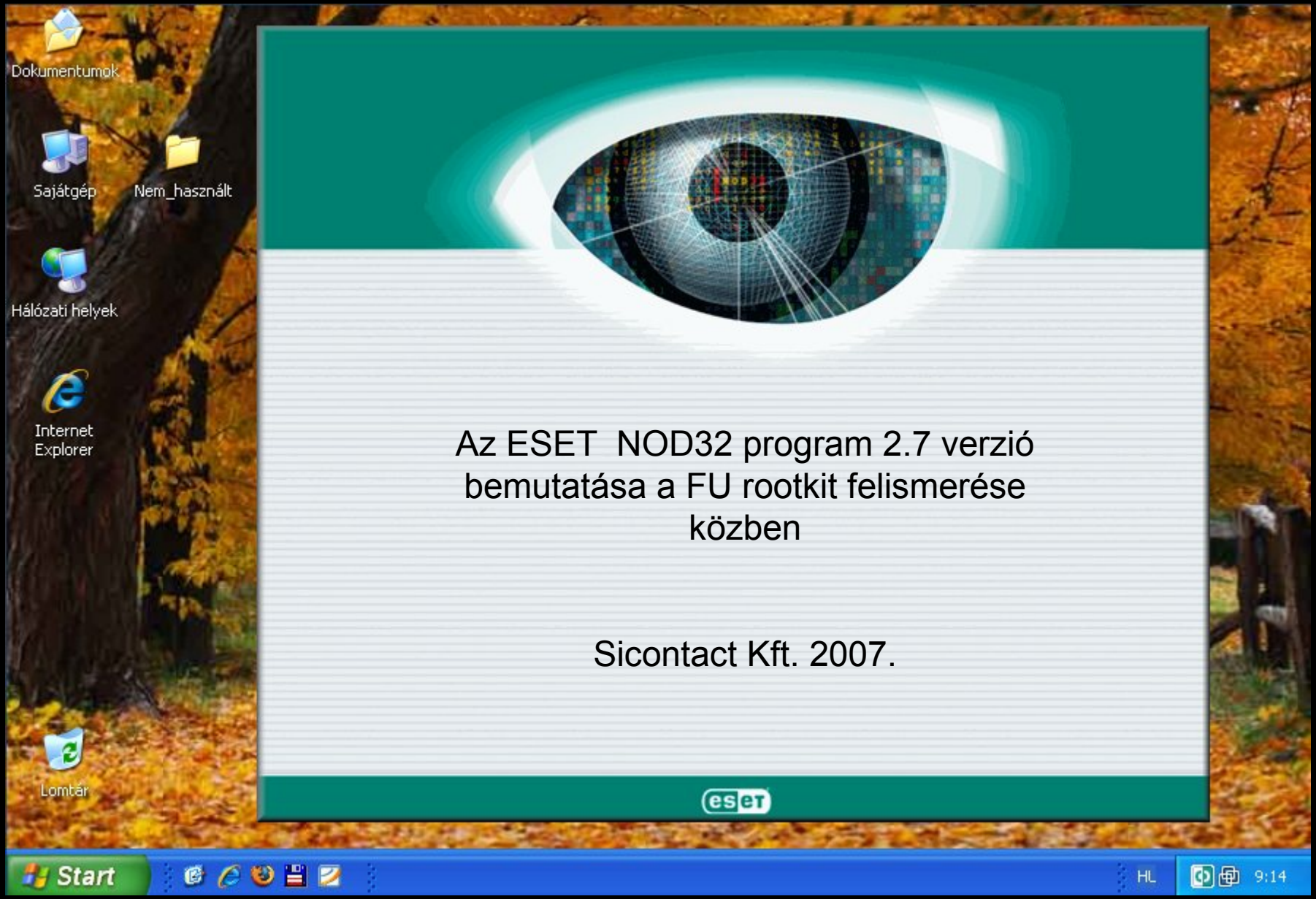

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Az ESET NOD32 program 2.7 verzió bemutatása a FU rootkit felismerése közben
Sicontact Kft. 2007.
eset
Start
HL
9:14

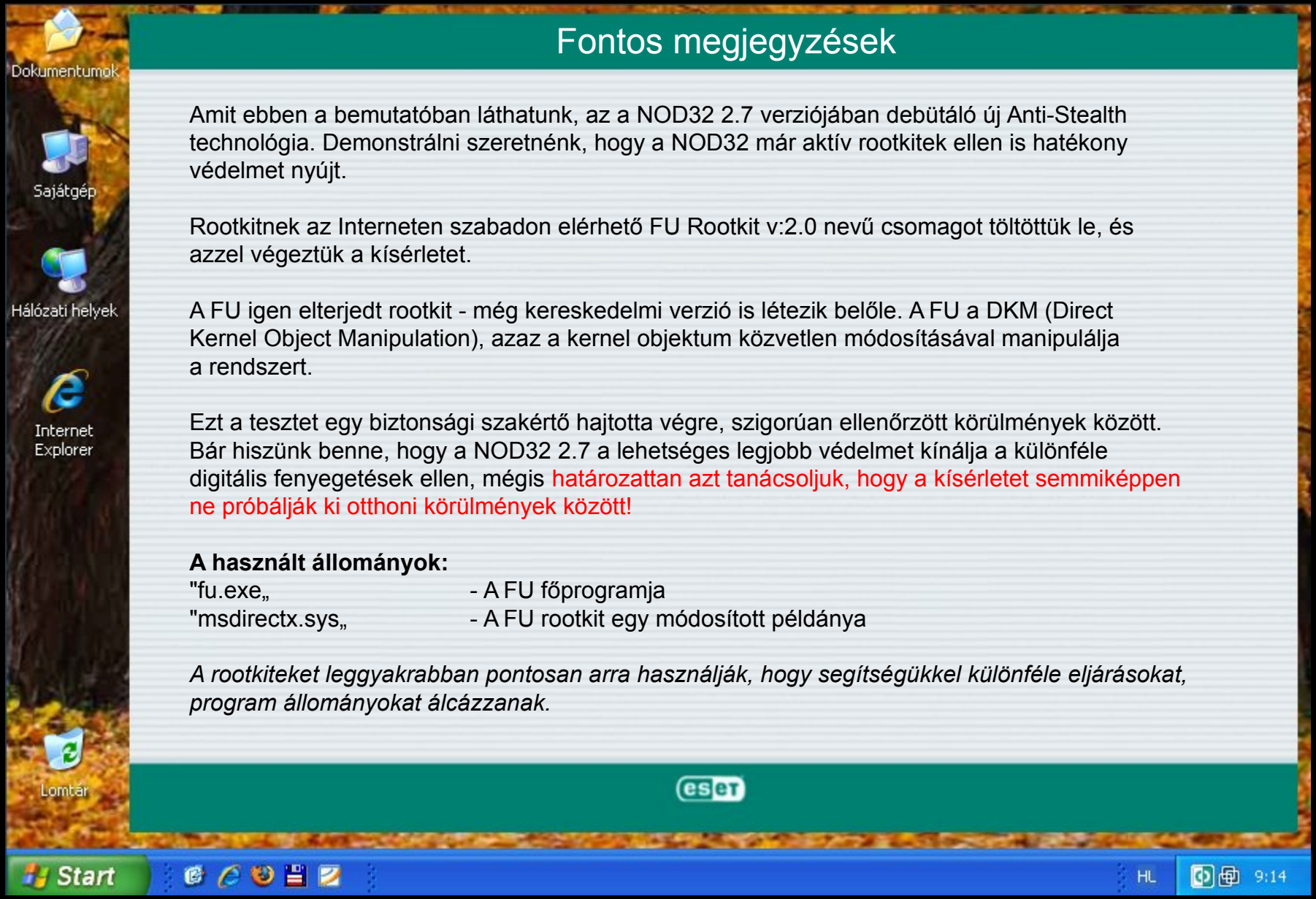
Előadás vázlat

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.

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

Elindítunk egy kézi víruskeresést a rendszeren.

A NOD32 megtalálja a rootkitet, és komponenseit, 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 FU Rootkit v:2.0 nevű csomagot töltöttük le, és azzel végeztük a kísérletet.

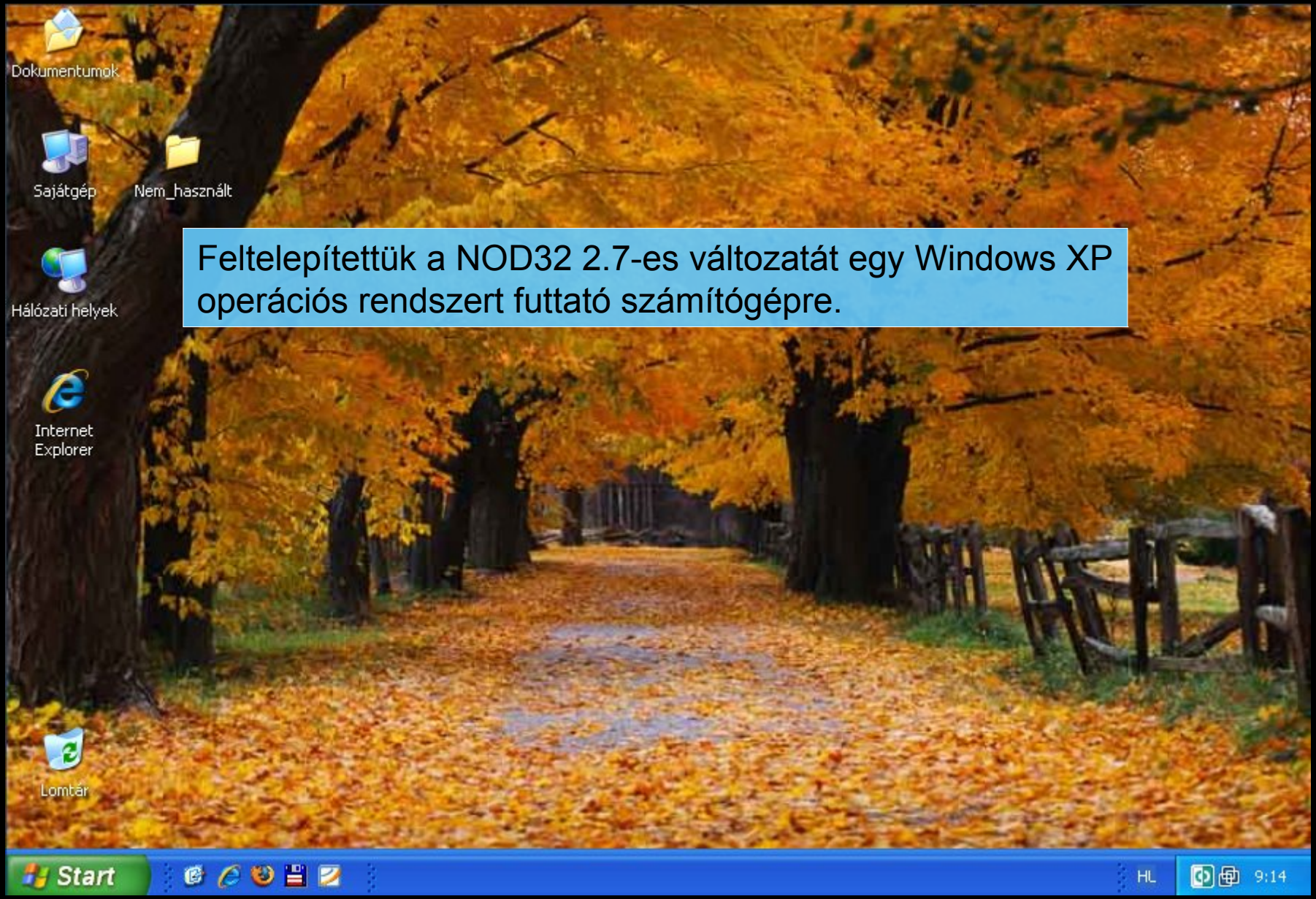
A FU igen elterjedt rootkit - még kereskedelmi verzió is létezik belőle. A FU a DKM (Direct Kernel Object Manipulation), azaz a kernel objektum közvetlen módosításával manipulálja a rendszert.

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:

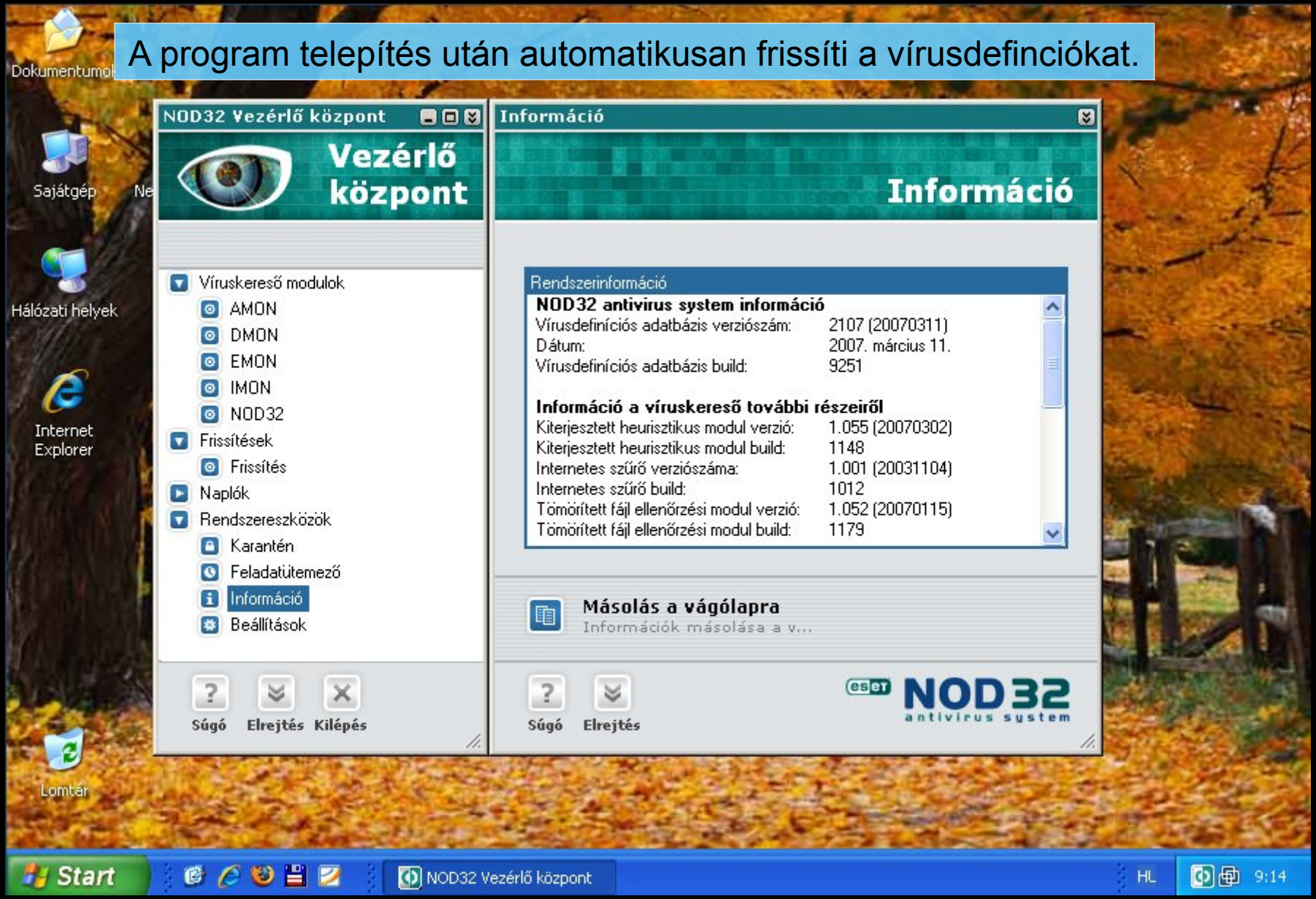
"fu.exe„	- A FU főprogramja
"msdirectx.sys„	- A FU rootkit egy módosított példánya

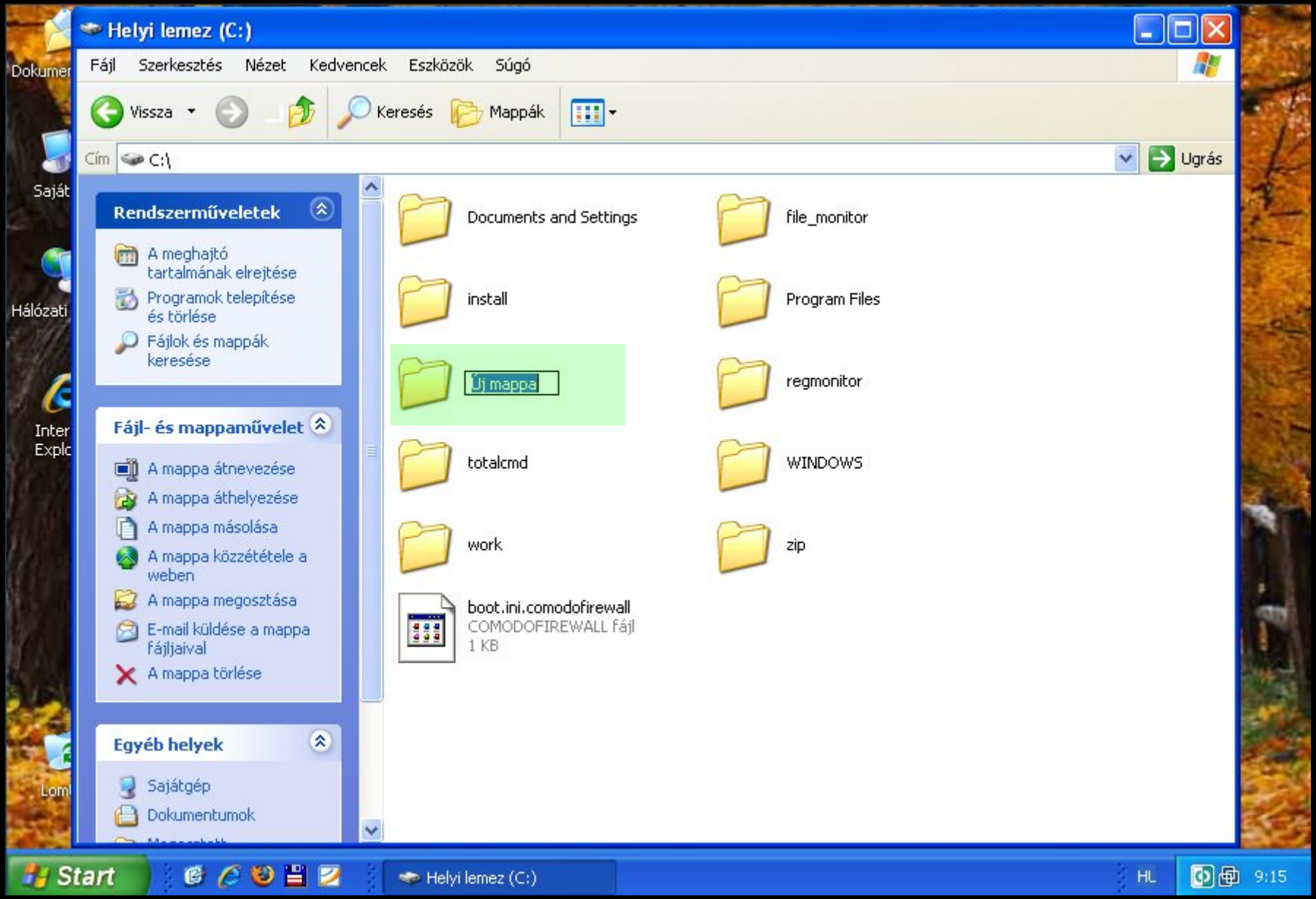
A rootkiteket leggyakrabban pontosan arra használják, hogy segítségükkel különféle eljárásokat, program állományokat álcázzanak.

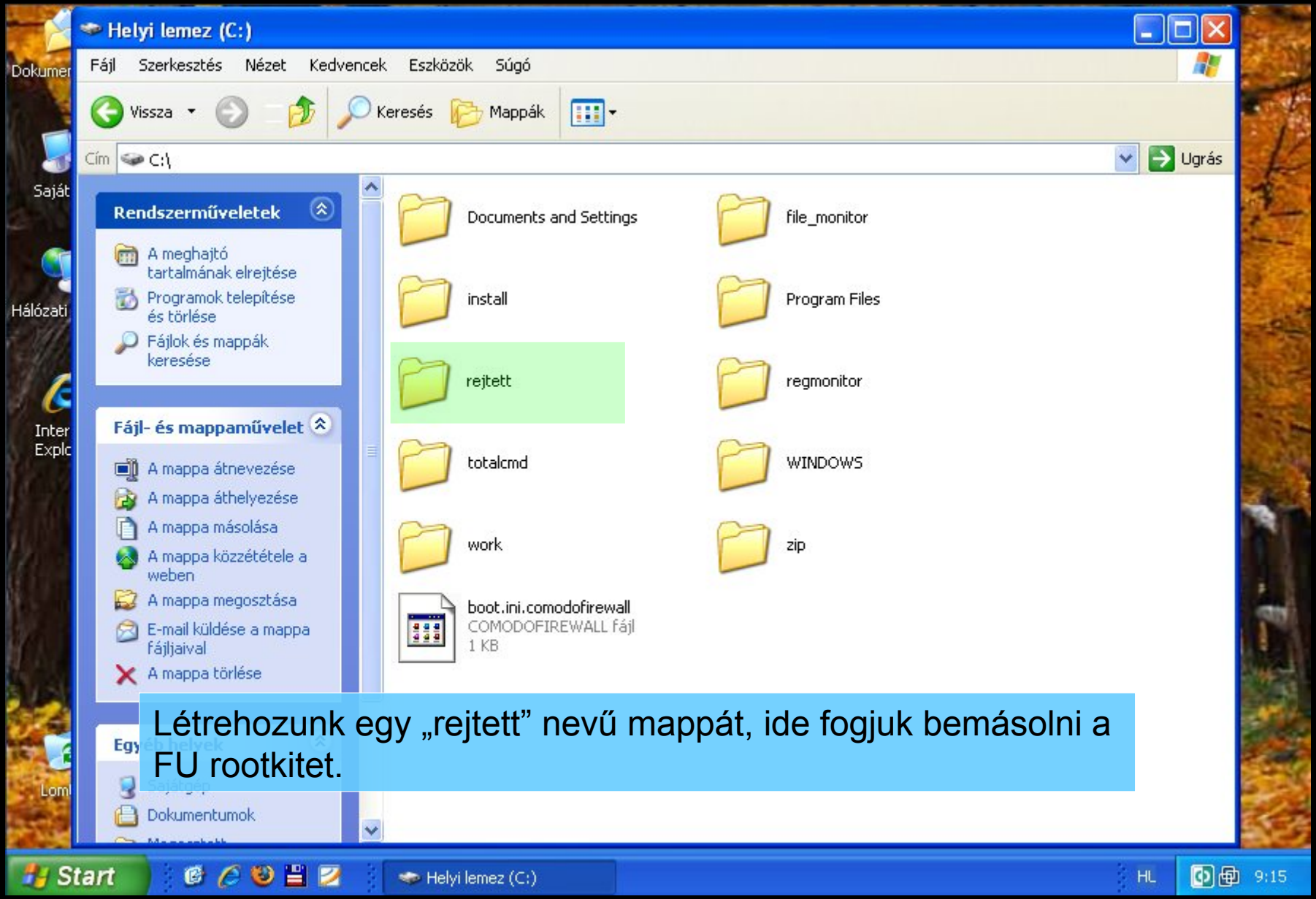


Feltelepítettük a NOD32 2.7-es változatát egy Windows XP operációs rendszert futtató számítógépre.

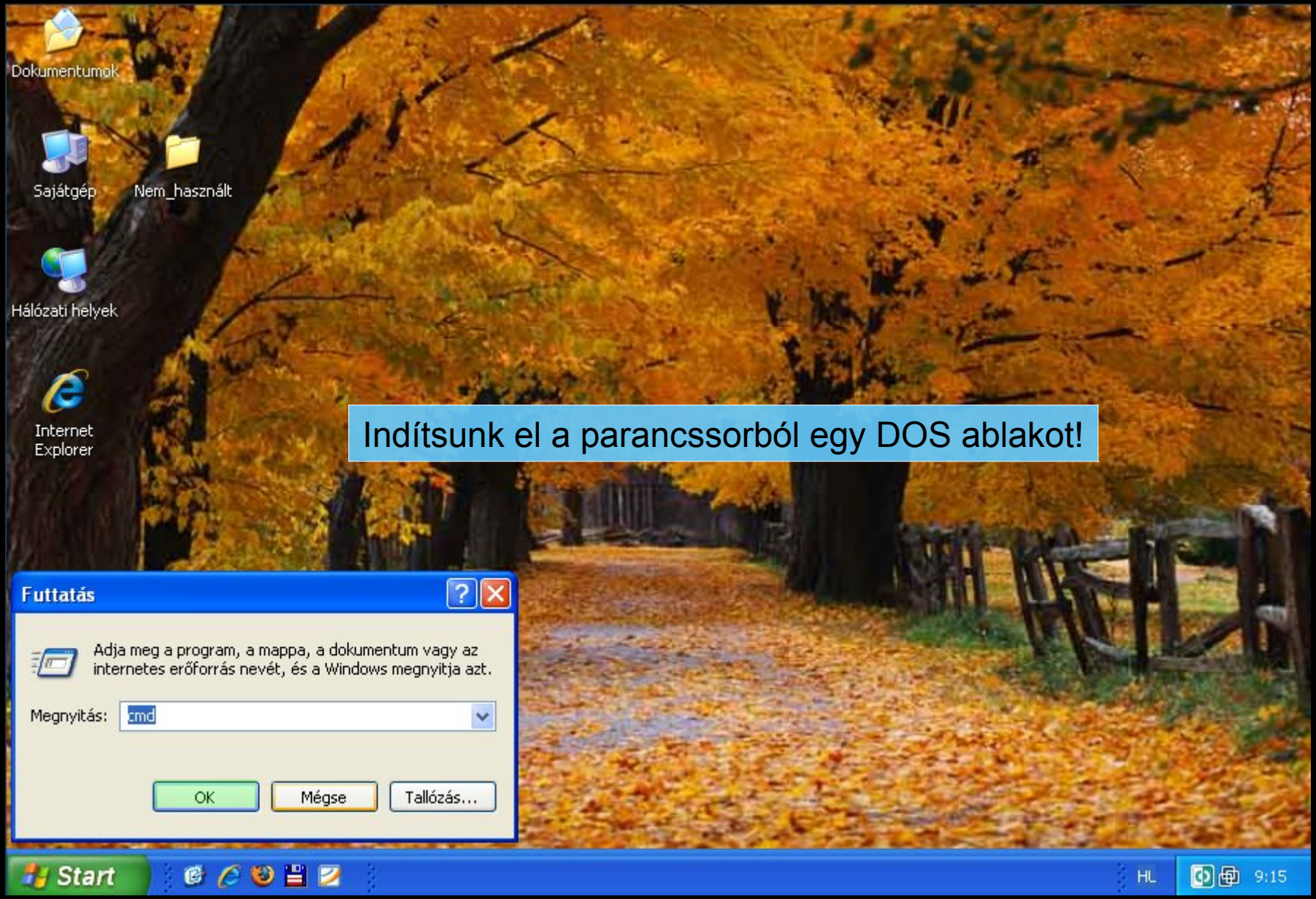
A program telepítés után automatikusan frissíti a vírusdefinciókat.

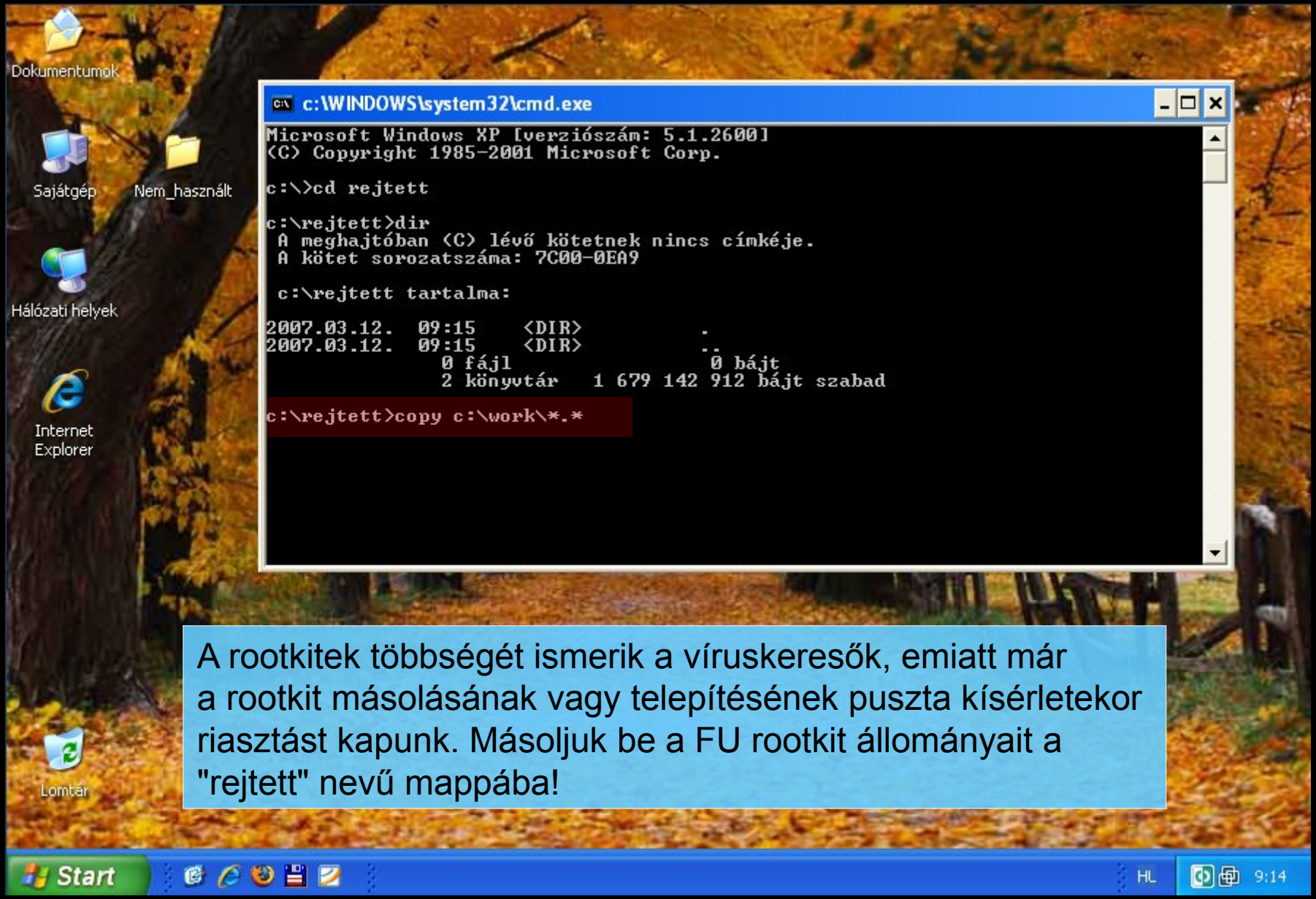



Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
A mappa átnevezése
A mappa áthelyezése
A mappa másolása
A mappa közzététele a weben
A mappa megosztása
E-mail küldése a mappa fájljaival
A mappa törlése
Egyéb helyek
Sajátgép
Dokumentumok
Documents and Settings
file_monitor
install
Program Files
Új mappa
regmonitor
totalcmd
WINDOWS
work
zip
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
Start
Helyi lemez (C:)
HL
9:15

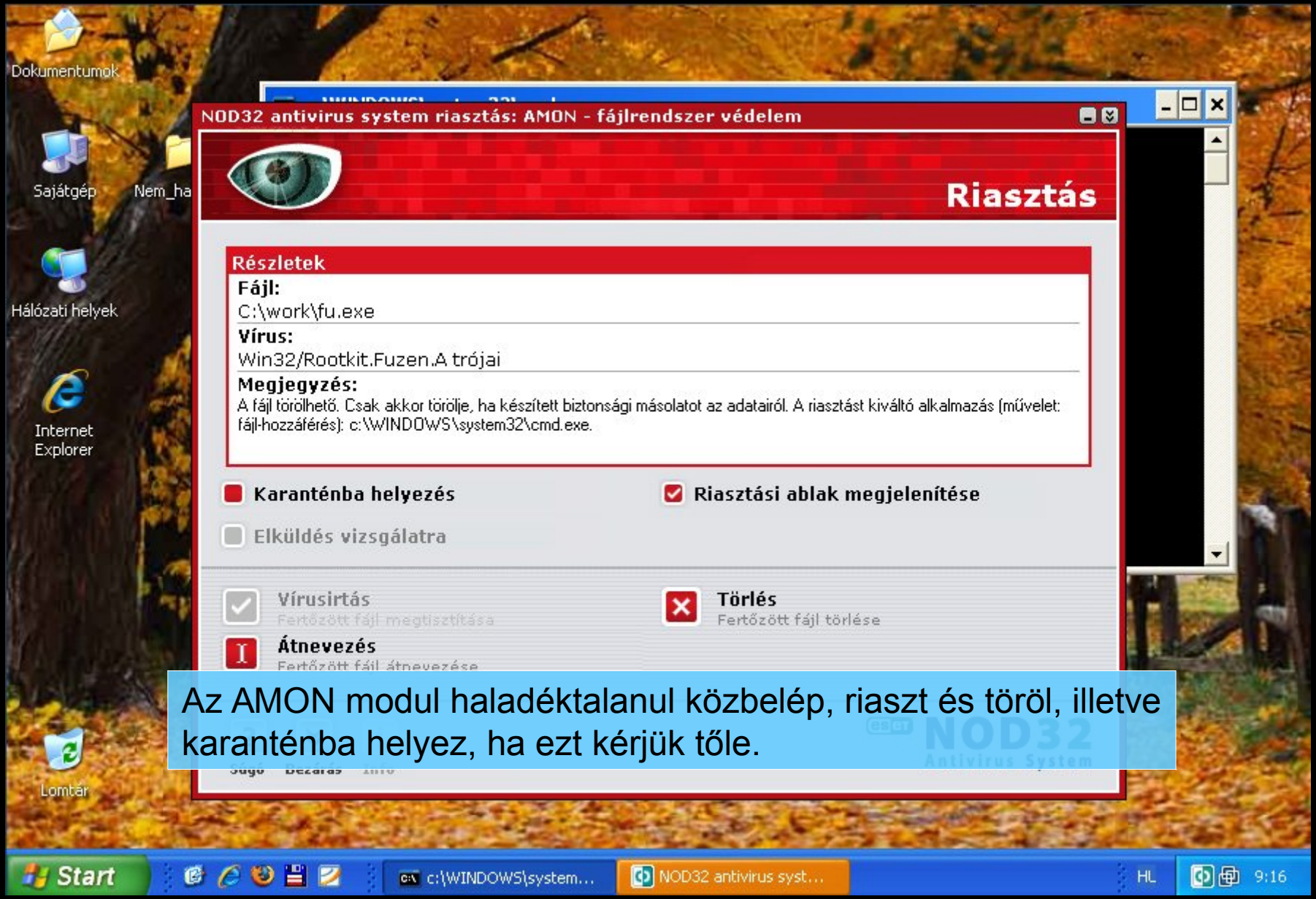


Létrehozunk egy „rejtett” nevű mappát, ide fogjuk bemásolni a FU rootkitet.

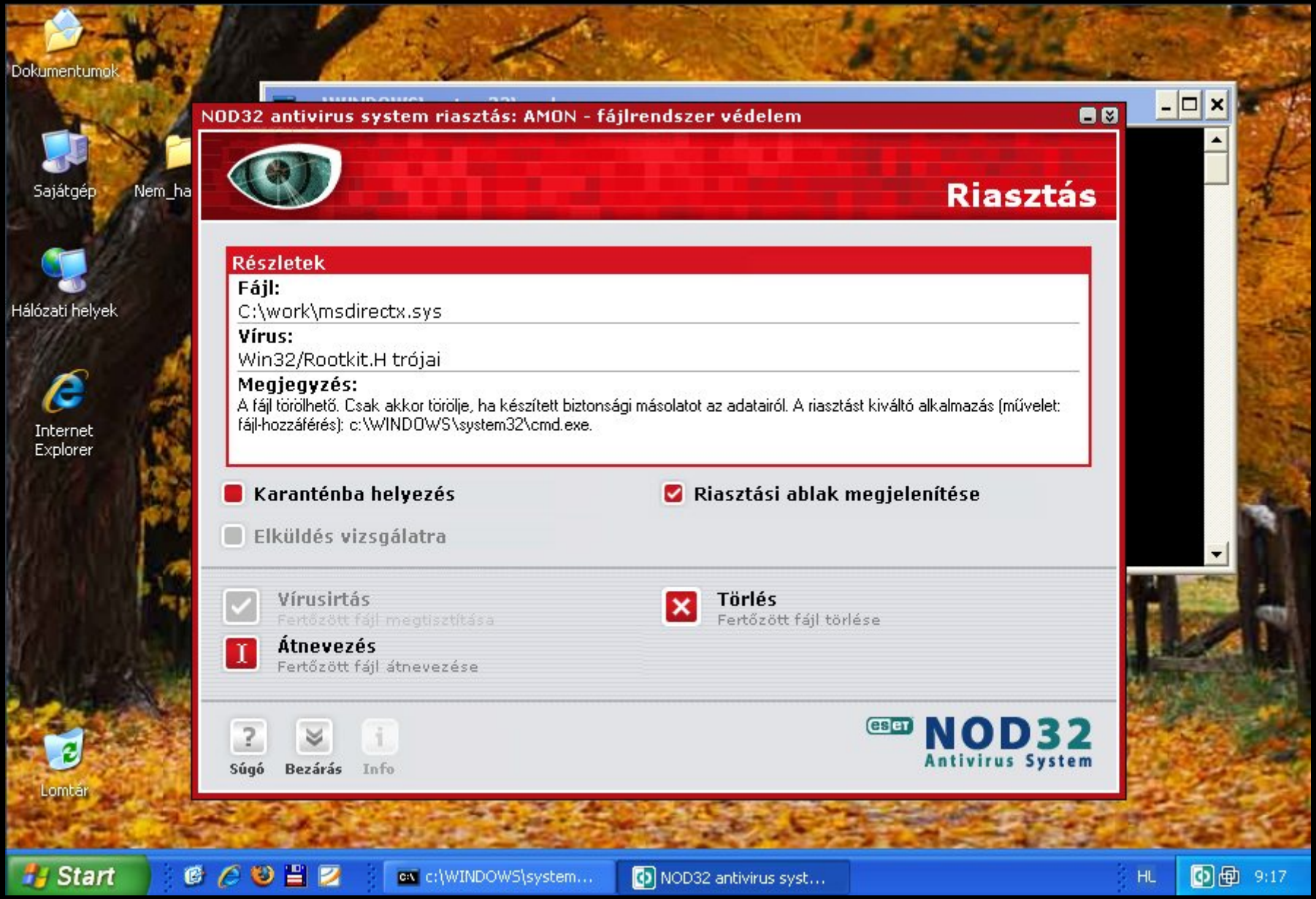

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Indítsunk el a parancssorból egy DOS ablakot!
Futtatás
Adja meg a program, a mappa, a dokumentum vagy az internetes erőforrás nevét, és a Windows megnyitja azt.
Megnyitás:
cmd
OK
Mégse
Tallózás...
Start
HL
9:15

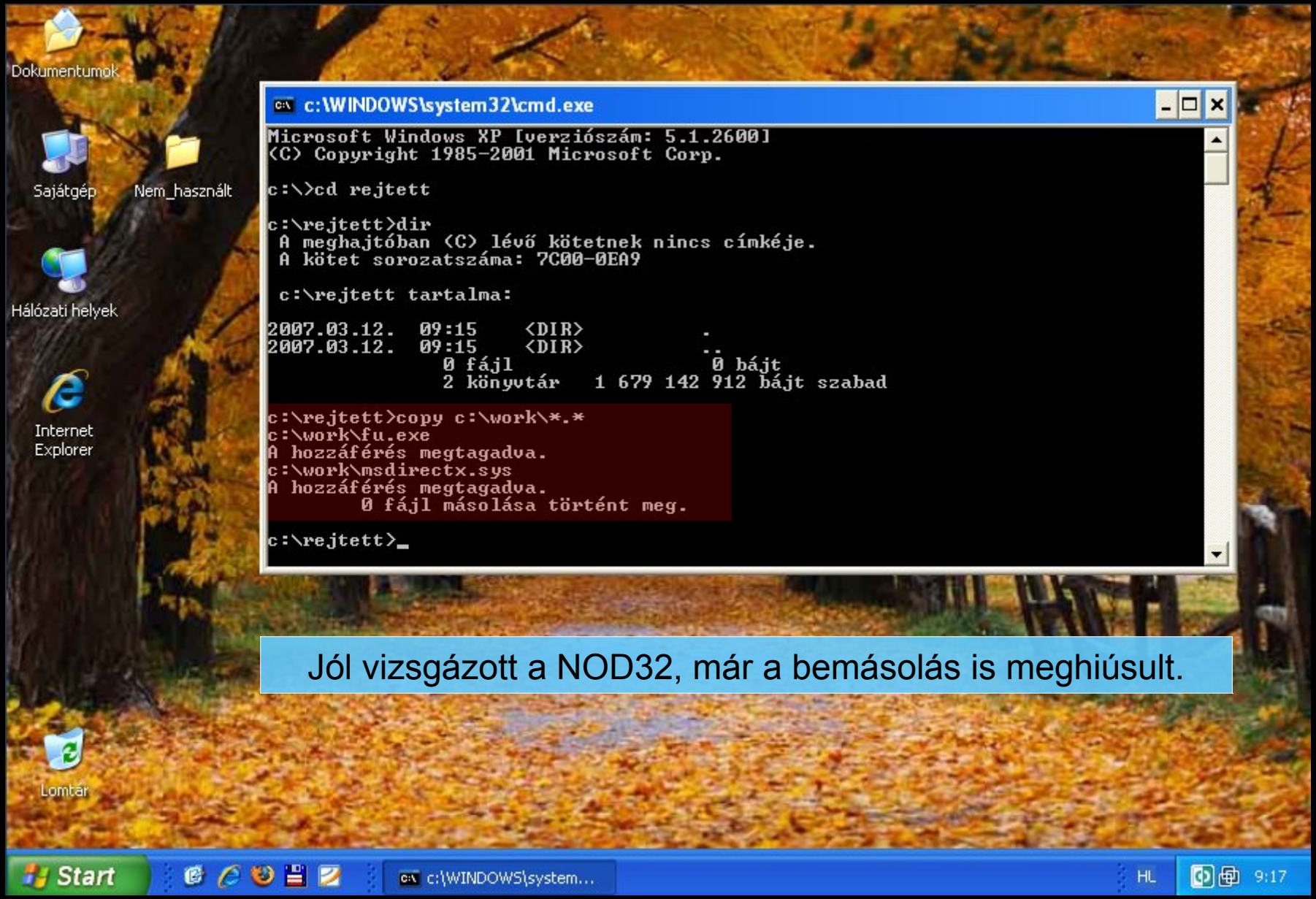


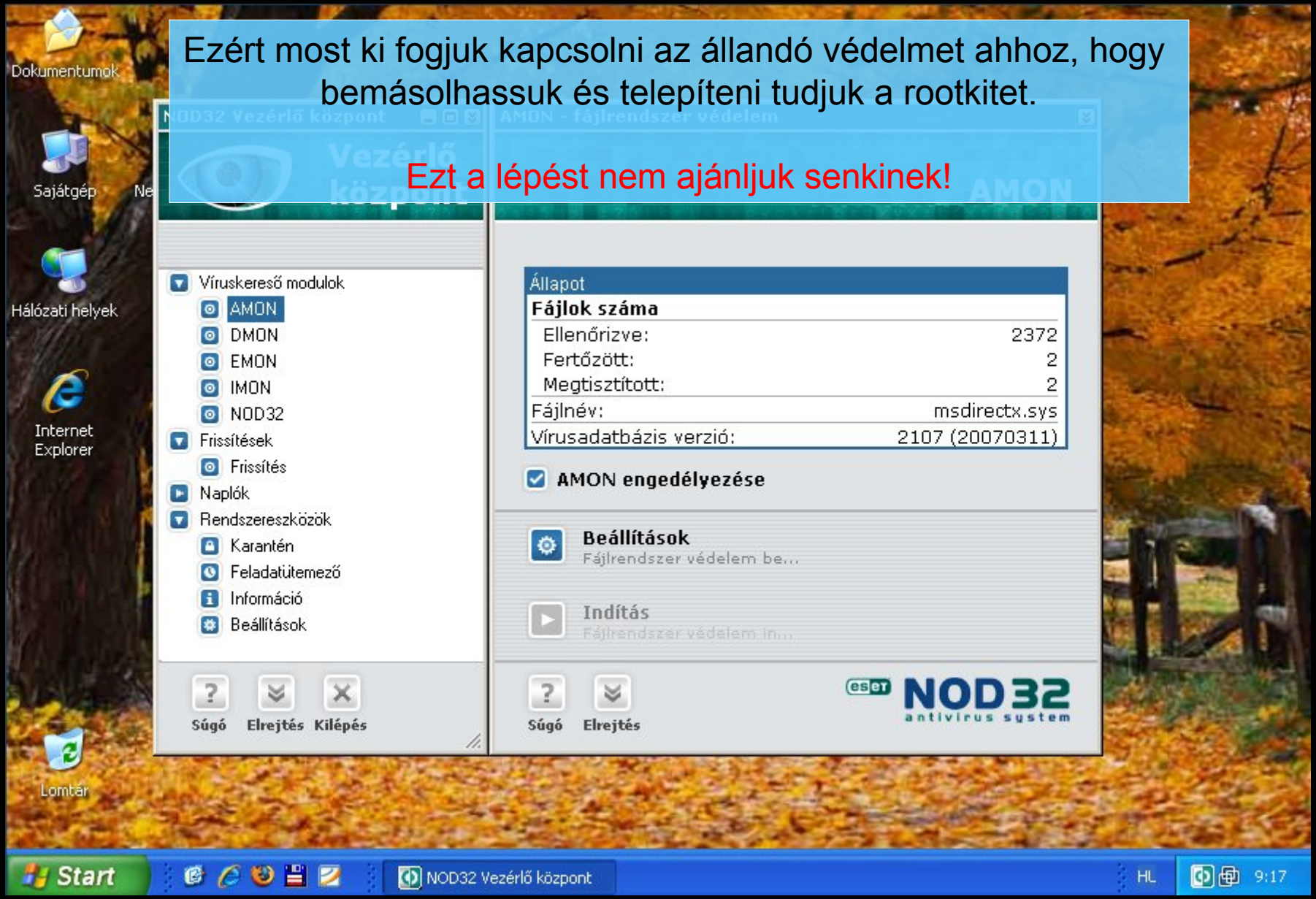
A rootkitek többségét ismerik a víruskeresők, emiatt már a rootkit másolásának vagy telepítésének puszta kísérletekor riasztást kapunk. Másoljuk be a FU rootkit állományait a "rejtett" nevű mappába!

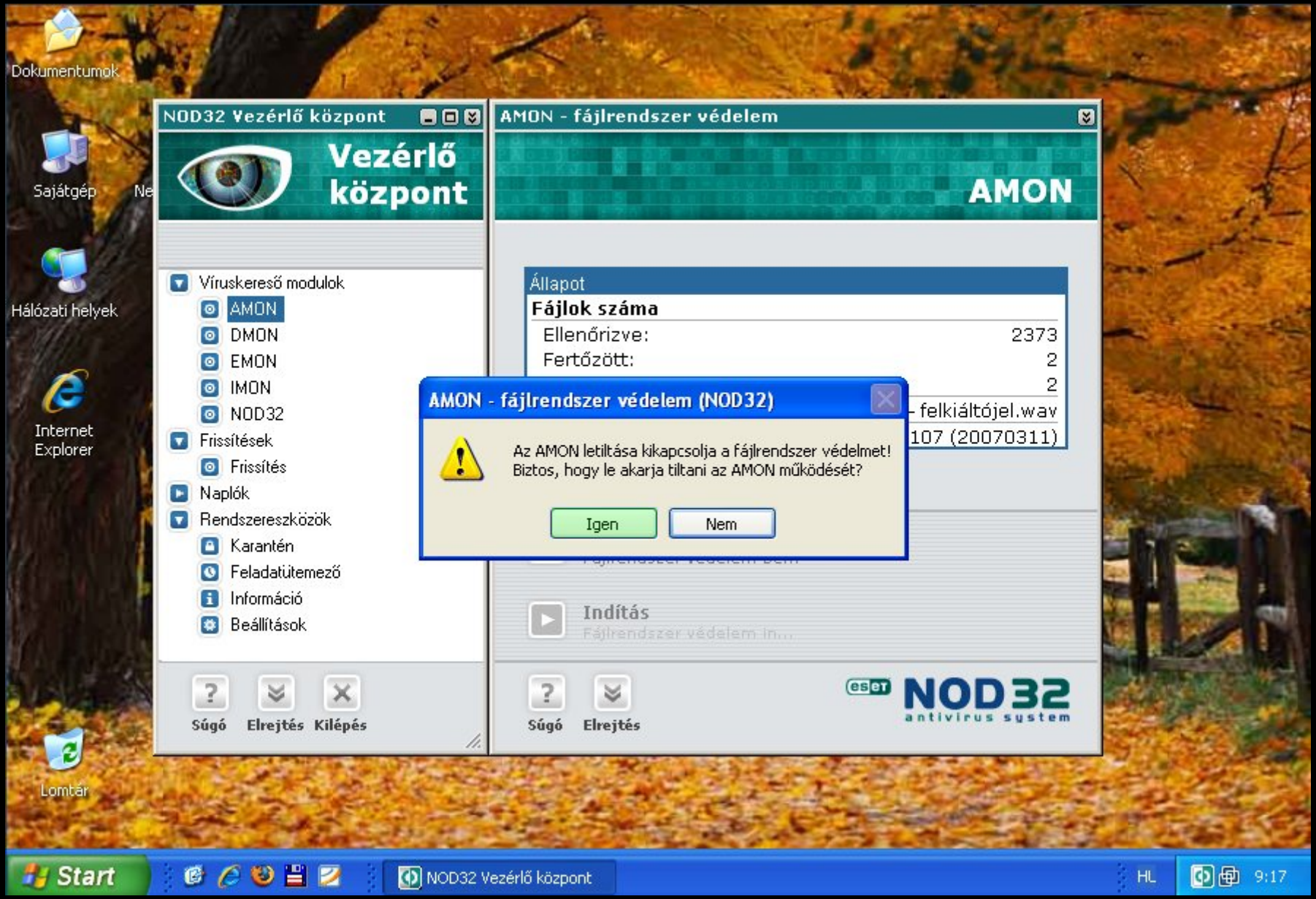


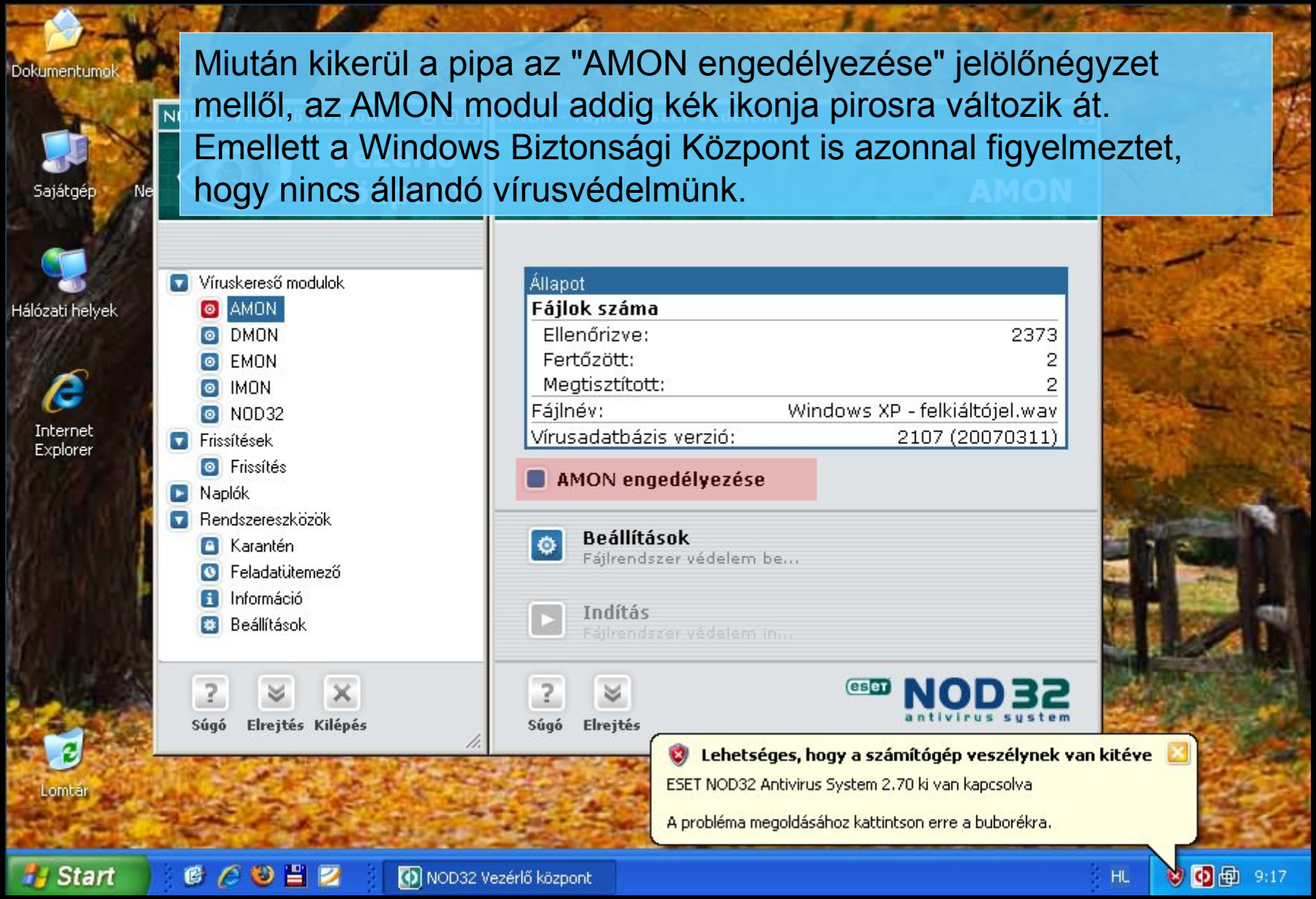
Az AMON modul haladéktalanul közbelép, riaszt és töröl, illetve karanténba helyez, ha ezt kérjük tőle.

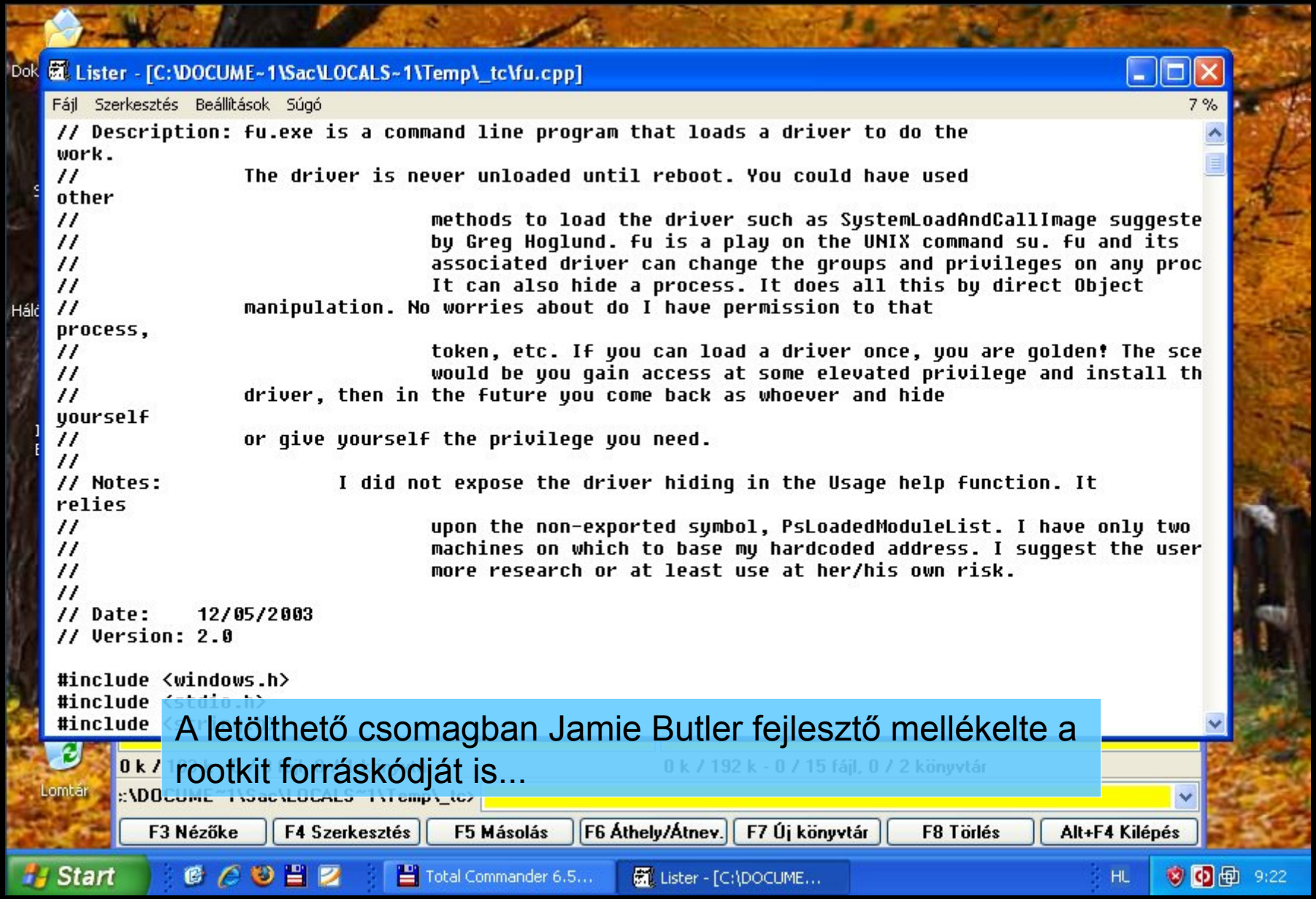

Dokumentumok
Sajátgép
Nem_ha
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system riasztás: AMON - fájlrendszer védelem
Riasztás
Részletek
Fájl:
C:\work\msdirectx.sys
Vírus:
Win32/Rootkit.H trójai
Megjegyzés:
A fájl törölhető. Csak akkor törölje, ha készített biztonsági másolatot az adatairól. A riasztást kiváltó alkalmazás (művelet: fájl-hozzáférés): c:\WINDOWS\system32\cmd.exe.
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
c:\WINDOWS\system...
NOD32 antivirus syst...
HL
9:17

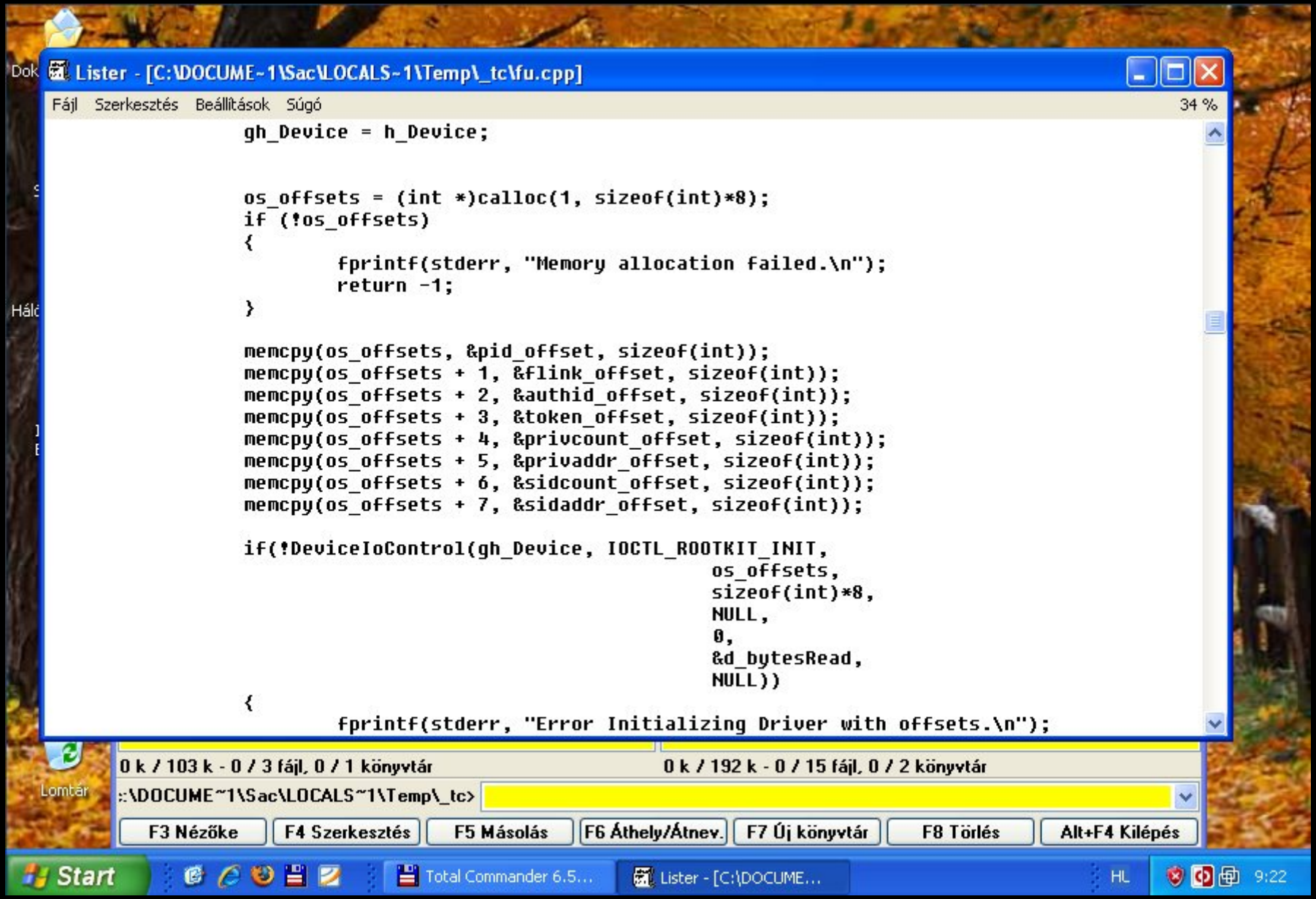

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [verziószám: 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
c:\>cd rejtett
c:\rejtett>dir
A meghajtóban (C) lévő kötetnek nincs címkéje.
A kötet sorozatszáma: 7C00-0EA9
c:\rejtett tartalma:
2007.03.12. 09:15 <DIR> .
2007.03.12. 09:15 <DIR> ..
0 fájl 0 bájt
2 könyvtár 1 679 142 912 bájt szabad
c:\rejtett>copy c:\work*.*
c:\work\fu.exe
A hozzáférés megtagadva.
c:\work\msdirectx.sys
A hozzáférés megtagadva.
0 fájl másolása történt meg.
c:\rejtett>_
Jól vizsgázott a NOD32, már a bemásolás is meghiúsult.
Start
c:\WINDOWS\system...
HL
9:17

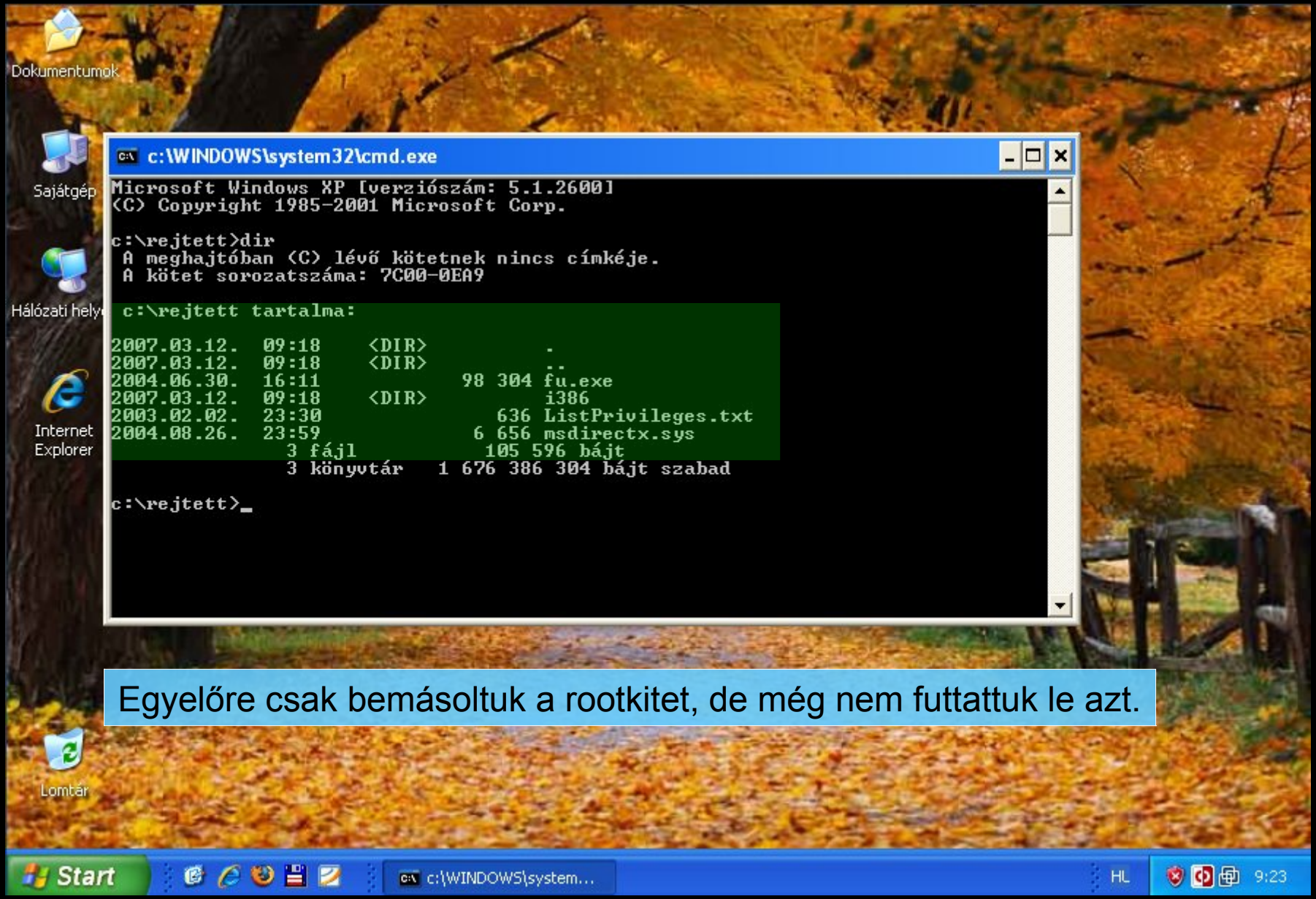

Ezért most ki fogjuk kapcsolni az állandó védelmet ahhoz, hogy bemásolhassuk és telepíteni tudjuk a rootkitet.
Ezt a lépést nem ajánljuk senkinek!
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
AMON - fájlrendszer védelem
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Karantén
Feladatütemező
Információ
Beállítások
Súgó
Elrejtés
Kilépés
Állapot
Fájlok száma
Ellenőrizve: 2372
Fertőzött: 2
Megtisztított: 2
Fájlnév: msdirectx.sys
Vírusadatbázis verzió: 2107 (20070311)
AMON engedélyezése
Beállítások
Fájlrendszer védelem be...
Indítás
Fájlrendszer védelem in...
Súgó
Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
HL
9:17

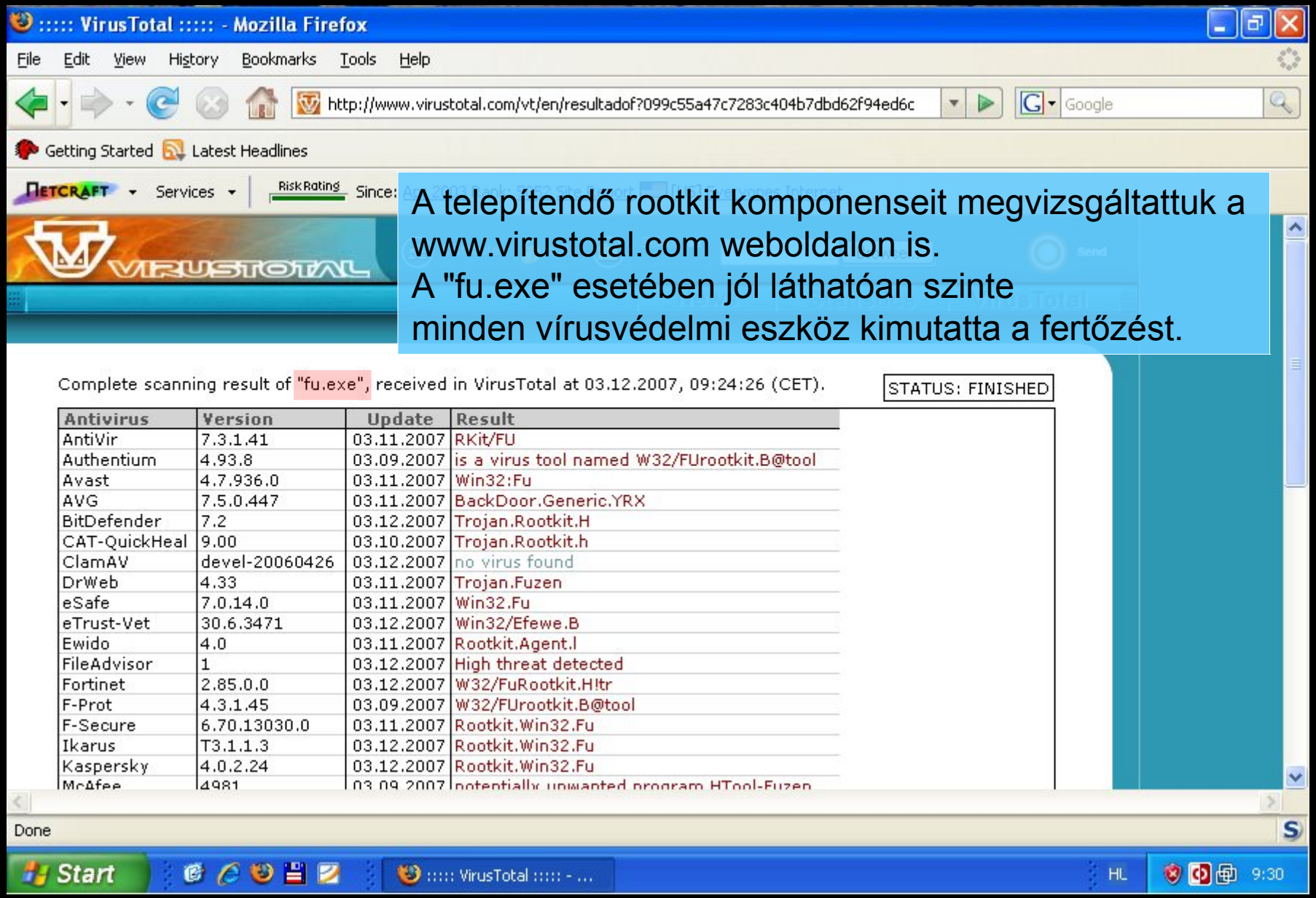

Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Karantén
Feladatütemező
Információ
Beállítások
Súgó
Elrejtés
Kilépés
AMON - fájlrendszer védelem
AMON
Állapot
Fájlok száma
Ellenőrizve: 2373
Fertőzött: 2
2
- felkiáltójel.wav
107 (20070311)
Indítás
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
9:17

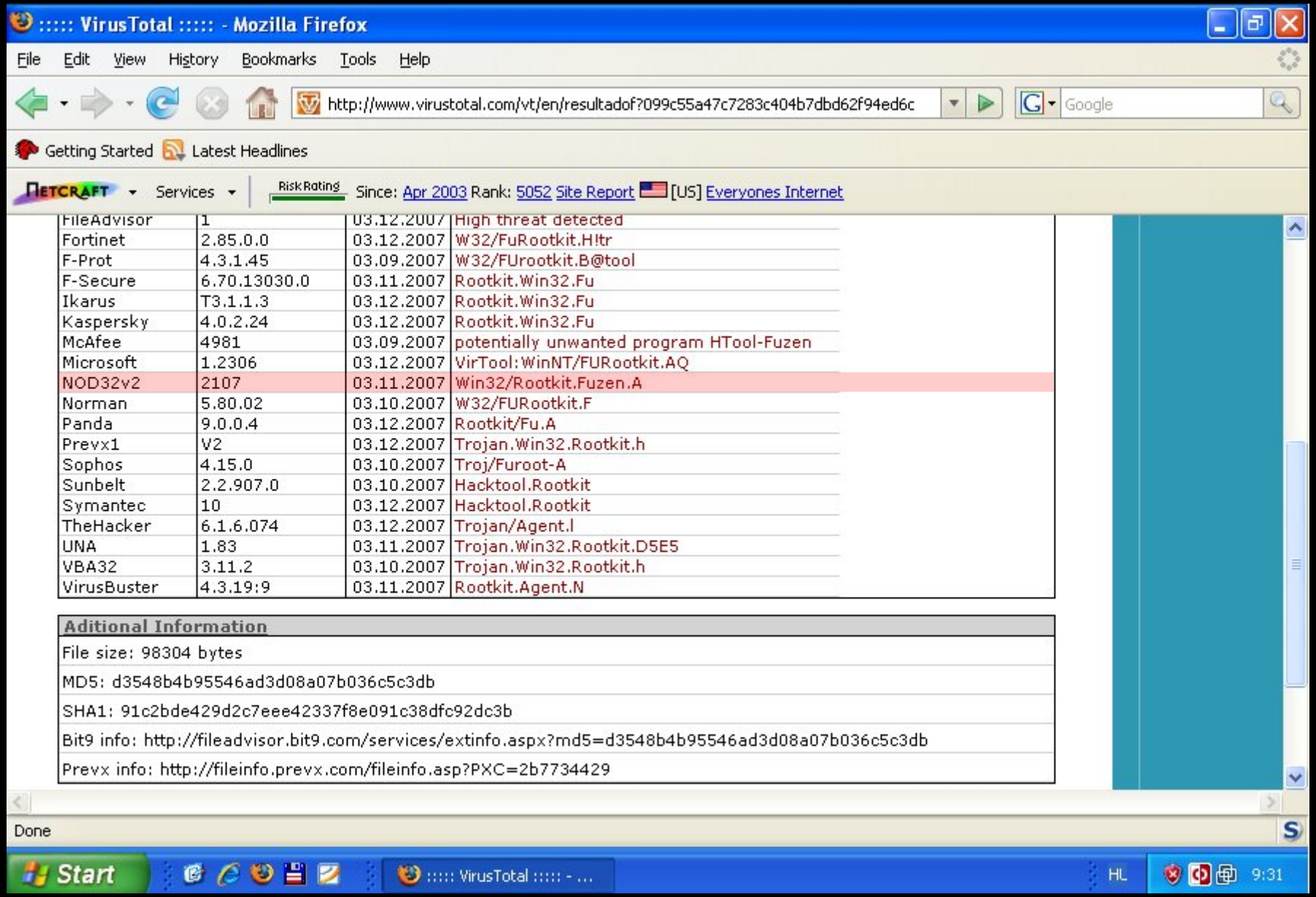

Miután kikerül a pipa az "AMON engedélyezése" jelölőnégyzet mellől, az AMON modul addig kék ikonja pirosra változik át. Emellett a Windows Biztonsági Központ is azonnal figyelmeztet, hogy nincs állandó vírusvédelmünk.
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Karantén
Feladatütemező
Információ
Beállítások
Súgó
Elrejtés
Kilépés
Állapot
Fájlok száma
Ellenőrizve: 2373
Fertőzött: 2
Megtisztított: 2
Fájlnév: Windows XP - felkiáltójel.wav
Vírusadatbázis verzió: 2107 (20070311)
AMON engedélyezése
Beállítások
Fájlrendszer védelem be...
Indítás
Fájlrendszer védelem in...
Súgó
Elrejtés
eset NOD32 antivirus system
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
9:17

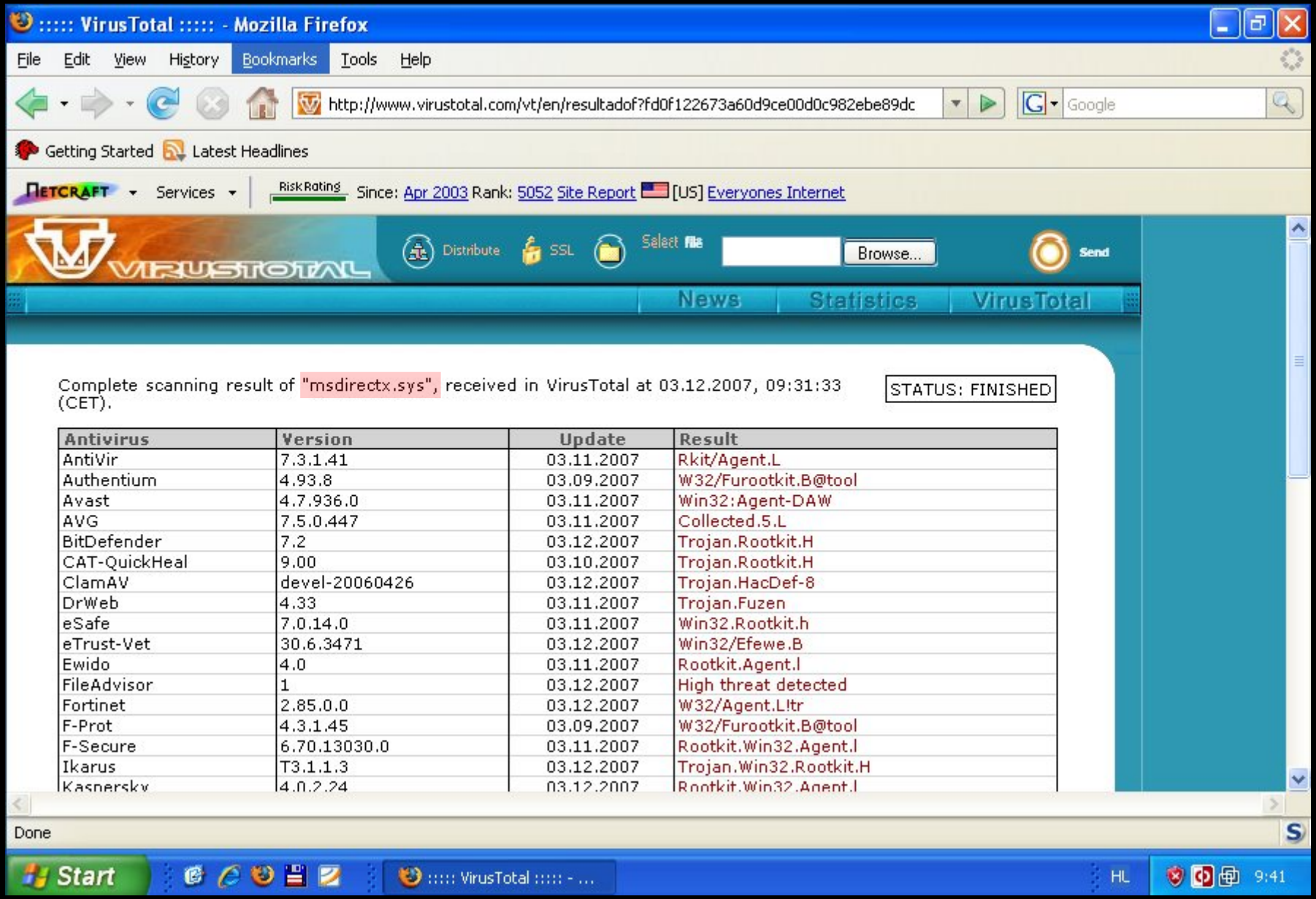

Lister - [C:\DOCUME~1\Sac\LOCALS~1\Temp_tc\fu.cpp]
Fájl Szerkesztés Beállítások Súgó
7 %
// Description: fu.exe is a command line program that loads a driver to do the
work.
// The driver is never unloaded until reboot. You could have used
other
// methods to load the driver such as SystemLoadAndCallImage suggeste
// by Greg Hoglund. fu is a play on the UNIX command su. fu and its
// associated driver can change the groups and privileges on any proc
// It can also hide a process. It does all this by direct Object
// manipulation. No worries about do I have permission to that
process,
// token, etc. If you can load a driver once, you are golden! The sce
// would be you gain access at some elevated privilege and install th
// driver, then in the future you come back as whoever and hide
yourself
// or give yourself the privilege you need.
//
// Notes: I did not expose the driver hiding in the Usage help function. It
relies
// upon the non-exported symbol, PsLoadedModuleList. I have only two
// machines on which to base my hardcoded address. I suggest the user
// more research or at least use at her/his own risk.
//
// Date: 12/05/2003
// Version: 2.0
#include <windows.h>
#include <stdio.h>
#include
A letölthető csomagban Jamie Butler fejlesztő mellékelte a rootkit forráskódját is...
0 k / 192 k - 0 / 15 fájl, 0 / 2 könyvtár
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...
HL
9:22
Lomtár

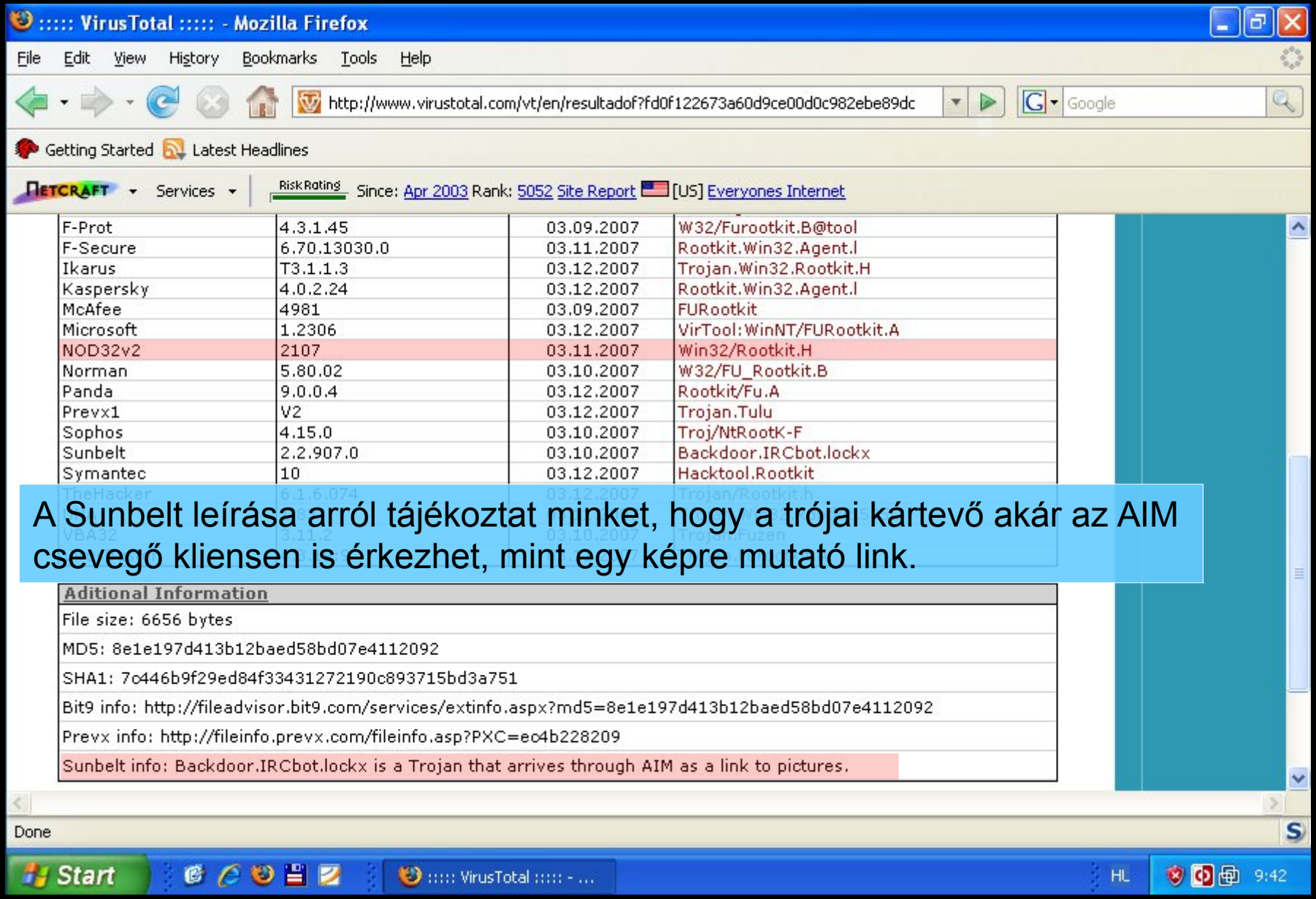

Lister - [C:\DOCUME~1\Sac\LOCALS~1\Temp_tc\fu.cpp]
Fájl Szerkesztés Beállítások Súgó 34 %
gh_Device = h_Device;
os_offsets = (int *)calloc(1, sizeof(int)*8);
if (!os_offsets)
{
fprintf(stderr, "Memory allocation failed.\n");
return -1;
}
memcpy(os_offsets, &pid_offset, sizeof(int));
memcpy(os_offsets + 1, &flink_offset, sizeof(int));
memcpy(os_offsets + 2, &authid_offset, sizeof(int));
memcpy(os_offsets + 3, &token_offset, sizeof(int));
memcpy(os_offsets + 4, &privcount_offset, sizeof(int));
memcpy(os_offsets + 5, &privaddr_offset, sizeof(int));
memcpy(os_offsets + 6, &sidcount_offset, sizeof(int));
memcpy(os_offsets + 7, &sidaddr_offset, sizeof(int));
if(!DeviceIoControl(gh_Device, IOCTL_ROOTKIT_INIT,
os_offsets,
sizeof(int)*8,
NULL,
0,
&d_bytesRead,
NULL))
{
fprintf(stderr, "Error Initializing Driver with offsets.\n");
0 k / 103 k - 0 / 3 fájl, 0 / 1 könyvtár
0 k / 192 k - 0 / 15 fájl, 0 / 2 könyvtár
:\DOCUME~1\Sac\LOCALS~1\Temp_tc>
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...
HL
9:22
Lomtár


Dokumentumok
Sajátgép
Hálózati hely
Internet Explorer
Lomtár
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [verziószám: 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
c:\rejtett>dir
A meghajtóban (C) lévő kötetnek nincs címkéje.
A kötet sorozatszáma: 7C00-0EA9
c:\rejtett tartalma:
2007.03.12. 09:18 <DIR> .
2007.03.12. 09:18 <DIR> ..
2004.06.30. 16:11 98 304 fu.exe
2007.03.12. 09:18 <DIR> i386
2003.02.02. 23:30 636 ListPrivileges.txt
2004.08.26. 23:59 6 656 msdirectx.sys
3 fájl 105 596 bájt
3 könyvtár 1 676 386 304 bájt szabad
c:\rejtett>
Egyelőre csak bemásoltuk a rootkitet, de még nem futtattuk le azt.
Start
c:\WINDOWS\system...
HL
9:23

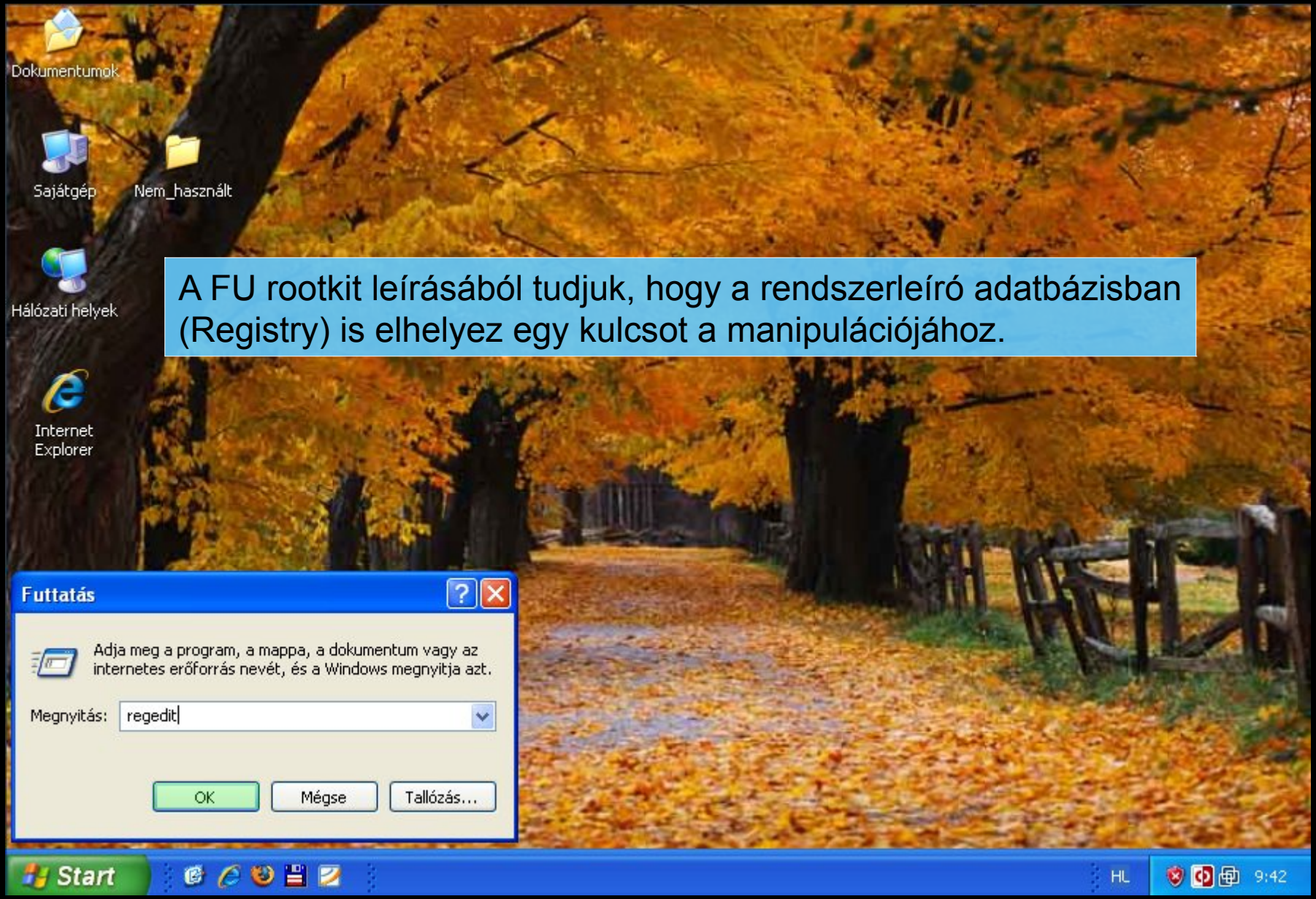

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?099c55a47c7283c404b7dbd62f94ed6c
Google
Getting Started
Latest Headlines
NETCRAFT
Services
Risk Rating
Since:
VIRUSTOTAL
A telepítendő rootkit komponenseit megvizsgáltattuk a www.virustotal.com weboldalon is.
A "fu.exe" esetében jól láthatóan szinte minden vírusvédelmi eszköz kimutatta a fertőzést.
Complete scanning result of "fu.exe", received in VirusTotal at 03.12.2007, 09:24:26 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.41 | 03.11.2007 | RKit/FU
Authentium | 4.93.8 | 03.09.2007 | is a virus tool named W32/FUrootkit.B@tool
Avast | 4.7.936.0 | 03.11.2007 | Win32:Fu
AVG | 7.5.0.447 | 03.11.2007 | BackDoor.Generic.YRX
BitDefender | 7.2 | 03.12.2007 | Trojan.Rootkit.H
CAT-QuickHeal | 9.00 | 03.10.2007 | Trojan.Rootkit.h
ClamAV | devel-20060426 | 03.12.2007 | no virus found
DrWeb | 4.33 | 03.11.2007 | Trojan.Fuzen
eSafe | 7.0.14.0 | 03.11.2007 | Win32.Fu
eTrust-Vet | 30.6.3471 | 03.12.2007 | Win32/Efewe.B
Ewido | 4.0 | 03.11.2007 | Rootkit.Agent.l
FileAdvisor | 1 | 03.12.2007 | High threat detected
Fortinet | 2.85.0.0 | 03.12.2007 | W32/FuRootkit.H!tr
F-Prot | 4.3.1.45 | 03.09.2007 | W32/FUrootkit.B@tool
F-Secure | 6.70.13030.0 | 03.11.2007 | Rootkit.Win32.Fu
Ikarus | T3.1.1.3 | 03.12.2007 | Rootkit.Win32.Fu
Kaspersky | 4.0.2.24 | 03.12.2007 | Rootkit.Win32.Fu
McAfee | 4981 | 03.09.2007 | potentially unwanted program HTool-Fuzen
Done
Start
:::: VirusTotal ::::: - ...
HL
9:30

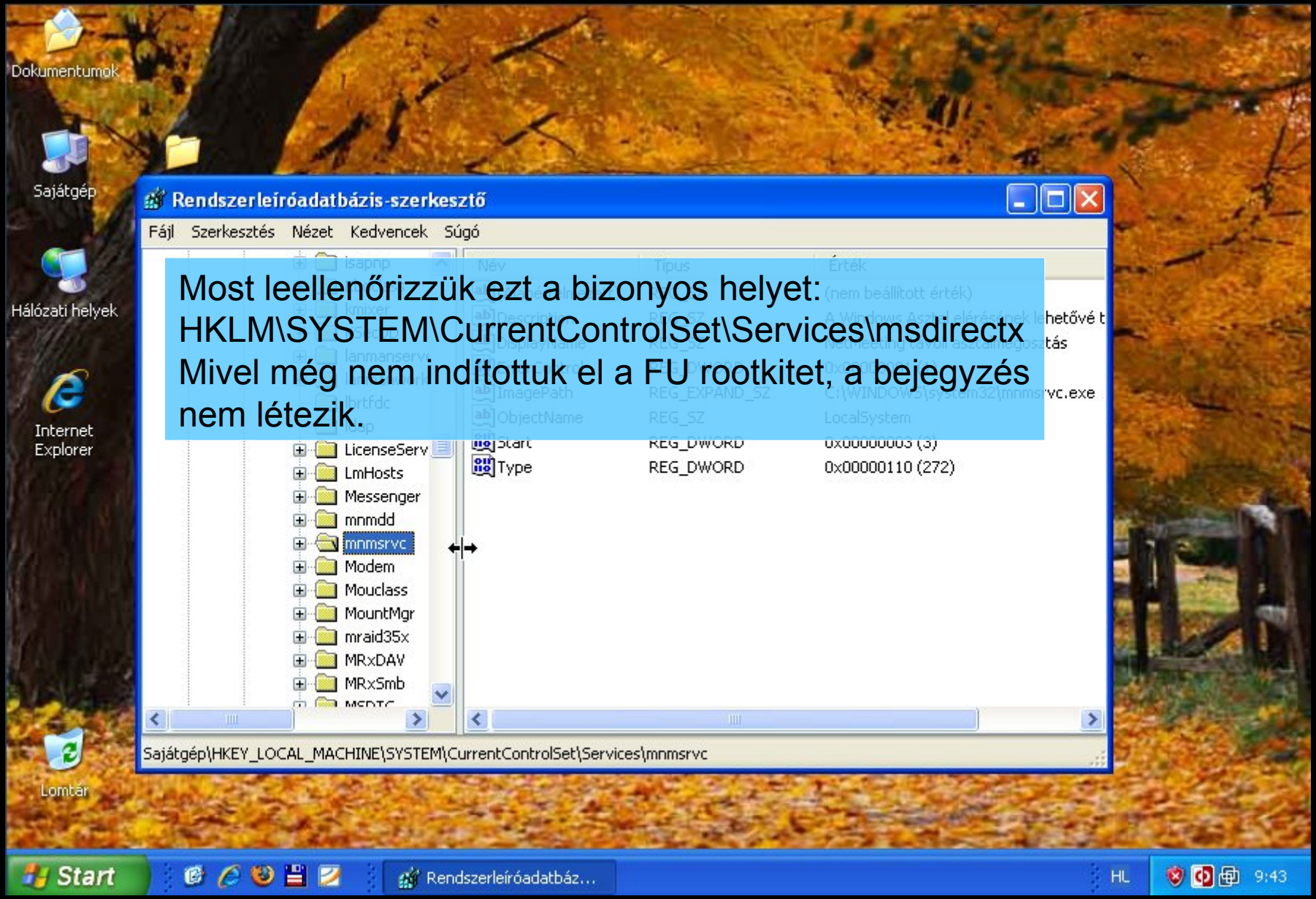

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?099c55a47c7283c404b7dbd62f94ed6c
Google
Getting Started
Latest Headlines
NETCRAFT
Services
Risk Rating
Since: Apr 2003 Rank: 5052 Site Report [US] Everyones Internet
FileAdvisor 1 03.12.2007 High threat detected
Fortinet 2.85.0.0 03.12.2007 W32/FuRootkit.H!tr
F-Prot 4.3.1.45 03.09.2007 W32/FUrootkit.B@tool
F-Secure 6.70.13030.0 03.11.2007 Rootkit.Win32.Fu
Ikarus T3.1.1.3 03.12.2007 Rootkit.Win32.Fu
Kaspersky 4.0.2.24 03.12.2007 Rootkit.Win32.Fu
McAfee 4981 03.09.2007 potentially unwanted program HTool-Fuzen
Microsoft 1.2306 03.12.2007 VirTool:WinNT/FURootkit.AQ
NOD32v2 2107 03.11.2007 Win32/Rootkit.Fuzen.A
Norman 5.80.02 03.10.2007 W32/FURootkit.F
Panda 9.0.0.4 03.12.2007 Rootkit/Fu.A
Prevx1 V2 03.12.2007 Trojan.Win32.Rootkit.h
Sophos 4.15.0 03.10.2007 Troj/Furoot-A
Sunbelt 2.2.907.0 03.10.2007 Hacktool.Rootkit
Symantec 10 03.12.2007 Hacktool.Rootkit
TheHacker 6.1.6.074 03.12.2007 Trojan/Agent.l
UNA 1.83 03.11.2007 Trojan.Win32.Rootkit.D5E5
VBA32 3.11.2 03.10.2007 Trojan.Win32.Rootkit.h
VirusBuster 4.3.19:9 03.11.2007 Rootkit.Agent.N
Aditional Information
File size: 98304 bytes
MD5: d3548b4b95546ad3d08a07b036c5c3db
SHA1: 91c2bde429d2c7eee42337f8e091c38dfc92dc3b
Bit9 info: http://fileadvisor.bit9.com/services/extinfo.aspx?md5=d3548b4b95546ad3d08a07b036c5c3db
Prevx info: http://fileinfo.prevx.com/fileinfo.asp?PXC=2b7734429
Done
Start
::::: VirusTotal ::::: - ...
HL
9:31

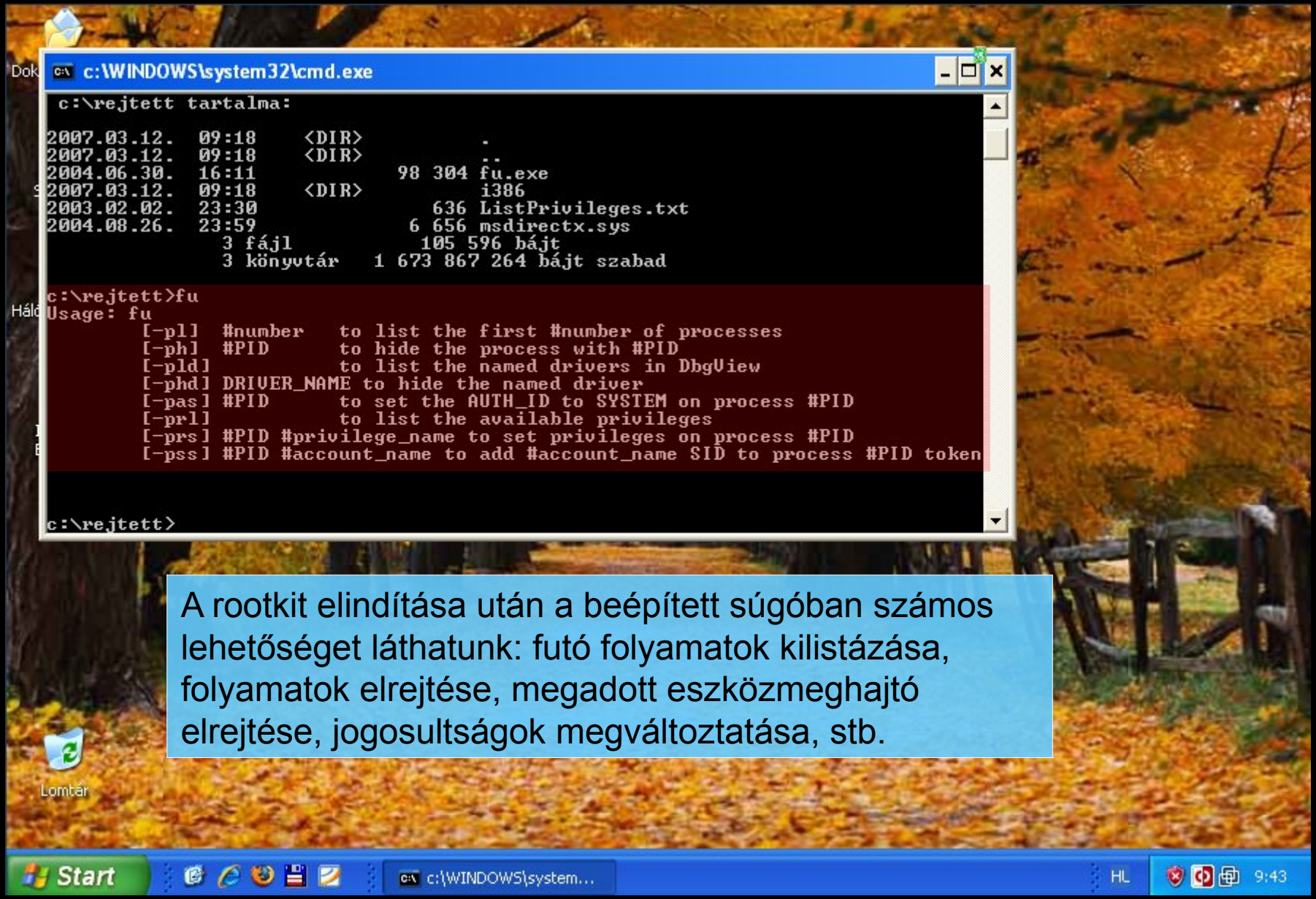

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadof?fd0f122673a60d9ce00d0c982ebe89dc
Google
Getting Started
Latest Headlines
NETCRAFT
Services
Risk Rating
Since: Apr 2003 Rank: 5052 Site Report
[US] Everyones Internet
VIRUSTOTAL
Distribute
SSL
Select file
Browse...
Send
News
Statistics
VirusTotal
Complete scanning result of "msdirectx.sys", received in VirusTotal at 03.12.2007, 09:31:33 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.41 | 03.11.2007 | Rkit/Agent.L
Authentium | 4.93.8 | 03.09.2007 | W32/Furootkit.B@tool
Avast | 4.7.936.0 | 03.11.2007 | Win32:Agent-DAW
AVG | 7.5.0.447 | 03.11.2007 | Collected.5.L
BitDefender | 7.2 | 03.12.2007 | Trojan.Rootkit.H
CAT-QuickHeal | 9.00 | 03.10.2007 | Trojan.Rootkit.H
ClamAV | devel-20060426 | 03.12.2007 | Trojan.HacDef-8
DrWeb | 4.33 | 03.11.2007 | Trojan.Fuzen
eSafe | 7.0.14.0 | 03.11.2007 | Win32.Rootkit.h
eTrust-Vet | 30.6.3471 | 03.12.2007 | Win32/Efewe.B
Ewido | 4.0 | 03.11.2007 | Rootkit.Agent.l
FileAdvisor | 1 | 03.12.2007 | High threat detected
Fortinet | 2.85.0.0 | 03.12.2007 | W32/Agent.L!tr
F-Prot | 4.3.1.45 | 03.09.2007 | W32/Furootkit.B@tool
F-Secure | 6.70.13030.0 | 03.11.2007 | Rootkit.Win32.Agent.l
Ikarus | T3.1.1.3 | 03.12.2007 | Trojan.Win32.Rootkit.H
Kaspersky | 4.0.2.24 | 03.12.2007 | Rootkit.Win32.Agent.l
Done
Start
::::: VirusTotal ::::: - ...
HL
9:41



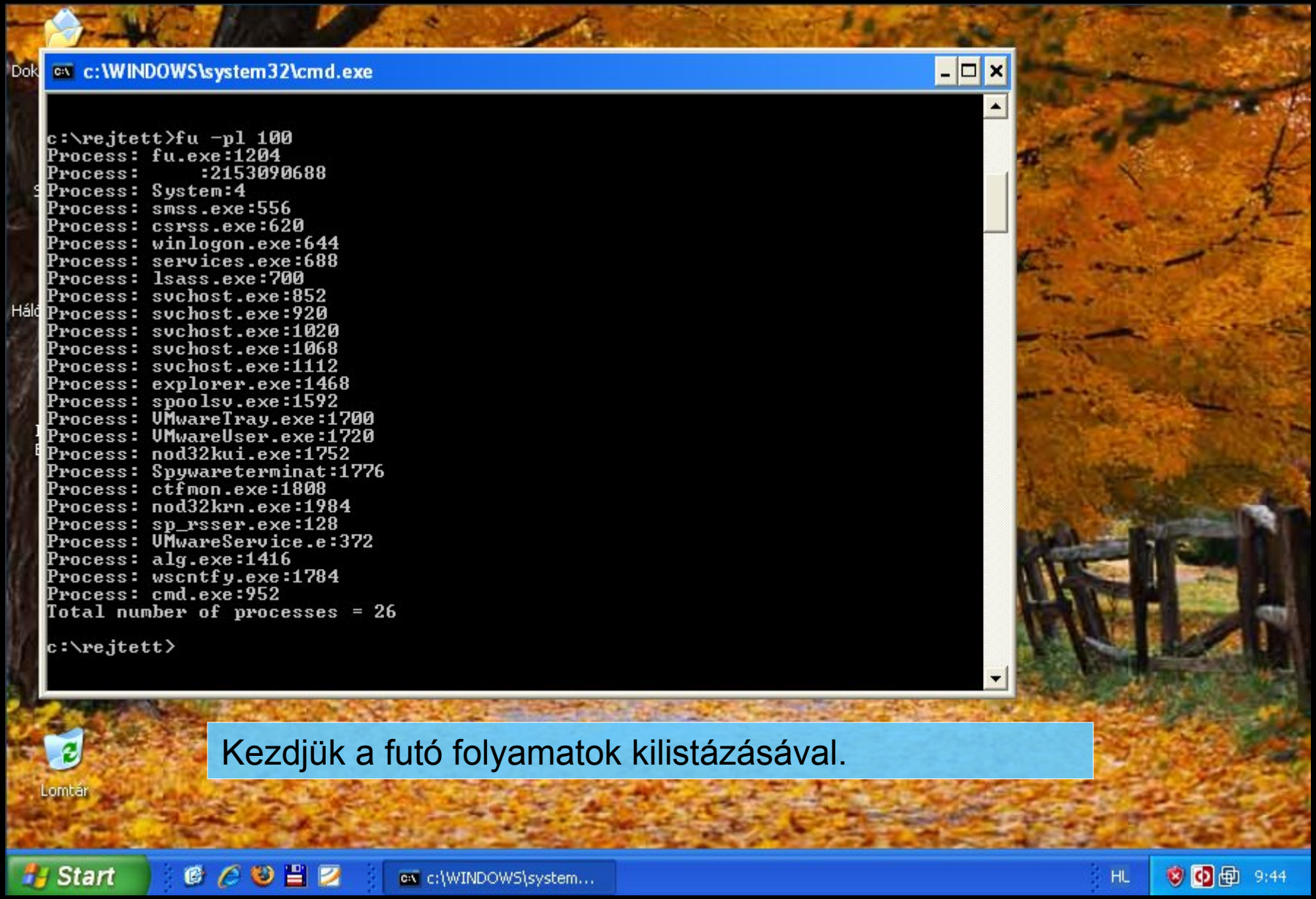
A Sunbelt leírása arról tájékoztat minket, hogy a trójai kártevő akár az AIM csevegő kliensen is érkezhet, mint egy képre mutató link.

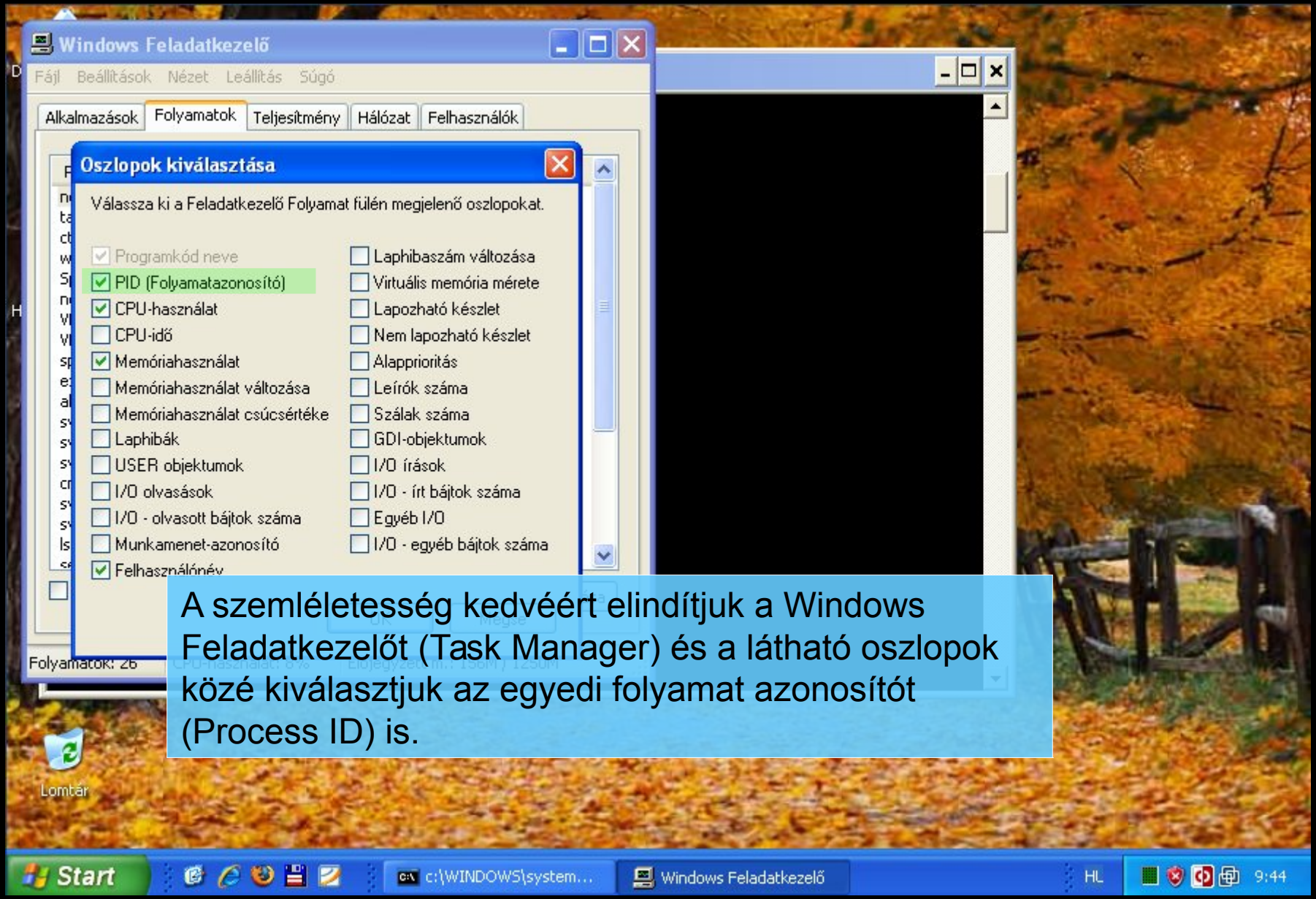

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
A FU rootkit leírásából tudjuk, hogy a rendszerleíró adatbázisban (Registry) is elhelyez egy kulcsot a manipulációjához.
Futtatás
Adja meg a program, a mappa, a dokumentum vagy az internetes erőforrás nevét, és a Windows megnyitja azt.
Megnyitás:
regedit
OK
Mégse
Tallózás...
Start
HL
9:42


Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Rendszerleíróadatbázis-szerkesztő
Fájl Szerkesztés Nézet Kedvencek Súgó
Most leellenőrizzük ezt a bizonyos helyet:
HKLM\SYSTEM\CurrentControlSet\Services\msdirectx
Mivel még nem indítottuk el a FU rootkitet, a bejegyzés nem létezik.
LicenseServ
LmHosts
Messenger
mnmdd
mnmsrvc
Modem
Mouclass
MountMgr
mraid35x
MRxDAV
MRxSmb
Type REG_DWORD 0x00000110 (272)
Sajátgép\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mnmsrvc
Start
Rendszerleíróadatbáz...
HL
9:43

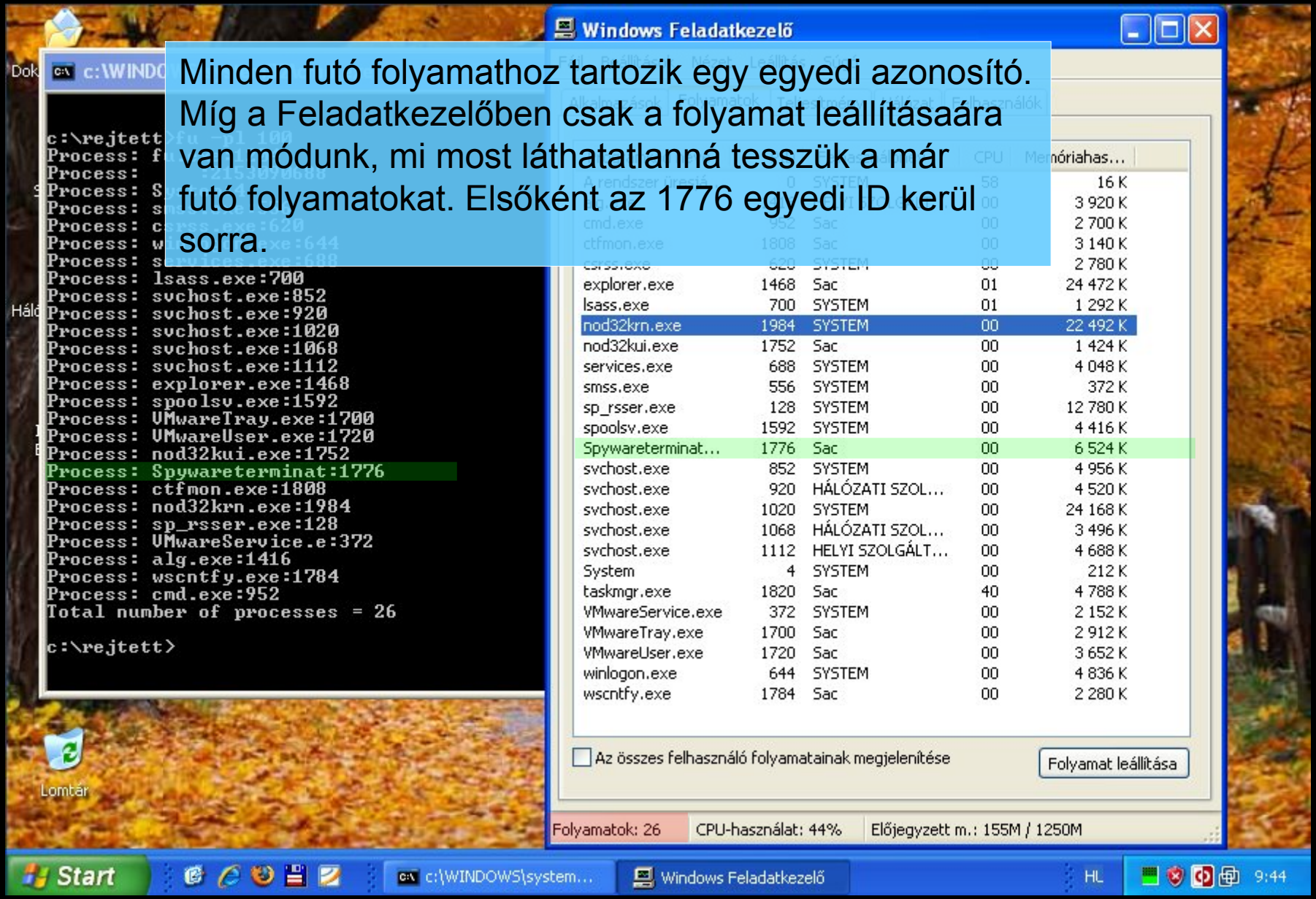


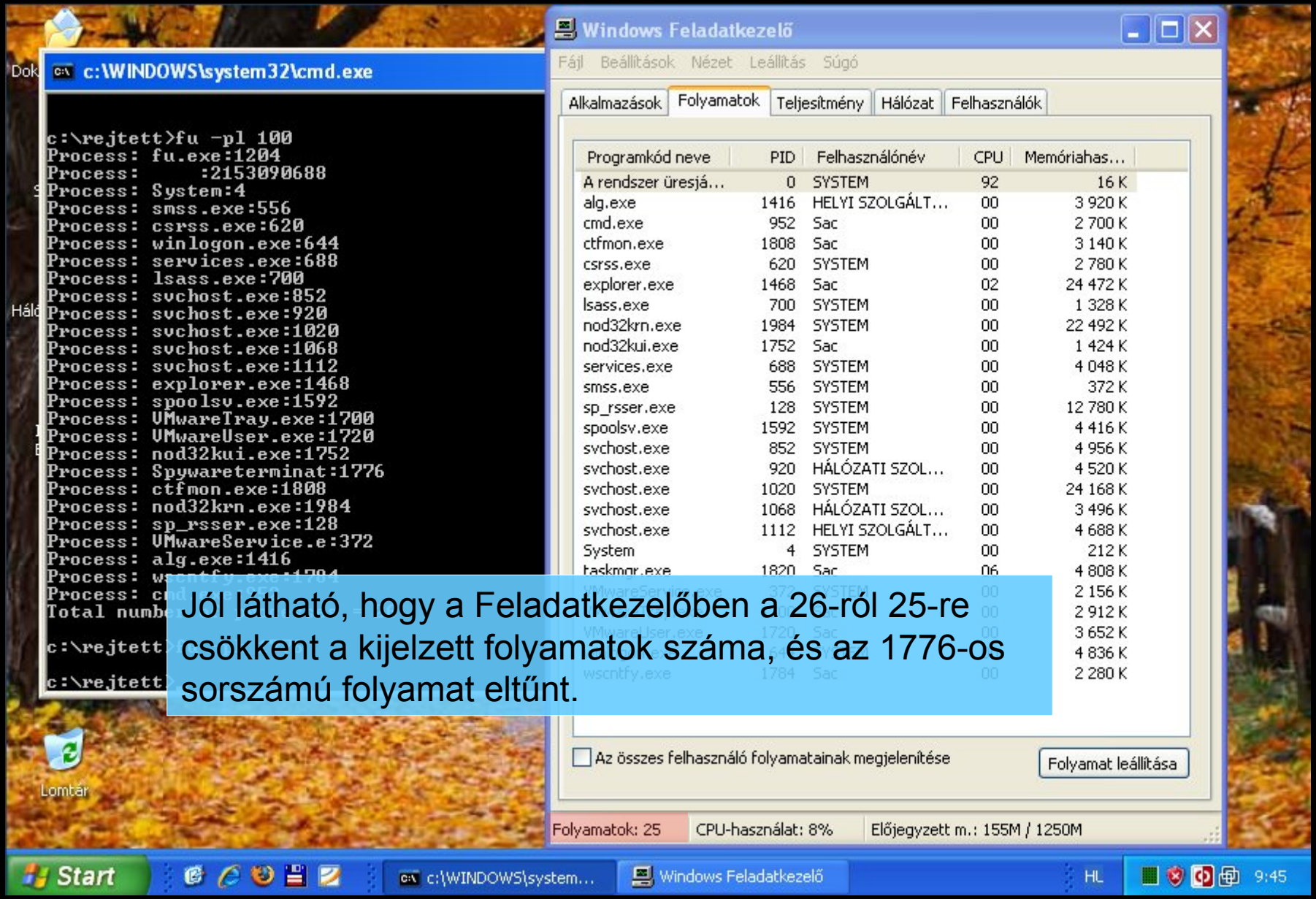
A rootkit elindítása után a beépített súgóban számos lehetőséget láthatunk: futó folyamatok kilistázása, folyamatok elrejtése, megadott eszközmeghajtó elrejtése, jogosultságok megváltoztatása, stb.

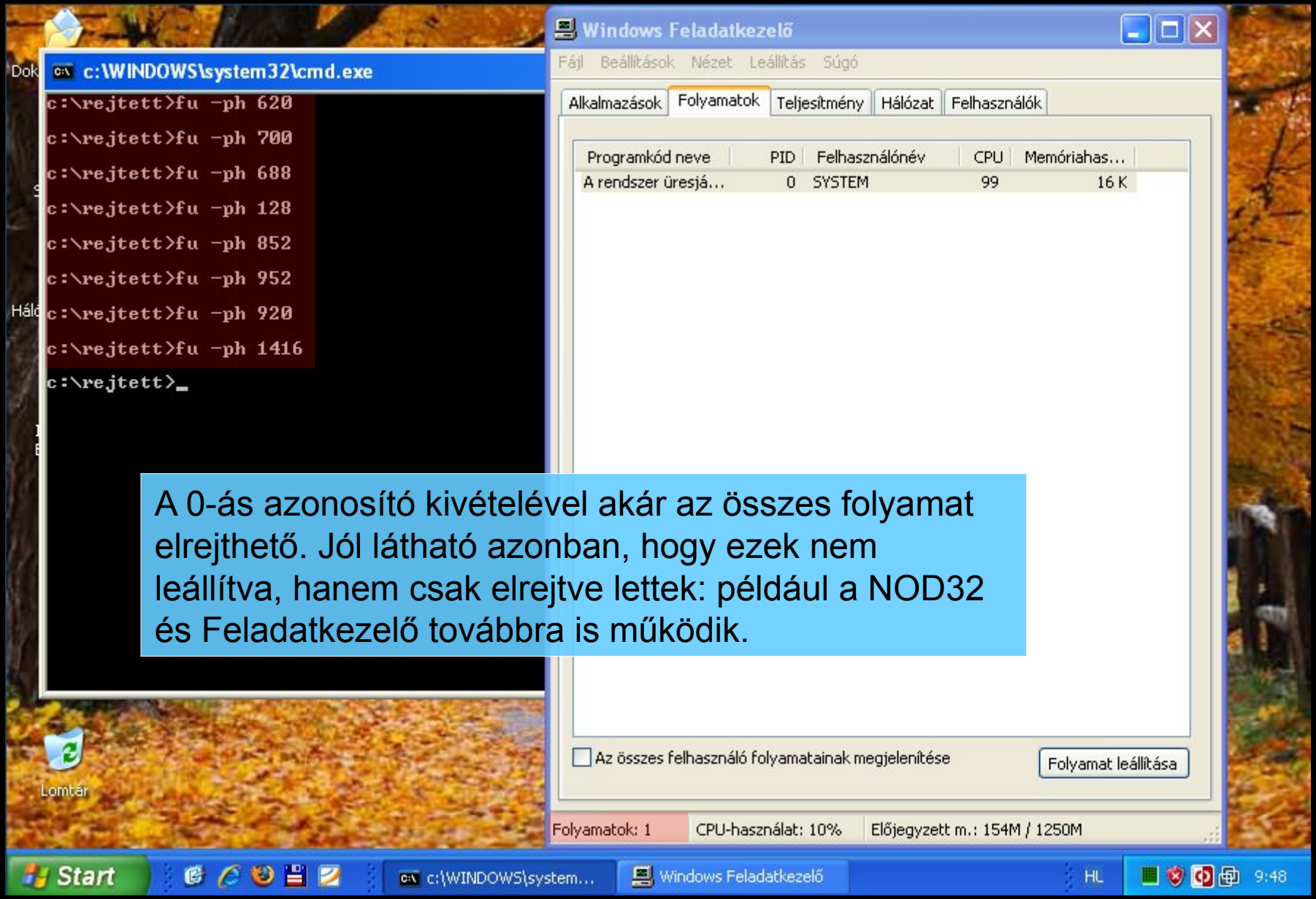

c:\WINDOWS\system32\cmd.exe
c:\rejtett>fu -pl 100
Process: fu.exe:1204
Process: :2153090688
Process: System:4
Process: smss.exe:556
Process: csrss.exe:620
Process: winlogon.exe:644
Process: services.exe:688
Process: lsass.exe:700
Process: svchost.exe:852
Process: svchost.exe:920
Process: svchost.exe:1020
Process: svchost.exe:1068
Process: svchost.exe:1112
Process: explorer.exe:1468
Process: spoolsv.exe:1592
Process: VMwareTray.exe:1700
Process: VMwareUser.exe:1720
Process: nod32kui.exe:1752
Process: Spywareterminat:1776
Process: ctfmon.exe:1808
Process: nod32krn.exe:1984
Process: sp_rsser.exe:128
Process: VMwareService.e:372
Process: alg.exe:1416
Process: wscntfy.exe:1784
Process: cmd.exe:952
Total number of processes = 26
c:\rejtett>
Kezdjük a futó folyamatok kilistázásával.
Lomtár
Start
c:\WINDOWS\system...
HL
9:44



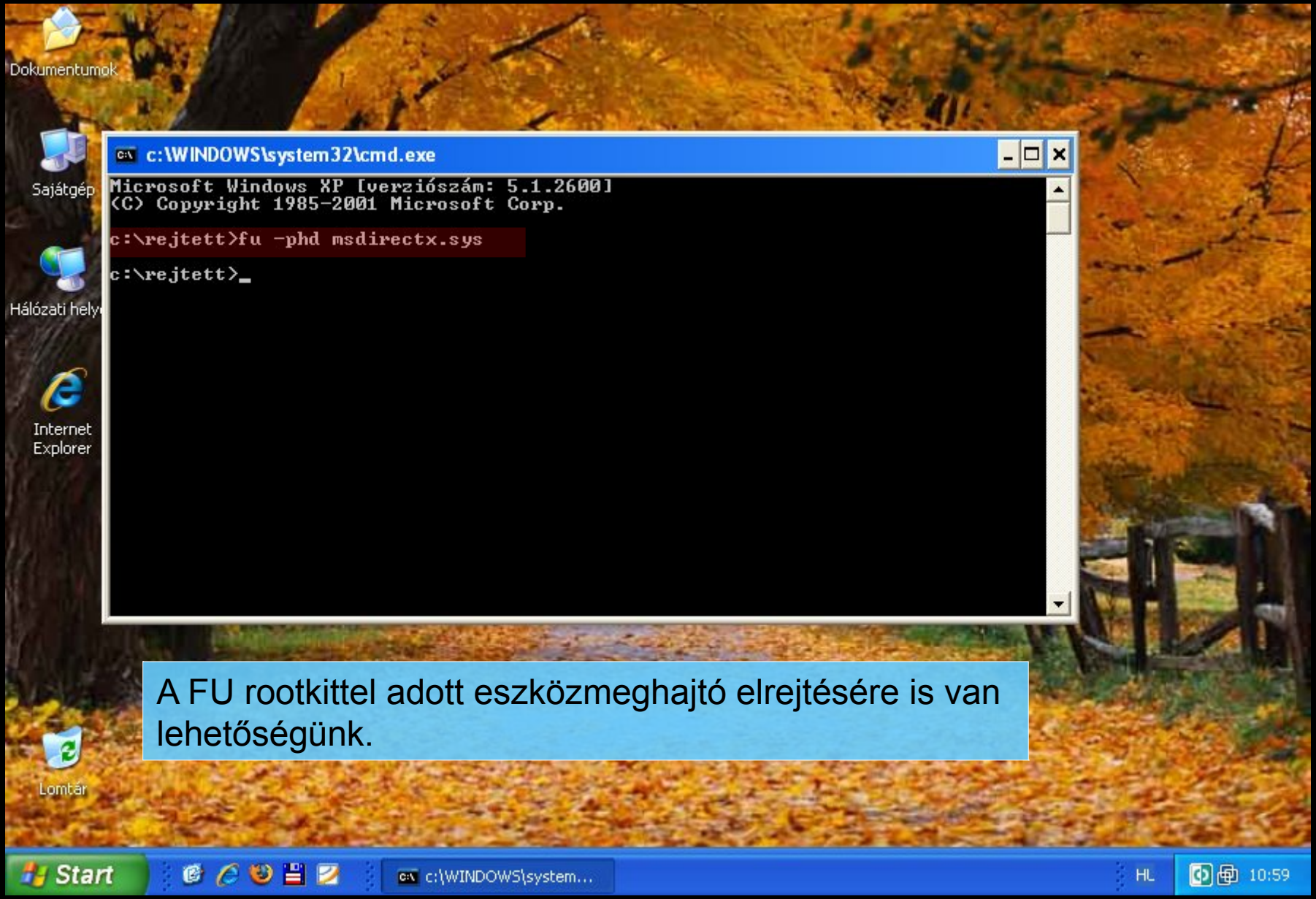
A szemléletesség kedvéért elindítjuk a Windows Feladatkezelőt (Task Manager) és a látható oszlopok közé kiválasztjuk az egyedi folyamat azonosítót (Process ID) is.

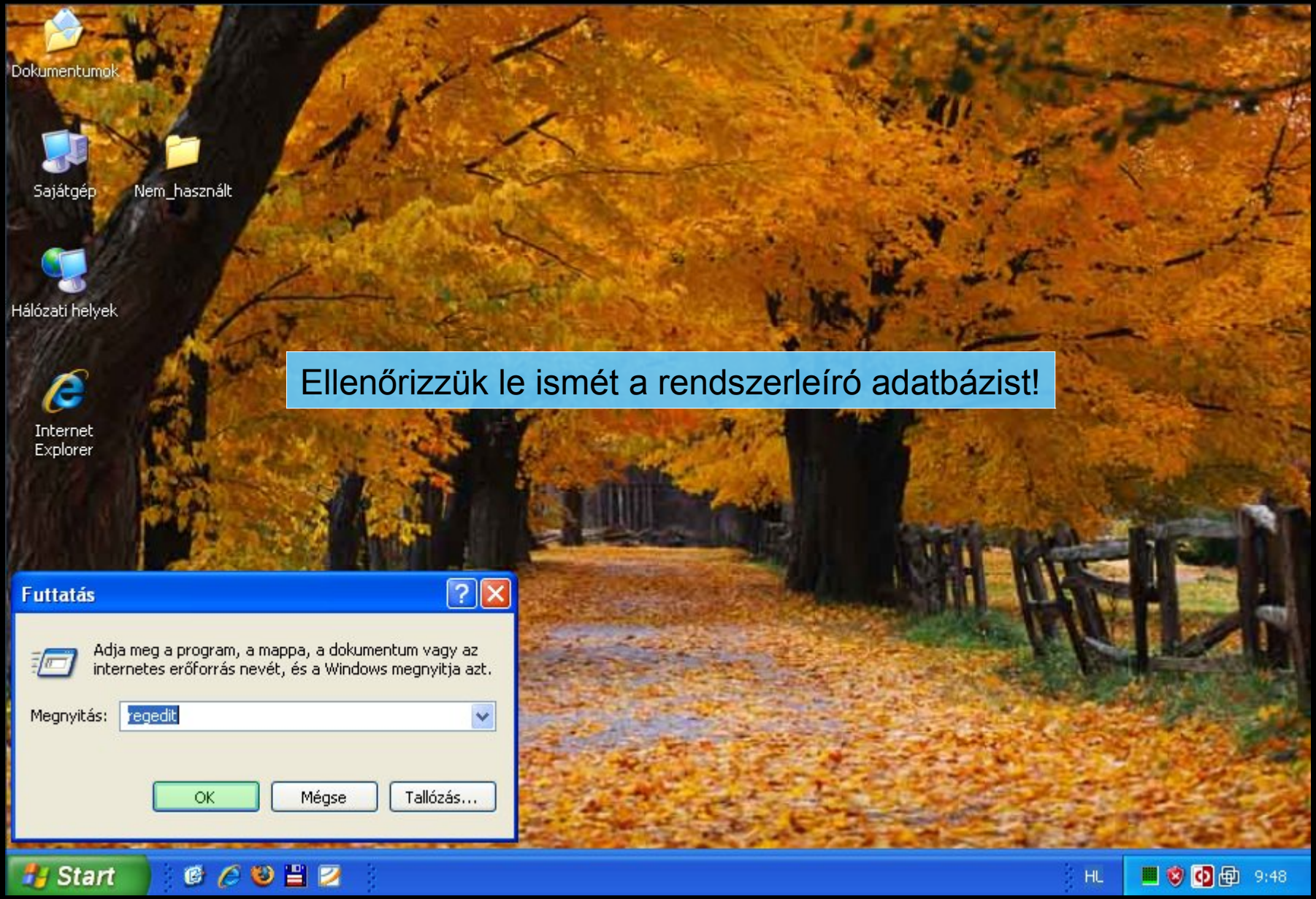

Minden futó folyamathoz tartozik egy egyedi azonosító. Míg a Feladatkezelőben csak a folyamat leállításaára van módunk, mi most láthatatlanná tesszük a már futó folyamatokat. Elsőként az 1776 egyedi ID kerül sorra.
c:\WINDO
c:\rejtett>fu -pl 100
Process: f
Process:
Process: S
Process: s
Process: c
Process: w
Process: s
Process: lsass.exe:700
Process: svchost.exe:852
Process: svchost.exe:920
Process: svchost.exe:1020
Process: svchost.exe:1068
Process: svchost.exe:1112
Process: explorer.exe:1468
Process: spoolsv.exe:1592
Process: VMwareTray.exe:1700
Process: VMwareUser.exe:1720
Process: nod32kui.exe:1752
Process: Spywareterminat:1776
Process: ctfmon.exe:1808
Process: nod32krn.exe:1984
Process: sp_rsser.exe:128
Process: VMwareService.e:372
Process: alg.exe:1416
Process: wscntfy.exe:1784
Process: cmd.exe:952
Total number of processes = 26
c:\rejtett>
Windows Feladatkezelő
Memóriahas...
explorer.exe 1468 Sac 01 24 472 K
lsass.exe 700 SYSTEM 01 1 292 K
nod32krn.exe 1984 SYSTEM 00 22 492 K
nod32kui.exe 1752 Sac 00 1 424 K
services.exe 688 SYSTEM 00 4 048 K
smss.exe 556 SYSTEM 00 372 K
sp_rsser.exe 128 SYSTEM 00 12 780 K
spoolsv.exe 1592 SYSTEM 00 4 416 K
Spywareterminat... 1776 Sac 00 6 524 K
svchost.exe 852 SYSTEM 00 4 956 K
svchost.exe 920 HÁLÓZATI SZOL... 00 4 520 K
svchost.exe 1020 SYSTEM 00 24 168 K
svchost.exe 1068 HÁLÓZATI SZOL... 00 3 496 K
svchost.exe 1112 HELYI SZOLGÁLT... 00 4 688 K
System 4 SYSTEM 00 212 K
taskmgr.exe 1820 Sac 40 4 788 K
VMwareService.exe 372 SYSTEM 00 2 152 K
VMwareTray.exe 1700 Sac 00 2 912 K
VMwareUser.exe 1720 Sac 00 3 652 K
winlogon.exe 644 SYSTEM 00 4 836 K
wscntfy.exe 1784 Sac 00 2 280 K
Az összes felhasználó folyamatainak megjelenítése
Folyamat leállítása
Folyamatok: 26
CPU-használat: 44%
Előjegyzett m.: 155M / 1250M
Lomtár
Start
c:\WINDOWS\system...
Windows Feladatkezelő
HL
9:44


c:\WINDOWS\system32\cmd.exe
c:\rejtett>fu -pl 100
Process: fu.exe:1204
Process: :2153090688
Process: System:4
Process: smss.exe:556
Process: csrss.exe:620
Process: winlogon.exe:644
Process: services.exe:688
Process: lsass.exe:700
Process: svchost.exe:852
Process: svchost.exe:920
Process: svchost.exe:1020
Process: svchost.exe:1068
Process: svchost.exe:1112
Process: explorer.exe:1468
Process: spoolsv.exe:1592
Process: VMwareTray.exe:1700
Process: VMwareUser.exe:1720
Process: nod32kui.exe:1752
Process: Spywareterminat:1776
Process: ctfmon.exe:1808
Process: nod32krn.exe:1984
Process: sp_rsser.exe:128
Process: VMwareService.e:372
Process: alg.exe:1416
Windows Feladatkezelő
Fájl Beállítások Nézet Leállítás Súgó
Alkalmazások Folyamatok Teljesítmény Hálózat Felhasználók
Programkód neve PID Felhasználónév CPU Memóriahas...
A rendszer üresjá... 0 SYSTEM 92 16 K
alg.exe 1416 HELYI SZOLGÁLT... 00 3 920 K
cmd.exe 952 Sac 00 2 700 K
ctfmon.exe 1808 Sac 00 3 140 K
csrss.exe 620 SYSTEM 00 2 780 K
explorer.exe 1468 Sac 02 24 472 K
lsass.exe 700 SYSTEM 00 1 328 K
nod32krn.exe 1984 SYSTEM 00 22 492 K
nod32kui.exe 1752 Sac 00 1 424 K
services.exe 688 SYSTEM 00 4 048 K
smss.exe 556 SYSTEM 00 372 K
sp_rsser.exe 128 SYSTEM 00 12 780 K
spoolsv.exe 1592 SYSTEM 00 4 416 K
svchost.exe 852 SYSTEM 00 4 956 K
svchost.exe 920 HÁLÓZATI SZOL... 00 4 520 K
svchost.exe 1020 SYSTEM 00 24 168 K
svchost.exe 1068 HÁLÓZATI SZOL... 00 3 496 K
svchost.exe 1112 HELYI SZOLGÁLT... 00 4 688 K
System 4 SYSTEM 00 212 K
Az összes felhasználó folyamatainak megjelenítése
Folyamat leállítása
Folyamatok: 25 CPU-használat: 8% Előjegyzett m.: 155M / 1250M
Jól látható, hogy a Feladatkezelőben a 26-ról 25-re csökkent a kijelzett folyamatok száma, és az 1776-os sorszámú folyamat eltűnt.
Lomtár
Start
c:\WINDOWS\system...
Windows Feladatkezelő
HL
9:45

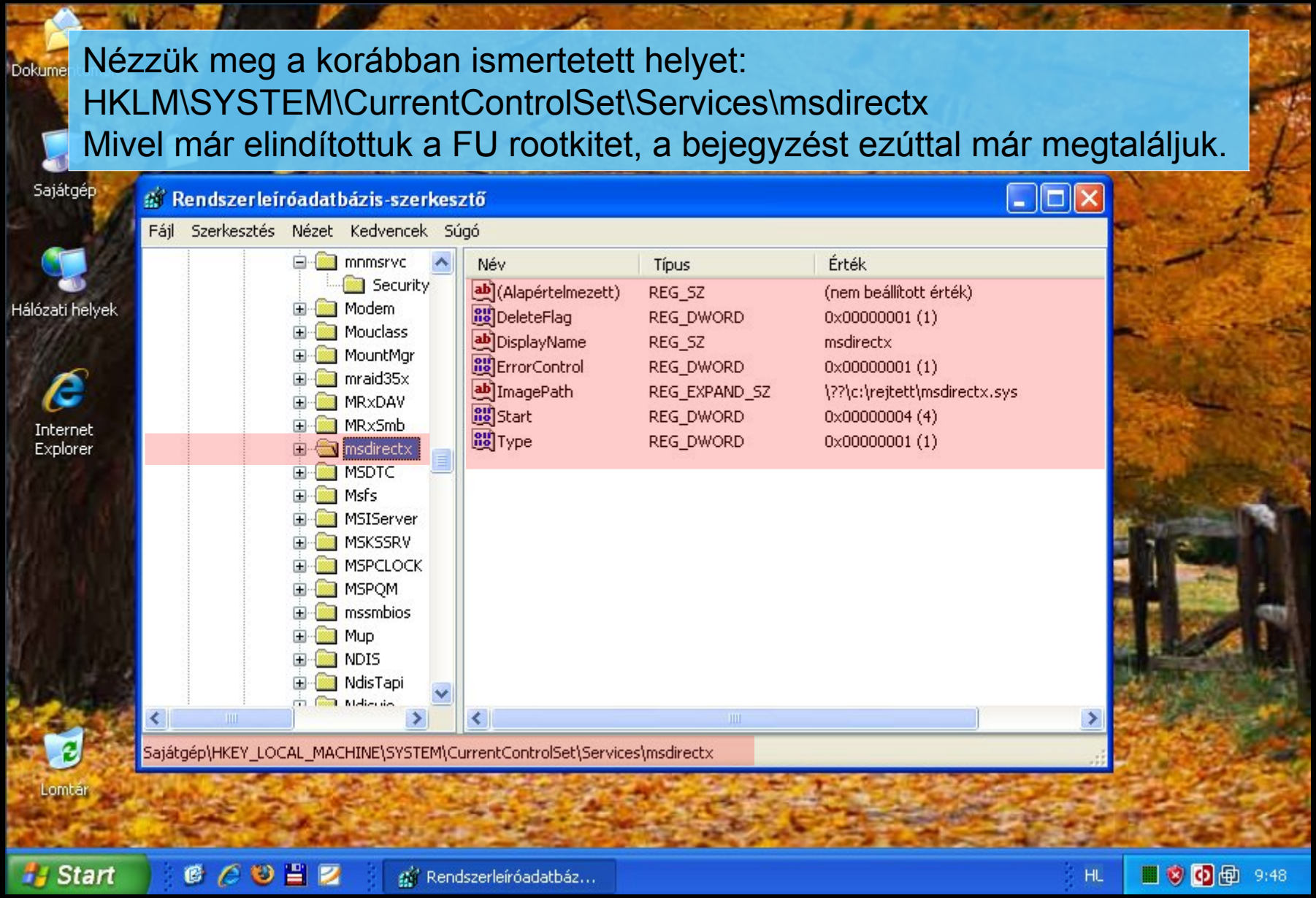


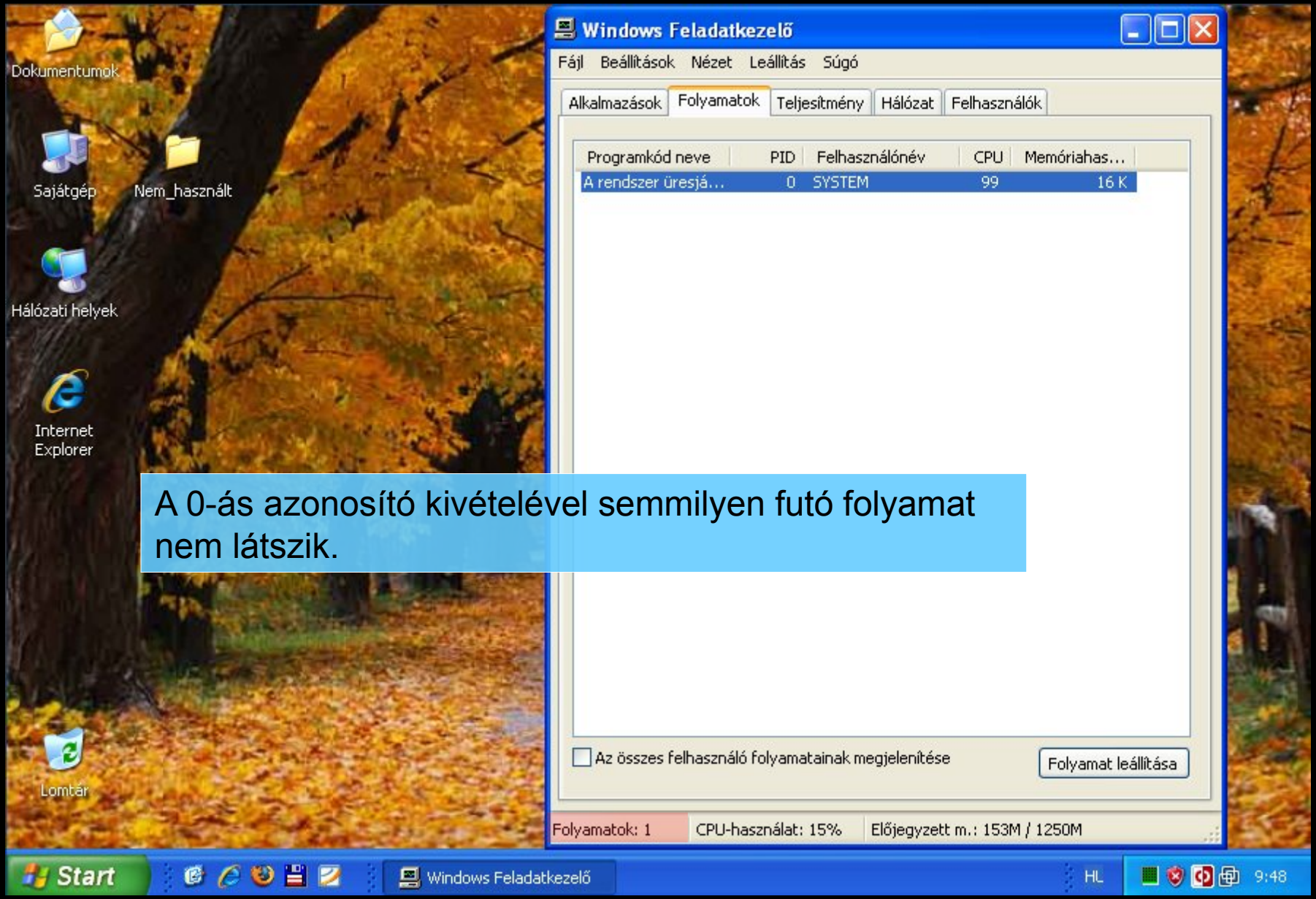
A 0-ás azonosító kivételével akár az összes folyamat elrejthető. Jól látható azonban, hogy ezek nem leállítva, hanem csak elrejtve lettek: például a NOD32 és Feladatkezelő továbbra is működik.


Dokumentumok
Sajátgép
Hálózati hely
Internet Explorer
Lomtár
c:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [verziószám: 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
c:\rejtett>fu -phd msdirectx.sys
c:\rejtett>_
A FU rootkittel adott eszközmeghajtó elrejtésére is van lehetőségünk.
Start
c:\WINDOWS\system...
HL
10:59


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Ellenőrizzük le ismét a rendszerleíró adatbázist!
Futtatás
Adja meg a program, a mappa, a dokumentum vagy az internetes erőforrás nevét, és a Windows megnyitja azt.
Megnyitás:
regedit
OK
Mégse
Tallózás...
Start
HL
9:48

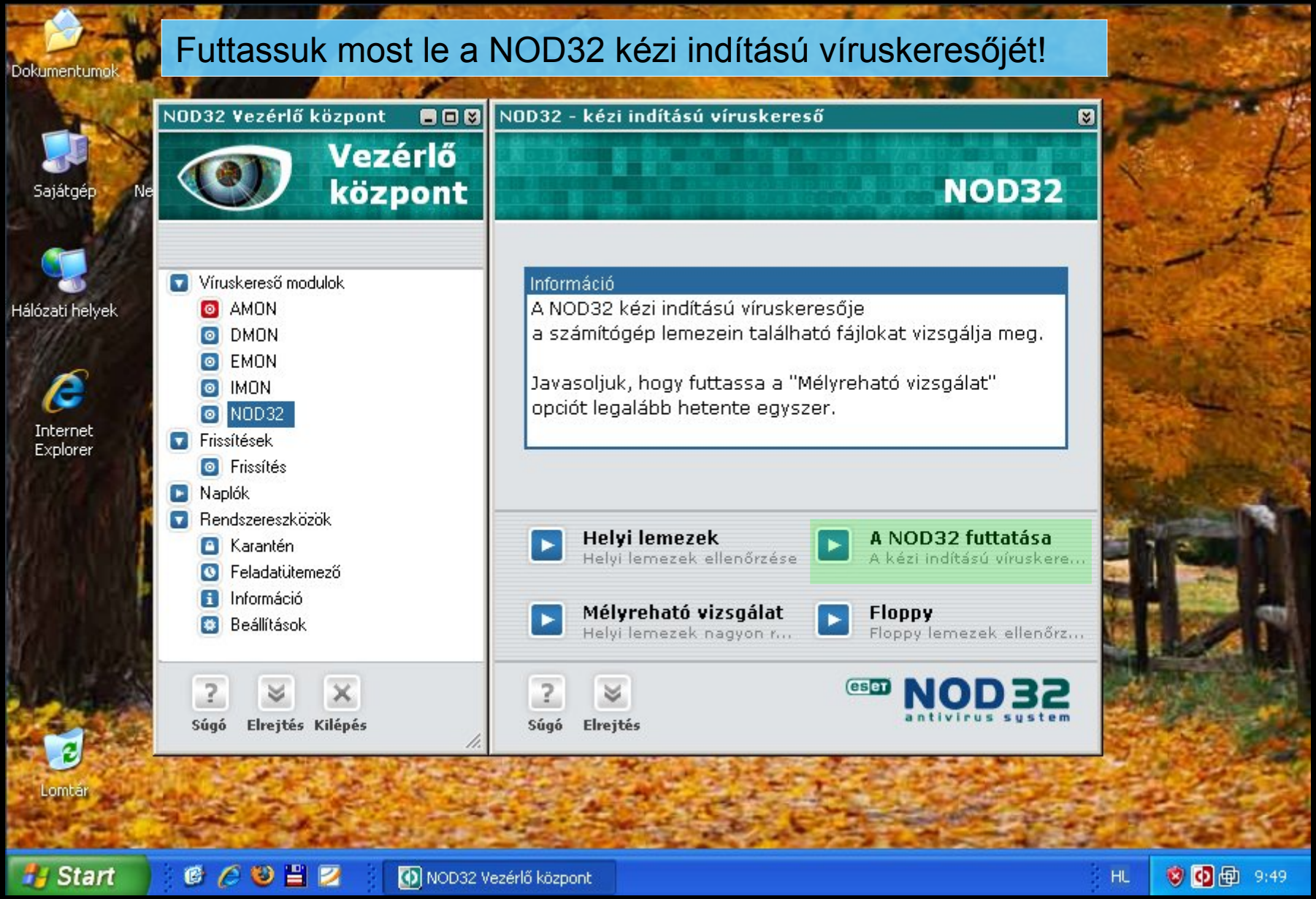
Nézzük meg a korábban ismertetett helyet:
HKLM\SYSTEM\CurrentControlSet\Services\msdirectx
Mivel már elindítottuk a FU rootkitet, a bejegyzést ezúttal már megtaláljuk.



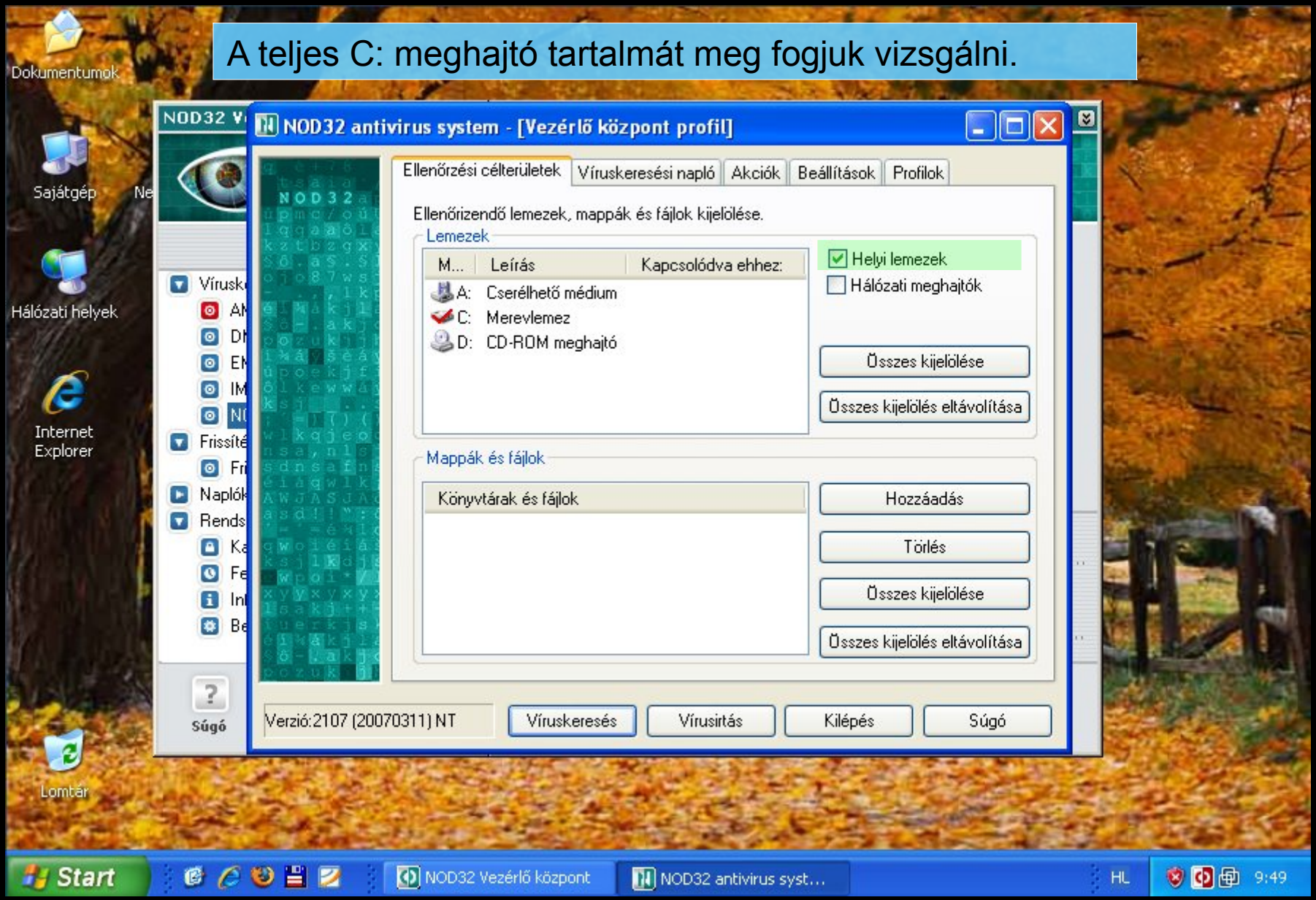


A 0-ás azonosító kivételével semmilyen futó folyamat nem látszik.

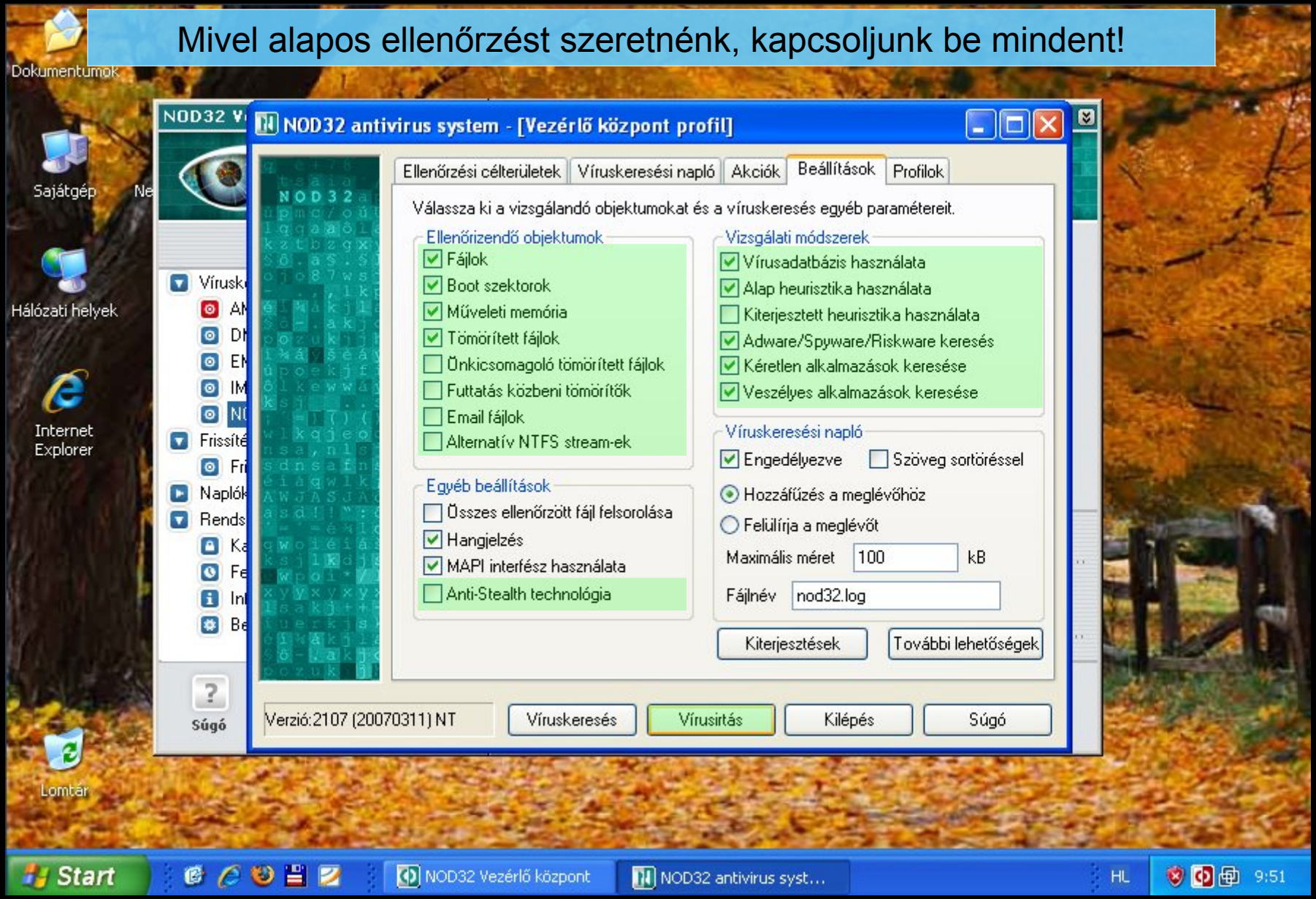
Futtassuk most le a NOD32 kézi indítású víruskeresőjét!

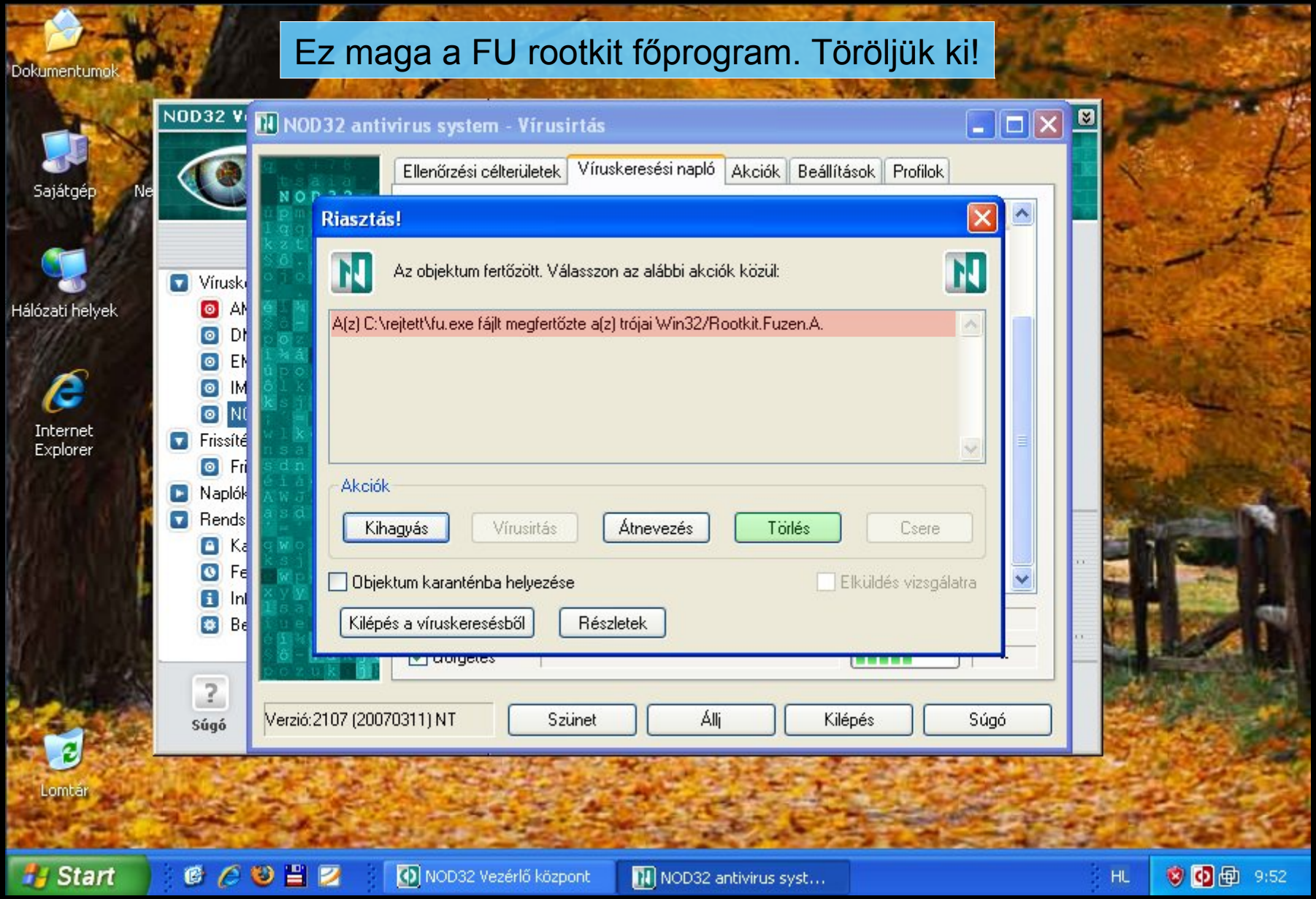


A teljes C: meghajtó tartalmát meg fogjuk vizsgálni.

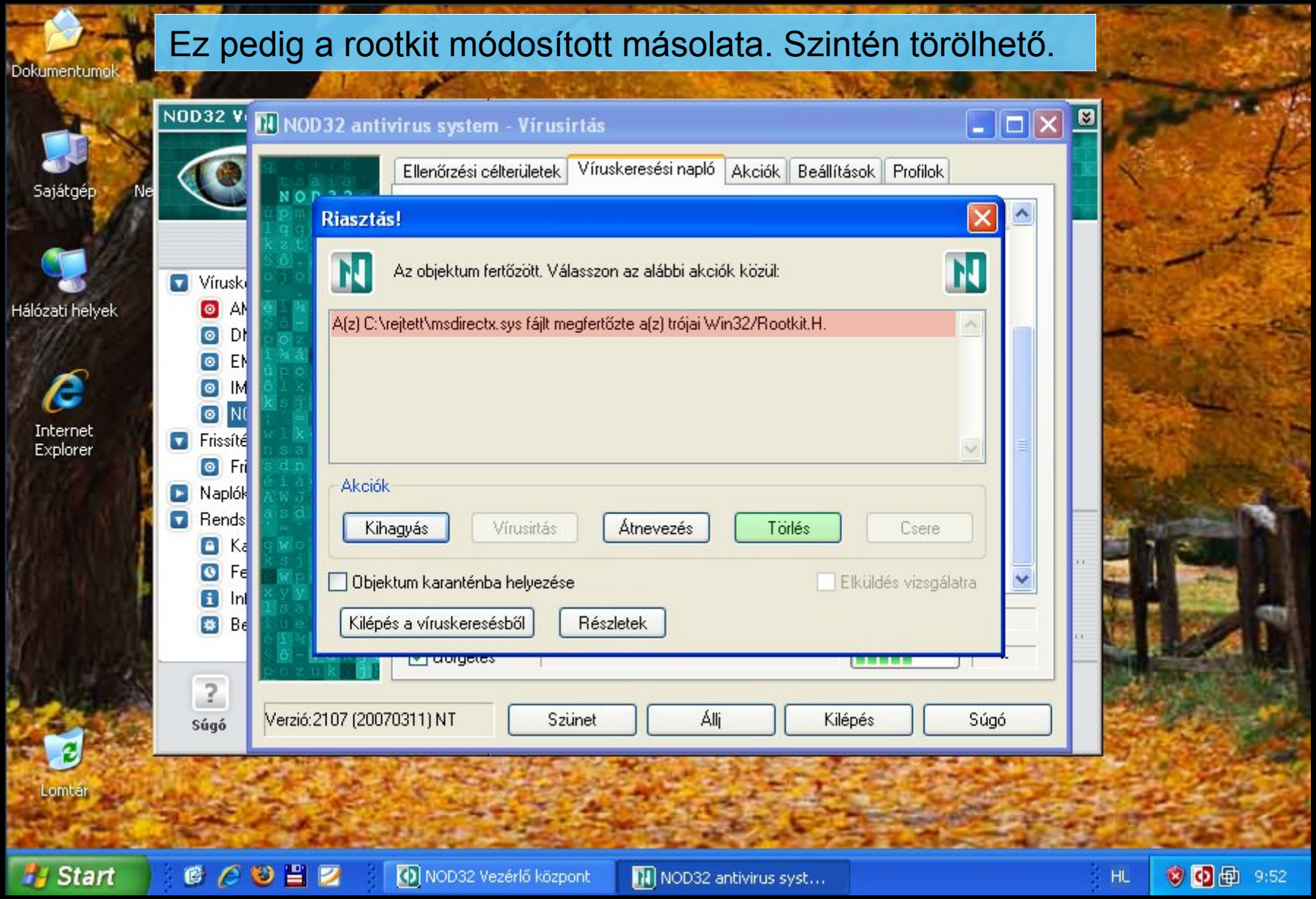


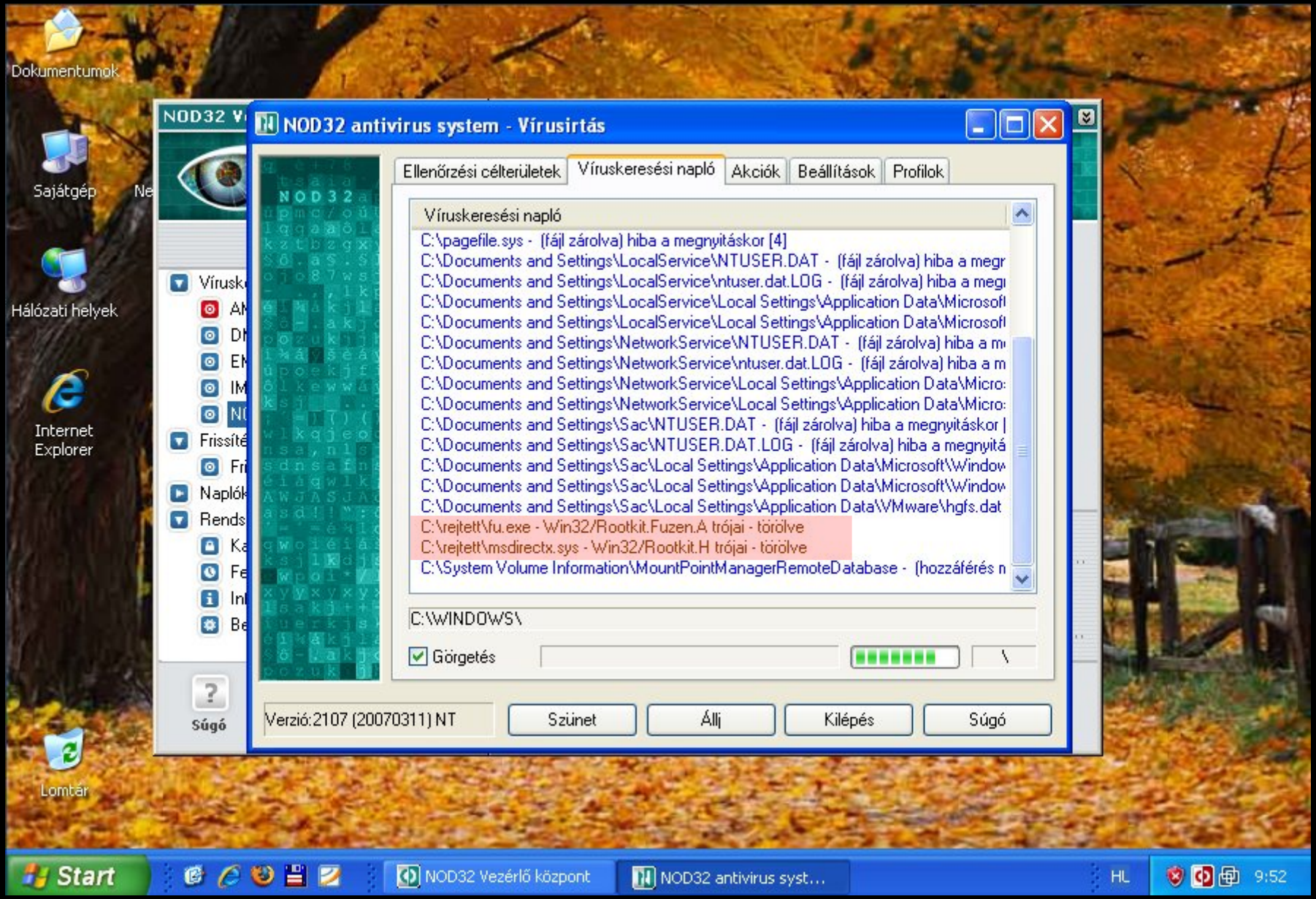
Mivel alapos ellenőrzést szeretnénk, kapcsoljunk be mindent!

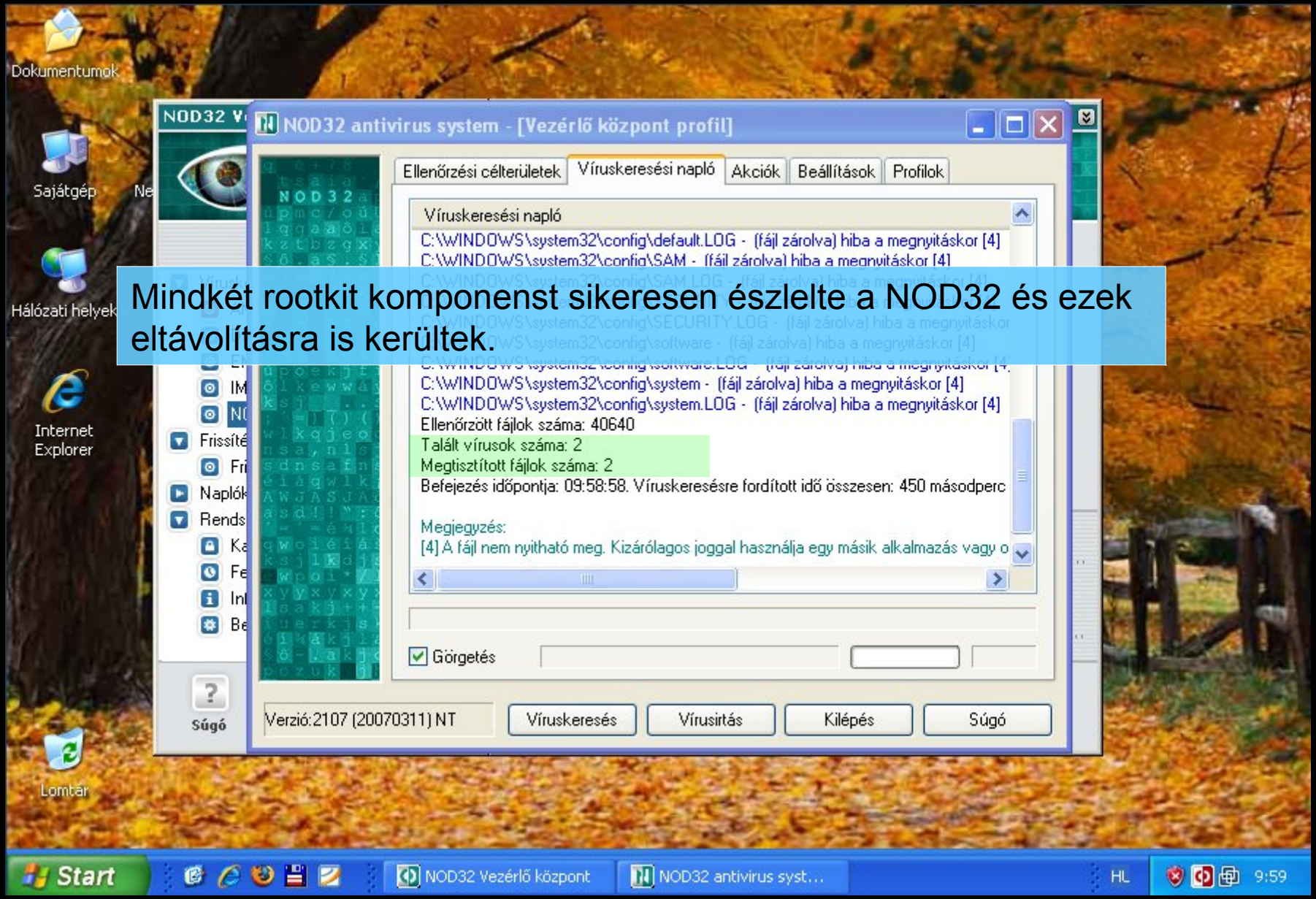



Ez maga a FU rootkit főprogram. Töröljük ki!
NOD32 antivirus system - Vírusirtás
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Riasztás!
Az objektum fertőzött. Válasszon az alábbi akciók közül:
A(z) C:\rejtett\fu.exe fájlt megfertőzte a(z) trójai Win32/Rootkit.Fuzen.A.
Akciók
Kihagyás
Vírusirtás
Átnevezés
Törlés
Csere
Objektum karanténba helyezése
Elküldés vizsgálatra
Kilépés a víruskeresésből
Részletek
Verzió:2107 (20070311) NT
Szünet
Állj
Kilépés
Súgó
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
9:52

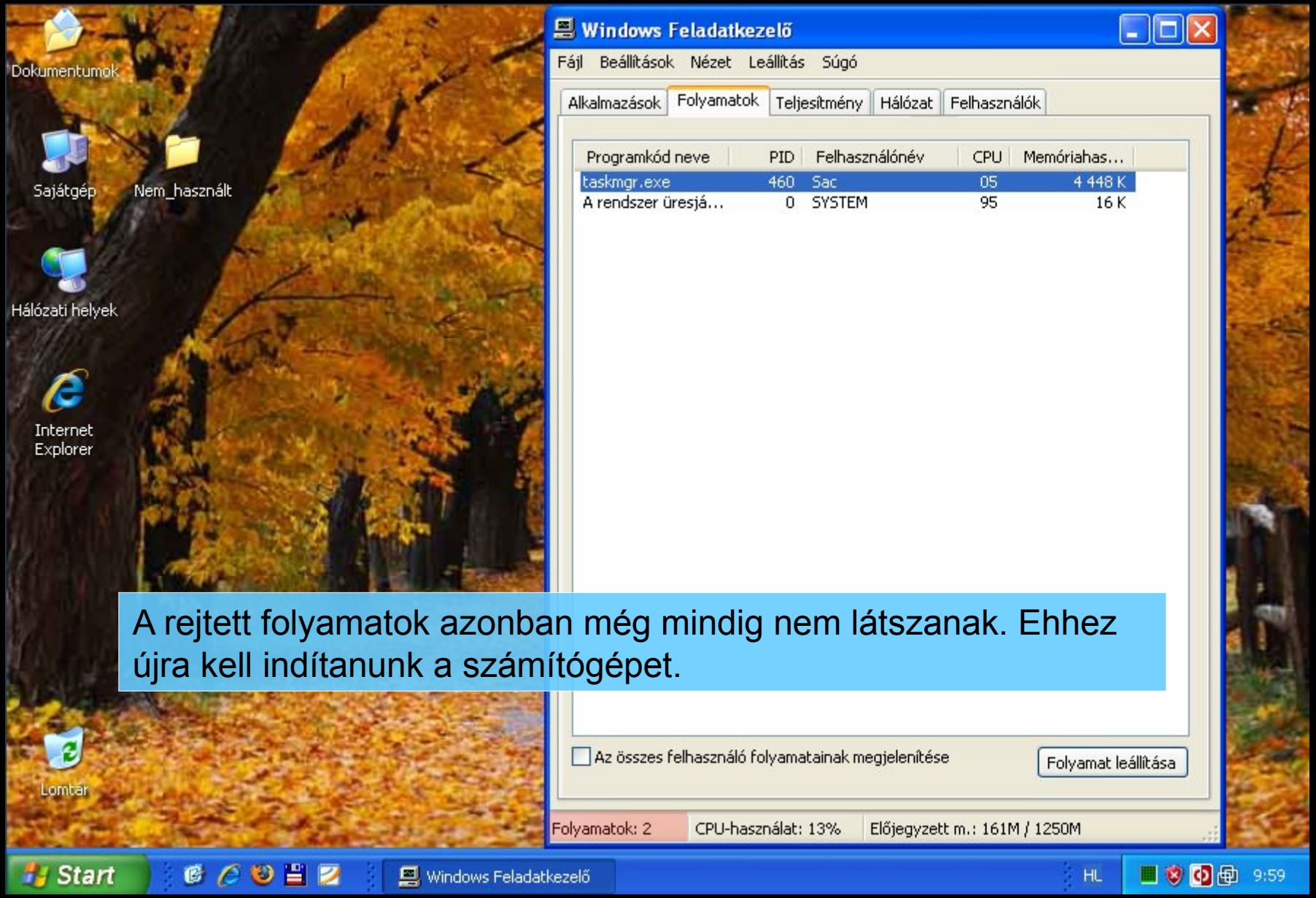
Ez pedig a rootkit módosított másolata. Szintén törölhető.

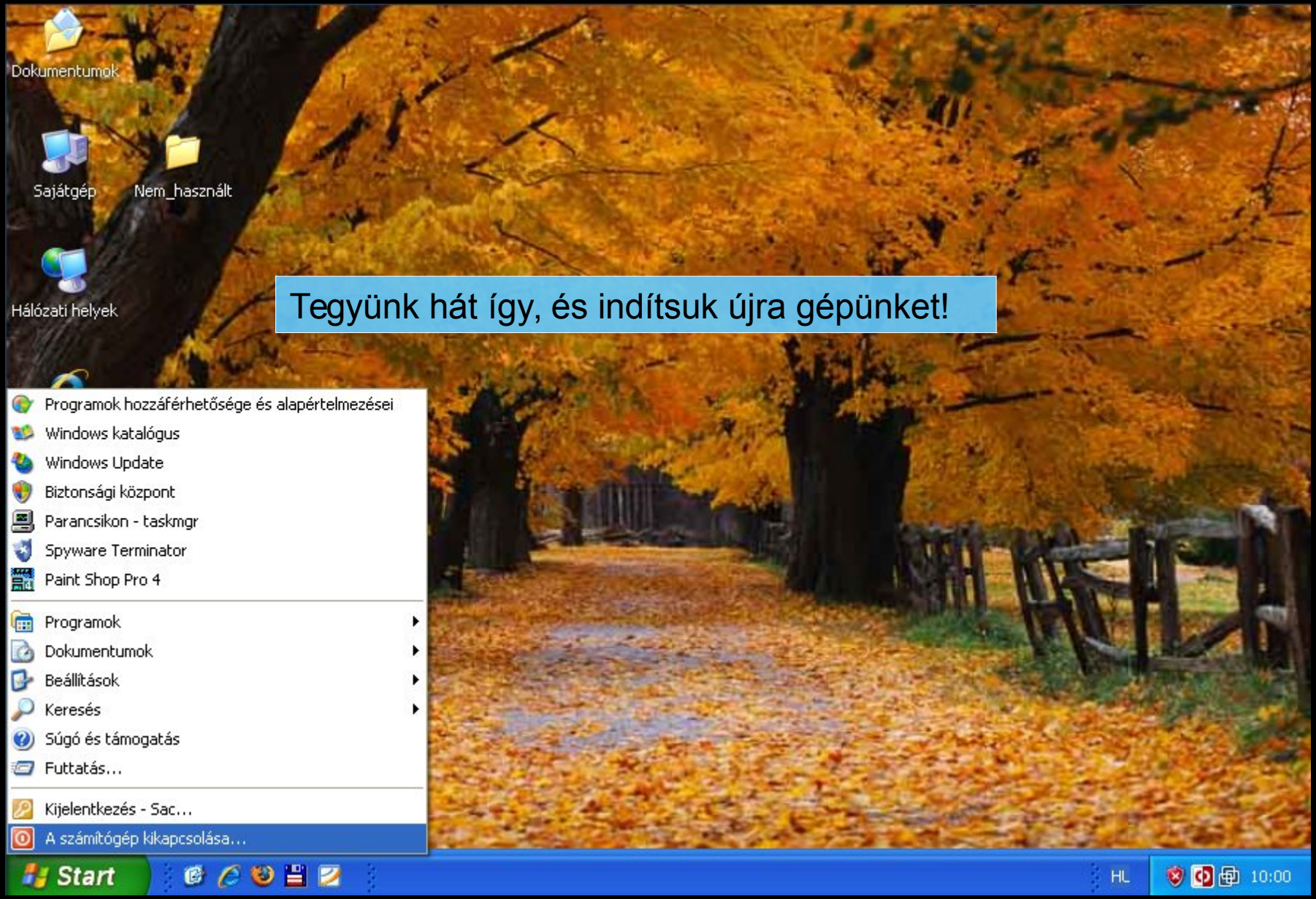


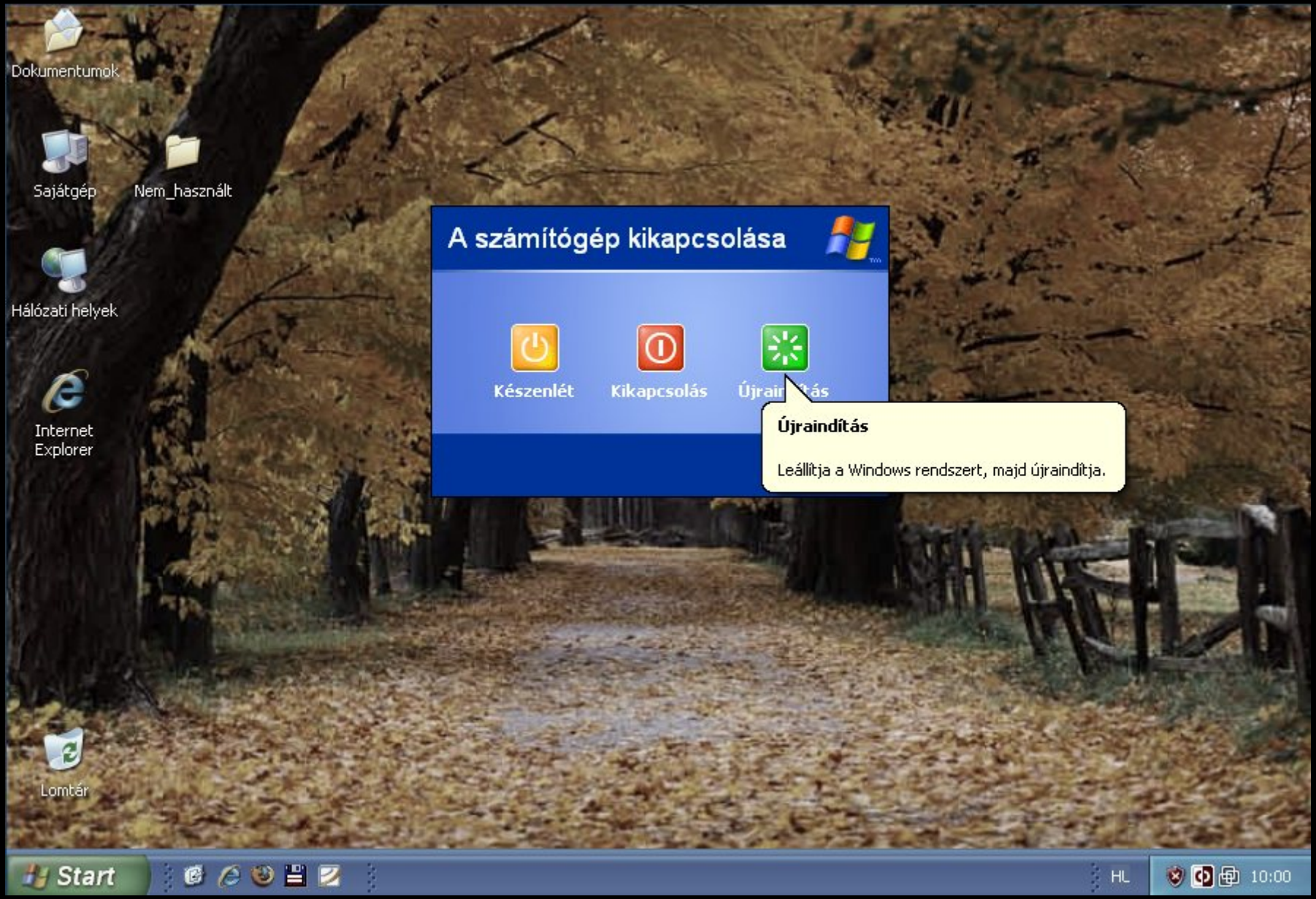

Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - Vírusirtás
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Víruskeresési napló
C:\pagefile.sys - (fájl zárolva) hiba a megnyitáskor [4]
C:\Documents and Settings\LocalService\NTUSER.DAT - (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\fu.exe - Win32/Rootkit.Fuzen.A trójai - törölve
C:\rejtett\msdirectx.sys - Win32/Rootkit.H trójai - törölve
C:\System Volume Information\MountPointManagerRemoteDatabase - (hozzáférés n
C:\WINDOWS\
Görgetés
Verzió:2107 (20070311) NT
Szünet
Állj
Kilépés
Súgó
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
9:52



Mindkét rootkit komponenst sikeresen észlelte a NOD32 és ezek eltávolításra is kerültek.


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Windows Feladatkezelő
Fájl Beállítások Nézet Leállítás Súgó
Alkalmazások Folyamatok Teljesítmény Hálózat Felhasználók
Programkód neve PID Felhasználónév CPU Memóriahas...
taskmgr.exe 460 Sac 05 4 448 K
A rendszer üresjá... 0 SYSTEM 95 16 K
Az összes felhasználó folyamatainak megjelenítése
Folyamat leállítása
Folyamatok: 2 CPU-használat: 13% Előjegyzett m.: 161M / 1250M
A rejtett folyamatok azonban még mindig nem látszanak. Ehhez újra kell indítanunk a számítógépet.
Start
Windows Feladatkezelő
HL
9:59

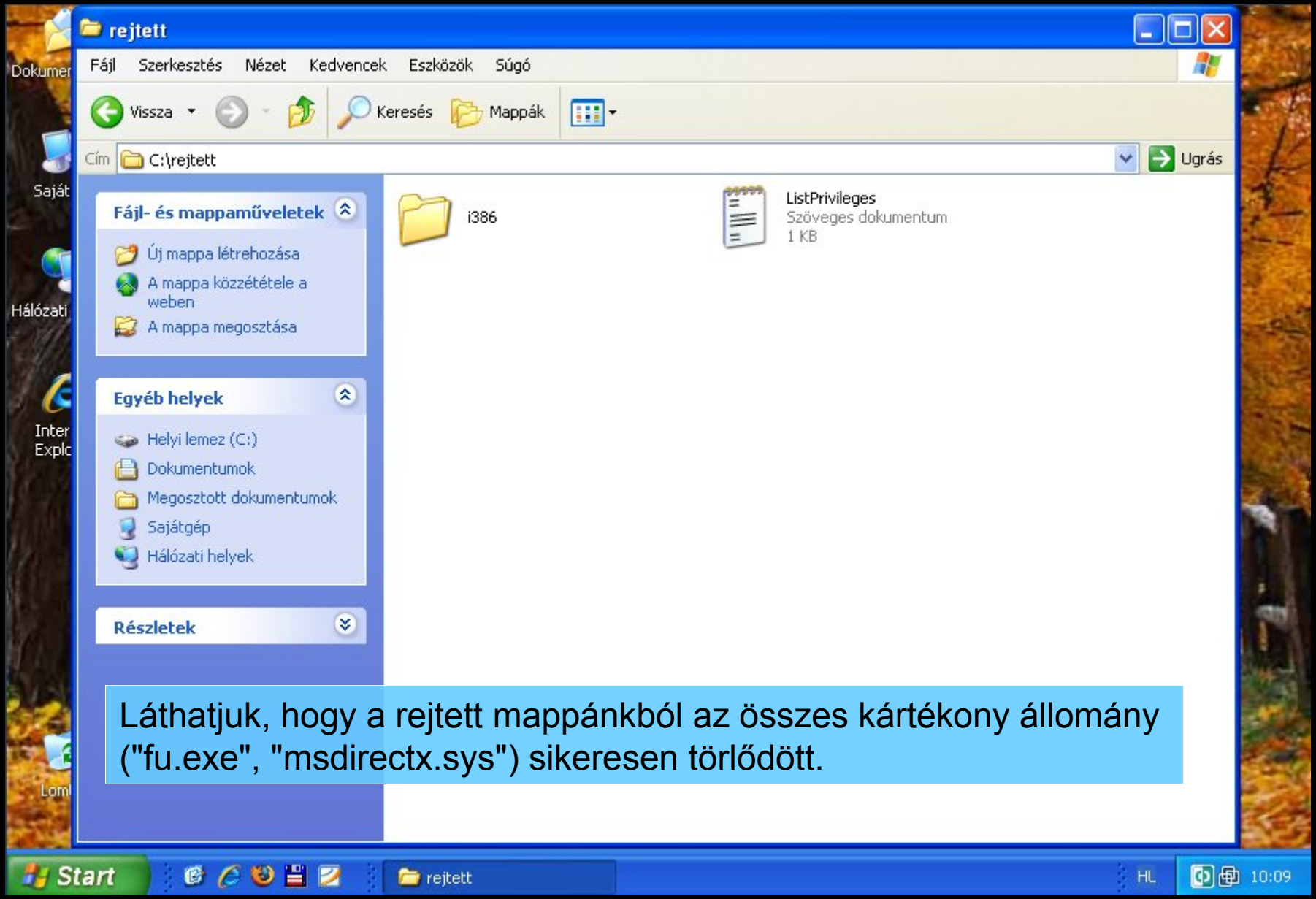

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Tegyünk hát így, és indítsuk újra gépünket!
Programok hozzáférhetősége és alapértelmezései
Windows katalógus
Windows Update
Biztonsági központ
Parancsikon - taskmgr
Spyware Terminator
Paint Shop Pro 4
Programok
Dokumentumok
Beállítások
Keresés
Súgó és támogatás
Futtatás...
Kijelentkezés - Sac...
A számítógép kikapcsolása...
Start
HL
10:00


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
A számítógép kikapcsolása
Készenlét
Kikapcsolás
Újraindítás
Újraindítás
Leállítja a Windows rendszert, majd újraindítja.
Start
HL
10:00

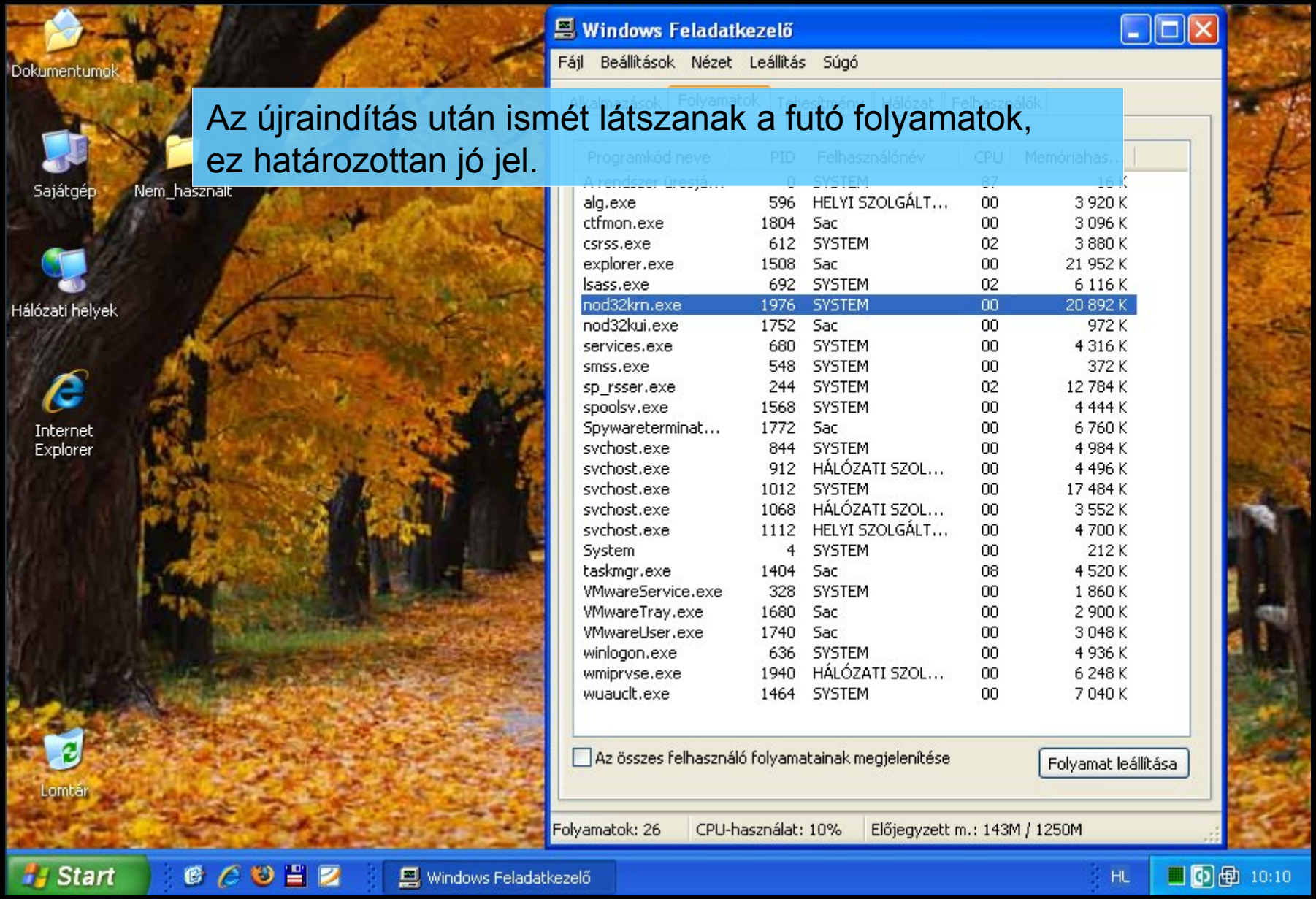
Kijelentkezés...

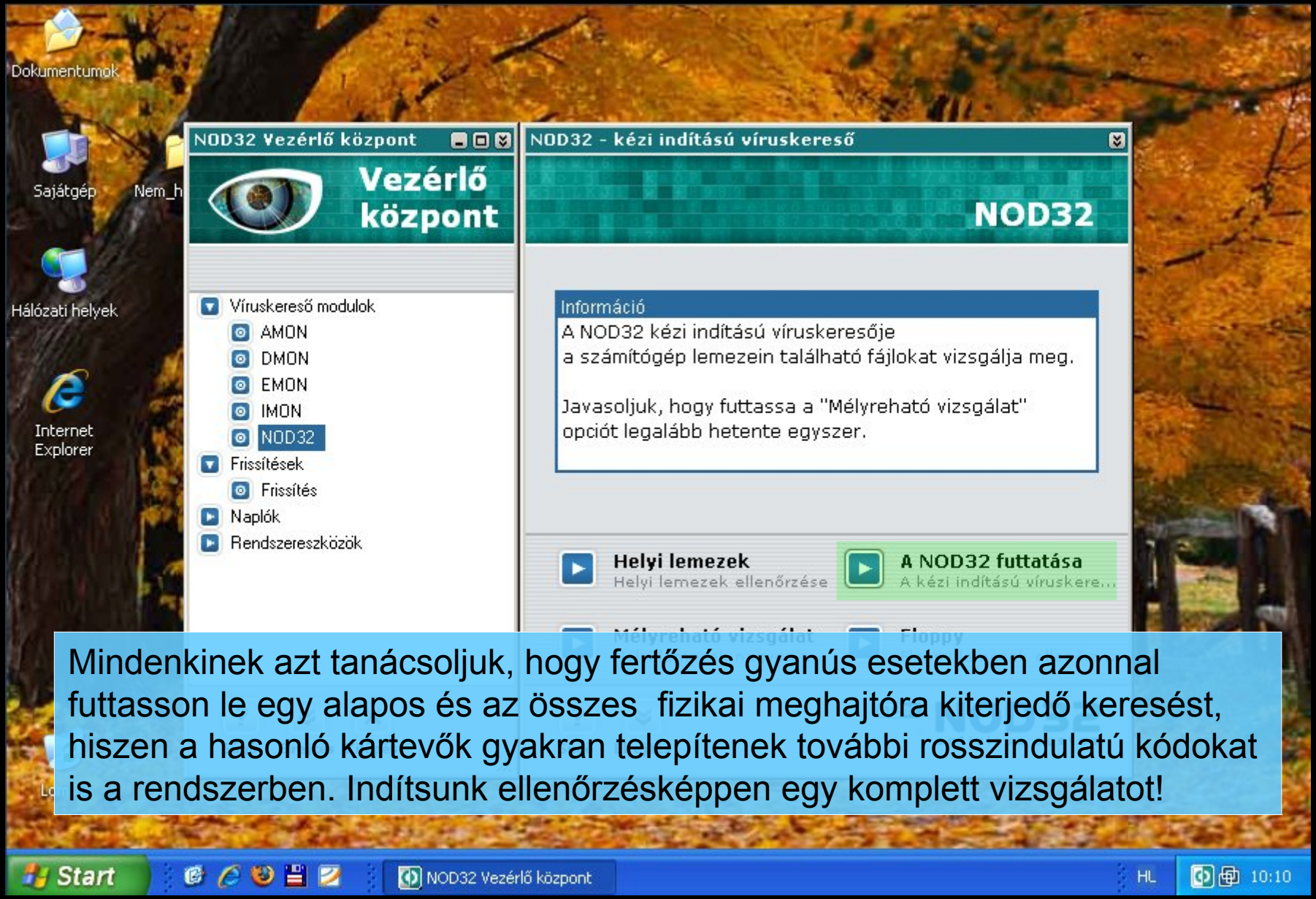

Microsoft®
Windows®xp
Copyright © Microsoft Corporation
Microsoft

Üdvözöljük

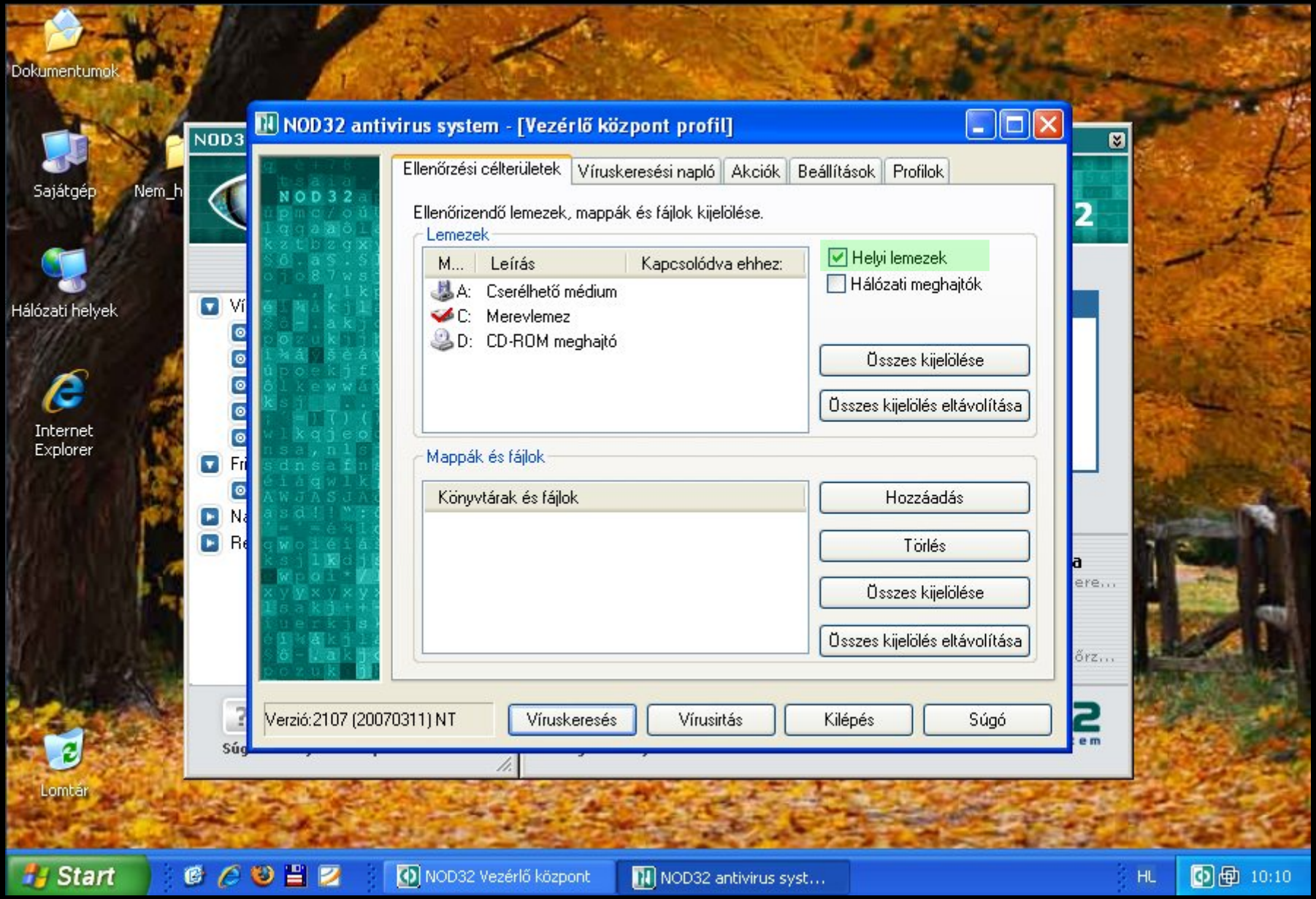


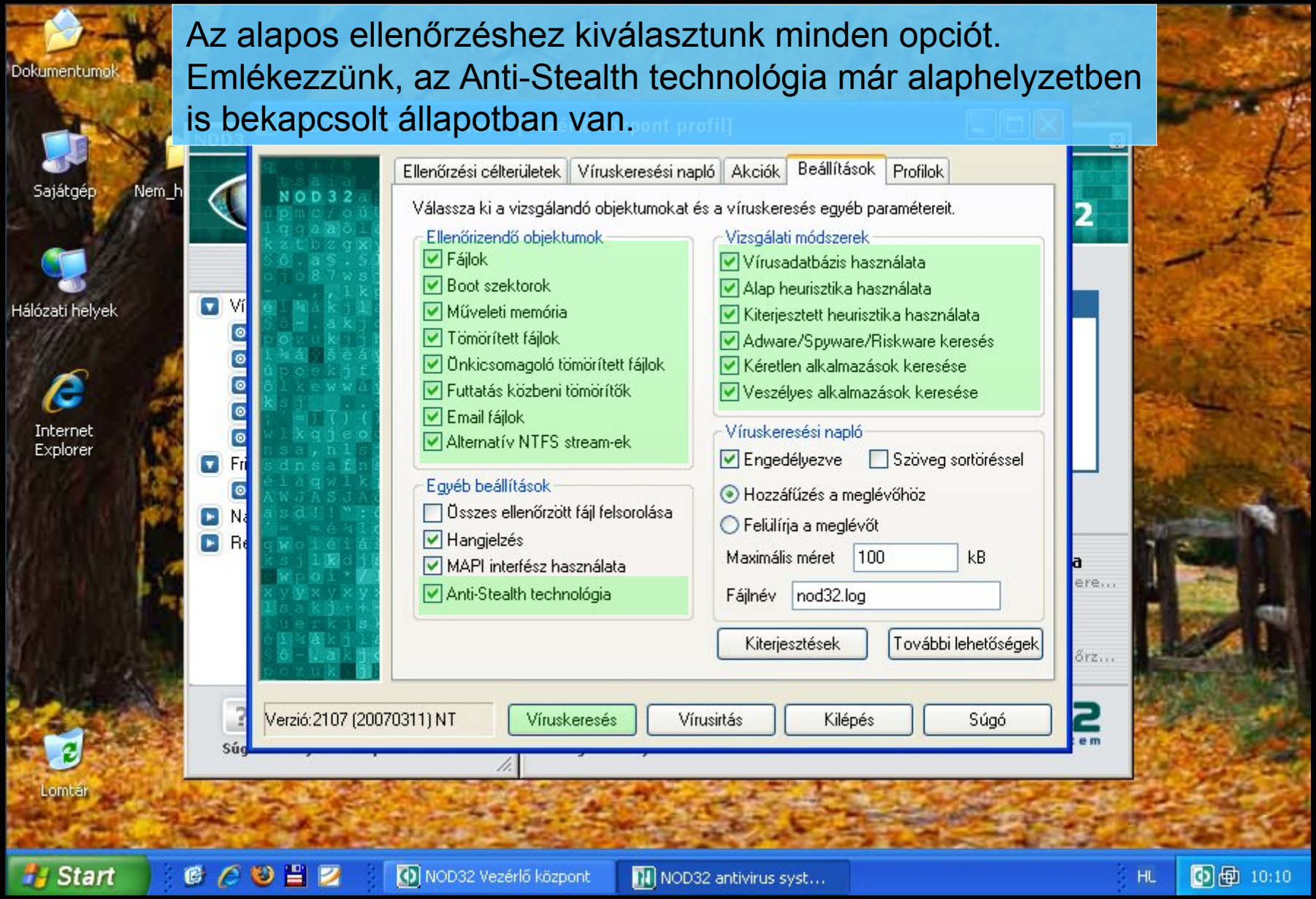
Láthatjuk, hogy a rejtett mappánkból az összes kártékony állomány ("fu.exe", "msdirectx.sys") sikeresen törlődött.

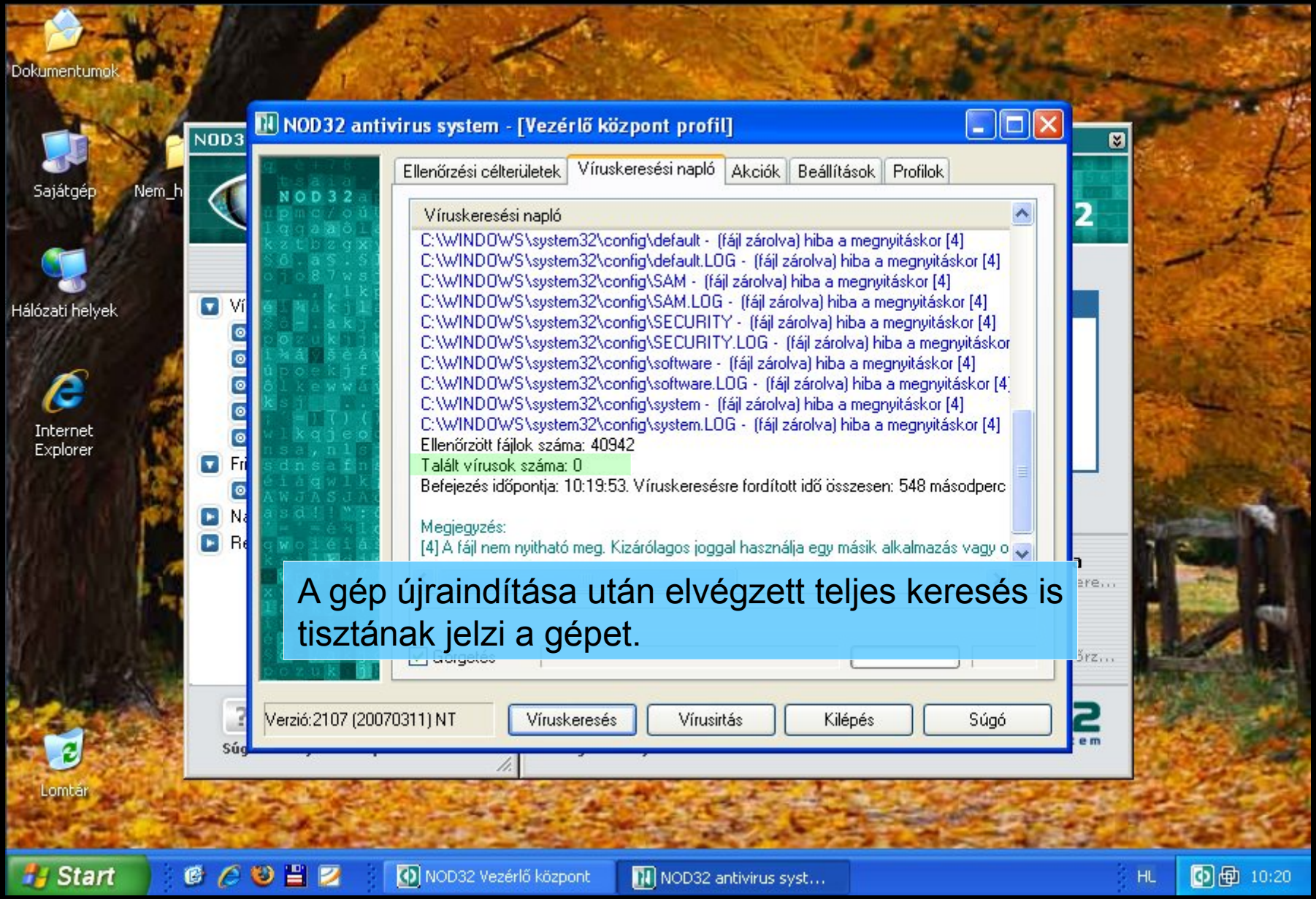

Az újraindítás után ismét látszanak a futó folyamatok, ez határozottan jó jel.
Windows Feladatkezelő
Fájl Beállítások Nézet Leállítás Súgó
Folyamatok
Programkód neve PID Felhasználónév CPU Memóriahas...
alg.exe 596 HELYI SZOLGÁLT... 00 3 920 K
ctfmon.exe 1804 Sac 00 3 096 K
csrss.exe 612 SYSTEM 02 3 880 K
explorer.exe 1508 Sac 00 21 952 K
lsass.exe 692 SYSTEM 02 6 116 K
nod32krn.exe 1976 SYSTEM 00 20 892 K
nod32kui.exe 1752 Sac 00 972 K
services.exe 680 SYSTEM 00 4 316 K
smss.exe 548 SYSTEM 00 372 K
sp_rsser.exe 244 SYSTEM 02 12 784 K
spoolsv.exe 1568 SYSTEM 00 4 444 K
Spywareterminat... 1772 Sac 00 6 760 K
svchost.exe 844 SYSTEM 00 4 984 K
svchost.exe 912 HÁLÓZATI SZOL... 00 4 496 K
svchost.exe 1012 SYSTEM 00 17 484 K
svchost.exe 1068 HÁLÓZATI SZOL... 00 3 552 K
svchost.exe 1112 HELYI SZOLGÁLT... 00 4 700 K
System 4 SYSTEM 00 212 K
taskmgr.exe 1404 Sac 08 4 520 K
VMwareService.exe 328 SYSTEM 00 1 860 K
VMwareTray.exe 1680 Sac 00 2 900 K
VMwareUser.exe 1740 Sac 00 3 048 K
winlogon.exe 636 SYSTEM 00 4 936 K
wmiprvse.exe 1940 HÁLÓZATI SZOL... 00 6 248 K
wuauclt.exe 1464 SYSTEM 00 7 040 K
Az összes felhasználó folyamatainak megjelenítése
Folyamat leállítása
Folyamatok: 26 CPU-használat: 10% Előjegyzett m.: 143M / 1250M
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Start
Windows Feladatkezelő
HL
10:10

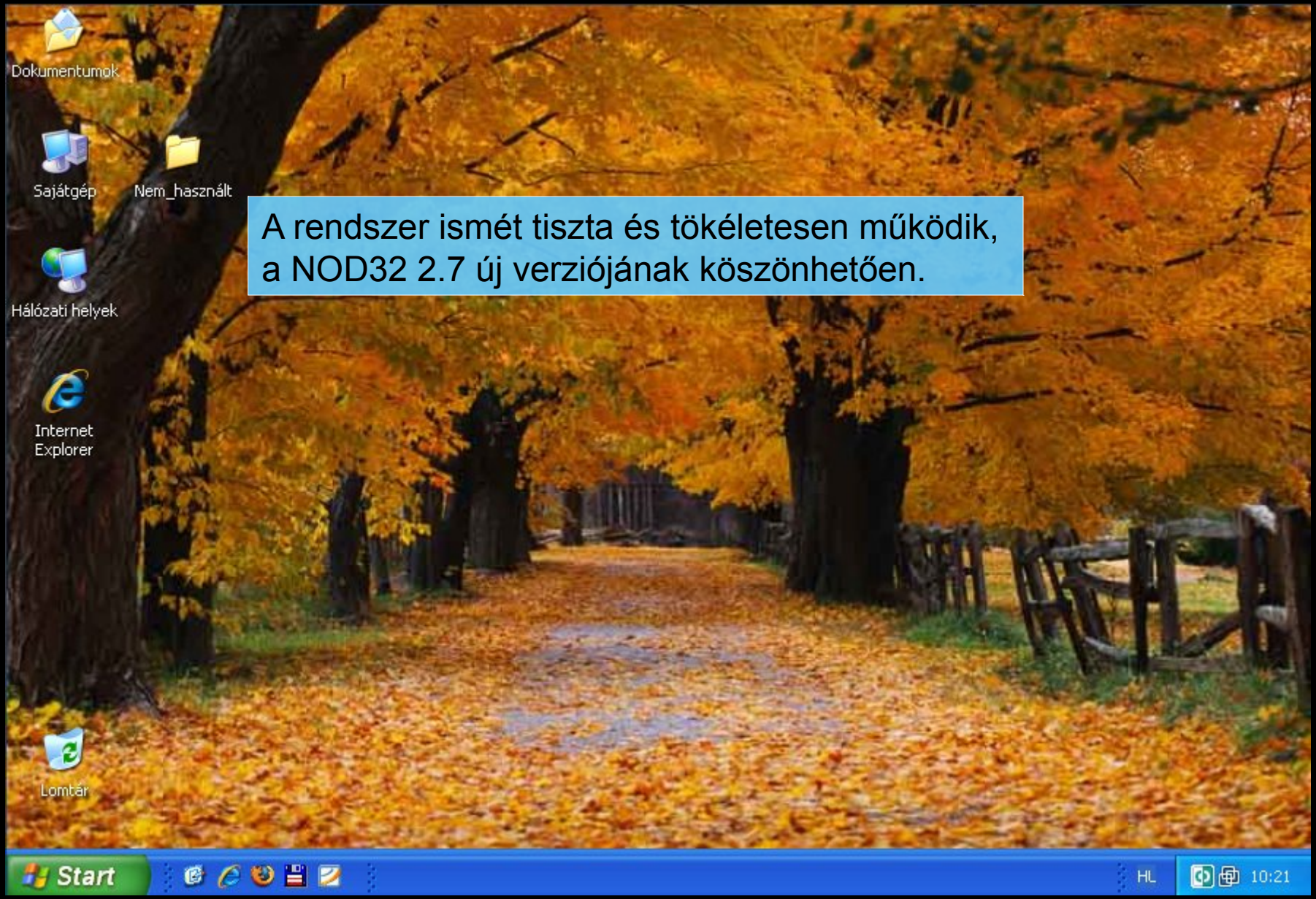


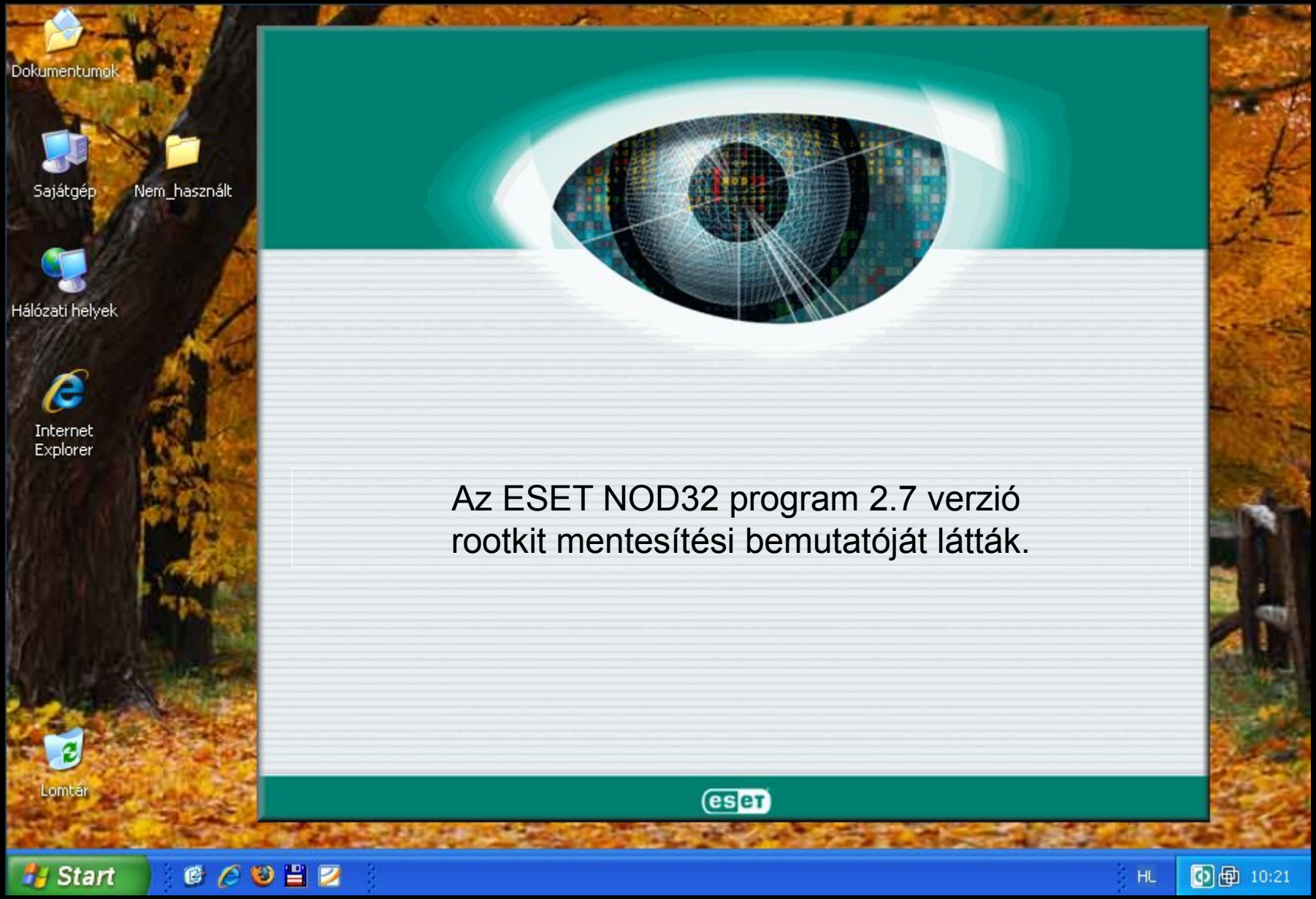
Mindenkinek azt tanácsoljuk, hogy fertőzés gyanús esetekben azonnal futtasson le egy alapos és az összes fizikai meghajtóra kiterjedő keresést, hiszen a hasonló kártevők gyakran telepítenek további rosszindulatú kódokat is a rendszerben. Indítsunk ellenőrzésképpen egy komplett vizsgálatot!


Dokumentumok
Sajátgép
Nem_h
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:2107 (20070311) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:10


Az alapos ellenőrzéshez kiválasztunk minden opciót. Emlékezzünk, az Anti-Stealth technológia már alaphelyzetben is bekapcsolt állapotban van.
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Válassza ki a vizsgálandó objektumokat és a víruskeresés egyéb paramétereit.
Ellenőrizendő objektumok
Fájlok
Boot szektorok
Műveleti memória
Tömörített fájlok
Önkicsomagoló tömörített fájlok
Futtatás közbeni tömörítők
Email fájlok
Alternatív NTFS stream-ek
Egyéb beállítások
Összes ellenőrzött fájl felsorolása
Hangjelzés
MAPI interfész használata
Anti-Stealth technológia
Vizsgálati módszerek
Vírusadatbázis használata
Alap heurisztika használata
Kiterjesztett heurisztika használata
Adware/Spyware/Riskware keresés
Kéretlen alkalmazások keresése
Veszélyes alkalmazások keresése
Víruskeresési napló
Engedélyezve
Szöveg sortöréssel
Hozzáfűzés a meglévőhöz
Felülírja a meglévőt
Maximális méret
100
kB
Fájlnév
nod32.log
Kiterjesztések
További lehetőségek
Verzió:2107 (20070311) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:10


Dokumentumok
Sajátgép
Nem_h
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 - (fájl zárolva) hiba a megnyitáskor [4]
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: 40942
Talált vírusok száma: 0
Befejezés időpontja: 10:19:53. Víruskeresésre fordított idő összesen: 548 másodperc
Megjegyzés:
[4] A fájl nem nyitható meg. Kizárólagos joggal használja egy másik alkalmazás vagy o
Verzió:2107 (20070311) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
A gép újraindítása után elvégzett teljes keresés is tisztának jelzi a gépet.
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
10:20


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
A rendszer ismét tiszta és tökéletesen működik, a NOD32 2.7 új verziójának köszönhetően.
Start
HL
10:21


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Az ESET NOD32 program 2.7 verzió rootkit mentesítési bemutatóját látták.
eset
Start
HL
10:21