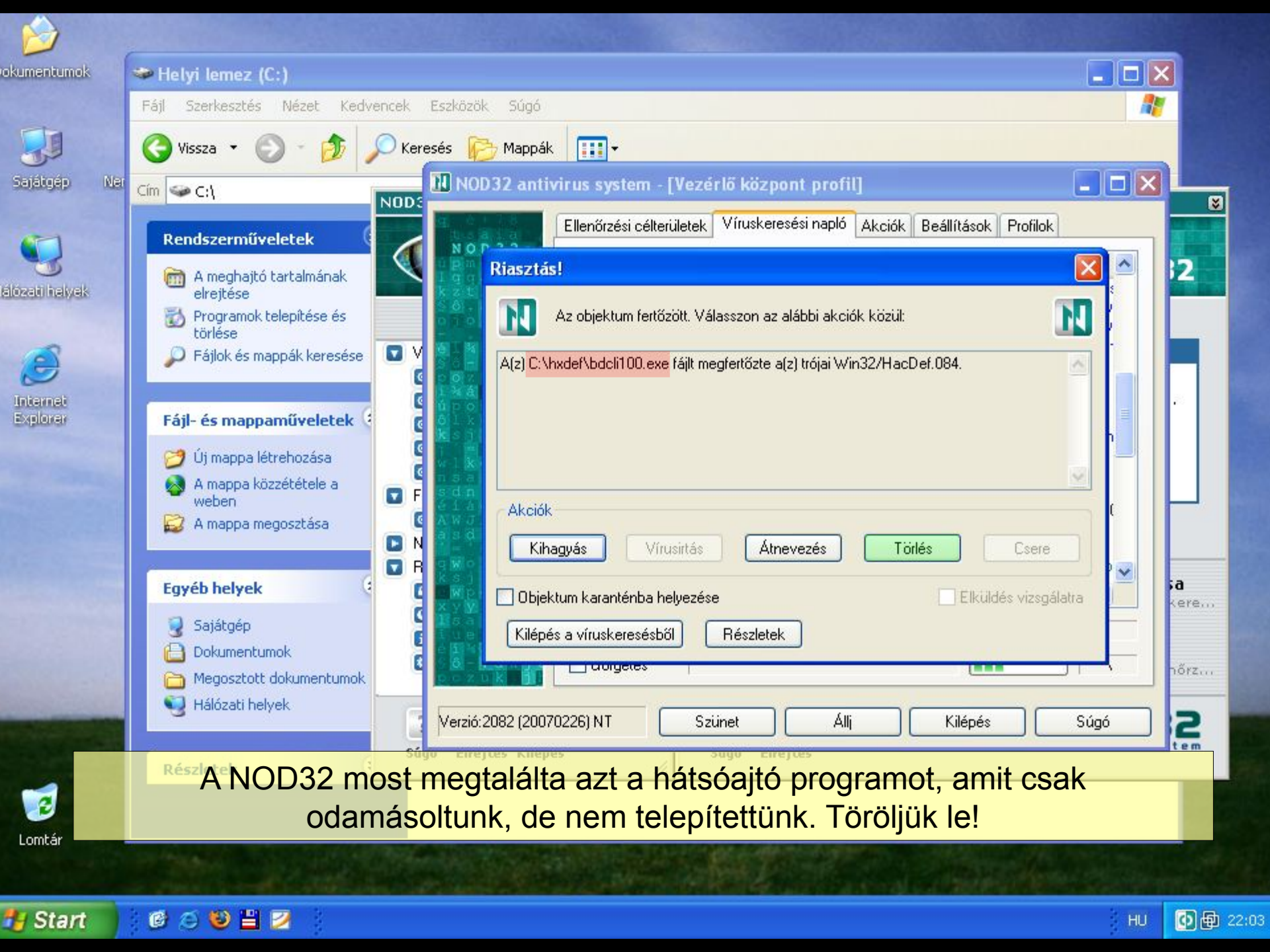
Mivel tudjuk, hol van a rejtett mappánk, időspórolás céljából akár ezt is megadhatnánk a teljes meghajtó ellenőrzése helyett.
A valóságban azonban mindig jobb végrehajtani egy teljes ellenőrzést a gyanús rendszeren.



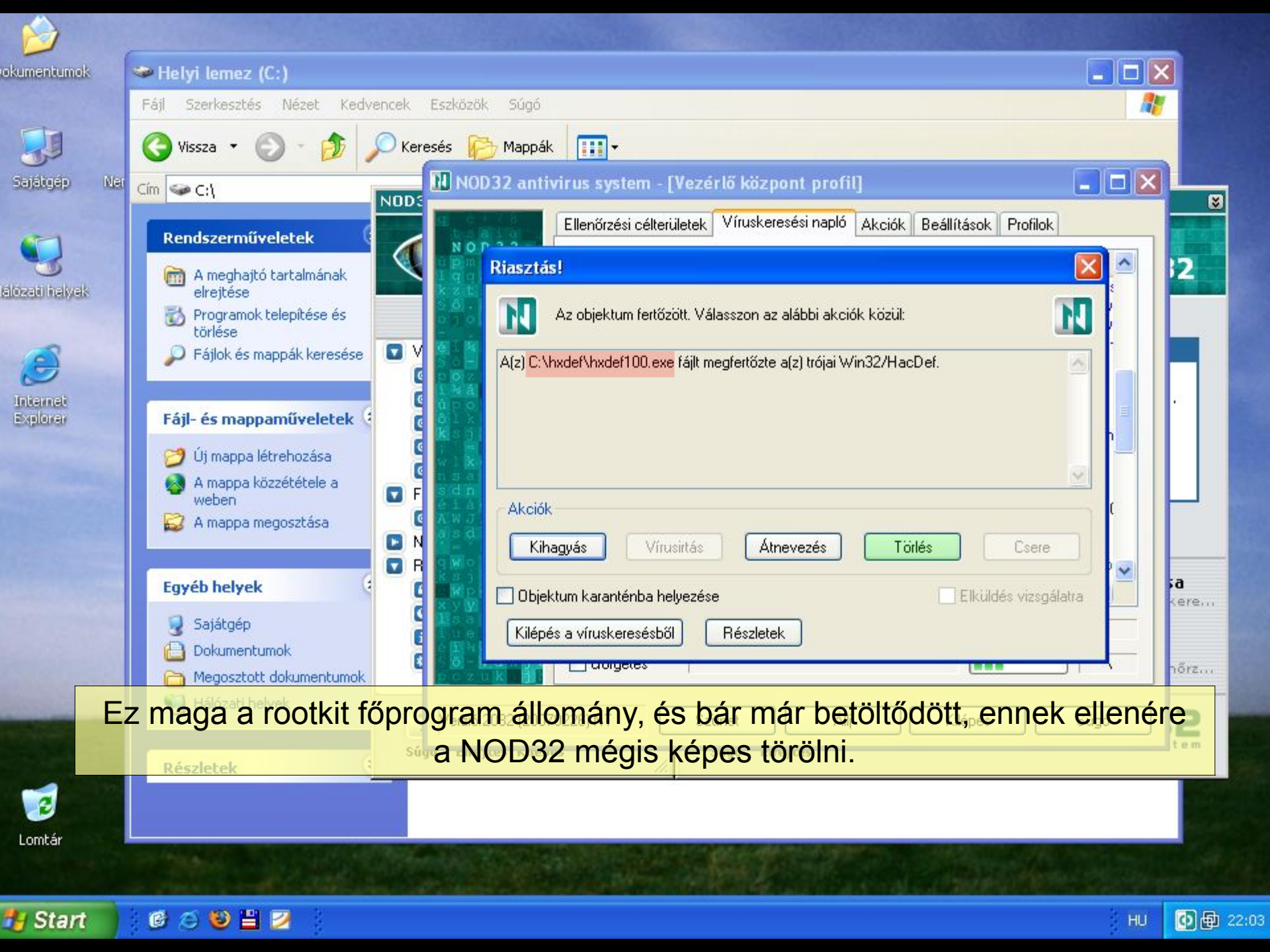
Láthatjuk, hogy kikapcsolt Anti-Stealth opcióval a teljes mappa, és a fertőzött rootkit állományok is rejtve maradtak a NOD32 előtt, az semmilyen fenyegetést nem észlelt.



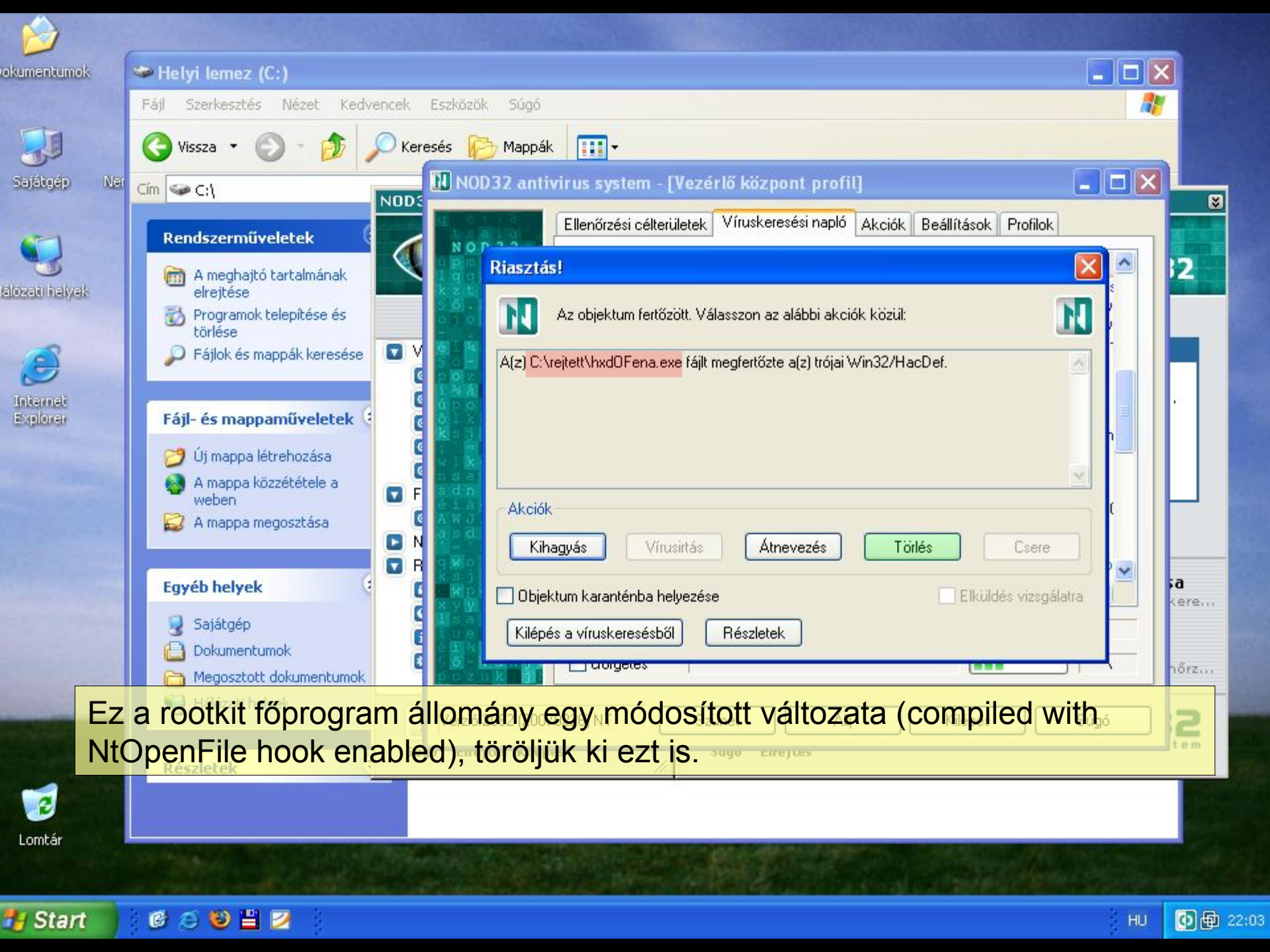
Eljött az ideje, hogy bekapcsoljuk az Anti-Stealth technológiát.
Most ezzel a beállítással ismételjük meg a kézi indítású víruskeresést!



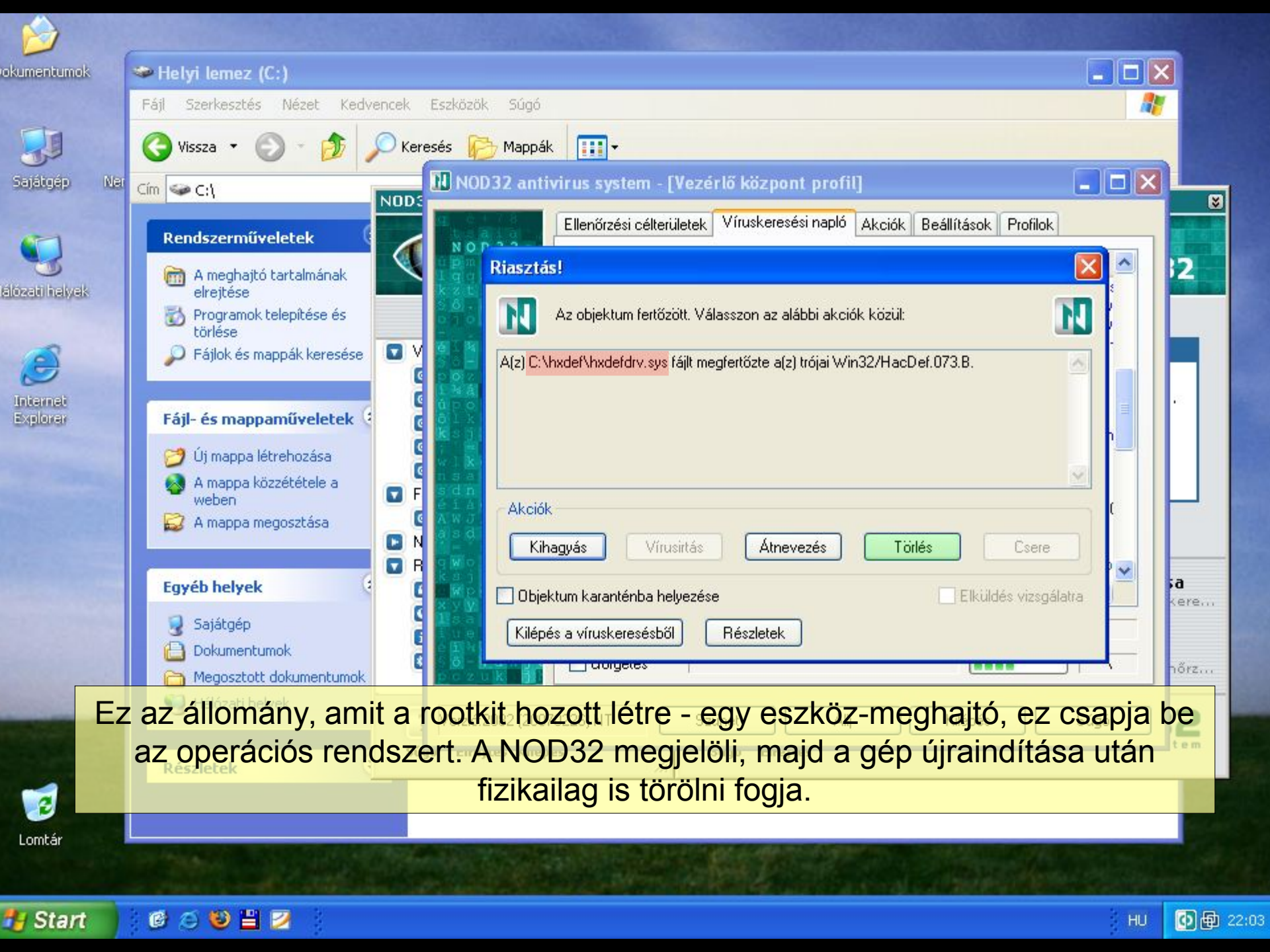
A NOD32 most megtalálta azt a hátsóajtó programot, amit csak odamásoltunk, de nem telepítettünk. Töröljük le!



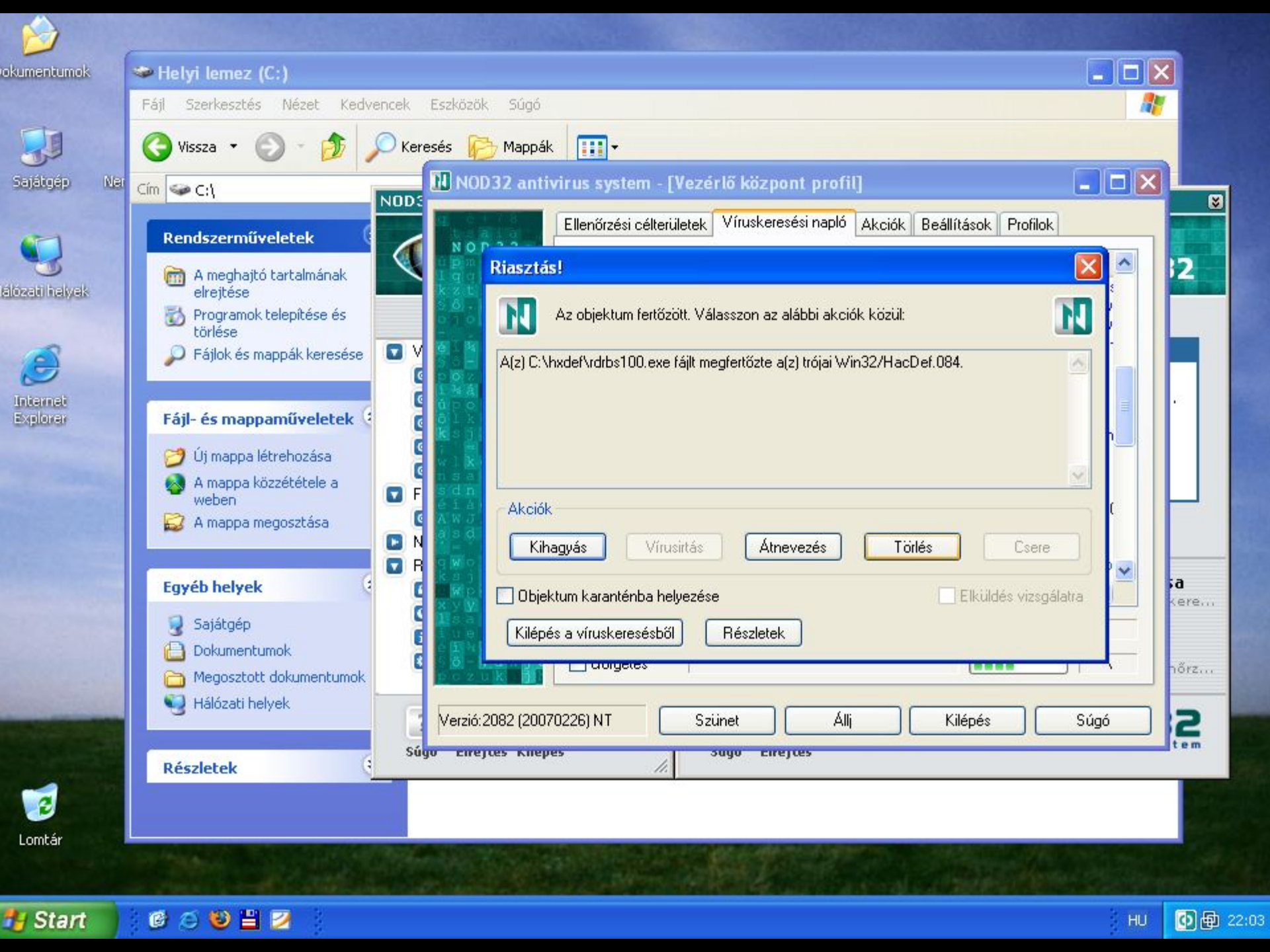
Ez maga a rootkit főprogram állomány, és bár már betöltődött, ennek ellenére a NOD32 mégis képes törölni.

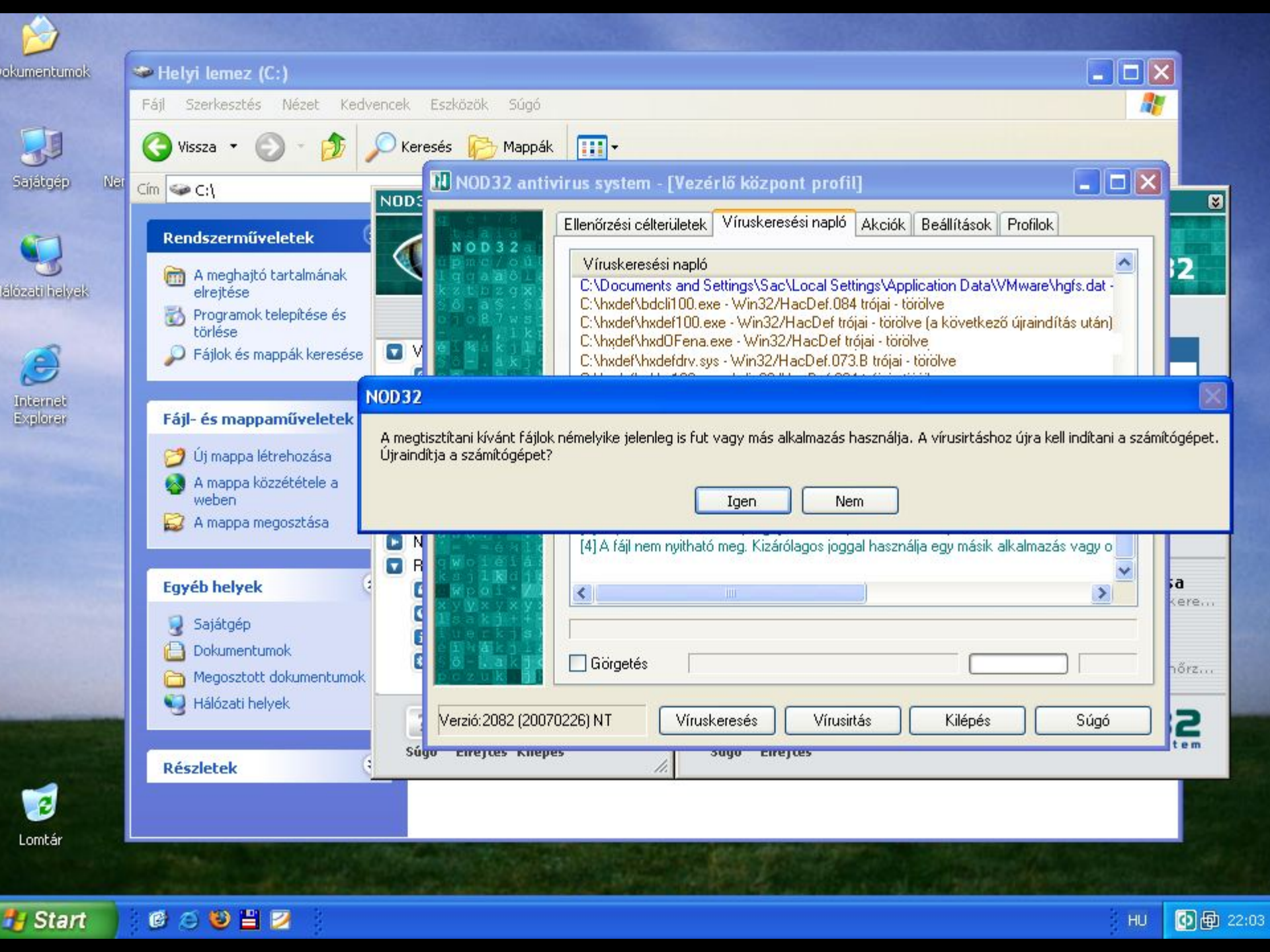


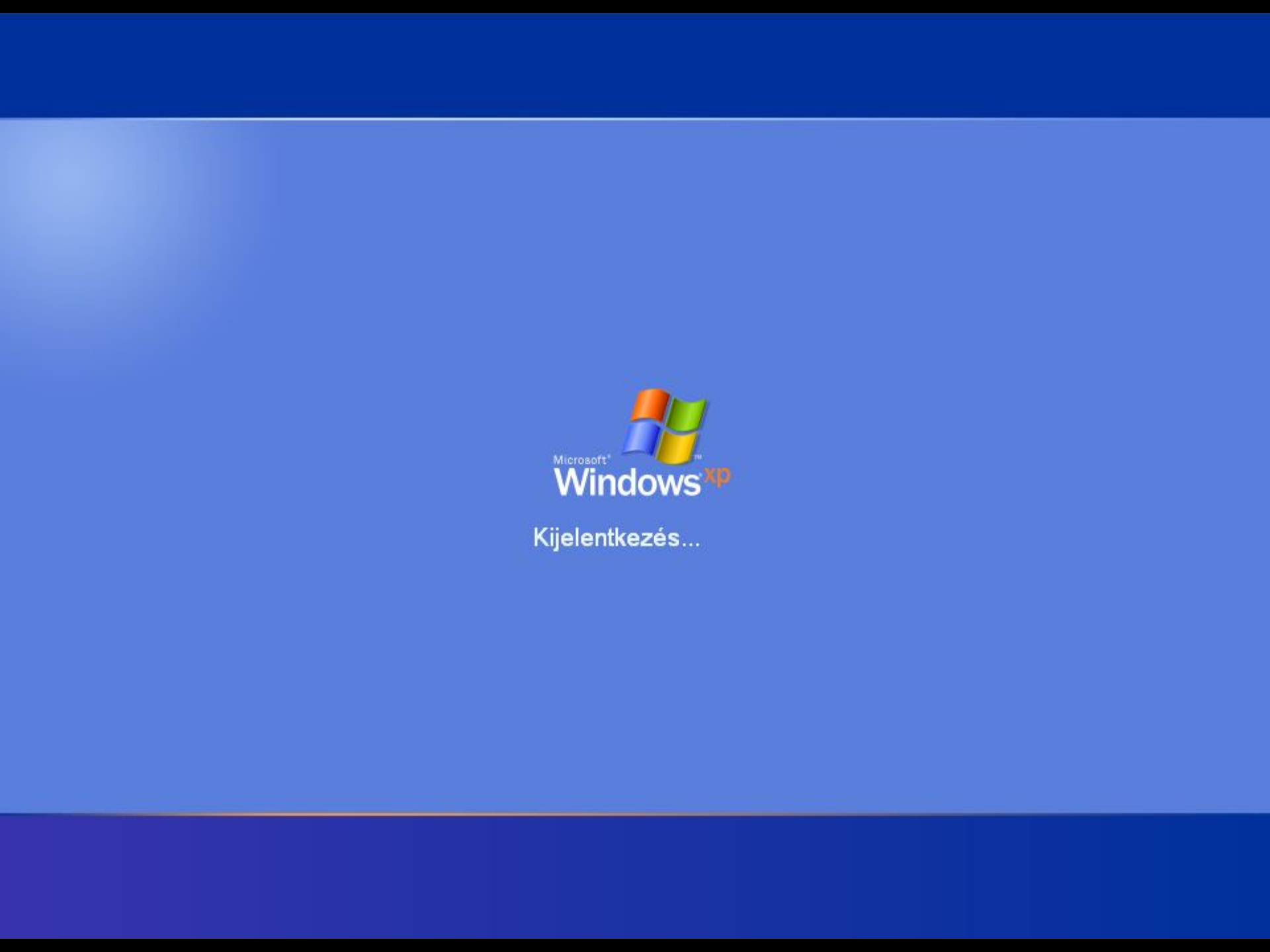
Ez a rootkit főprogram állomány egy módosított változata (compiled with NtOpenFile hook enabled), töröljük ki ezt is.



Ez az állomány, amit a rootkit hozott létre - egy eszköz-meghajtó, ez csapja be az operációs rendszert. A NOD32 megjelöli, majd a gép újraindítása után fizikailag is törölni fogja.

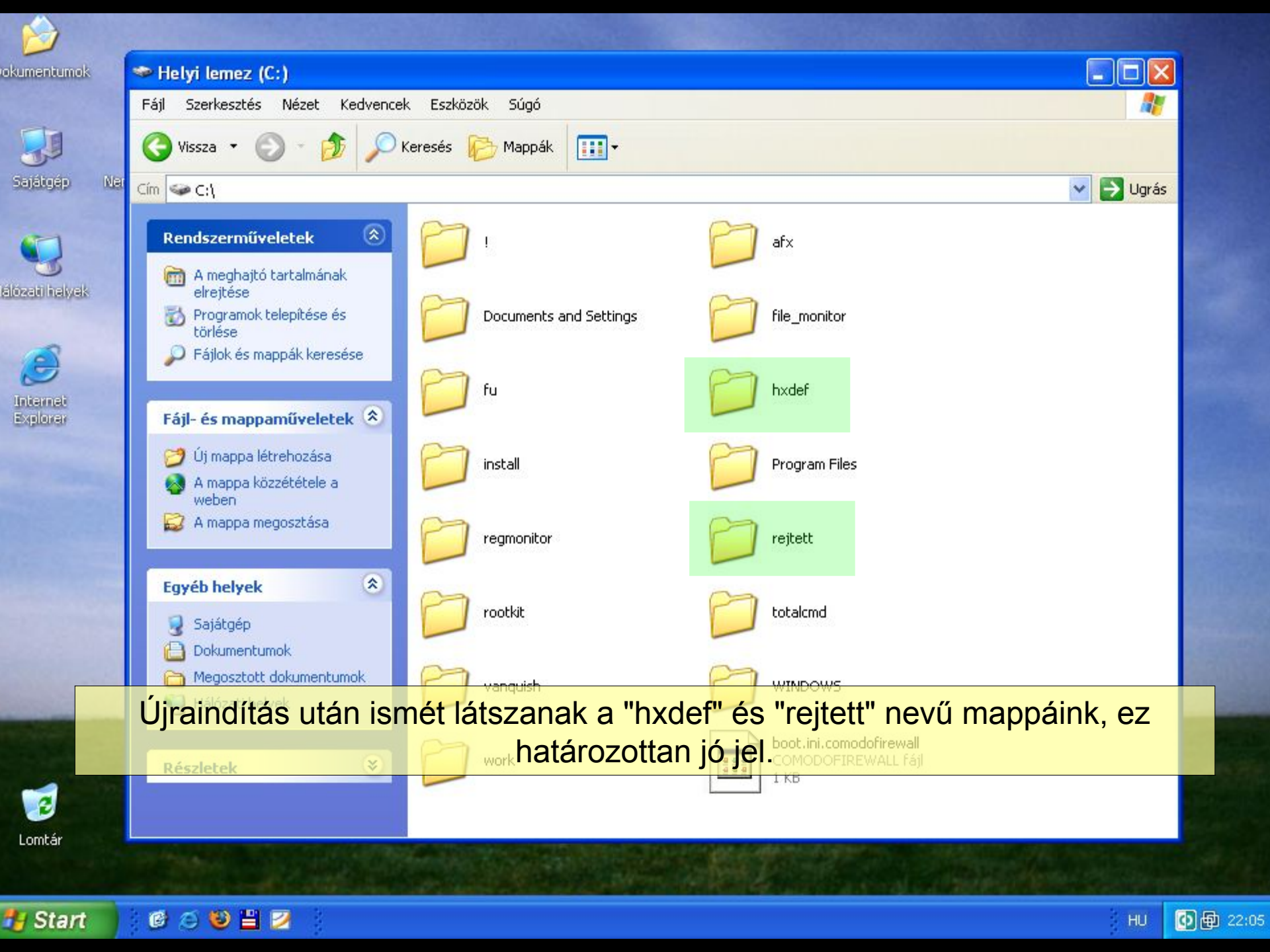

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza Keresés Mappák
Cím C:\
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaműveletek
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
Sajátgép
Dokumentumok
Megosztott dokumentumok
Hálózati helyek
Részletek
NOD32 antivirus system - [Vezérlő központ profil]
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Riasztás!
Az objektum fertőzött. Válasszon az alábbi akciók közül:
A(z) C:\hxdef\rdrbs100.exe fájlt megfertőzte a(z) trójai Win32/HacDef.084.
Akciók
Kihagyás
Vírusirtás
Átnevezés
Törlés
Csere
Objektum karanténba helyezése
Elküldés vizsgálatra
Kilépés a víruskeresésből
Részletek
Verzió:2082 (20070226) NT
Szünet
Állj
Kilépés
Súgó
Sajátgép
Internet Explorer
Lomtár
Start
HU
22:03


Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza Keresés Mappák
Cím C:\
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaműveletek
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
Sajátgép
Dokumentumok
Megosztott dokumentumok
Hálózati helyek
Részletek
NOD32 antivirus system - [Vezérlő központ profil]
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Víruskeresési napló
C:\Documents and Settings\Sac\Local Settings\Application Data\VMware\hgfs.dat -
C:\hxdef\bdcli100.exe - Win32/HacDef.084 trójai - törölve
C:\hxdef\hxdef100.exe - Win32/HacDef trójai - törölve (a következő újraindítás után)
C:\hxdef\hxdOFena.exe - Win32/HacDef trójai - törölve
C:\hxdef\hxdefdrv.sys - Win32/HacDef.073.B trójai - törölve
NOD32
A megtisztítani kívánt fájlok némelyike jelenleg is fut vagy más alkalmazás használja. A vírusirtáshoz újra kell indítani a számítógépet. Újraindítja a számítógépet?
Igen
Nem
[4] A fájl nem nyitható meg. Kizárólagos joggal használja egy másik alkalmazás vagy o
Görgetés
Verzió:2082 (20070226) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
Sajátgép
Internet Explorer
Lomtár
Start
HU
22:03

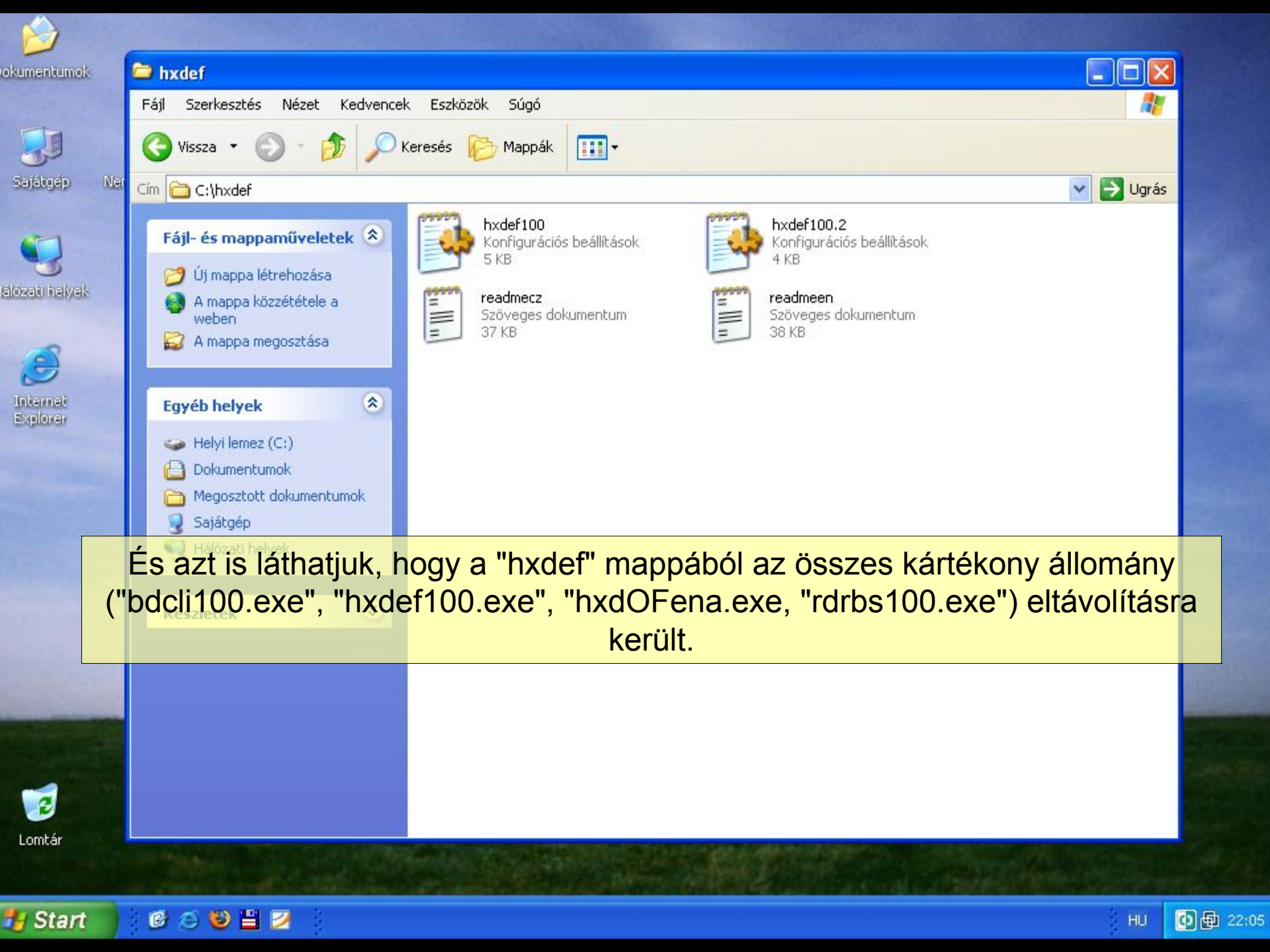

Microsoft
Windows xp
Kijelentkezés...


Microsoft®
Windows®xp
Copyright © Microsoft Corporation
Microsoft

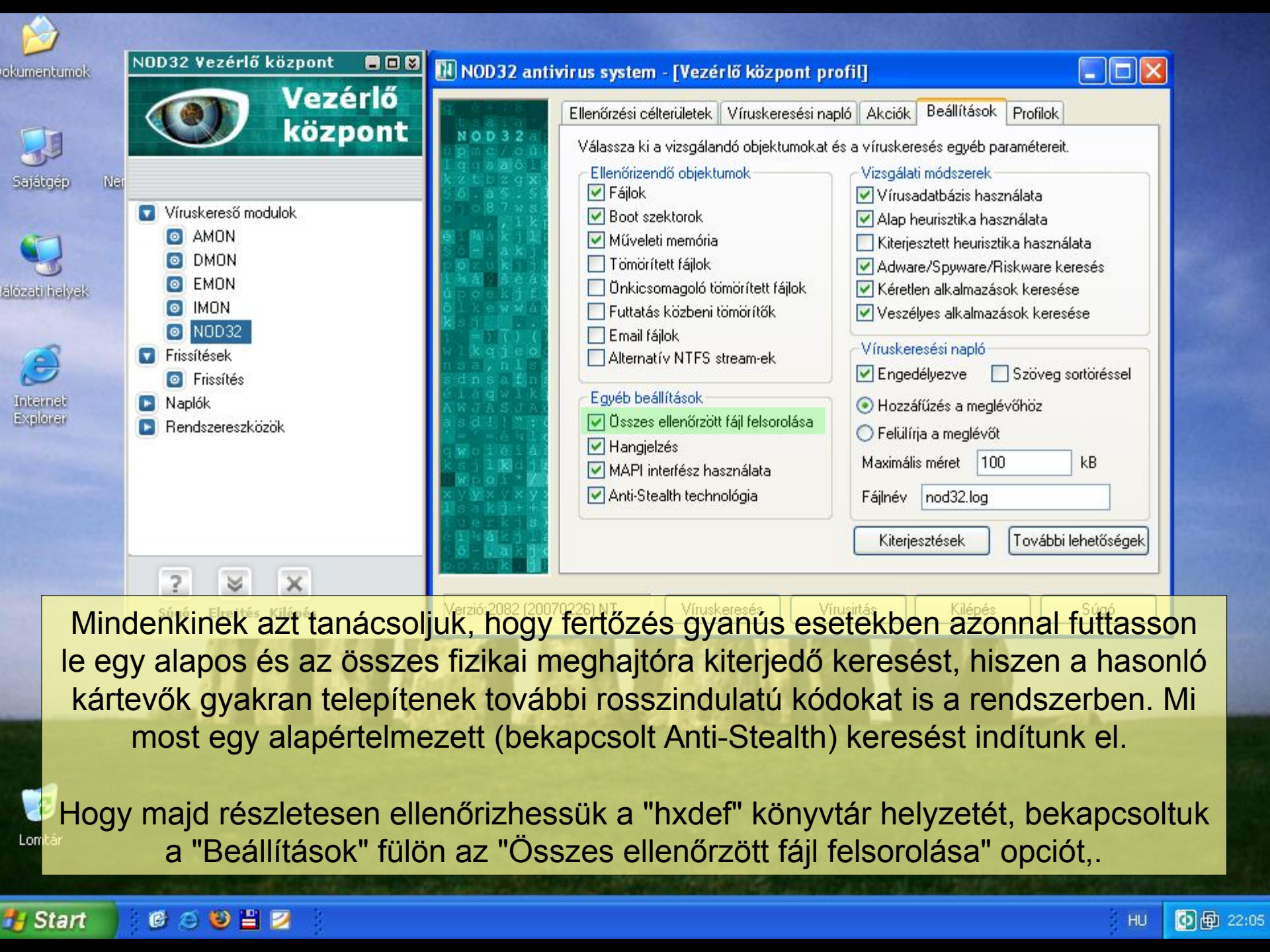
Üdvözöljük



Újraindítás után ismét látszanak a "hxdef" és "rejtett" nevű mappáink, ez határozottan jó jel.

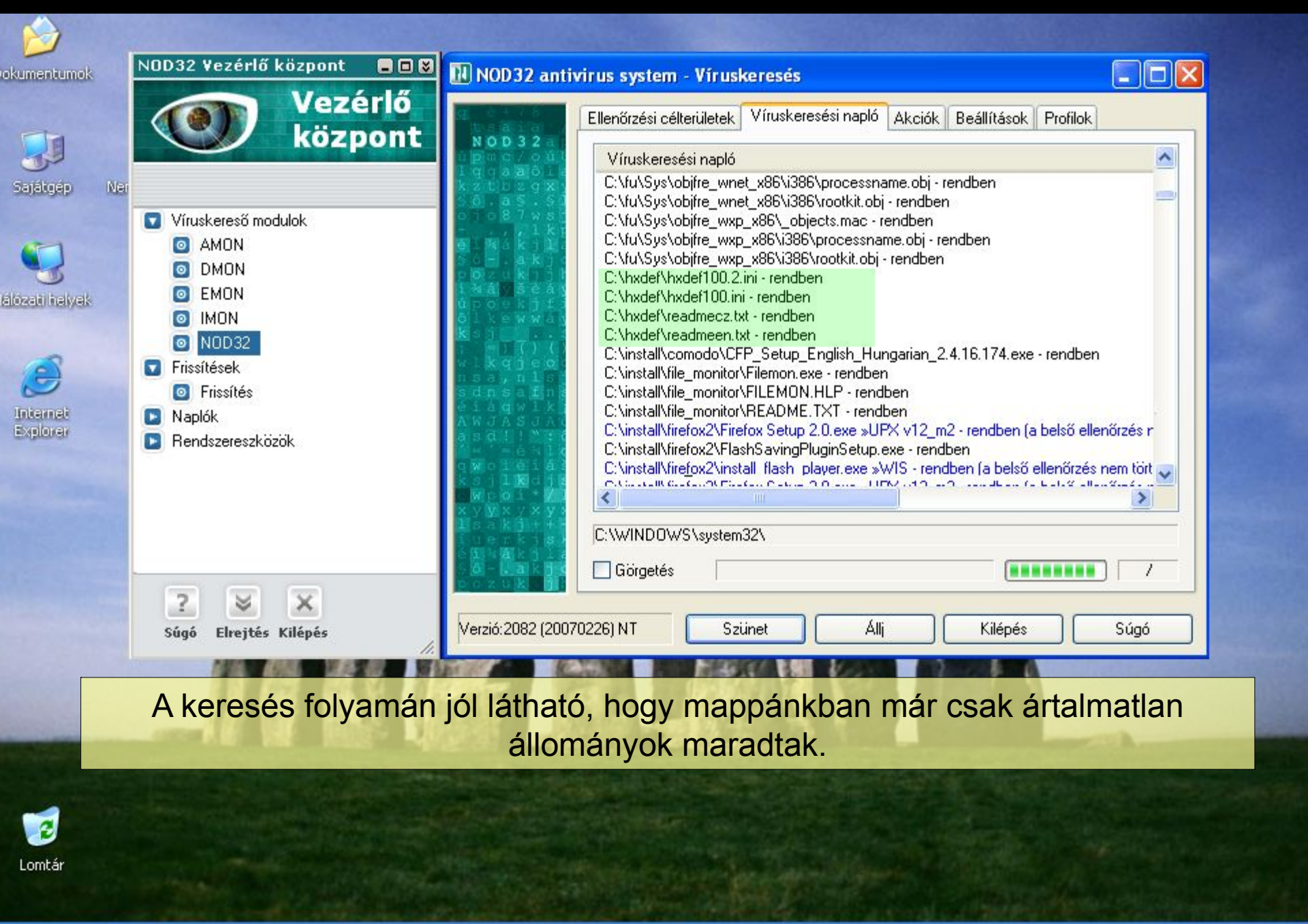


És azt is láthatjuk, hogy a "hxdef" mappából az összes kártékony állomány ("bdcli100.exe", "hxdef100.exe", "hxdOFena.exe, "rdrbs100.exe") eltávolításra került.

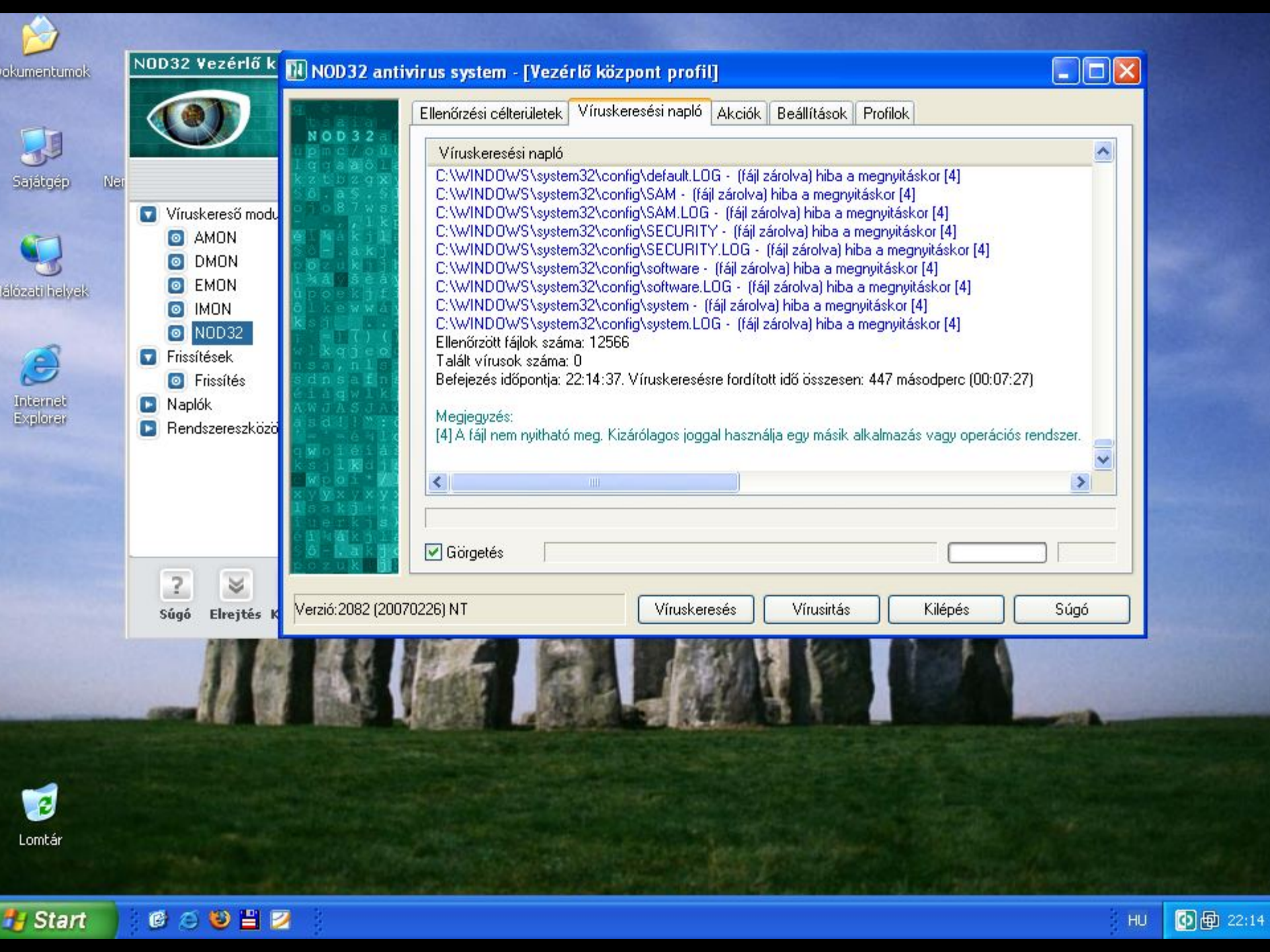


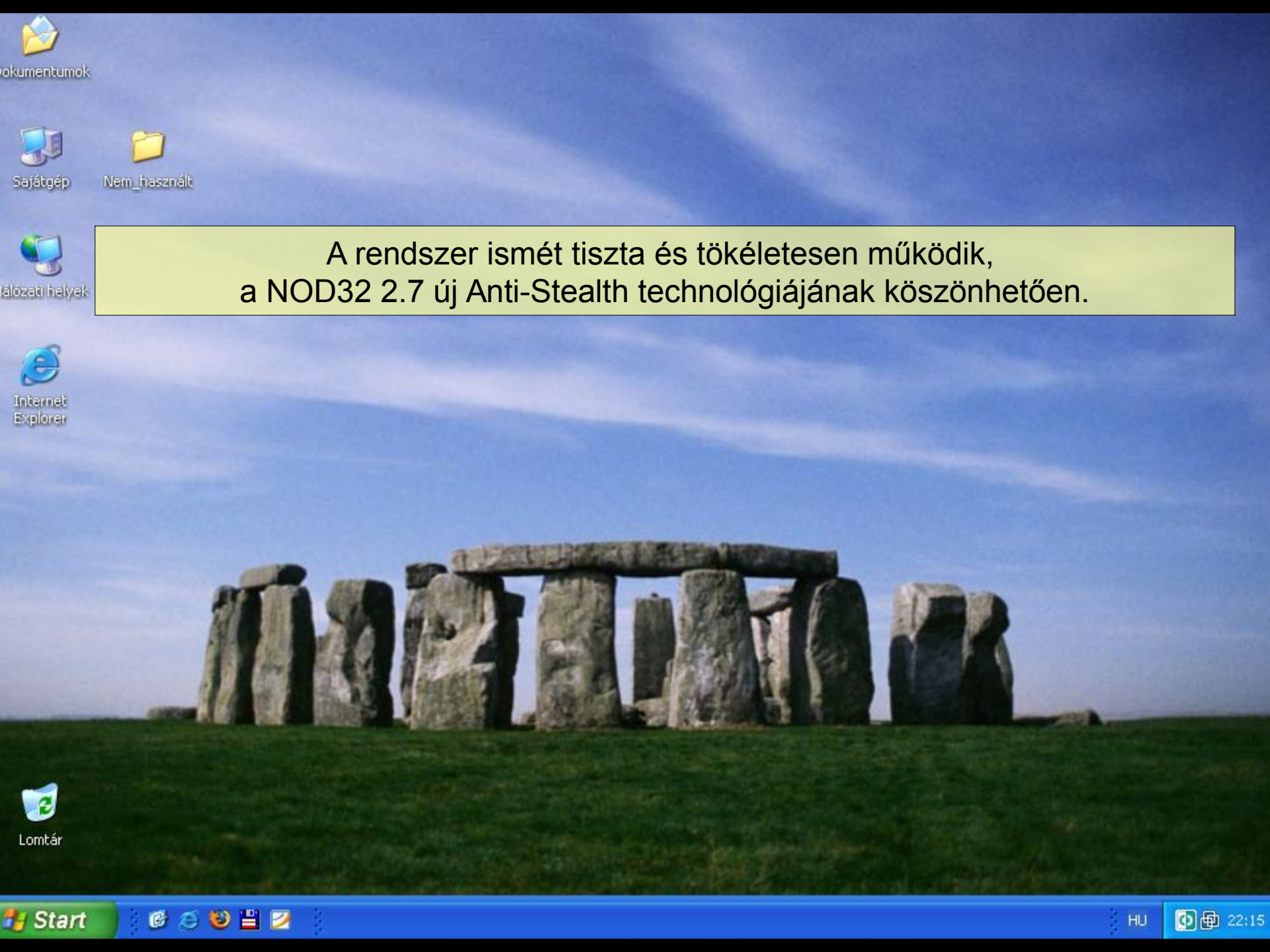
Mindenkinek azt tanácsoljuk, hogy fertőzés gyanús esetekben azonnal futtasson le egy alapos és az összes fizikai meghajtóra kiterjedő keresést, hiszen a hasonló kártevők gyakran telepítenek további rosszindulatú kódokat is a rendszerben. Mi most egy alapértelmezett (bekapcsolt Anti-Stealth) keresést indítunk el.

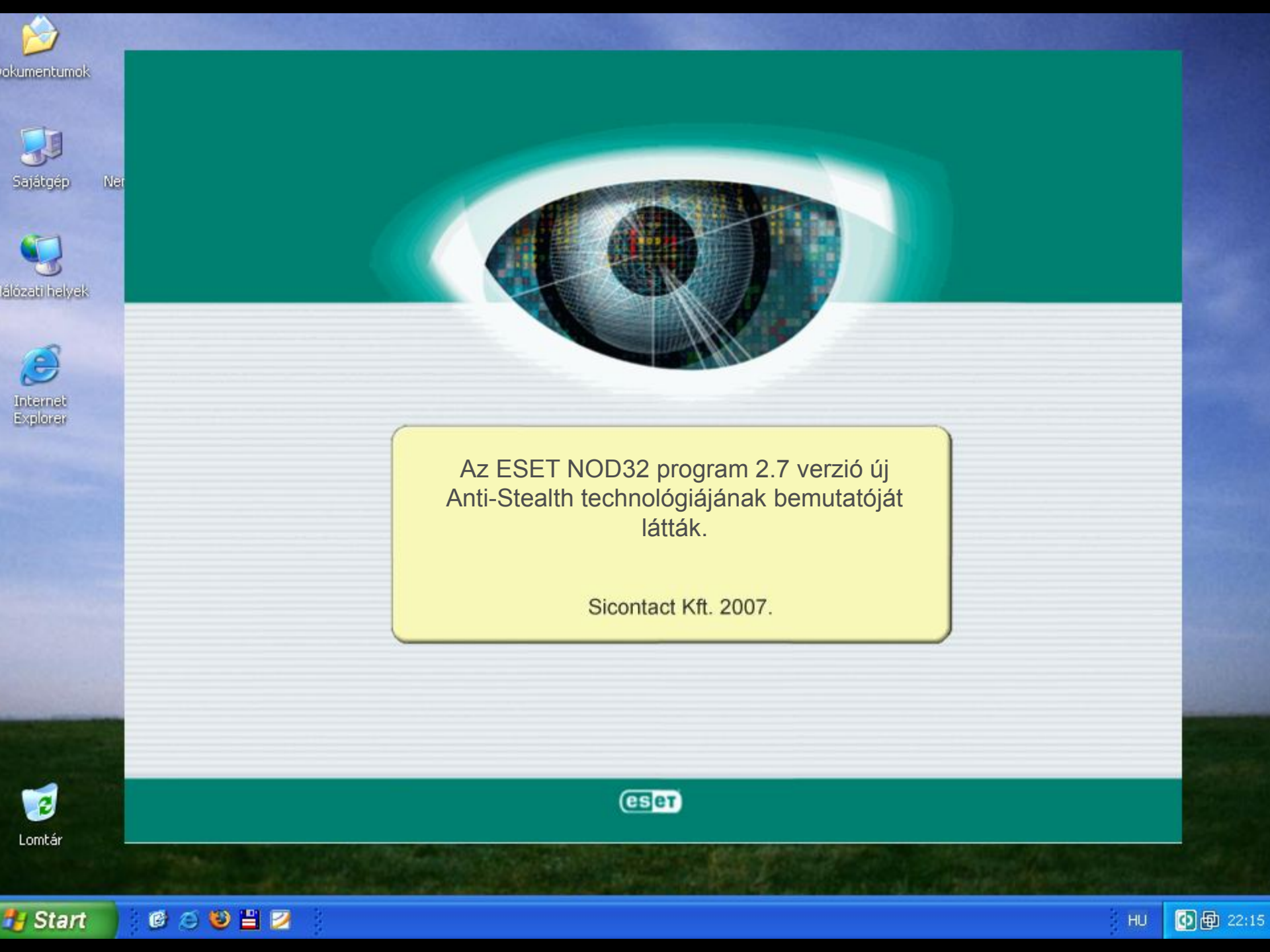
Hogy majd részletesen ellenőrizhessük a "hxdef" könyvtár helyzetét, bekapcsoltuk a "Beállítások" fülön az "Összes ellenőrzött fájl felsorolása" opciót,.



A keresés folyamán jól látható, hogy mappánkban már csak ártalmatlan állományok maradtak.


NOD32 Vezérlő k
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 [4]
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: 12566
Talált vírusok száma: 0
Befejezés időpontja: 22:14:37. Víruskeresésre fordított idő összesen: 447 másodperc (00:07:27)
Megjegyzés:
[4] A fájl nem nyitható meg. Kizárólagos joggal használja egy másik alkalmazás vagy operációs rendszer.
Görgetés
Verzió:2082 (20070226) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
Víruskereső modu
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközö
Súgó
Elrejtés
Sajátgép
Internet Explorer
Lomtár
Start
HU
22:14


okumentumok
Sajátgép
Nem_használt
lózati helyek
Internet Explorer
Lomtár
A rendszer ismét tiszta és tökéletesen működik,
a NOD32 2.7 új Anti-Stealth technológiájának köszönhetően.
Start
HU
22:15


okumentumok
Sajátgép
Ner
lózati helyek
Internet Explorer
Lomtár
Az ESET NOD32 program 2.7 verzió új Anti-Stealth technológiájának bemutatóját látták.
Sicontact Kft. 2007.
eset
Start
HU
22:15