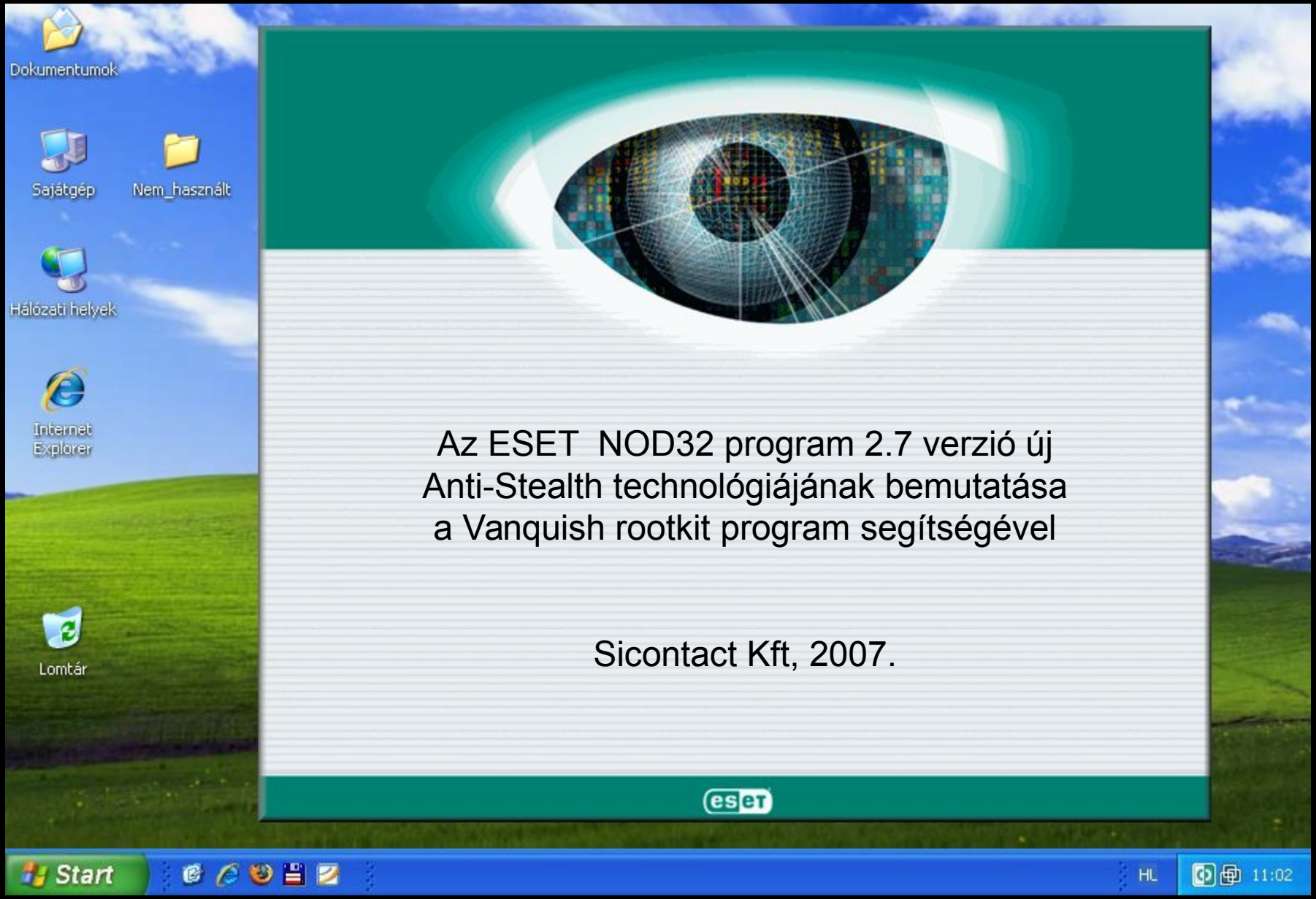

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Az ESET NOD32 program 2.7 verzió új
Anti-Stealth technológiájának bemutatása
a Vanquish rootkit program segítségével
Sicontact Kft, 2007.
eset
Start
HL
11:02

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 Vanquish Rootkit v:0.2.1. nevű csomagot töltöttük le, és azzel végeztük a kísérletet.

A Vanquish igen elterjedt rootkit - még kereskedelmi verzió is létezik belőle. A Vanquish a "KERNEL32.DLL" függvénykönyvtár foltozásával (kernel32.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!

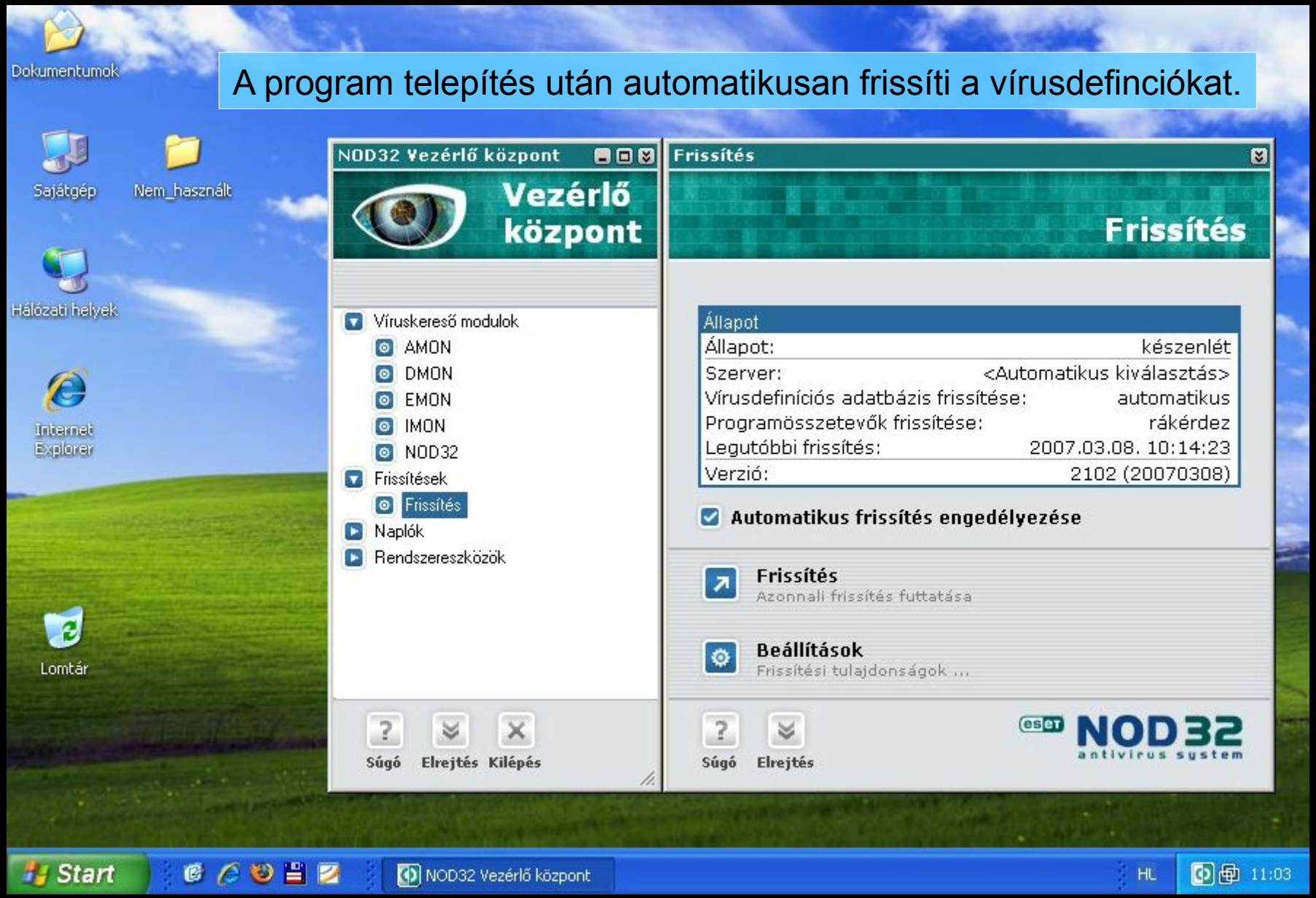
A használt állományok:

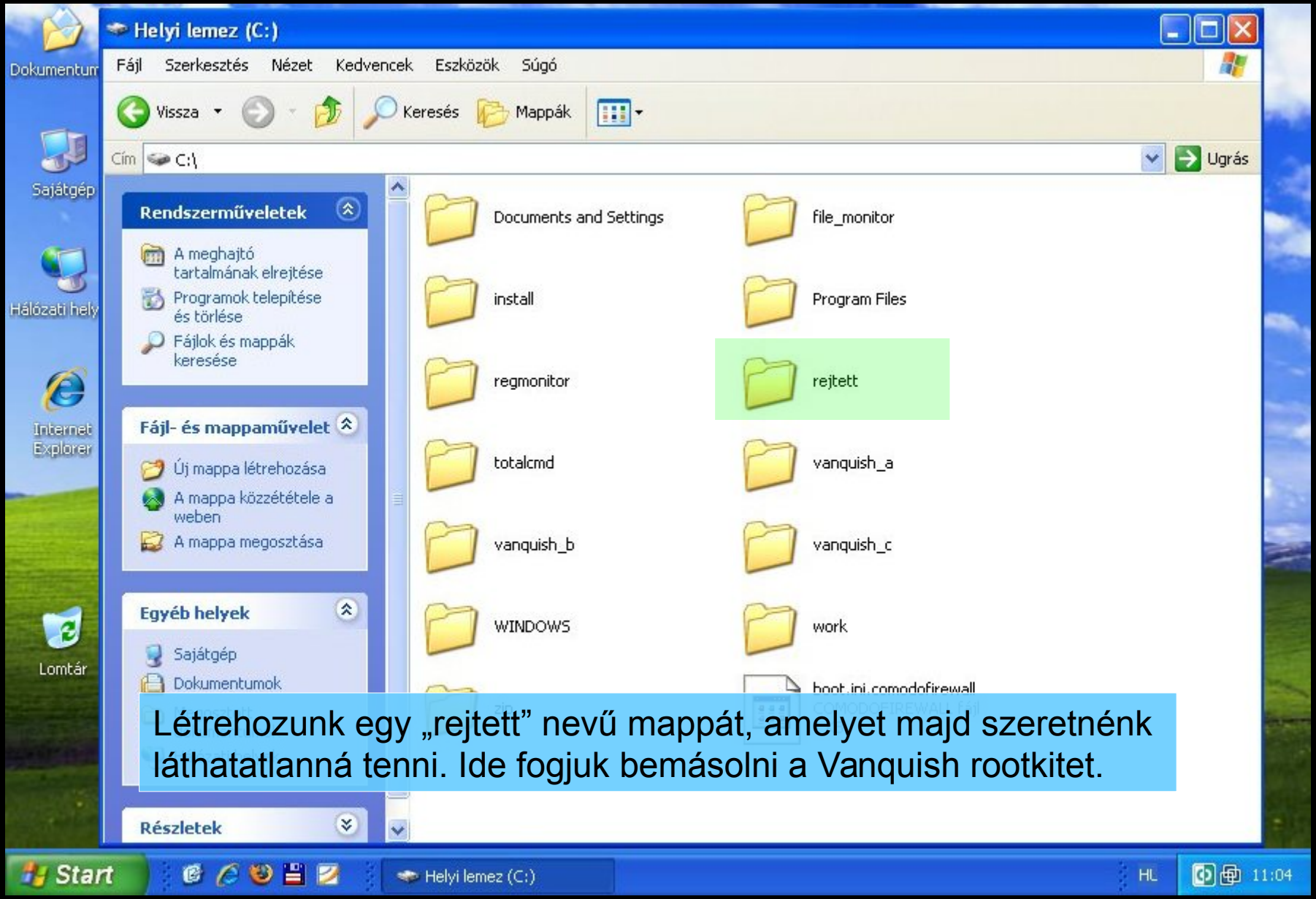
"vanquish.exe„ - A Vanquish főprogramja
"vanquish.dll„ - A Vanquish dinamikus könyvtár állománya

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

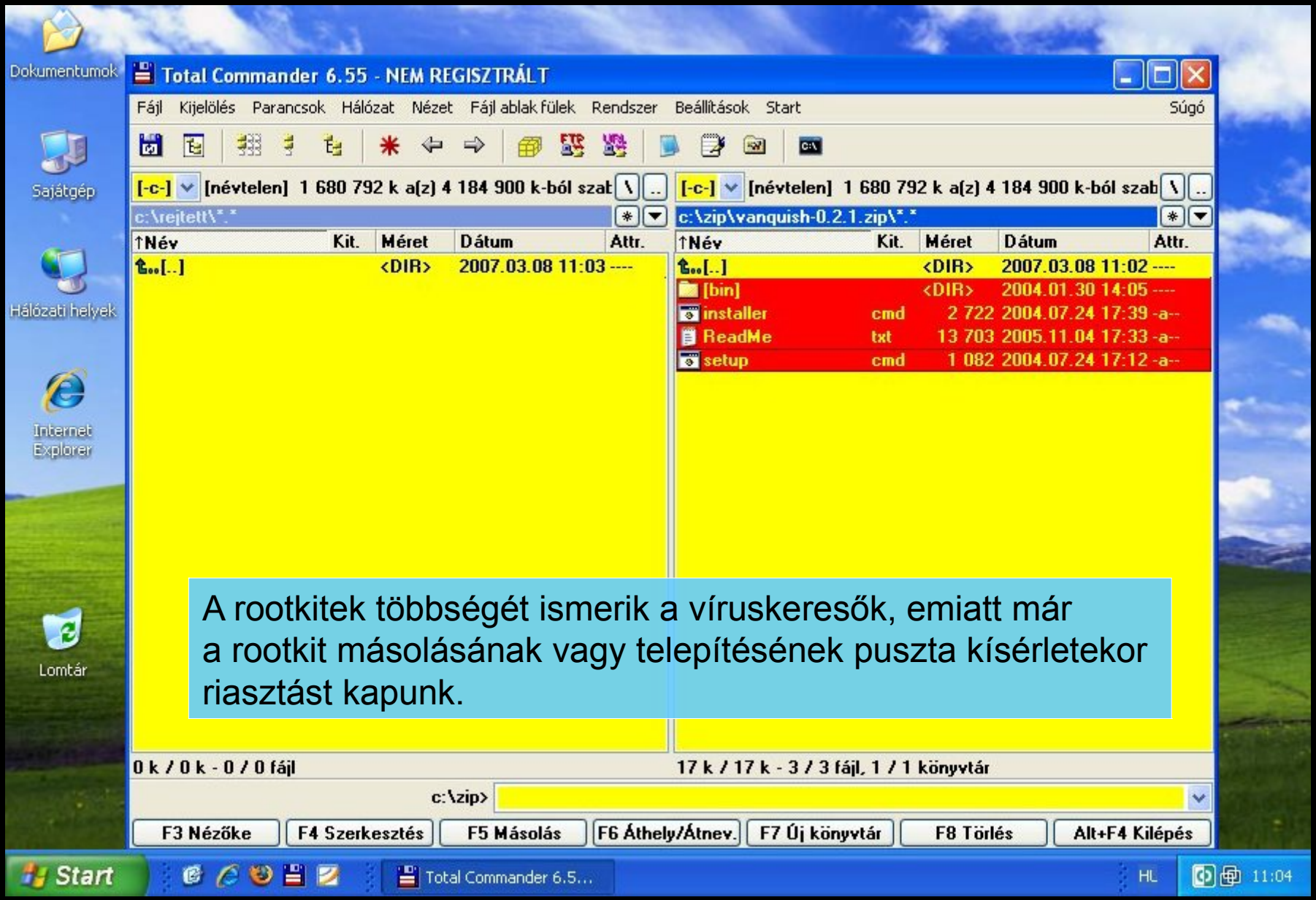
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Start
HL
11:02

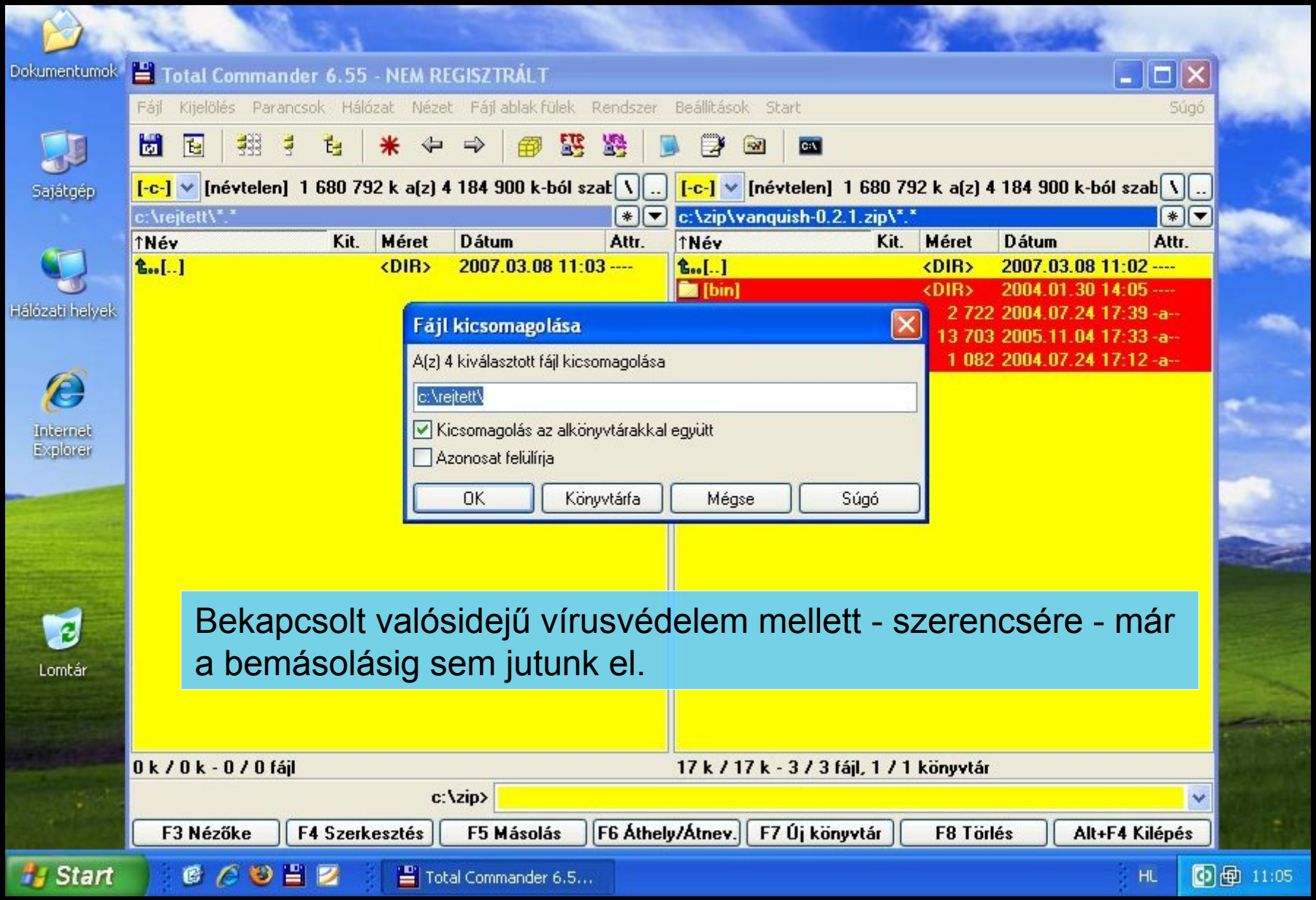

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Feltelepítettük a NOD32 2.7-es változatát egy Windows XP operációs rendszert futtató számítógépre.
Start
HL
11:02


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: 2007.03.08. 10:14:23
Verzió: 2102 (20070308)
Automatikus frissítés engedélyezése
Frissítés
Azonnali frissítés futtatása
Beállítások
Frissítési tulajdonságok ...
Súgó
Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
HL
11:03

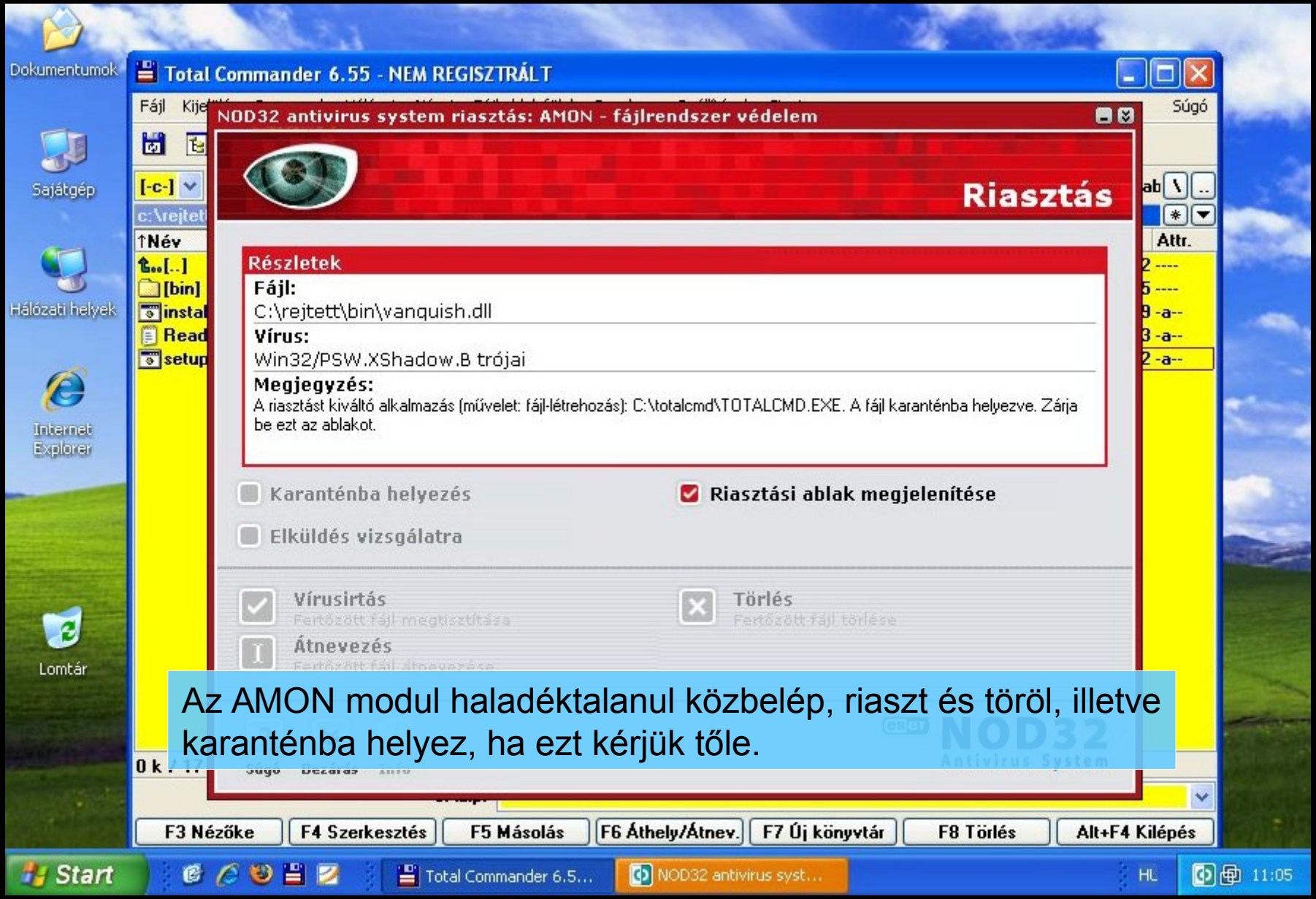


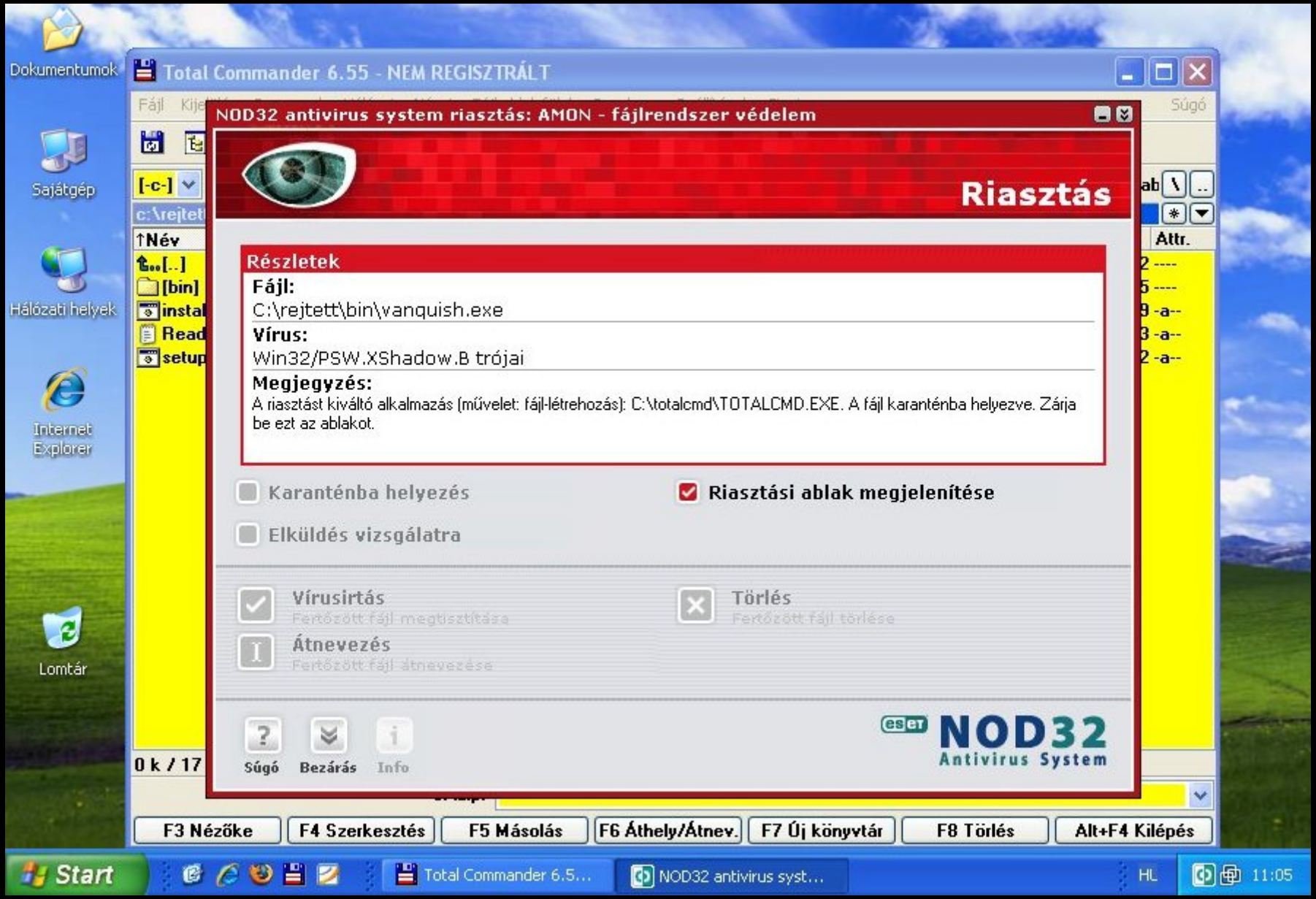
Létrehozunk egy „rejtett” nevű mappát, amelyet majd szeretnénk láthatatlanná tenni. Ide fogjuk bemásolni a Vanquish rootkitet.

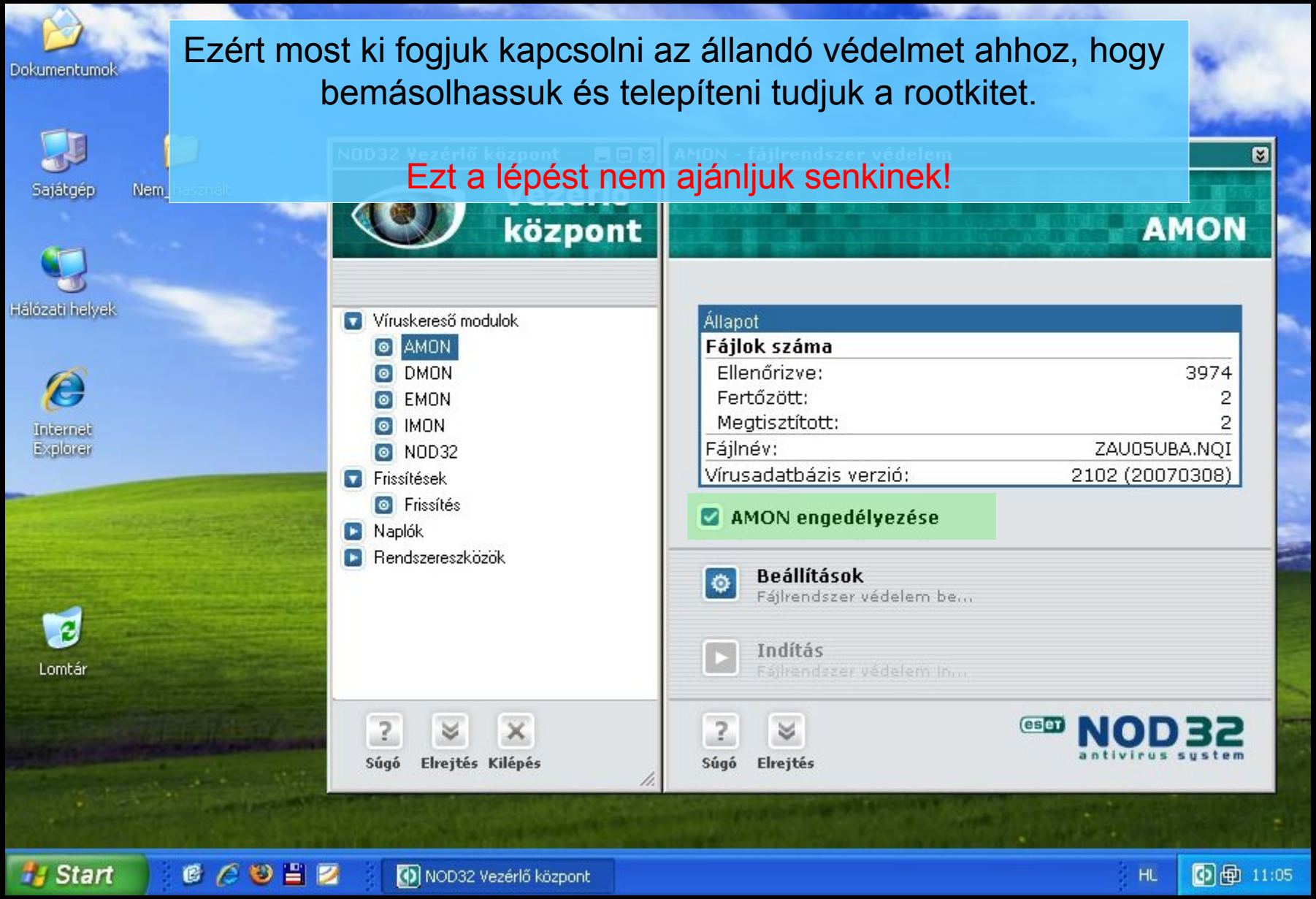

Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Total Commander 6.55 - NEM REGISZTRÁLT
Fájl Kijelölés Parancsok Hálózat Nézet Fájl ablak fülek Rendszer Beállítások Start Súgó
[-c-] [névtelen] 1 680 792 k a(z) 4 184 900 k-ból szab
c:\rejtett*.*
↑Név Kit. Méret Dátum Attr.
[..] <DIR> 2007.03.08 11:03 ----
[-c-] [névtelen] 1 680 792 k a(z) 4 184 900 k-ból szab
c:\zip\vanquish-0.2.1.zip*.*
↑Név Kit. Méret Dátum Attr.
[..] <DIR> 2007.03.08 11:02 ----
[bin] <DIR> 2004.01.30 14:05 ----
installer cmd 2 722 2004.07.24 17:39 -a--
ReadMe txt 13 703 2005.11.04 17:33 -a--
setup cmd 1 082 2004.07.24 17:12 -a--
A rootkitek többségét ismerik a víruskeresők, emiatt már a rootkit másolásának vagy telepítésének puszta kísérletekor riasztást kapunk.
0 k / 0 k - 0 / 0 fájl
17 k / 17 k - 3 / 3 fájl, 1 / 1 könyvtár
c:\zip>
F3 Nézőke F4 Szerkesztés F5 Másolás F6 Áthely/Átnev. F7 Új könyvtár F8 Törlés Alt+F4 Kilépés
Start
Total Commander 6.5...
HL
11:04

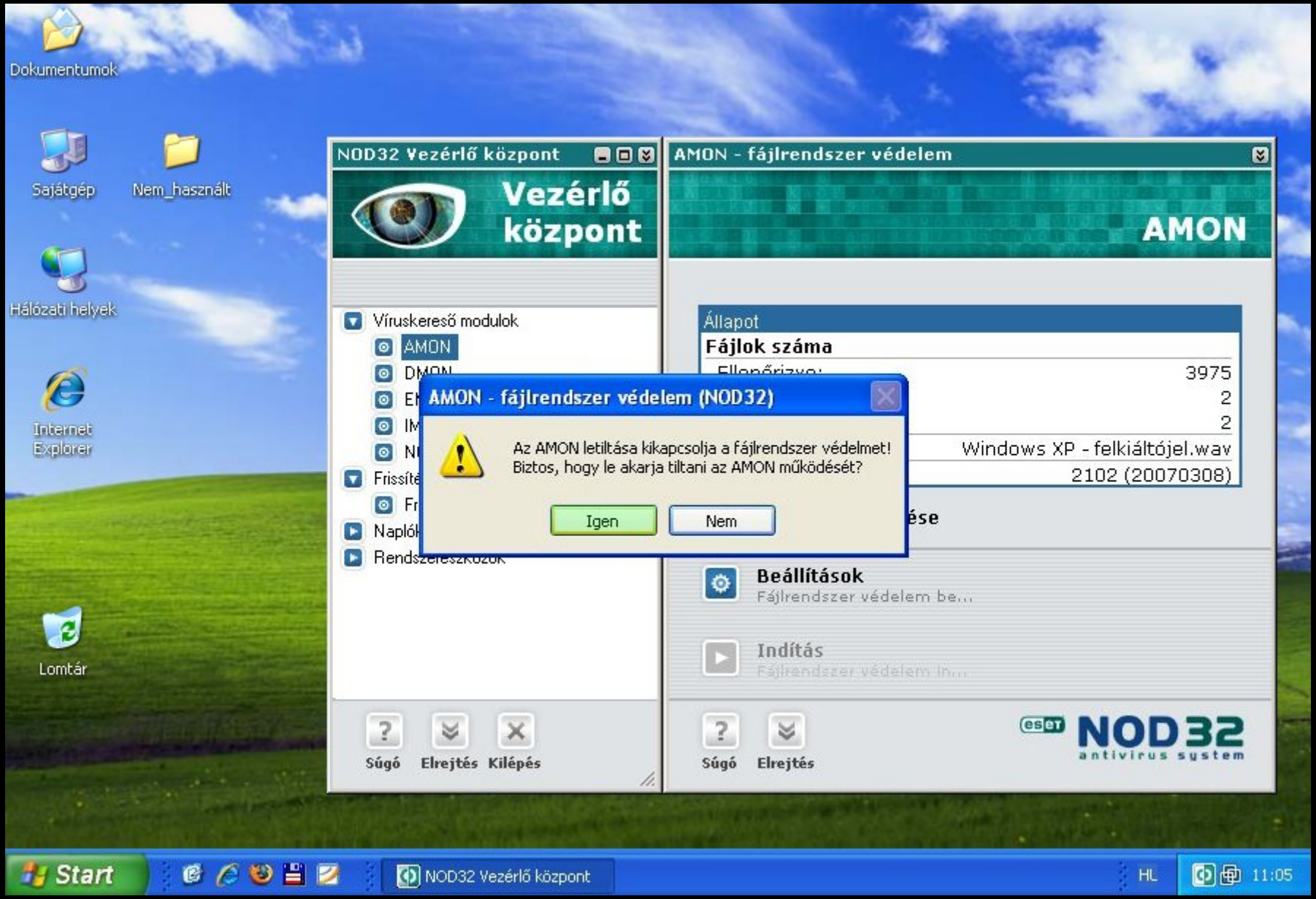


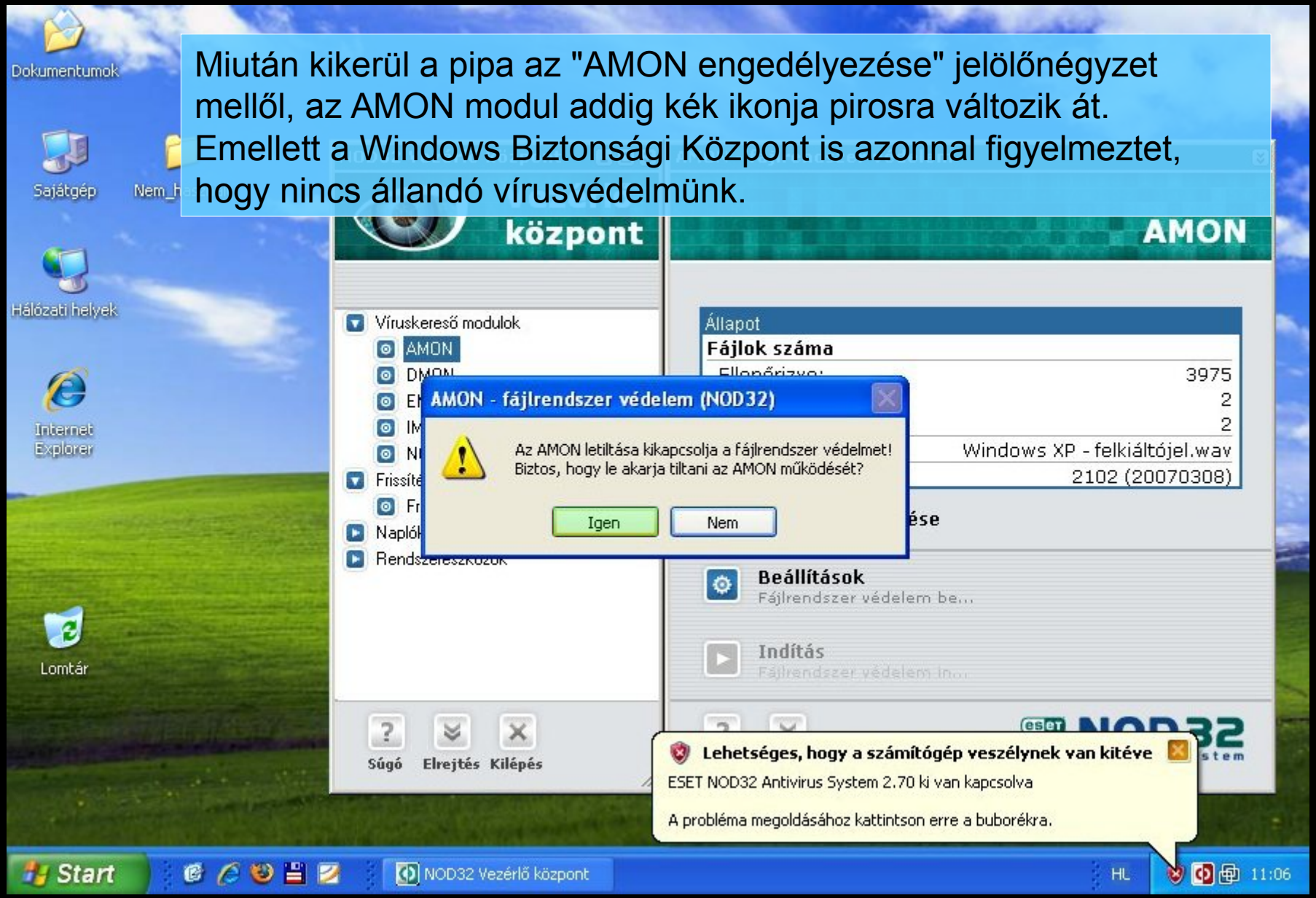
Bekapcsolt valósidejű vírusvédelem mellett - szerencsére - már a bemásolásig sem jutunk el.

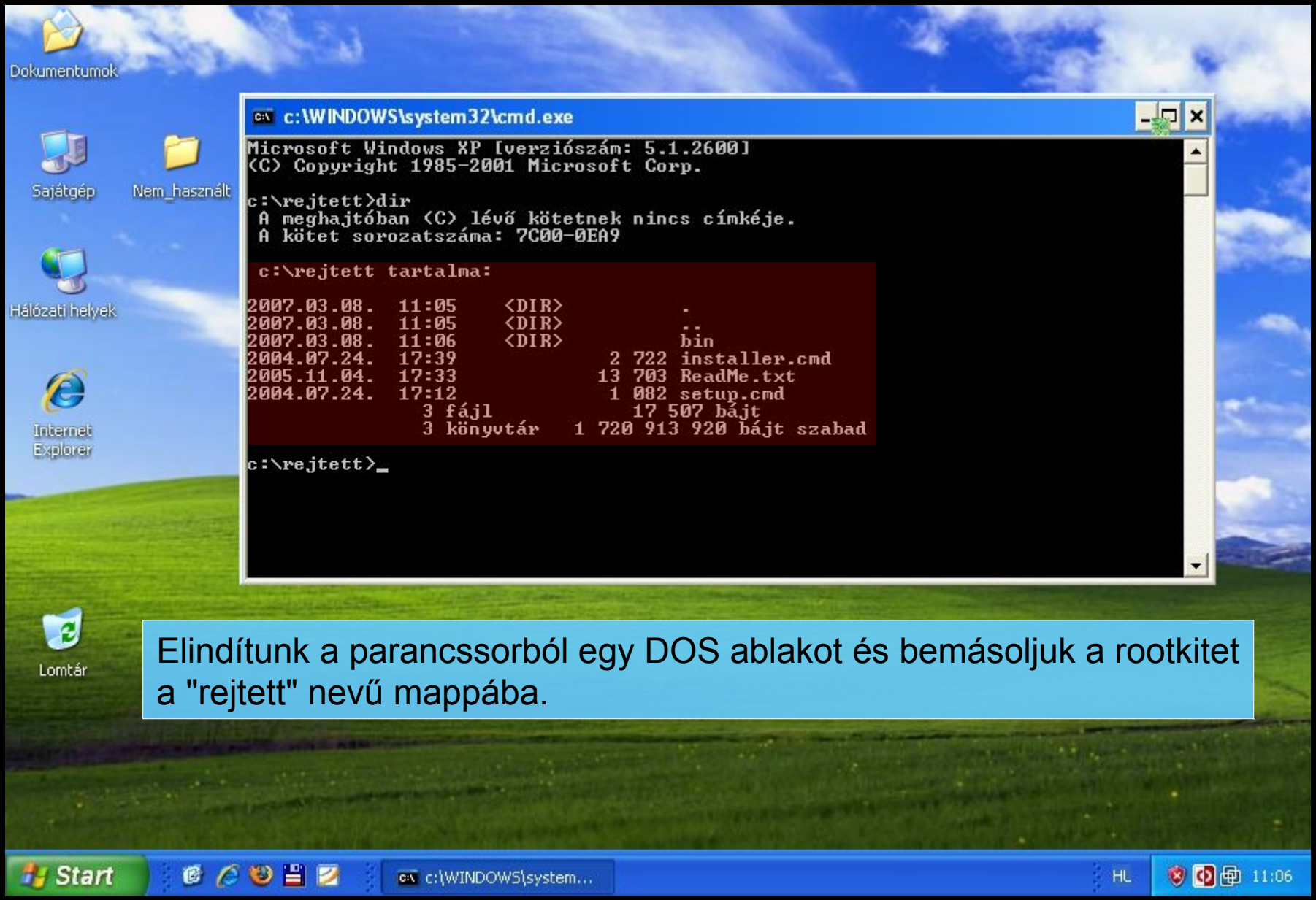

Total Commander 6.55 - NEM REGISZTRÁLT
NOD32 antivirus system riasztás: AMON - fájlrendszer védelem
Riasztás
Részletek
Fájl:
C:\rejtett\bin\vanquish.dll
Vírus:
Win32/PSW.XShadow.B trójai
Megjegyzés:
A riasztást kiváltó alkalmazás (művelet: fájl-létrehozás): C:\totalcmd\TOTALCMD.EXE. A fájl karanténba helyezve. Zárja be ezt az ablakot.
Karanténba helyezés
Riasztási ablak megjelenítése
Elküldés vizsgálatra
Vírusirtás
Törlés
Átnevezés
Az AMON modul haladéktalanul közbelép, riaszt és töröl, illetve karanténba helyez, ha ezt kérjük tőle.
F3 Nézőke
F4 Szerkesztés
F5 Másolás
F6 Áthely/Átnev.
F7 Új könyvtár
F8 Törlés
Alt+F4 Kilépés
Start
Total Commander 6.5...
NOD32 antivirus syst...
HU
11:05


Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Total Commander 6.55 - NEM REGISZTRÁLT
NOD32 antivirus system riasztás: AMON - fájlrendszer védelem
Riasztás
Részletek
Fájl:
C:\rejtett\bin\vanquish.exe
Vírus:
Win32/PSW.XShadow.B 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
Törlés
Átnevezés
Súgó
Bezárás
Info
NOD32 Antivirus System
F3 Nézőke
F4 Szerkesztés
F5 Másolás
F6 Áthely/Átnev.
F7 Új könyvtár
F8 Törlés
Alt+F4 Kilépés
Start
Total Commander 6.5...
NOD32 antivirus syst...
HU
11:05

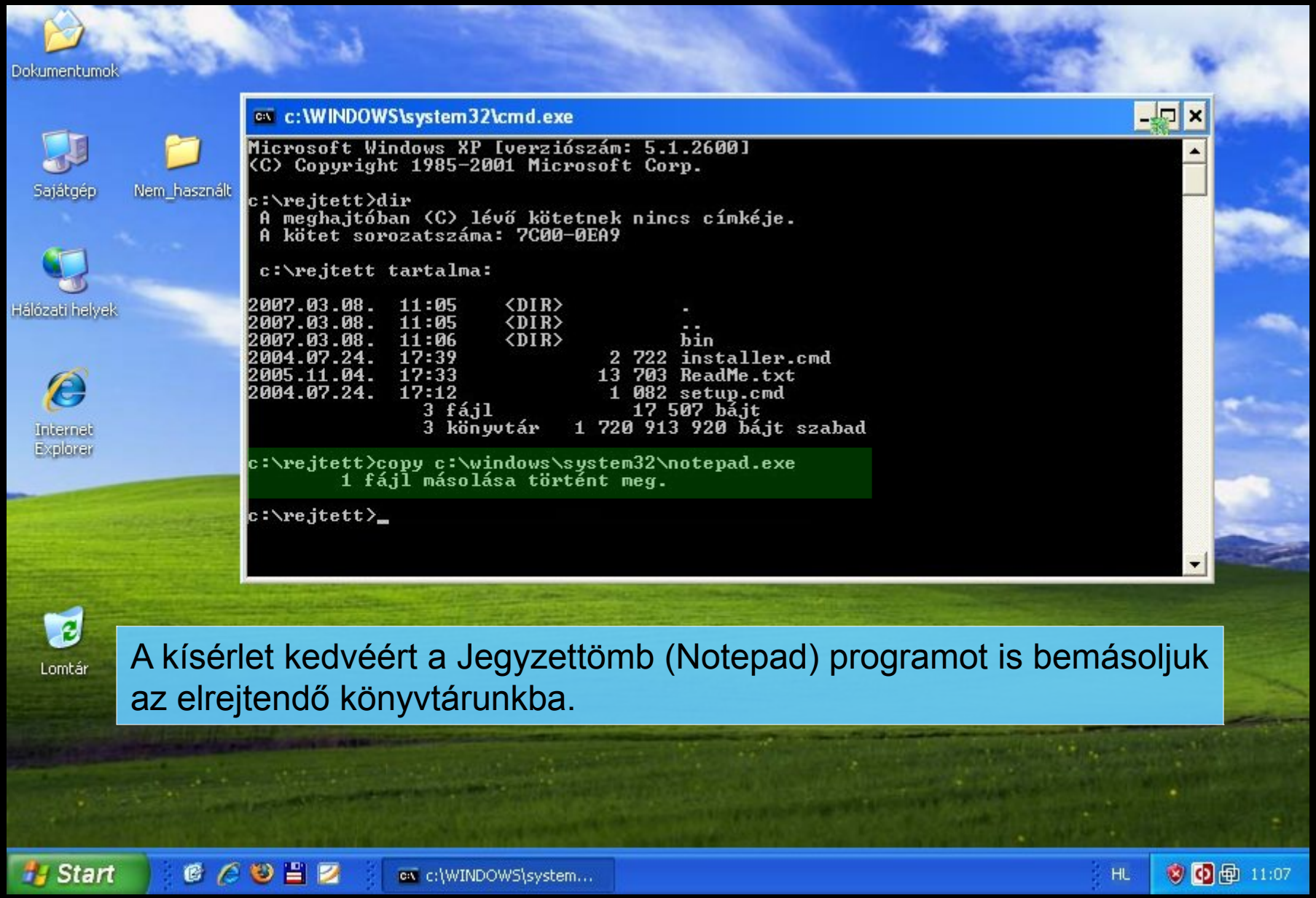

Ezért most ki fogjuk kapcsolni az állandó védelmet ahhoz, hogy bemásolhassuk és telepíteni tudjuk a rootkitet.
Ezt a lépést nem ajánljuk senkinek!
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
központ
AMON
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Állapot
Fájlok száma
Ellenőrizve: 3974
Fertőzött: 2
Megtisztított: 2
Fájlnév: ZAU05UBA.NQI
Vírusadatbázis verzió: 2102 (20070308)
AMON engedélyezése
Beállítások
Fájlrendszer védelem be...
Indítás
Súgó
Elrejtés
Kilépés
Súgó
Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
HL
11:05

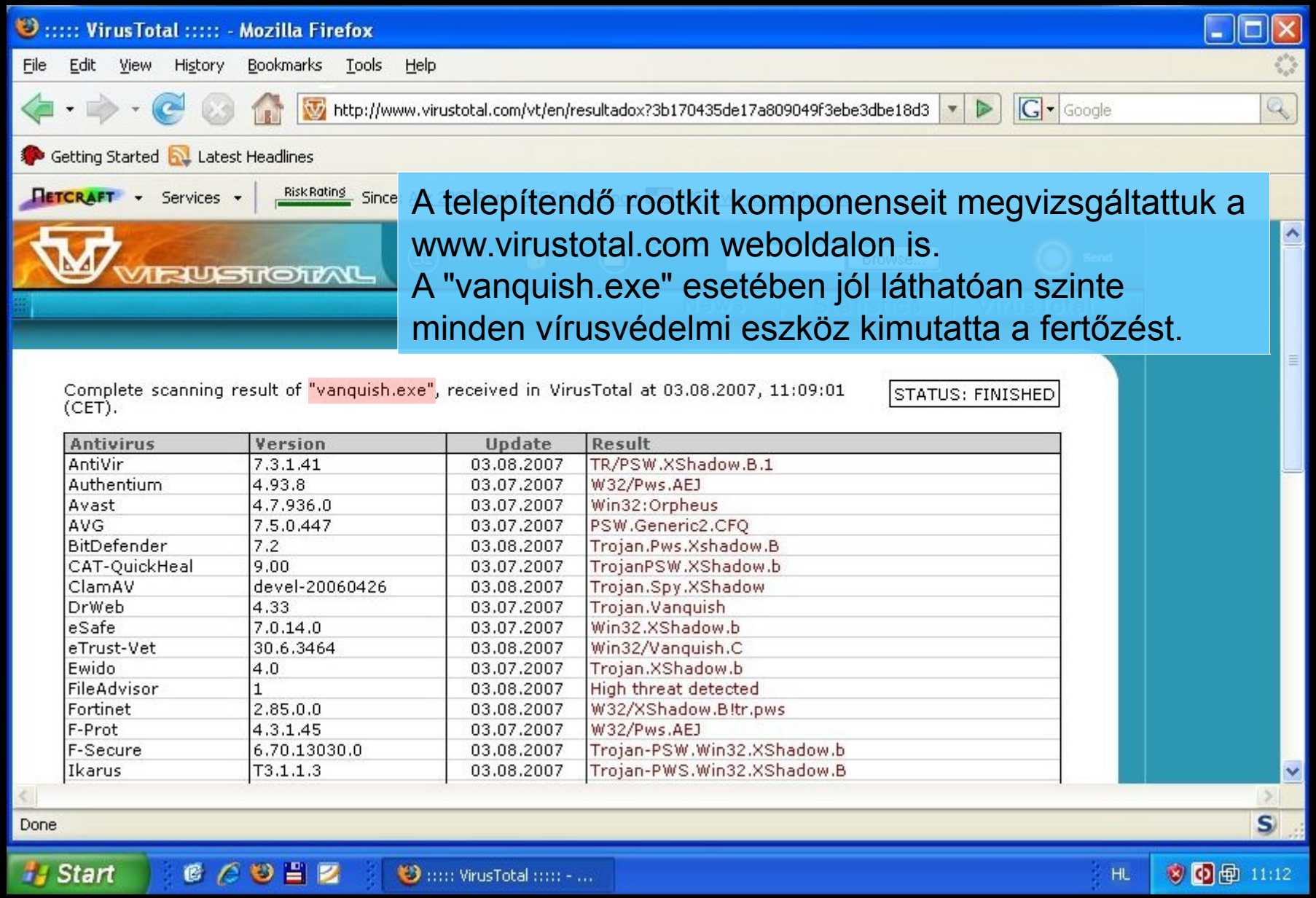

Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
Frissítés
Naplók
Rendszereszközök
Súgó
Elrejtés
Kilépés
AMON - fájlrendszer védelem
AMON
Állapot
Fájlok száma
3975
2
2
Windows XP - felkiáltójel.wav
2102 (20070308)
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
11:05

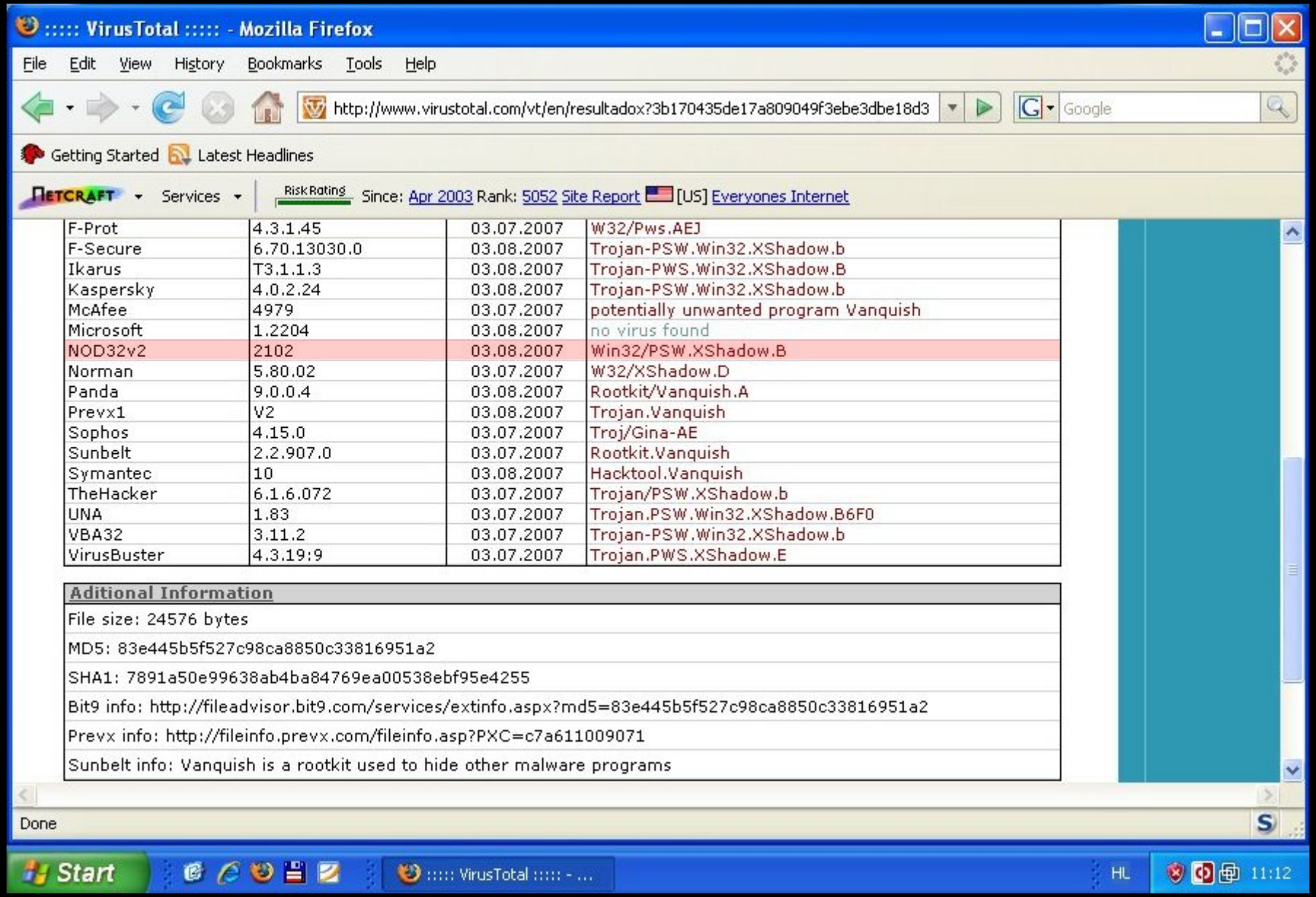

Miután kikerül a pipa az "AMON engedélyezése" jelölőnégyzet mellől, az AMON modul addig kék ikonja pirosra változik át. Emellett a Windows Biztonsági Központ is azonnal figyelmeztet, hogy nincs állandó vírusvédelmünk.
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
központ
AMON
Víruskereső modulok
AMON
Frissíté
Naplók
Rendszereszközök
Állapot
Fájlok száma
3975
2
2
Windows XP - felkiáltójel.wav
2102 (20070308)
AMON - fájlrendszer védelem (NOD32)
Az AMON letiltása kikapcsolja a fájlrendszer védelmet!
Biztos, hogy le akarja tiltani az AMON működését?
Igen
Nem
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
11:06

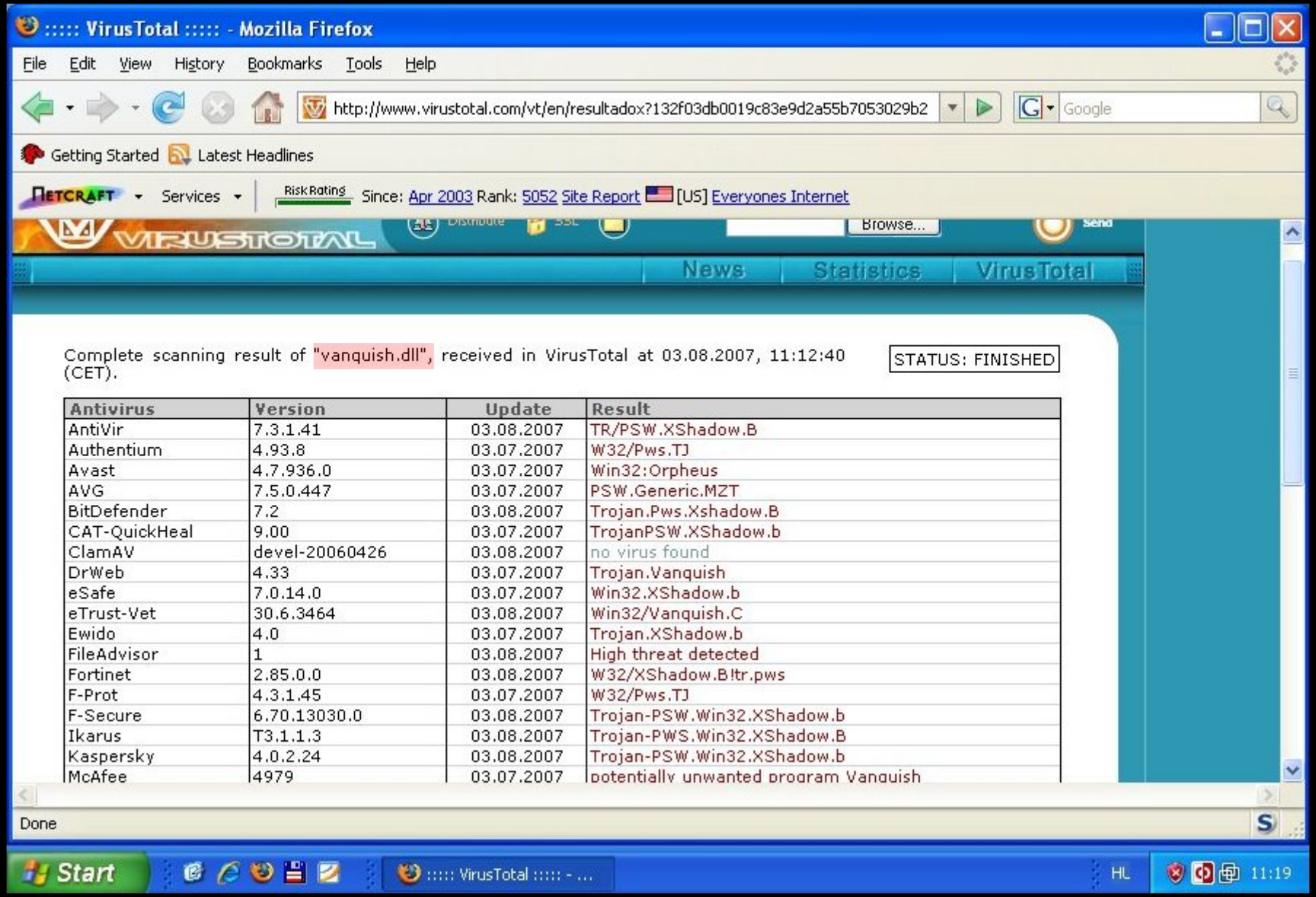


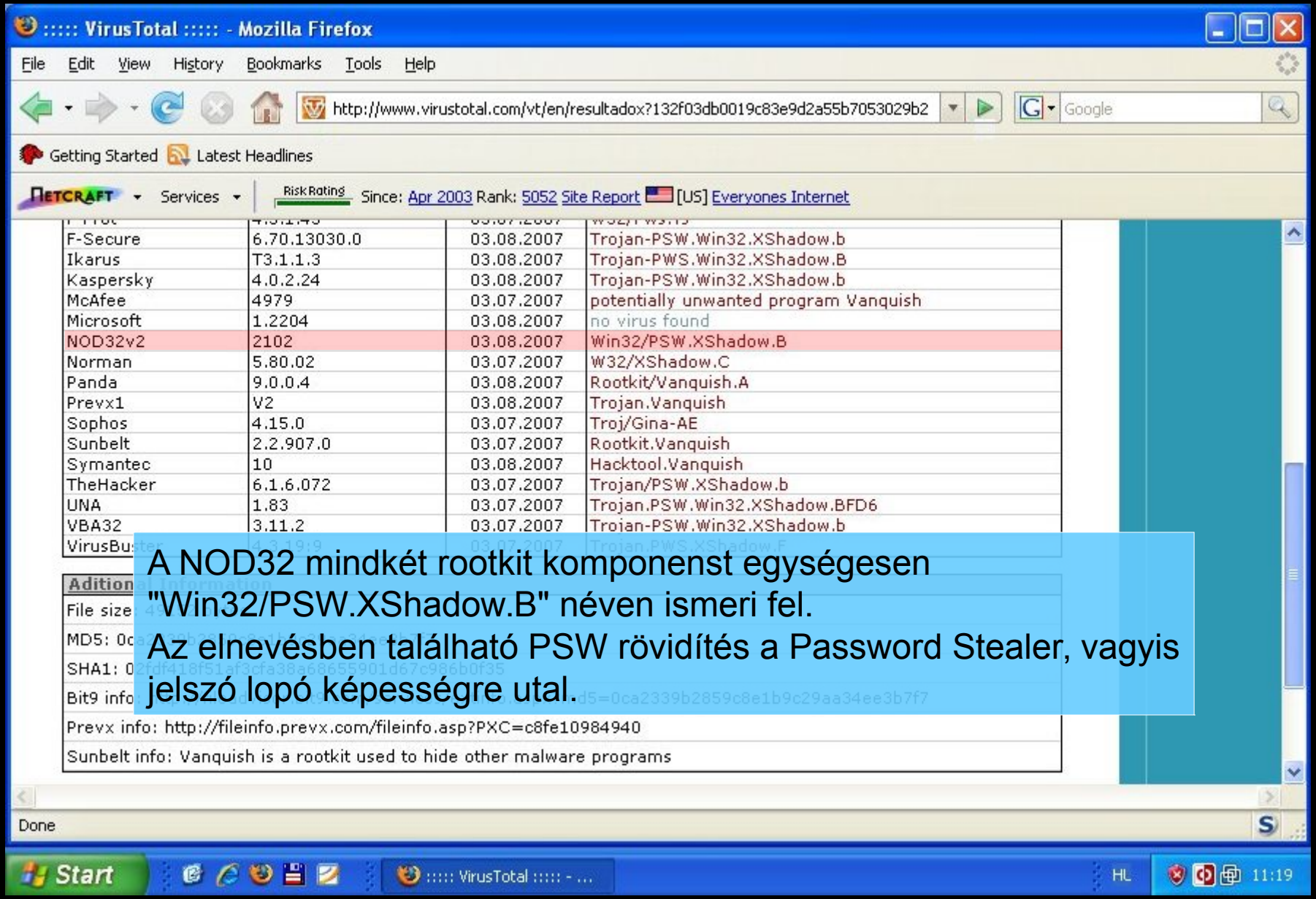
Elindítunk a parancssorból egy DOS ablakot és bemásoljuk a rootkitet a "rejtett" nevű mappába.


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:\rejtett>dir
A meghajtóban (C) lévő kötetnek nincs címkéje.
A kötet sorozatszáma: 7C00-0EA9
c:\rejtett tartalma:
2007.03.08. 11:05 <DIR> .
2007.03.08. 11:05 <DIR> ..
2007.03.08. 11:06 <DIR> bin
2004.07.24. 17:39 2 722 installer.cmd
2005.11.04. 17:33 13 703 ReadMe.txt
2004.07.24. 17:12 1 082 setup.cmd
3 fájl 17 507 bájt
3 könyvtár 1 720 913 920 bájt szabad
c:\rejtett>copy c:\windows\system32\notepad.exe
1 fájl másolása történt meg.
c:\rejtett>
A kísérlet kedvéért a Jegyzettömb (Notepad) programot is bemásoljuk az elrejtendő könyvtárunkba.
Start
c:\WINDOWS\system...
HL
11:07

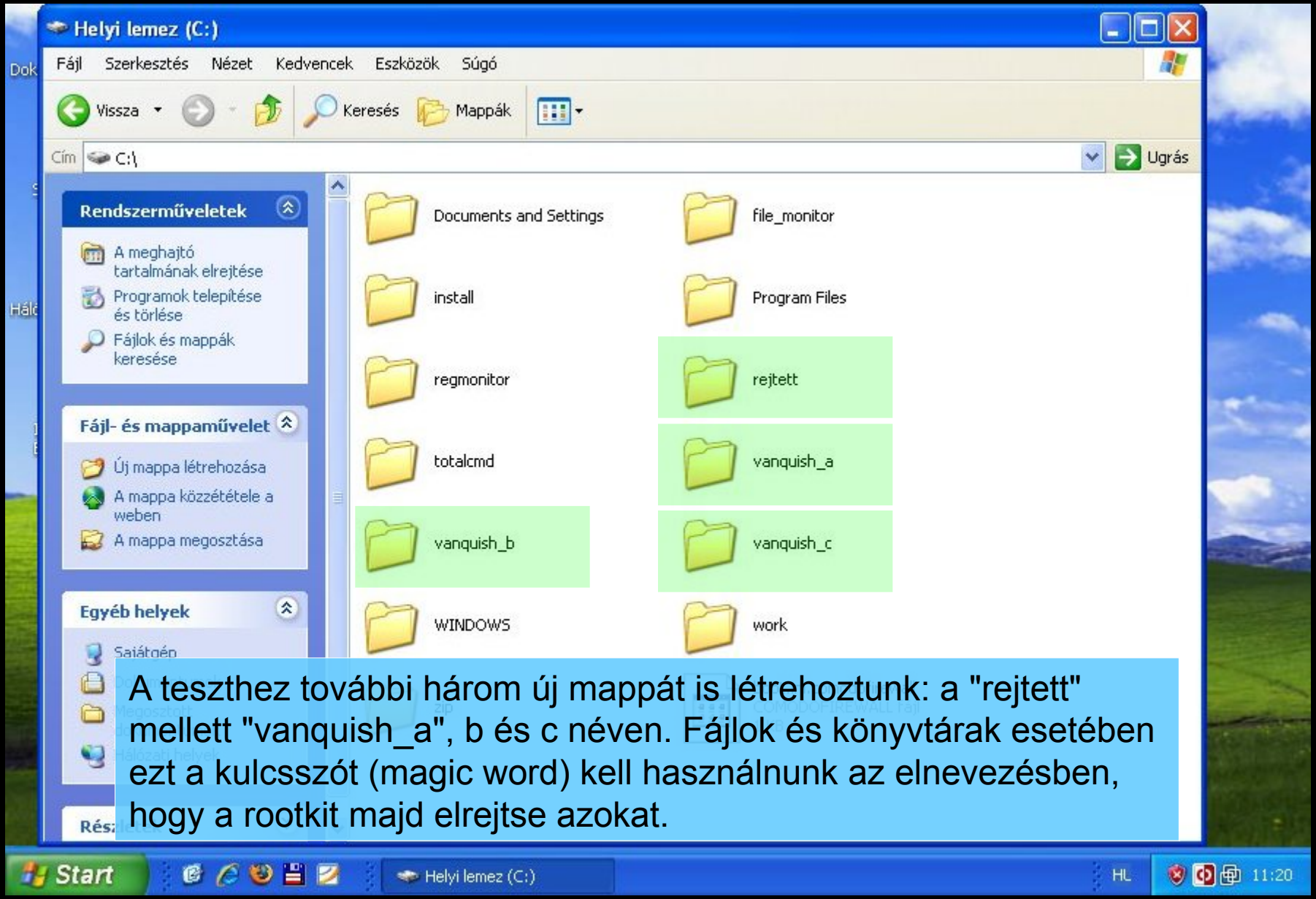

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadox?3b170435de17a809049f3ebe3dbe18d3
Google
Getting Started
Latest Headlines
NETCRAFT
Services
Risk Rating
Since
VIRUSTOTAL
A telepítendő rootkit komponenseit megvizsgáltattuk a www.virustotal.com weboldalon is.
A "vanquish.exe" esetében jól láthatóan szinte minden vírusvédelmi eszköz kimutatta a fertőzést.
Complete scanning result of "vanquish.exe", received in VirusTotal at 03.08.2007, 11:09:01 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.41 | 03.08.2007 | TR/PSW.XShadow.B.1
Authentium | 4.93.8 | 03.07.2007 | W32/Pws.AEJ
Avast | 4.7.936.0 | 03.07.2007 | Win32:Orpheus
AVG | 7.5.0.447 | 03.07.2007 | PSW.Generic2.CFQ
BitDefender | 7.2 | 03.08.2007 | Trojan.Pws.Xshadow.B
CAT-QuickHeal | 9.00 | 03.07.2007 | TrojanPSW.XShadow.b
ClamAV | devel-20060426 | 03.08.2007 | Trojan.Spy.XShadow
DrWeb | 4.33 | 03.07.2007 | Trojan.Vanquish
eSafe | 7.0.14.0 | 03.07.2007 | Win32.XShadow.b
eTrust-Vet | 30.6.3464 | 03.08.2007 | Win32/Vanquish.C
Ewido | 4.0 | 03.07.2007 | Trojan.XShadow.b
FileAdvisor | 1 | 03.08.2007 | High threat detected
Fortinet | 2.85.0.0 | 03.08.2007 | W32/XShadow.B!tr.pws
F-Prot | 4.3.1.45 | 03.07.2007 | W32/Pws.AEJ
F-Secure | 6.70.13030.0 | 03.08.2007 | Trojan-PSW.Win32.XShadow.b
Ikarus | T3.1.1.3 | 03.08.2007 | Trojan-PWS.Win32.XShadow.B
Done
Start
::::: VirusTotal ::::: - ...
HL
11:12

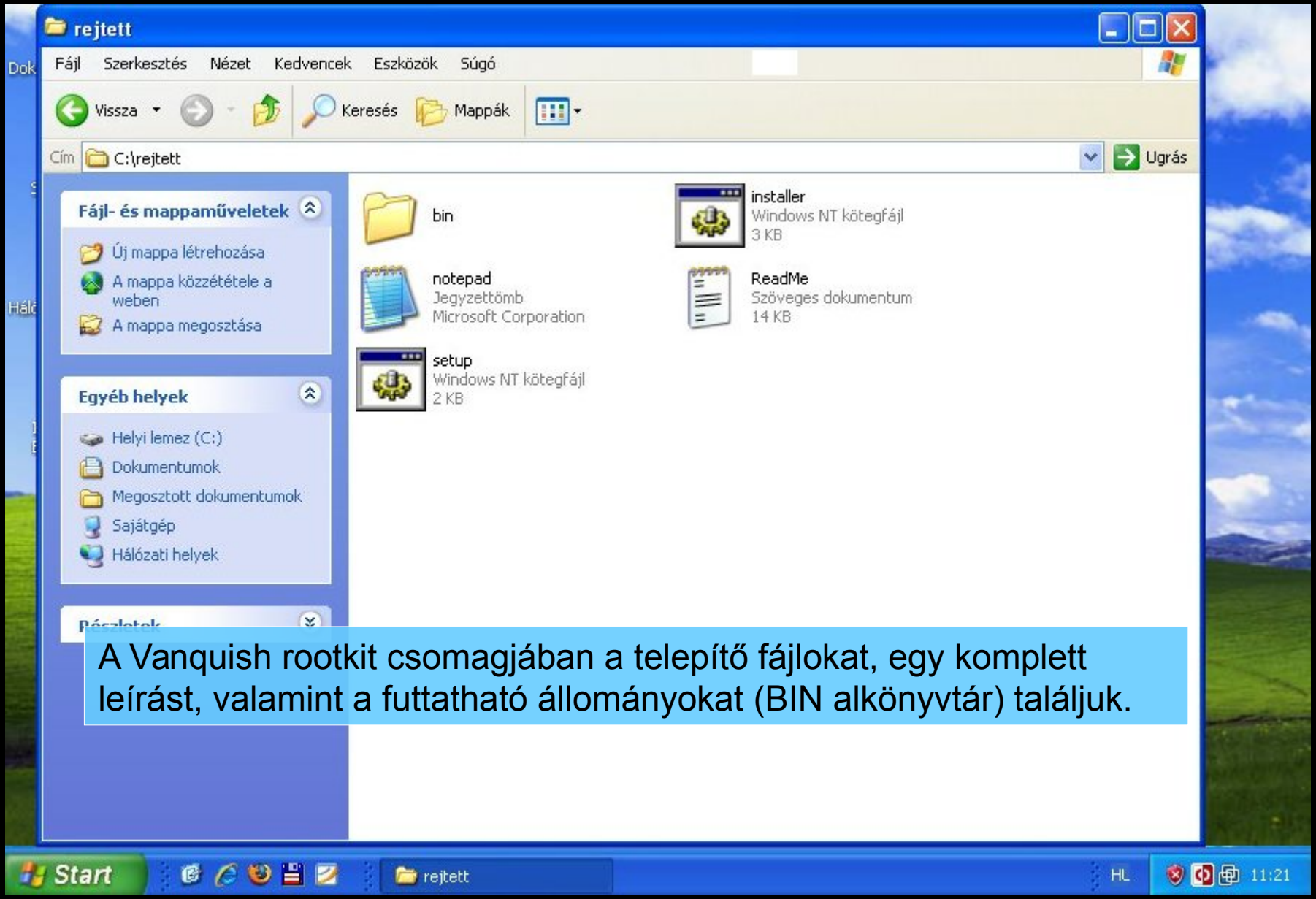

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadox?3b170435de17a809049f3ebe3dbe18d3
Google
Getting Started
Latest Headlines
NETCRAFT
Services
Risk Rating
Since: Apr 2003 Rank: 5052 Site Report [US] Everyones Internet
F-Prot 4.3.1.45 03.07.2007 W32/Pws.AEJ
F-Secure 6.70.13030.0 03.08.2007 Trojan-PSW.Win32.XShadow.b
Ikarus T3.1.1.3 03.08.2007 Trojan-PWS.Win32.XShadow.B
Kaspersky 4.0.2.24 03.08.2007 Trojan-PSW.Win32.XShadow.b
McAfee 4979 03.07.2007 potentially unwanted program Vanquish
Microsoft 1.2204 03.08.2007 no virus found
NOD32v2 2102 03.08.2007 Win32/PSW.XShadow.B
Norman 5.80.02 03.07.2007 W32/XShadow.D
Panda 9.0.0.4 03.08.2007 Rootkit/Vanquish.A
Prevx1 V2 03.08.2007 Trojan.Vanquish
Sophos 4.15.0 03.07.2007 Troj/Gina-AE
Sunbelt 2.2.907.0 03.07.2007 Rootkit.Vanquish
Symantec 10 03.08.2007 Hacktool.Vanquish
TheHacker 6.1.6.072 03.07.2007 Trojan/PSW.XShadow.b
UNA 1.83 03.07.2007 Trojan.PSW.Win32.XShadow.B6F0
VBA32 3.11.2 03.07.2007 Trojan-PSW.Win32.XShadow.b
VirusBuster 4.3.19:9 03.07.2007 Trojan.PWS.XShadow.E
Aditional Information
File size: 24576 bytes
MD5: 83e445b5f527c98ca8850c33816951a2
SHA1: 7891a50e99638ab4ba84769ea00538ebf95e4255
Bit9 info: http://fileadvisor.bit9.com/services/extinfo.aspx?md5=83e445b5f527c98ca8850c33816951a2
Prevx info: http://fileinfo.prevx.com/fileinfo.asp?PXC=c7a611009071
Sunbelt info: Vanquish is a rootkit used to hide other malware programs
Done
Start
::::: VirusTotal ::::: - ...
HL
11:12

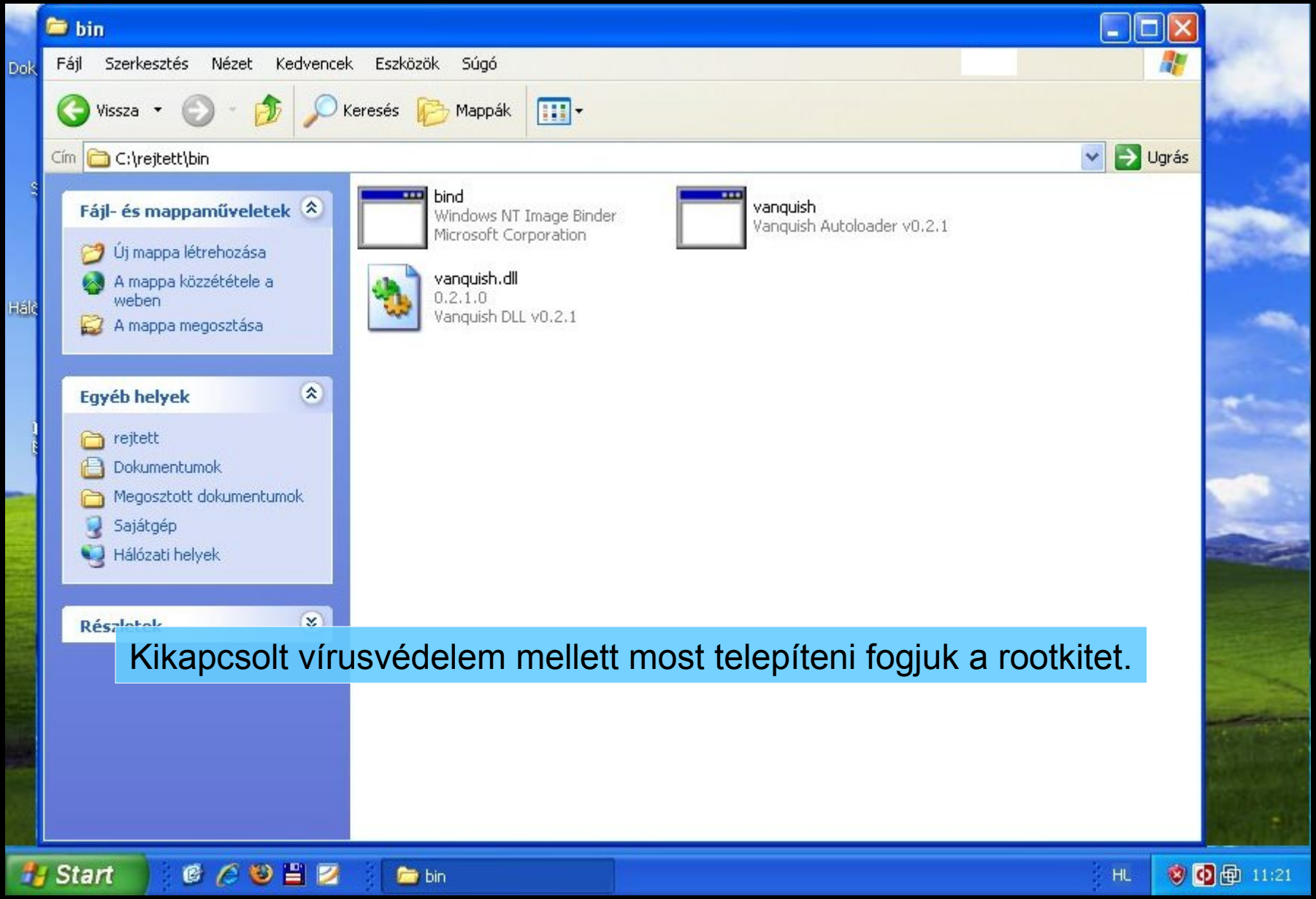

::::: VirusTotal ::::: - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.virustotal.com/vt/en/resultadox?132f03db0019c83e9d2a55b7053029b2
Google
Getting Started Latest Headlines
NETCRAFT Services Risk Rating Since: Apr 2003 Rank: 5052 Site Report [US] Everyones Internet
VIRUSTOTAL
Browse...
News Statistics VirusTotal
Complete scanning result of "vanquish.dll", received in VirusTotal at 03.08.2007, 11:12:40 (CET).
STATUS: FINISHED
Antivirus | Version | Update | Result
AntiVir | 7.3.1.41 | 03.08.2007 | TR/PSW.XShadow.B
Authentium | 4.93.8 | 03.07.2007 | W32/Pws.TJ
Avast | 4.7.936.0 | 03.07.2007 | Win32:Orpheus
AVG | 7.5.0.447 | 03.07.2007 | PSW.Generic.MZT
BitDefender | 7.2 | 03.08.2007 | Trojan.Pws.Xshadow.B
CAT-QuickHeal | 9.00 | 03.07.2007 | TrojanPSW.XShadow.b
ClamAV | devel-20060426 | 03.08.2007 | no virus found
DrWeb | 4.33 | 03.07.2007 | Trojan.Vanquish
eSafe | 7.0.14.0 | 03.07.2007 | Win32.XShadow.b
eTrust-Vet | 30.6.3464 | 03.08.2007 | Win32/Vanquish.C
Ewido | 4.0 | 03.07.2007 | Trojan.XShadow.b
FileAdvisor | 1 | 03.08.2007 | High threat detected
Fortinet | 2.85.0.0 | 03.08.2007 | W32/XShadow.B!tr.pws
F-Prot | 4.3.1.45 | 03.07.2007 | W32/Pws.TJ
F-Secure | 6.70.13030.0 | 03.08.2007 | Trojan-PSW.Win32.XShadow.b
Ikarus | T3.1.1.3 | 03.08.2007 | Trojan-PWS.Win32.XShadow.B
Kaspersky | 4.0.2.24 | 03.08.2007 | Trojan-PSW.Win32.XShadow.b
McAfee | 4979 | 03.07.2007 | potentially unwanted program Vanquish
Done
Start
::::: VirusTotal ::::: - ...
HL
11:19

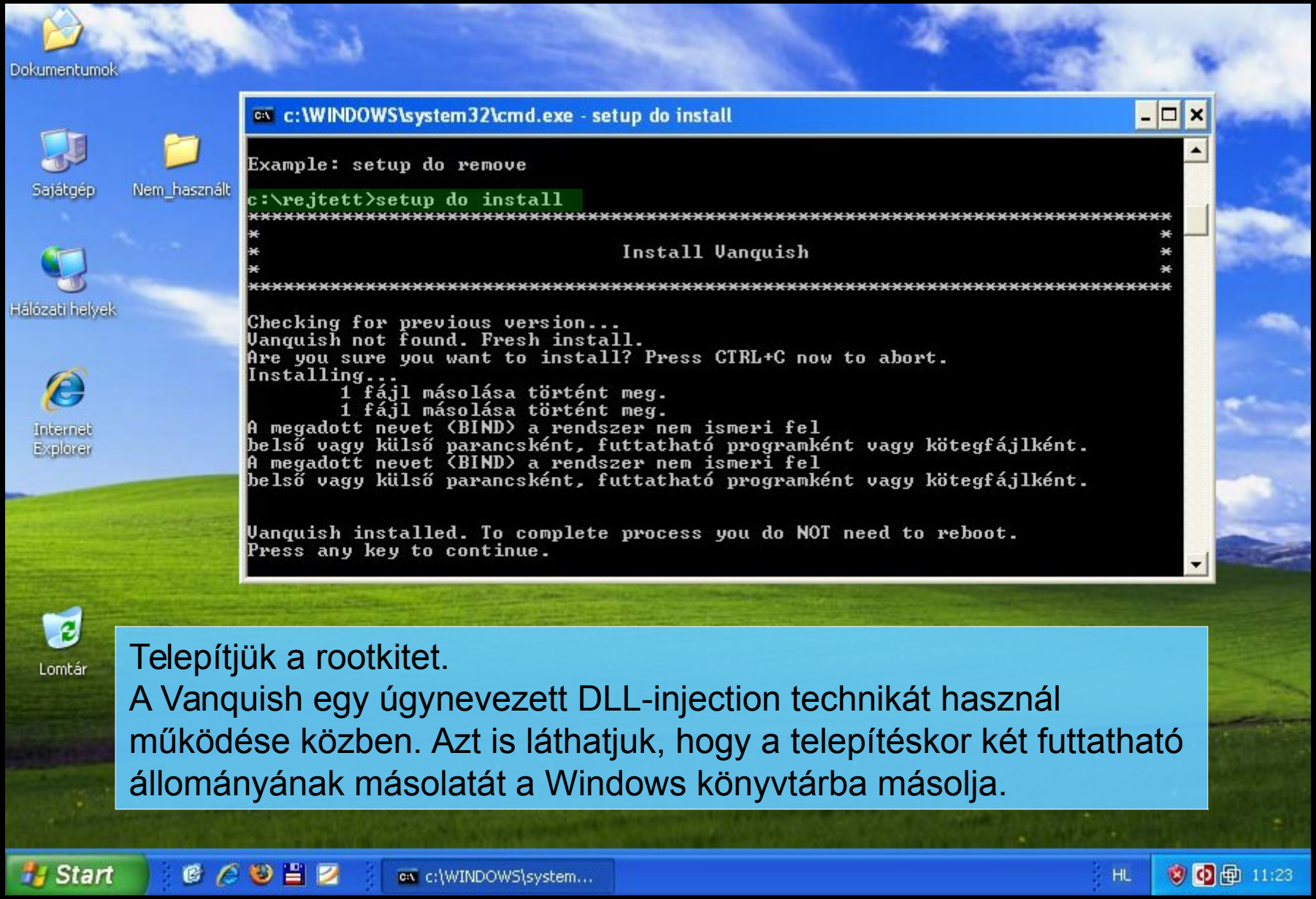


A NOD32 mindkét rootkit komponenst egységesen "Win32/PSW.XShadow.B" néven ismeri fel.
Az elnevésben található PSW rövidítés a Password Stealer, vagyis jelszó lopó képességre utal.

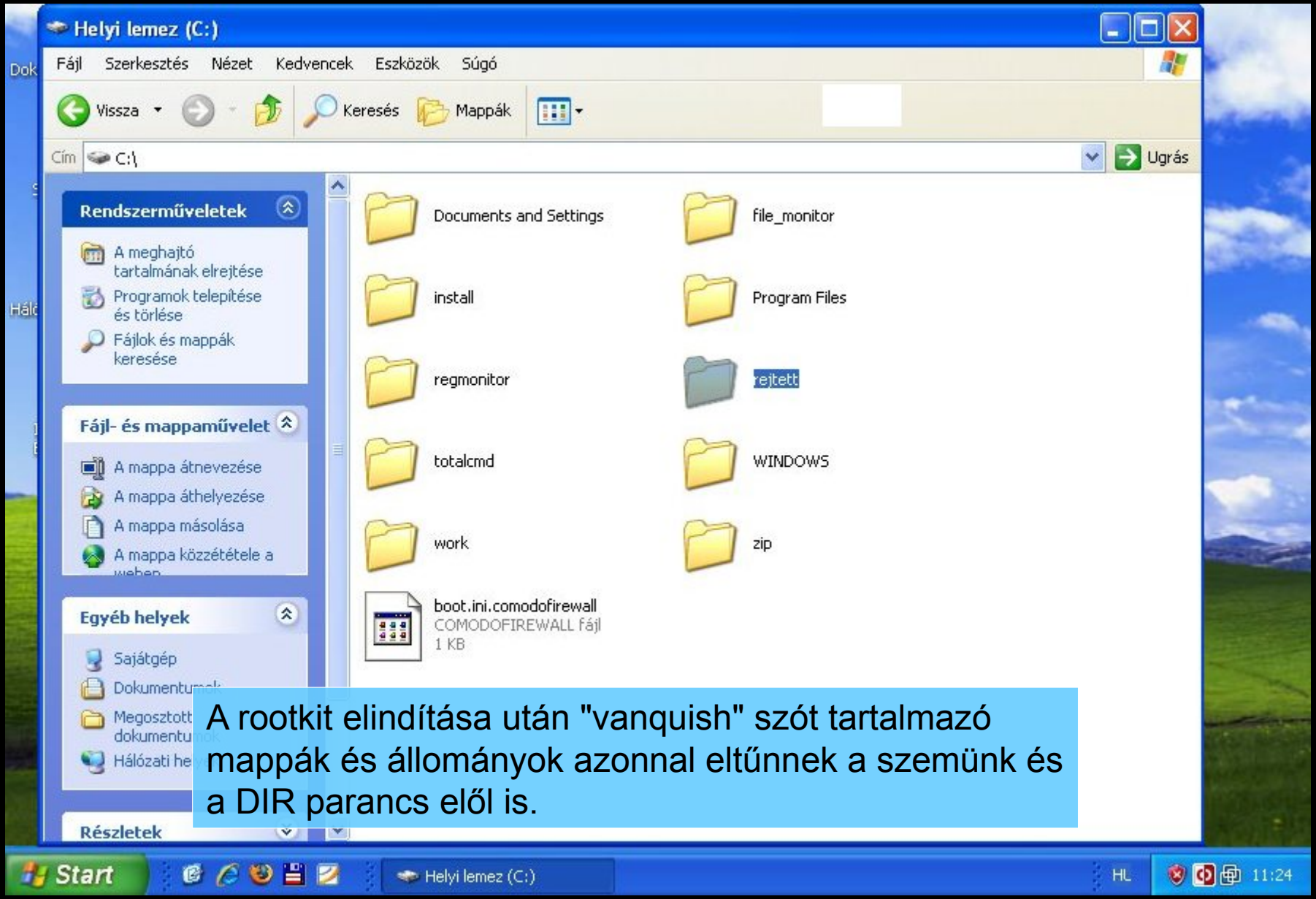

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
Documents and Settings
file_monitor
install
Program Files
regmonitor
rejtett
totalcmd
vanquish_a
vanquish_b
vanquish_c
WINDOWS
work
A teszthez további három új mappát is létrehoztunk: a "rejtett" mellett "vanquish_a", b és c néven. Fájlok és könyvtárak esetében ezt a kulcsszót (magic word) kell használnunk az elnevezésben, hogy a rootkit majd elrejtse azokat.
Start
Helyi lemez (C:)
HL
11:20

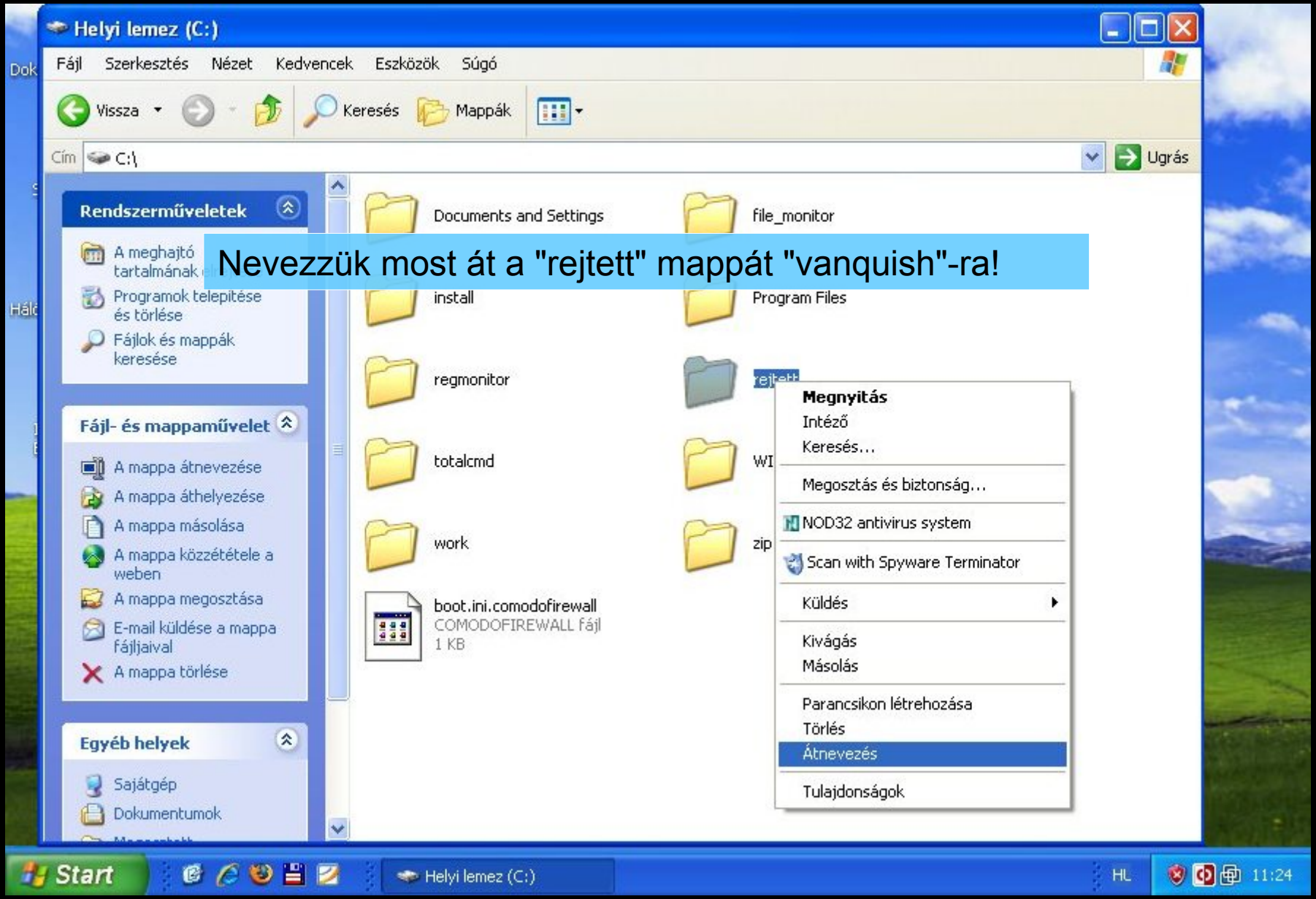

rejtett
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\rejtett
Ugrás
Fájl- és mappaműveletek
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
Helyi lemez (C:)
Dokumentumok
Megosztott dokumentumok
Sajátgép
Hálózati helyek
bin
installer
Windows NT kötegfájl
3 KB
notepad
Jegyzettömb
Microsoft Corporation
ReadMe
Szöveges dokumentum
14 KB
setup
Windows NT kötegfájl
2 KB
A Vanquish rootkit csomagjában a telepítő fájlokat, egy komplett leírást, valamint a futtatható állományokat (BIN alkönyvtár) találjuk.
Start
rejtett
HL
11:21

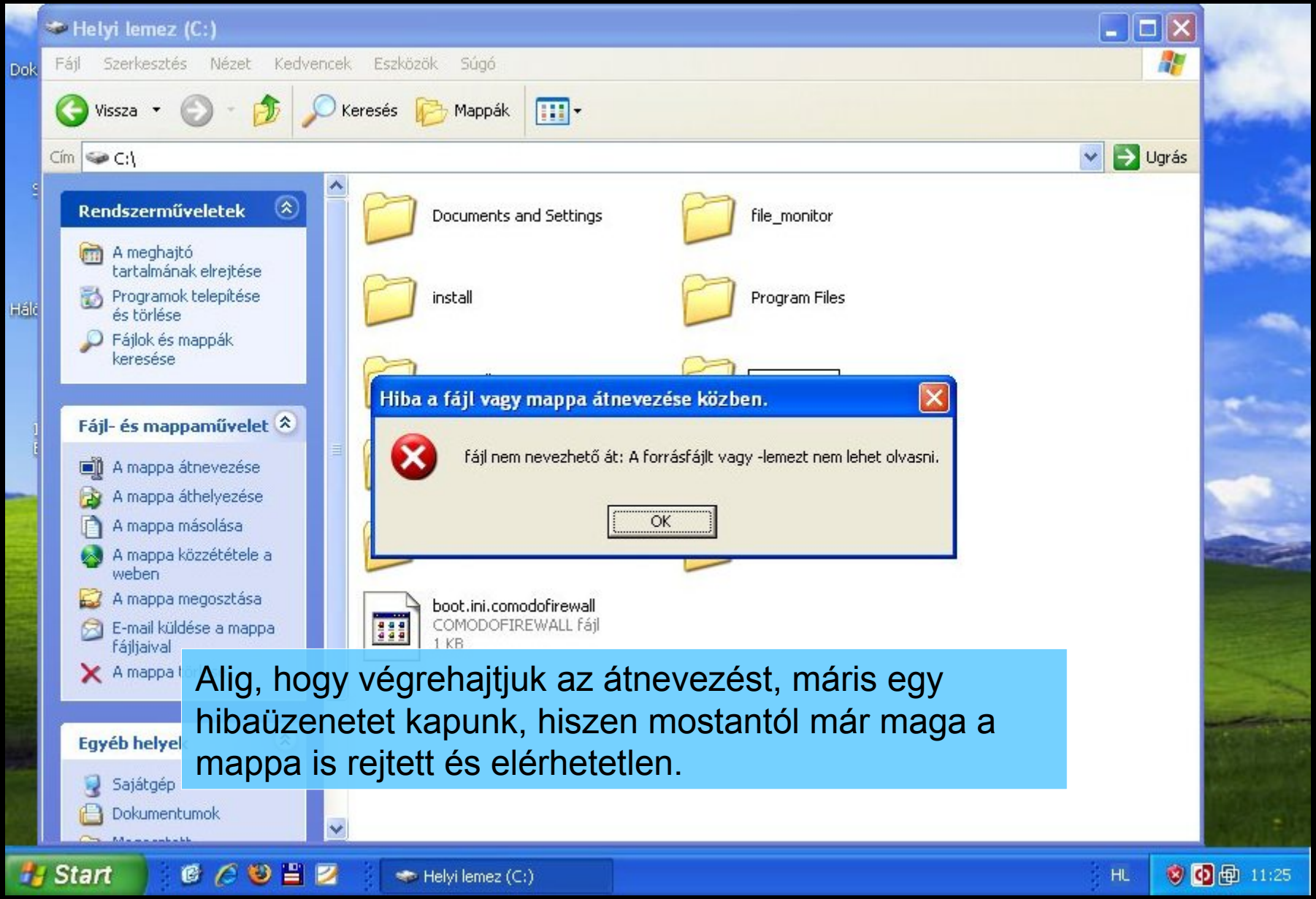

bin
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím
C:\rejtett\bin
Ugrás
Fájl- és mappaműveletek
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
rejtett
Dokumentumok
Megosztott dokumentumok
Sajátgép
Hálózati helyek
bind
Windows NT Image Binder
Microsoft Corporation
vanquish
Vanquish Autoloader v0.2.1
vanquish.dll
0.2.1.0
Vanquish DLL v0.2.1
Kikapcsolt vírusvédelem mellett most telepíteni fogjuk a rootkitet.
Start
bin
HL
11:21



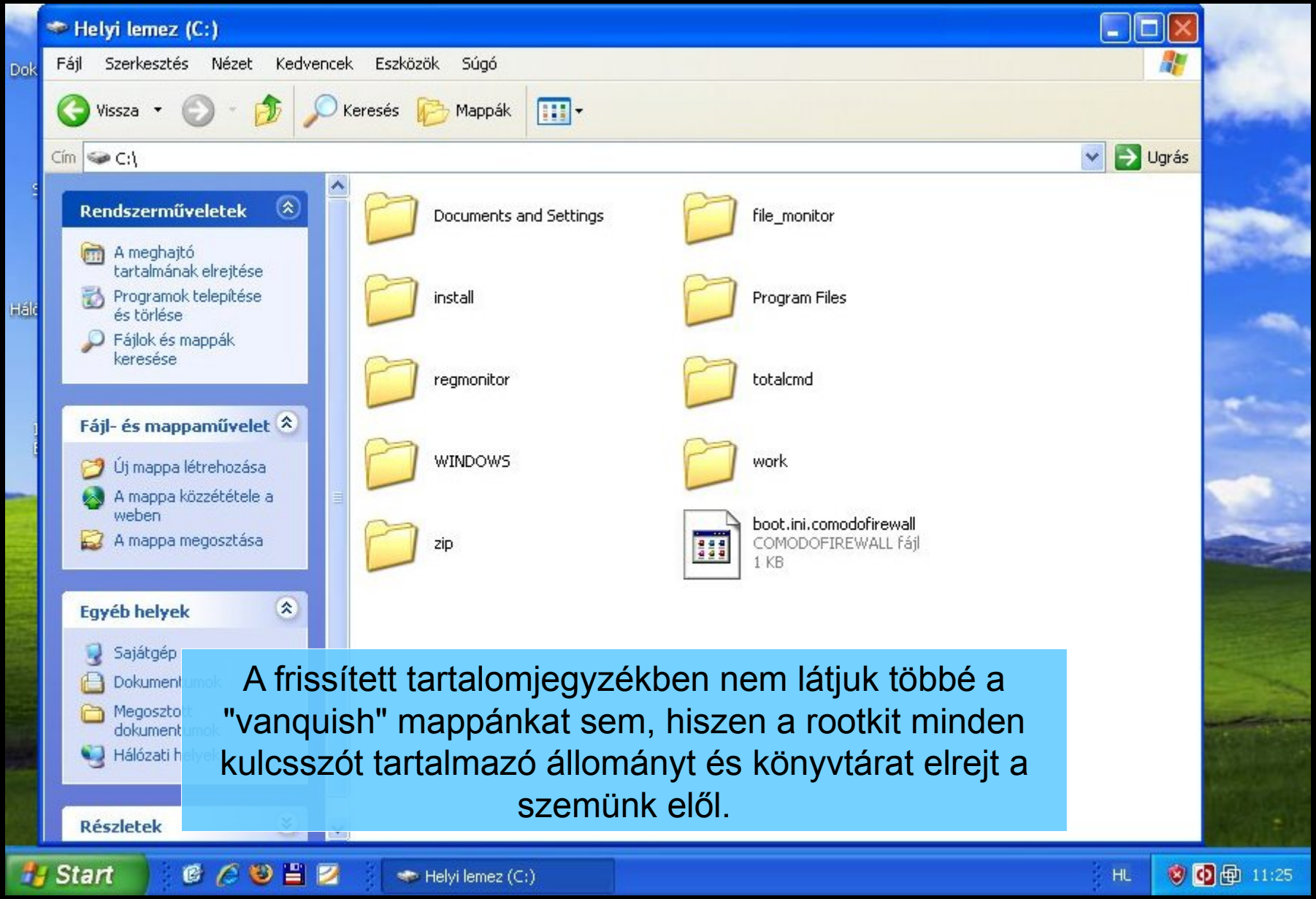
Telepítjük a rootkitet.
A Vanquish egy úgynevezett DLL-injection technikát használ működése közben. Azt is láthatjuk, hogy a telepítéskor két futtatható állományának másolatát a Windows könyvtárba másolja.

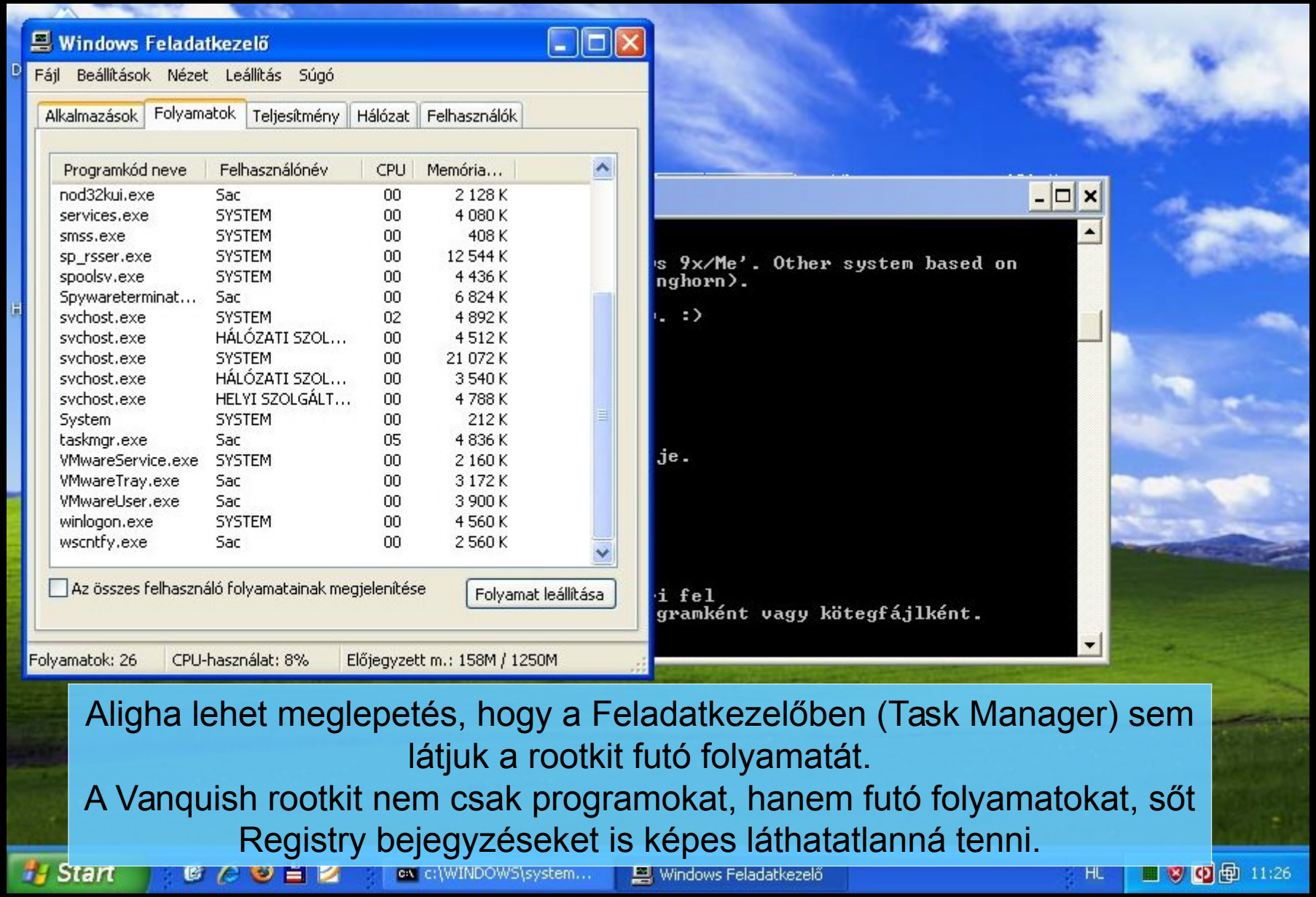

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
A mappa átnevezése
A mappa áthelyezése
A mappa másolása
A mappa közzététele a weben
Egyéb helyek
Sajátgép
Dokumentumok
Megosztott dokumentumok
Hálózati helyek
Részletek
Documents and Settings
file_monitor
install
Program Files
regmonitor
rejtett
totalcmd
WINDOWS
work
zip
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
A rootkit elindítása után "vanquish" szót tartalmazó mappák és állományok azonnal eltűnnek a szemünk és a DIR parancs elől is.
Start
Helyi lemez (C:)
HL
11:24


Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának
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
regmonitor
totalcmd
work
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
Nevezzük most át a "rejtett" mappát "vanquish"-ra!
Megnyitás
Intéző
Keresés...
Megosztás és biztonság...
NOD32 antivirus system
Scan with Spyware Terminator
Küldés
Kivágás
Másolás
Parancsikon létrehozása
Törlés
Átnevezés
Tulajdonságok
Start
Helyi lemez (C:)
HL
11:24

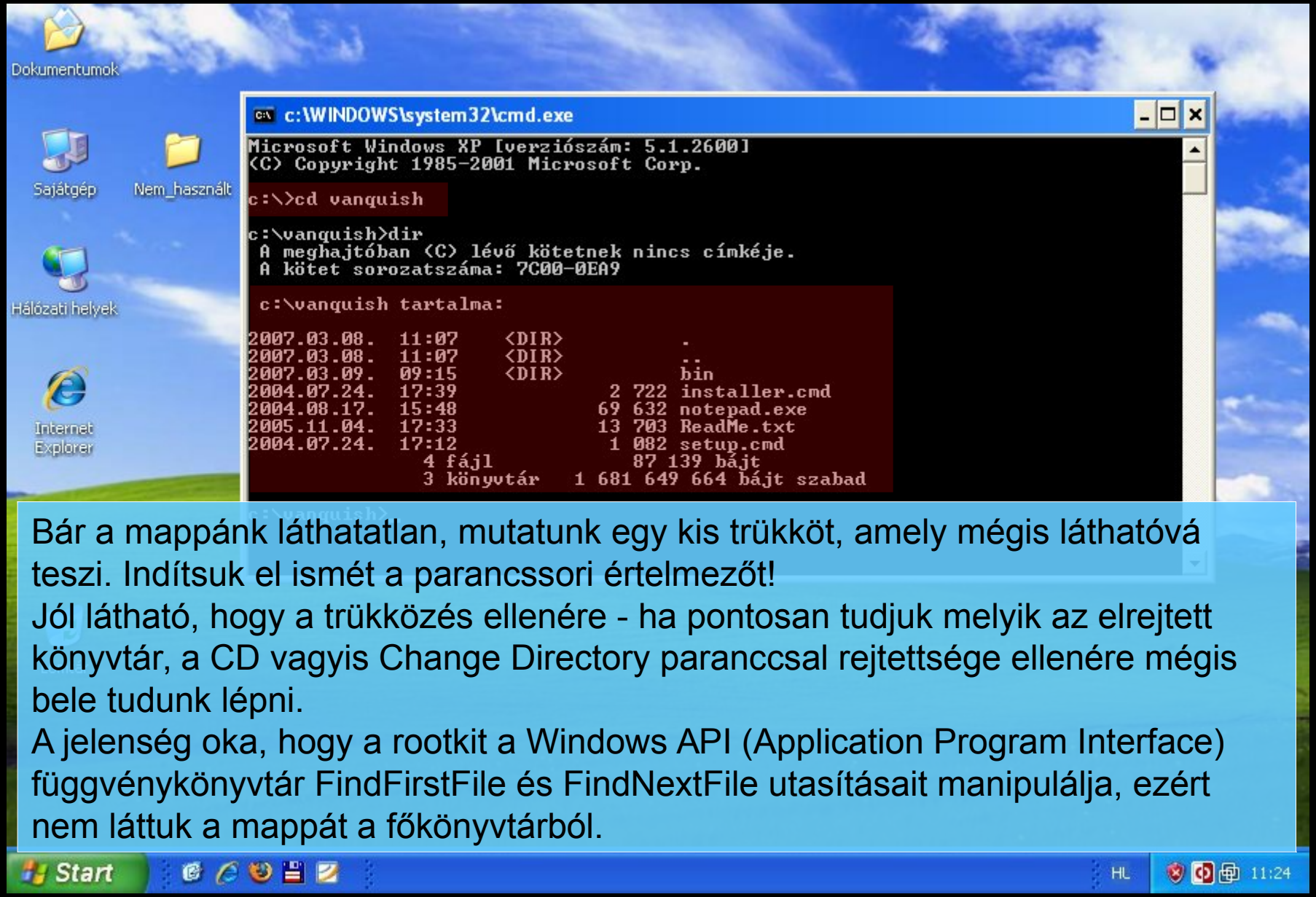


Alig, hogy végrehajtjuk az átnevezést, máris egy hibaüzenetet kapunk, hiszen mostantól már maga a mappa is rejtett és elérhetetlen.

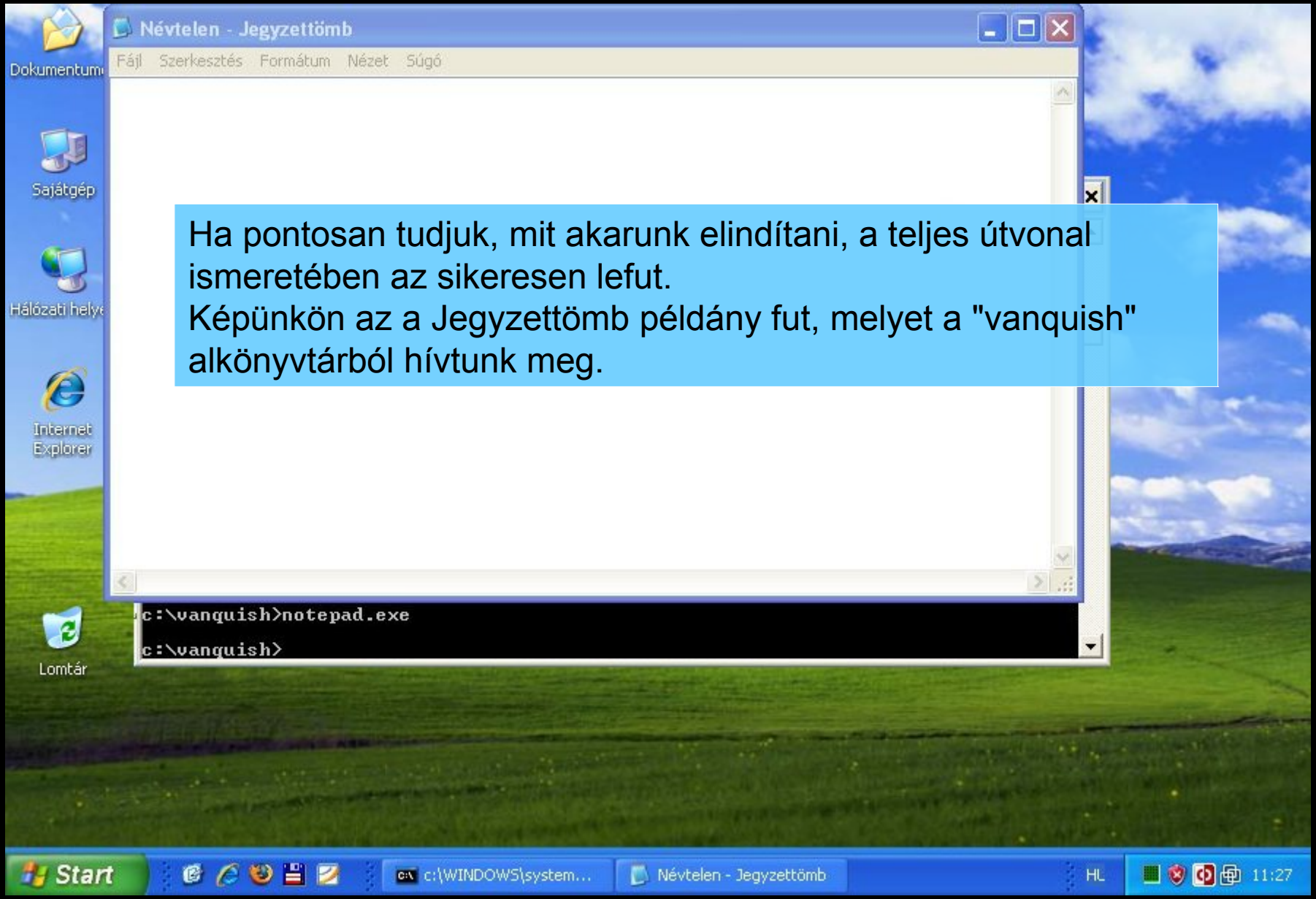

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\
Ugrás
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
Sajátgép
Hálózati helyek
Részletek
Documents and Settings
file_monitor
install
Program Files
regmonitor
totalcmd
WINDOWS
work
zip
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
A frissített tartalomjegyzékben nem látjuk többé a "vanquish" mappánkat sem, hiszen a rootkit minden kulcsszót tartalmazó állományt és könyvtárat elrejt a szemünk elől.
Start
Helyi lemez (C:)
HL
11:25

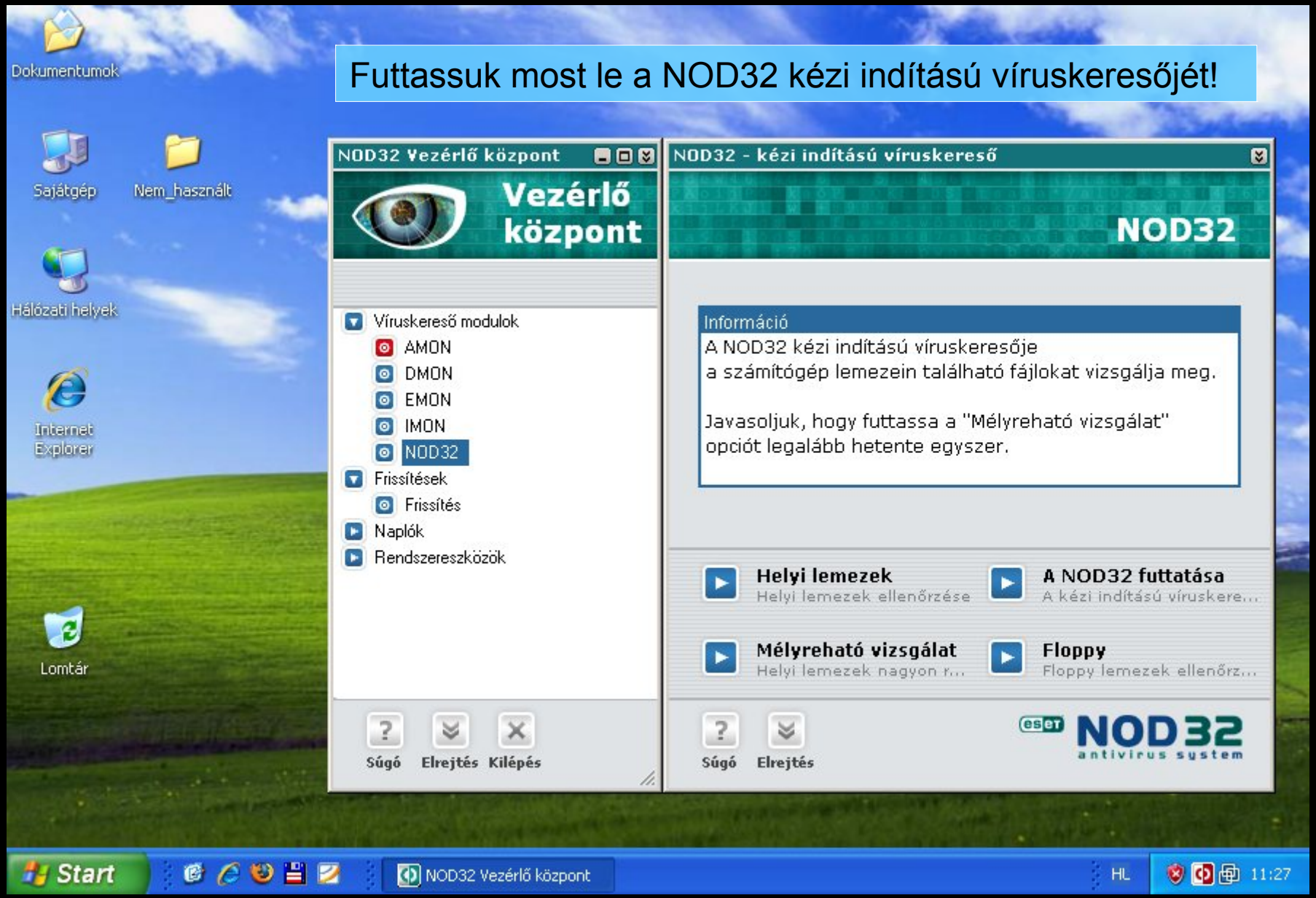


Aligha lehet meglepetés, hogy a Feladatkezelőben (Task Manager) sem látjuk a rootkit futó folyamatát.
A Vanquish rootkit nem csak programokat, hanem futó folyamatokat, sőt Registry bejegyzéseket is képes láthatatlanná tenni.

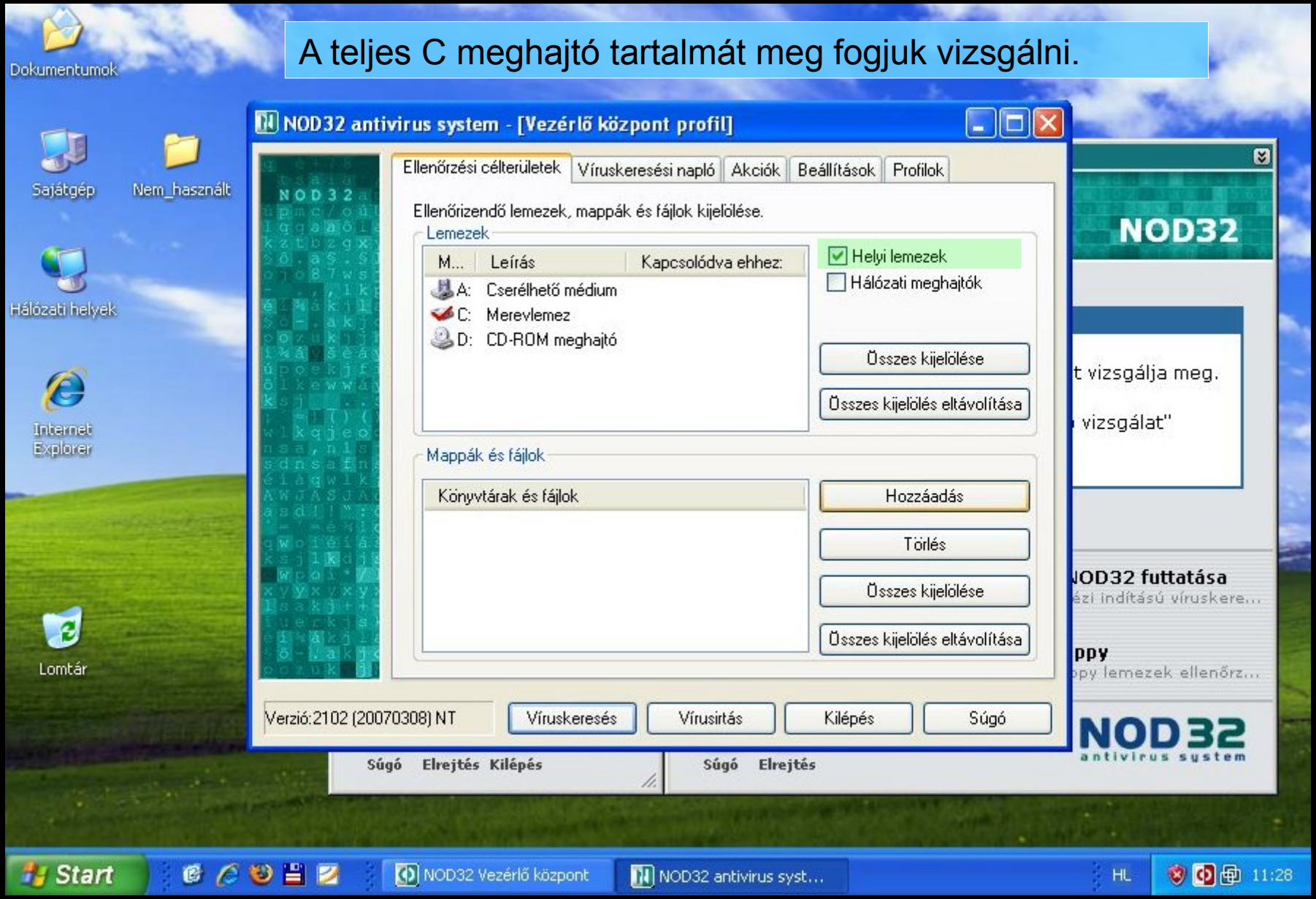


Bár a mappánk láthatatlan, mutatunk egy kis trükköt, amely mégis láthatóvá teszi. Indítsuk el ismét a parancssori értelmezőt!
Jól látható, hogy a trükközés ellenére - ha pontosan tudjuk melyik az elrejtett könyvtár, a CD vagyis Change Directory paranccsal rejtettsége ellenére mégis bele tudunk lépni.
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.

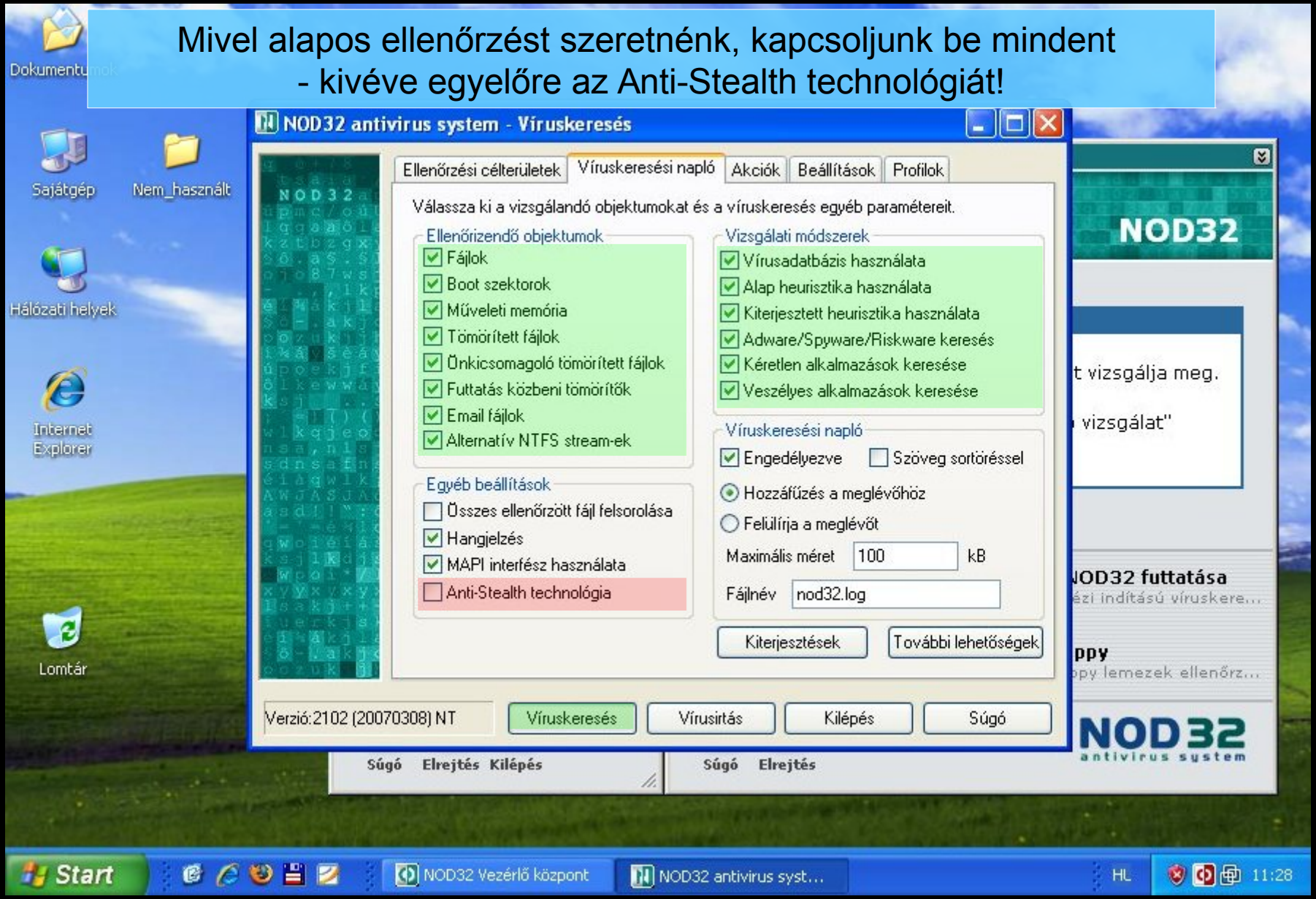

Névtelen - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó
Ha pontosan tudjuk, mit akarunk elindítani, a teljes útvonal ismeretében az sikeresen lefut.
Képünkön az a Jegyzettömb példány fut, melyet a "vanquish" alkönyvtárból hívtunk meg.
c:\vanquish>notepad.exe
c:\vanquish>
Dokumentum
Sajátgép
Hálózati helye
Internet Explorer
Lomtár
Start
c:\WINDOWS\system...
Névtelen - Jegyzettömb
HL
11:27

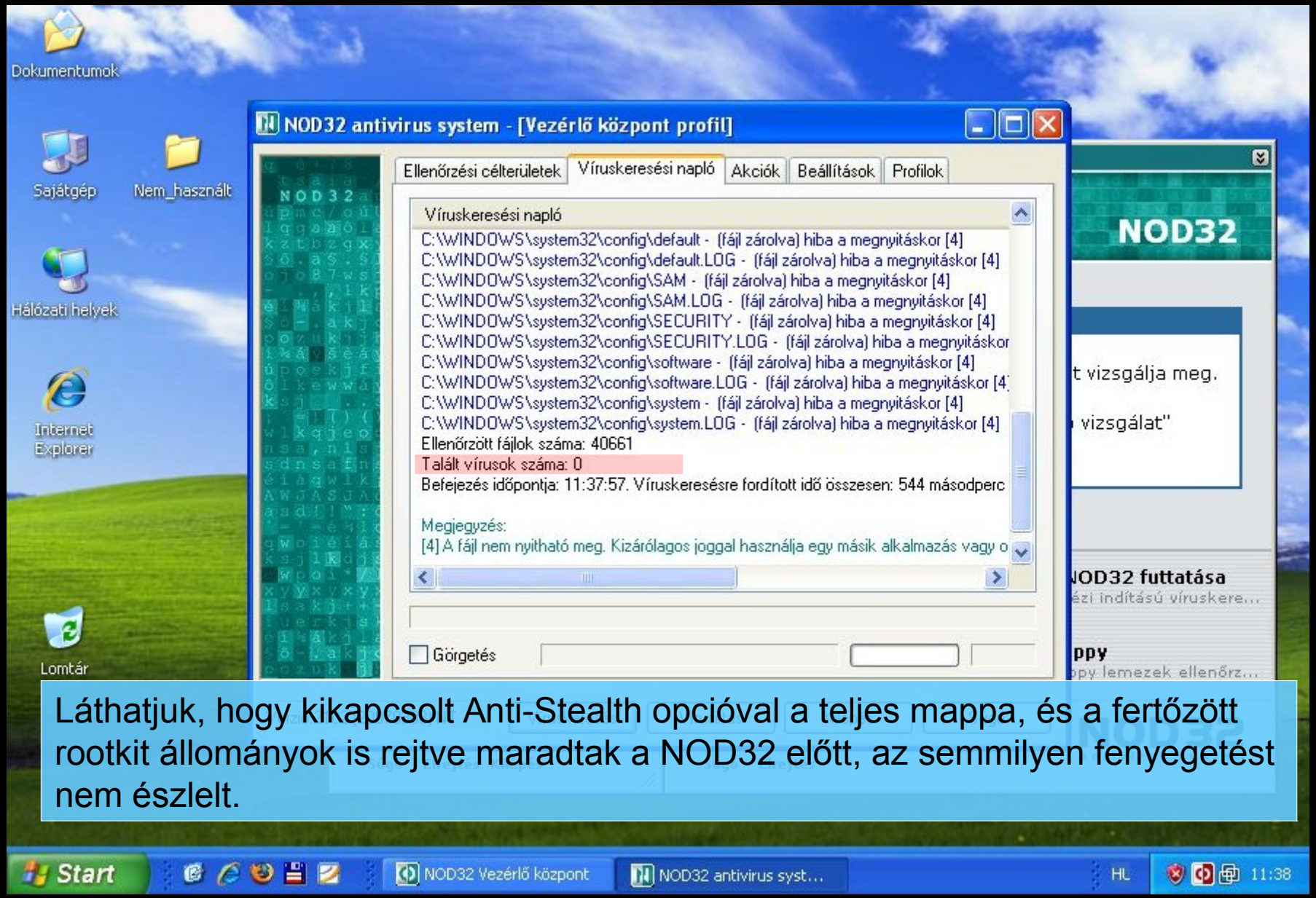

Futtassuk most le a NOD32 kézi indítású víruskeresőjét!
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 Vezérlő központ
Vezérlő központ
Víruskereső modulok
AMON
DMON
EMON
IMON
NOD32
Frissítések
Frissítés
Naplók
Rendszereszközök
Súgó
Elrejtés
Kilépés
NOD32 - kézi indítású 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
NOD32 antivirus system
Start
NOD32 Vezérlő központ
HL
11:27

A teljes C meghajtó tartalmát meg fogjuk vizsgálni.

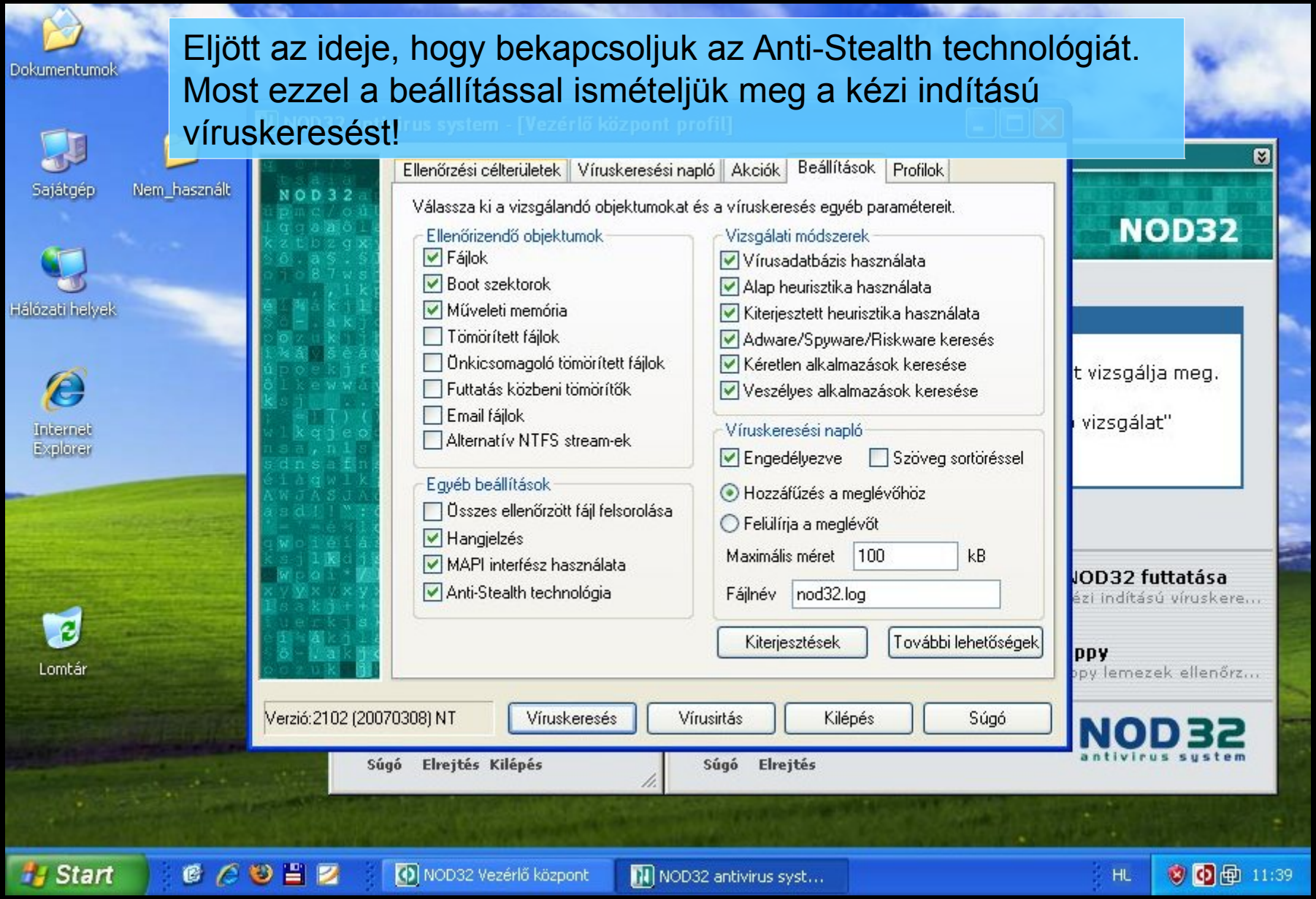


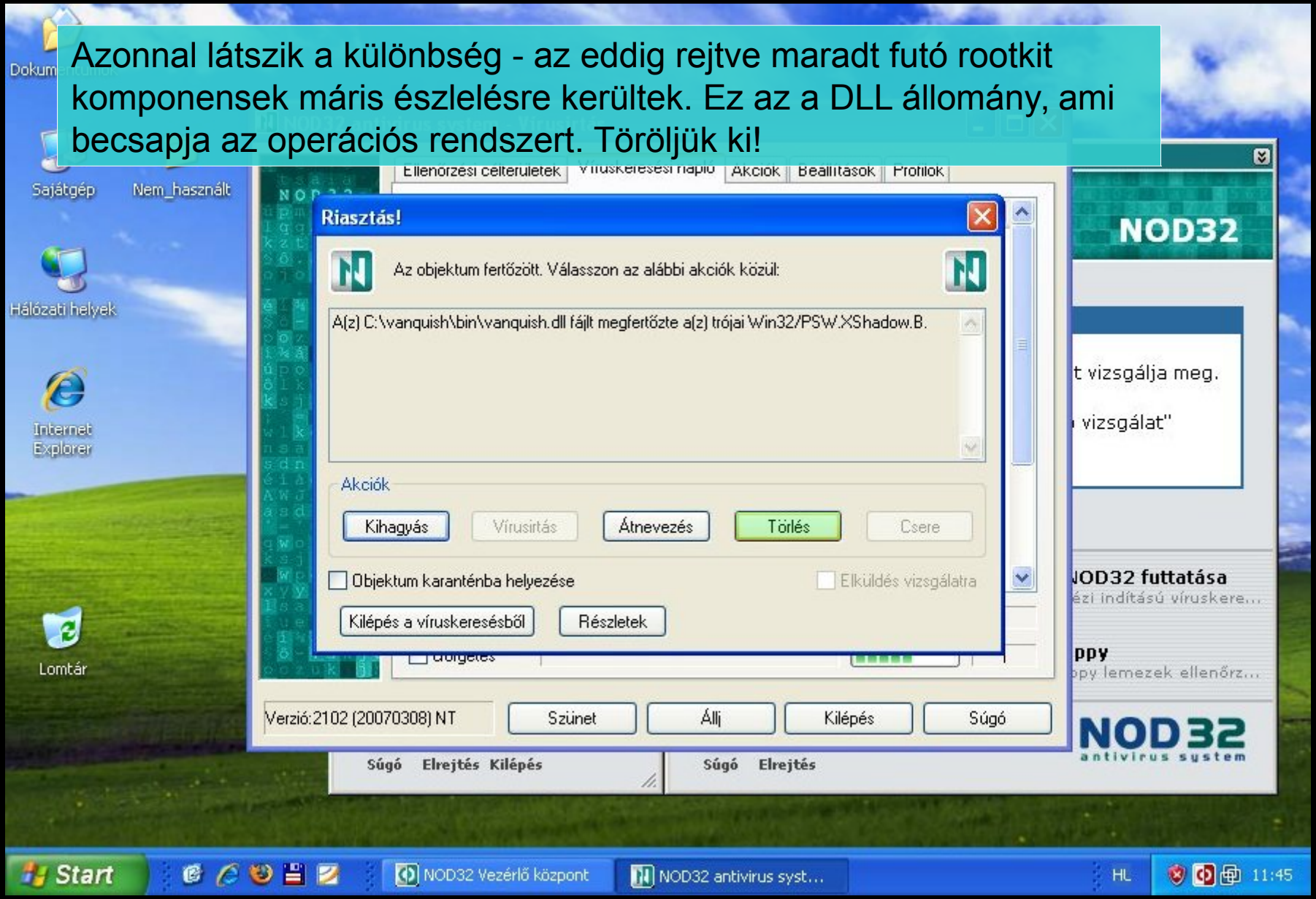
Mivel alapos ellenőrzést szeretnénk, kapcsoljunk be mindent
- kivéve egyelőre az Anti-Stealth technológiát!

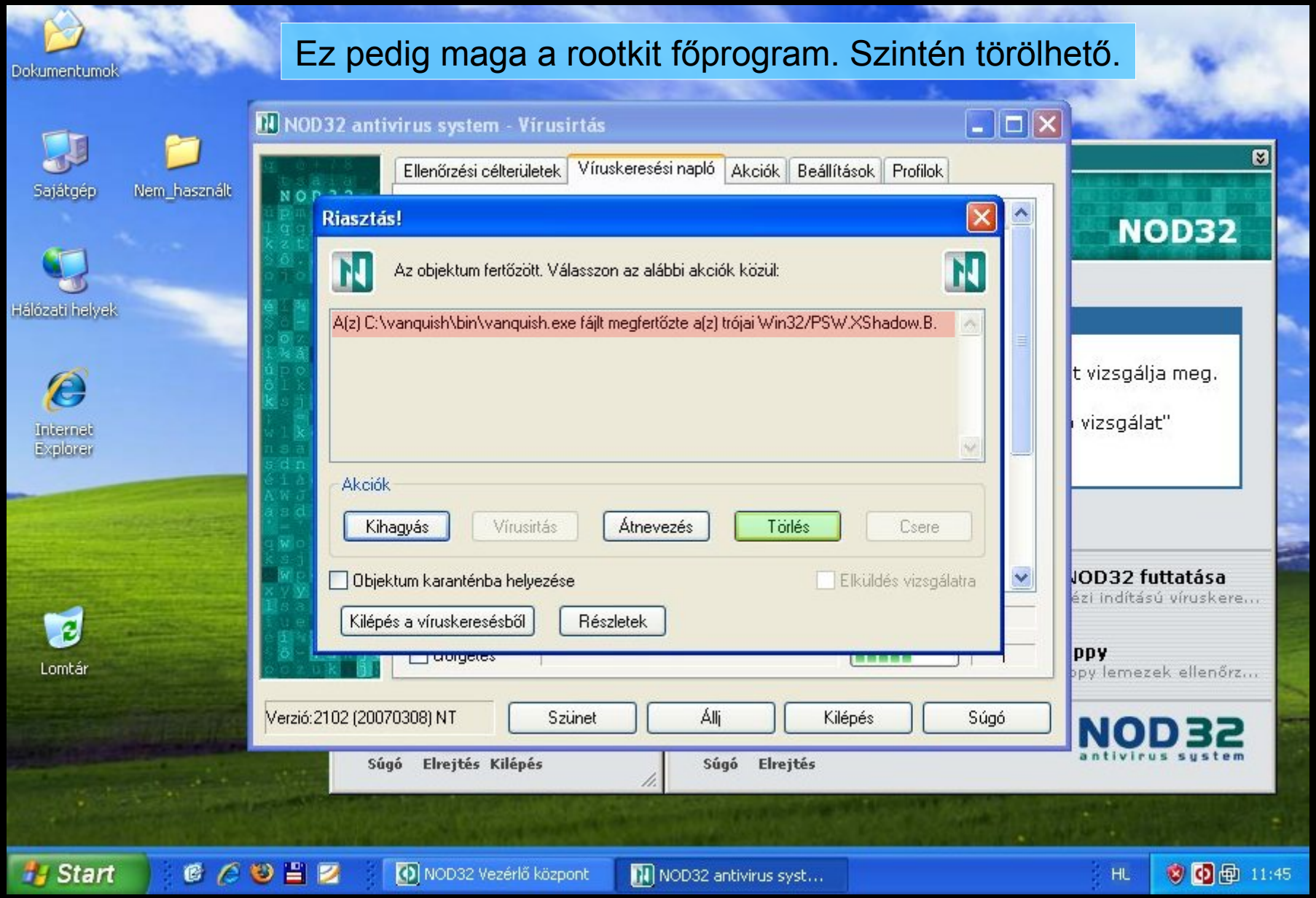




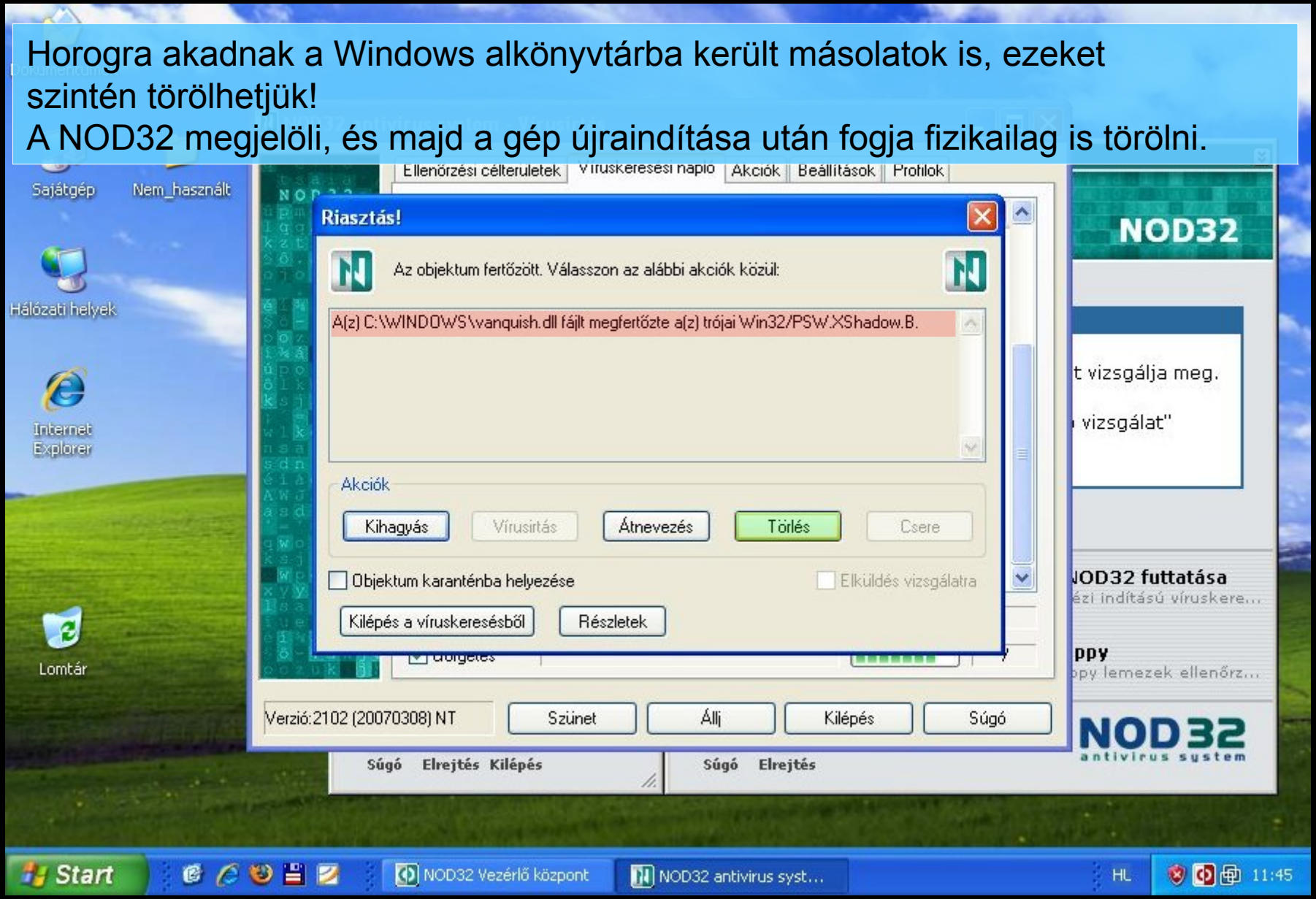
Láthatjuk, hogy kikapcsolt Anti-Stealth opcióval a teljes mappa, és a fertőzött rootkit állományok is rejtve maradtak a NOD32 előtt, az semmilyen fenyegetést nem észlelt.

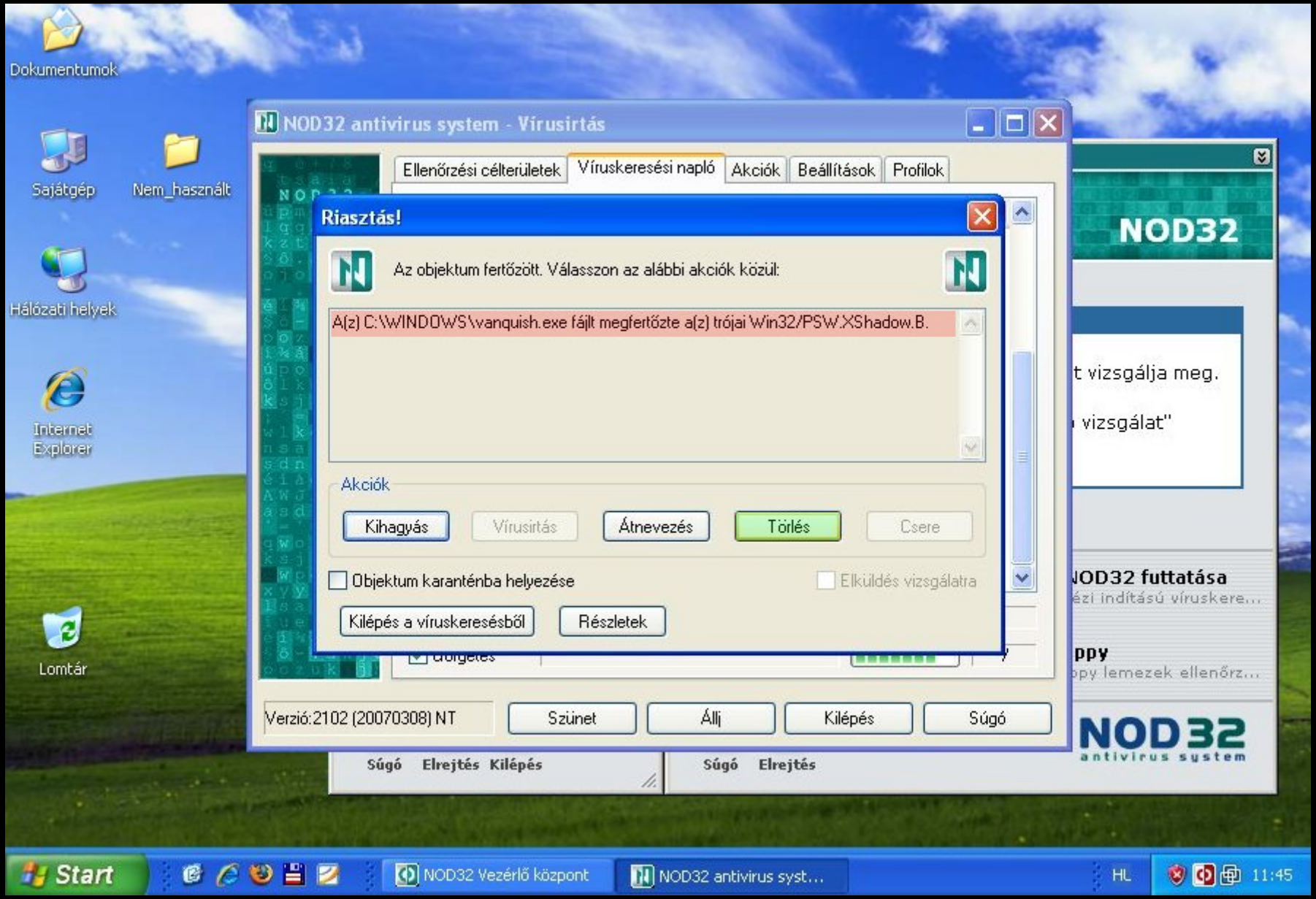

Eljött az ideje, hogy bekapcsoljuk az Anti-Stealth technológiát. Most ezzel a beállítással ismételjük meg a kézi indítású víruskeresést!
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Válassza ki a vizsgálandó 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:2102 (20070308) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
NOD32
antivirus system
Súgó Elrejtés Kilépés
Súgó Elrejtés
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
11:39

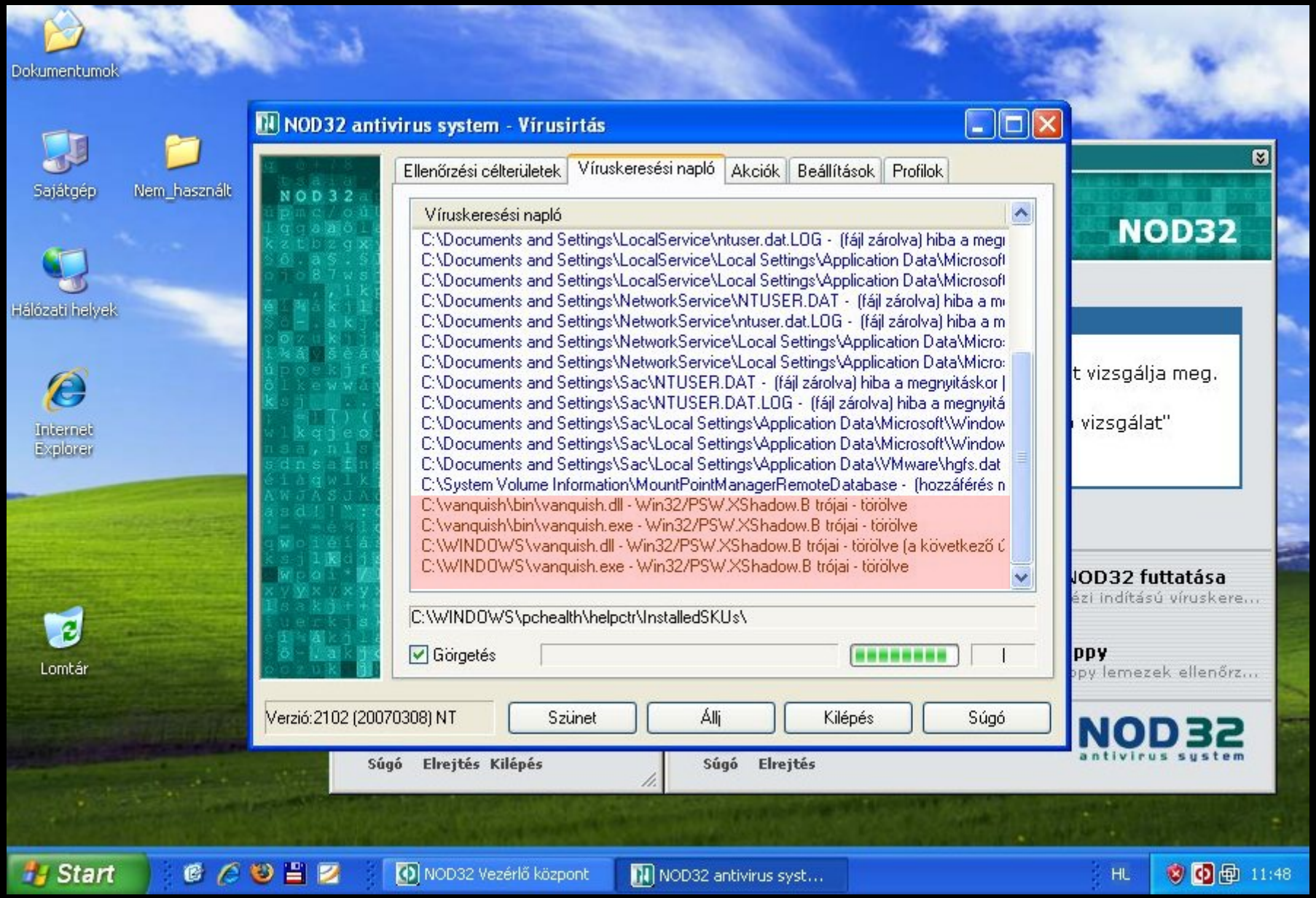

Azonnal látszik a különbség - az eddig rejtve maradt futó rootkit komponensek máris észlelésre kerültek. Ez az a DLL állomány, ami becsapja az operációs rendszert. Töröljük ki!
Riasztás!
Az objektum fertőzött. Válasszon az alábbi akciók közül:
A(z) C:\vanquish\bin\vanquish.dll fájlt megfertőzte a(z) trójai Win32/PSW.XShadow.B.
Akciók
Kihagyás
Vírusirtás
Átnevezés
Törlés
Csere
Objektum karanténba helyezése
Elküldés vizsgálatra
Kilépés a víruskeresésből
Részletek
Verzió:2102 (20070308) NT
Szünet
Állj
Kilépés
Súgó
NOD32
antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
11:45

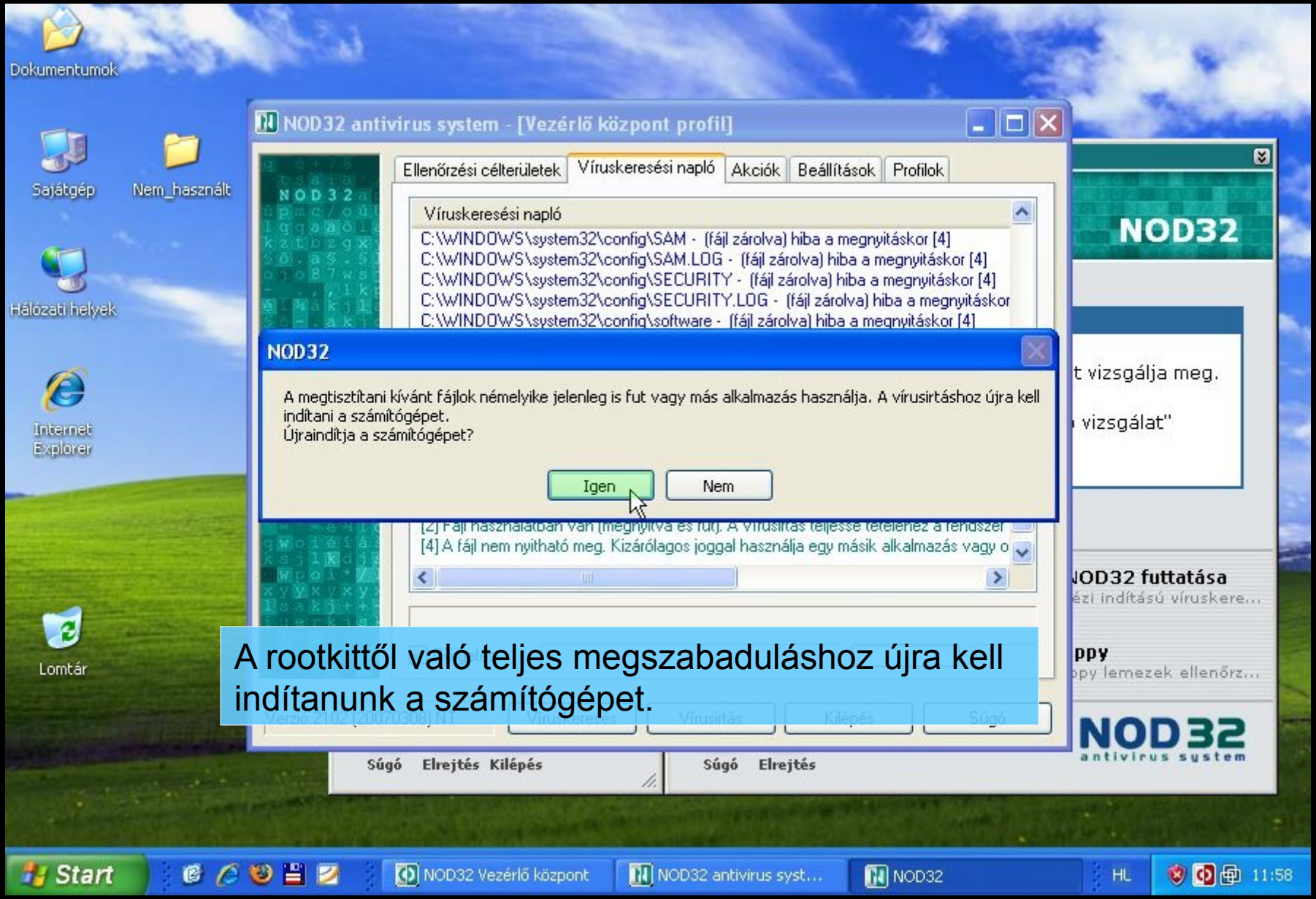

Ez pedig maga a rootkit főprogram. Szintén törölhető.
Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - Vírusirtás
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Riasztás!
Az objektum fertőzött. Válasszon az alábbi akciók közül:
A(z) C:\vanquish\bin\vanquish.exe fájlt megfertőzte a(z) trójai Win32/PSW.XShadow.B.
Akciók
Kihagyás
Vírusirtás
Átnevezés
Törlés
Csere
Objektum karanténba helyezése
Elküldés vizsgálatra
Kilépés a víruskeresésből
Részletek
Verzió:2102 (20070308) NT
Szünet
Állj
Kilépés
Súgó
NOD32
Súgó Elrejtés Kilépés
Súgó Elrejtés
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
11:45

Horogra akadnak a Windows alkönyvtárba került másolatok is, ezeket szintén törölhetjük!
A NOD32 megjelöli, és majd a gép újraindítása után fogja fizikailag is törölni.




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:\WINDOWS\vanquish.exe fájlt megfertőzte a(z) trójai Win32/PSW.XShadow.B.
Akciók
Kihagyás
Vírusirtás
Átnevezés
Törlés
Csere
Objektum karanténba helyezése
Elküldés vizsgálatra
Kilépés a víruskeresésből
Részletek
Verzió:2102 (20070308) NT
Szünet
Állj
Kilépés
Súgó
NOD32
vizsgálja meg.
vizsgálat"
NOD32 futtatása
Súgó Elrejtés Kilépés
Súgó Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
11:45


Dokumentumok
Sajátgép
Nem_használt
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - Vírusirtás
Ellenőrzési célterületek
Víruskeresési napló
Akciók
Beállítások
Profilok
Víruskeresési napló
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 mı
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:\System Volume Information\MountPointManagerRemoteDatabase - (hozzáférés n
C:\vanquish\bin\vanquish.dll - Win32/PSW.XShadow.B trójai - törölve
C:\vanquish\bin\vanquish.exe - Win32/PSW.XShadow.B trójai - törölve
C:\WINDOWS\vanquish.dll - Win32/PSW.XShadow.B trójai - törölve (a következő ú
C:\WINDOWS\vanquish.exe - Win32/PSW.XShadow.B trójai - törölve
C:\WINDOWS\pchealth\helpctr\InstalledSKUs\
Görgetés
Verzió:2102 (20070308) NT
Szünet
Állj
Kilépés
Súgó
NOD32
t vizsgálja meg.
vizsgálat"
NOD32 futtatása
Súgó Elrejtés Kilépés
Súgó Elrejtés
NOD32 antivirus system
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
11:48

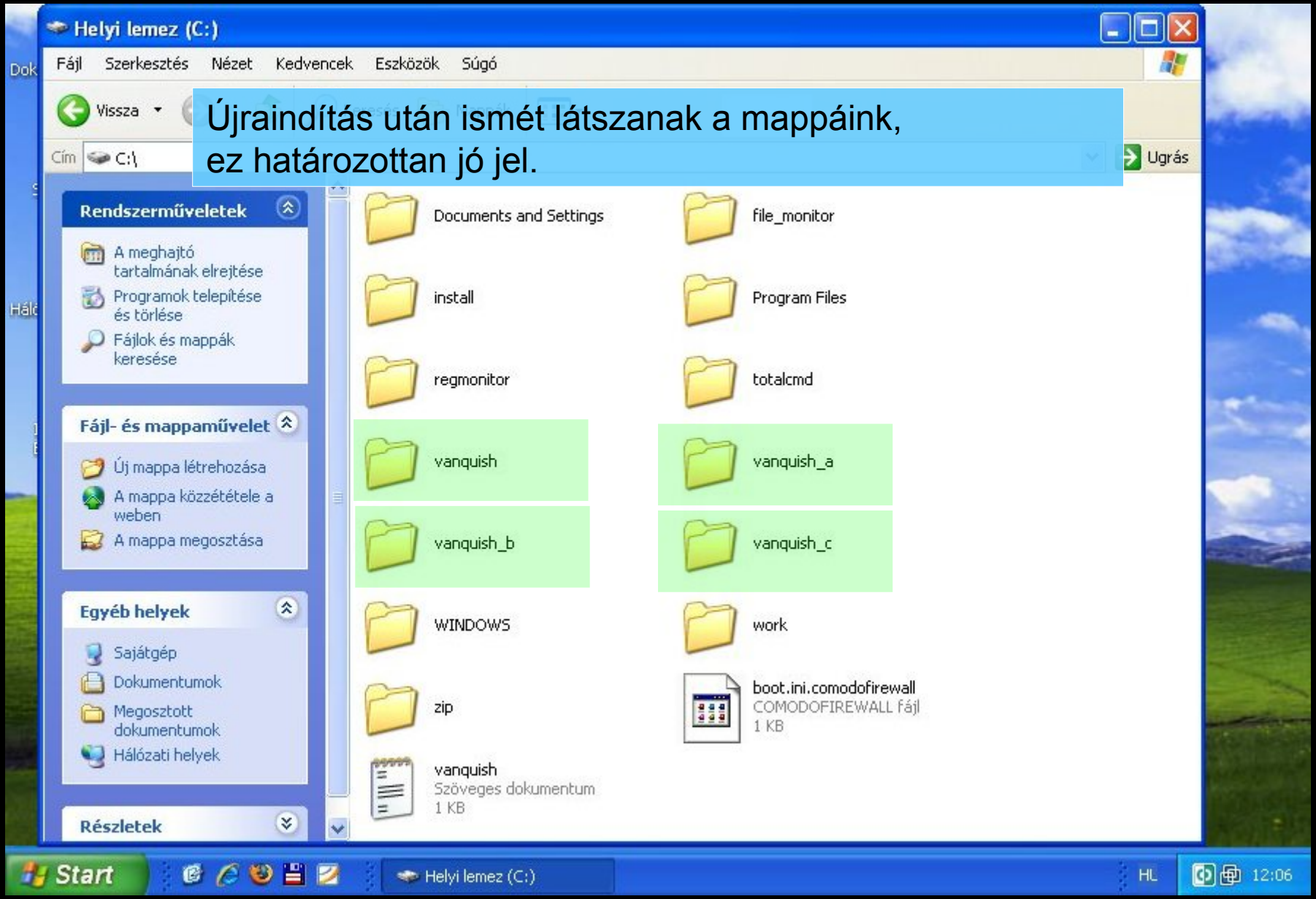


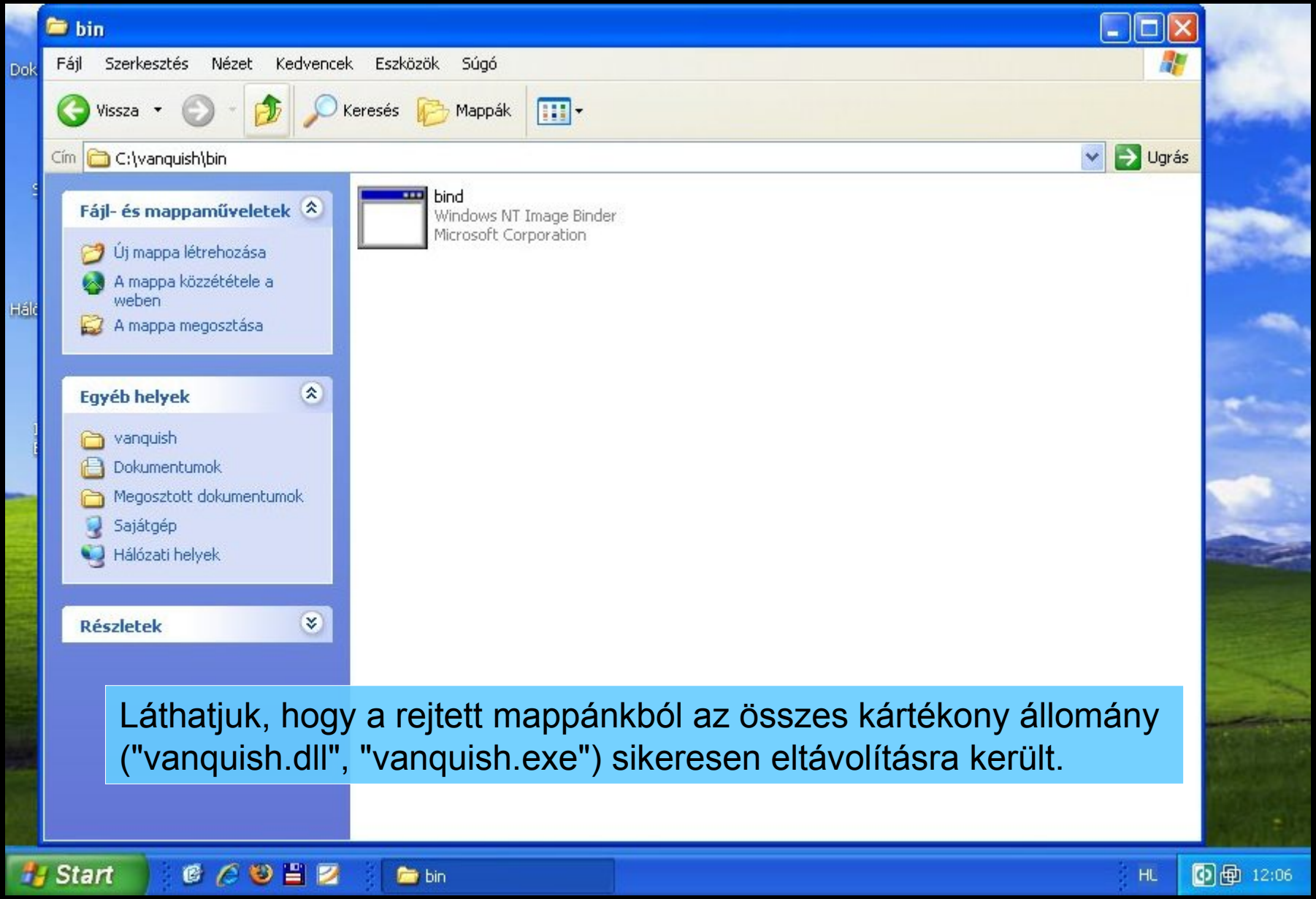
A rootkittől való teljes megszabaduláshoz újra kell indítanunk a számítógépet.

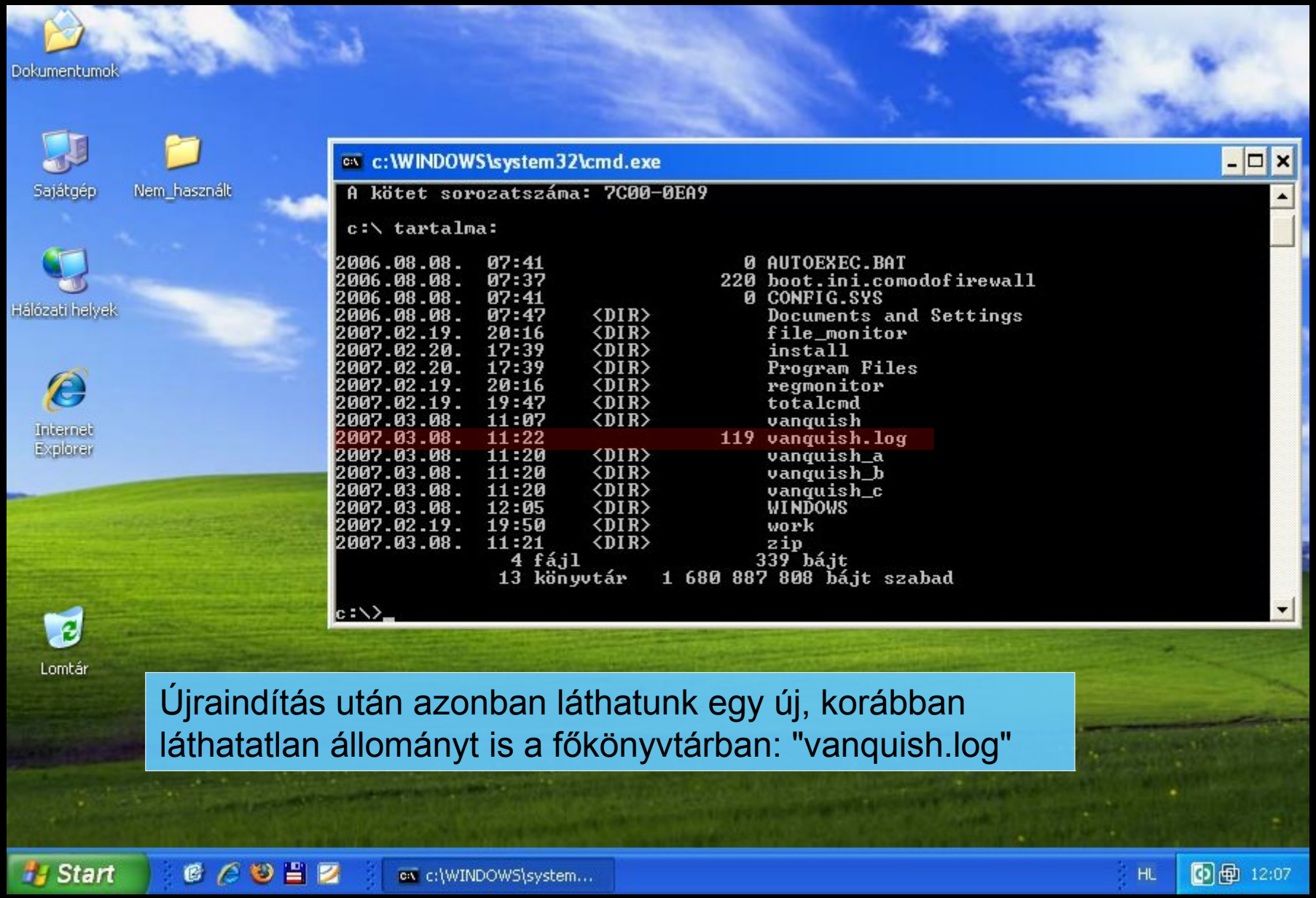
Kijelentkezés...


Microsoft®
Windows®xp
Copyright © Microsoft Corporation
Microsoft

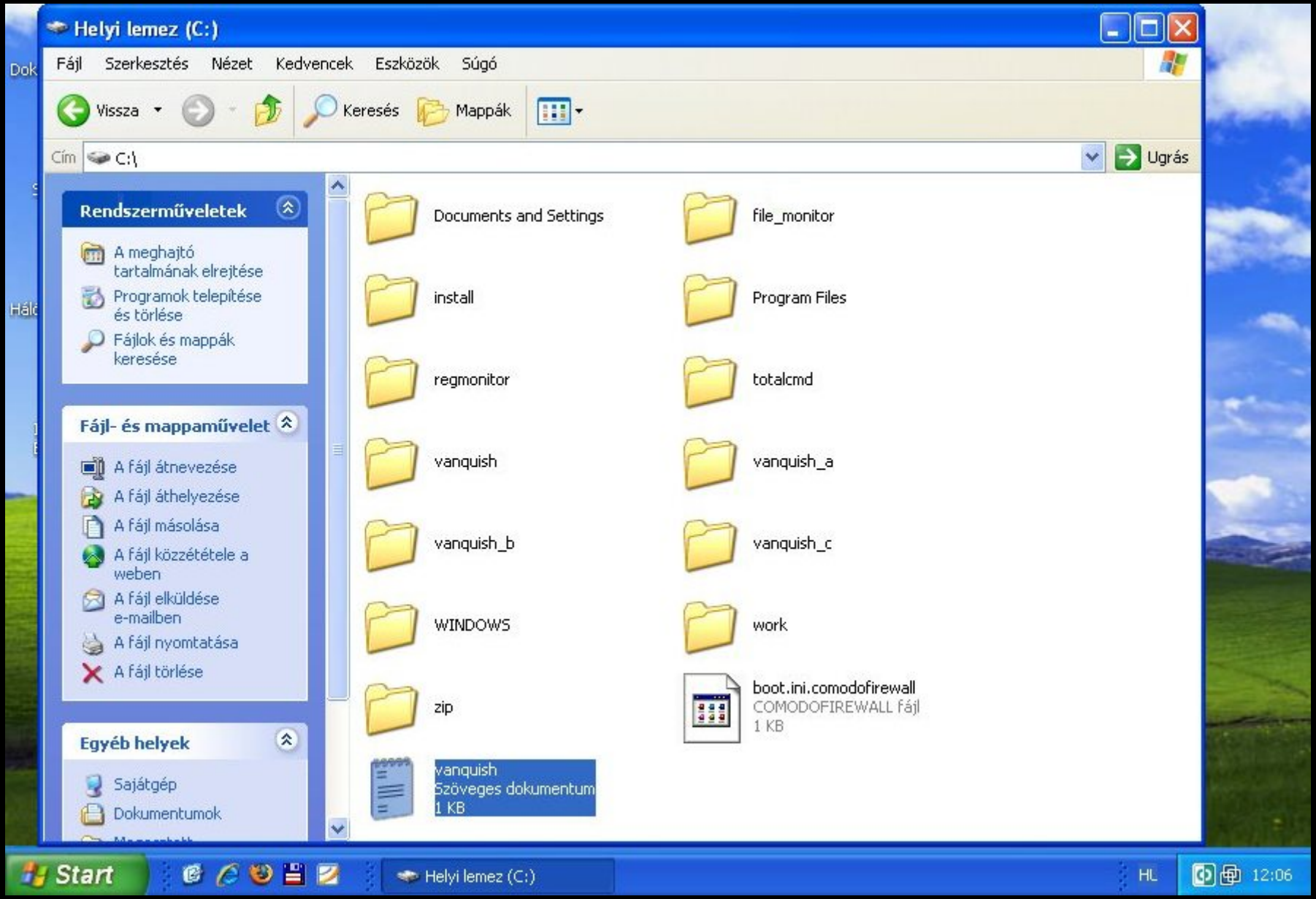
Üdvözöljük

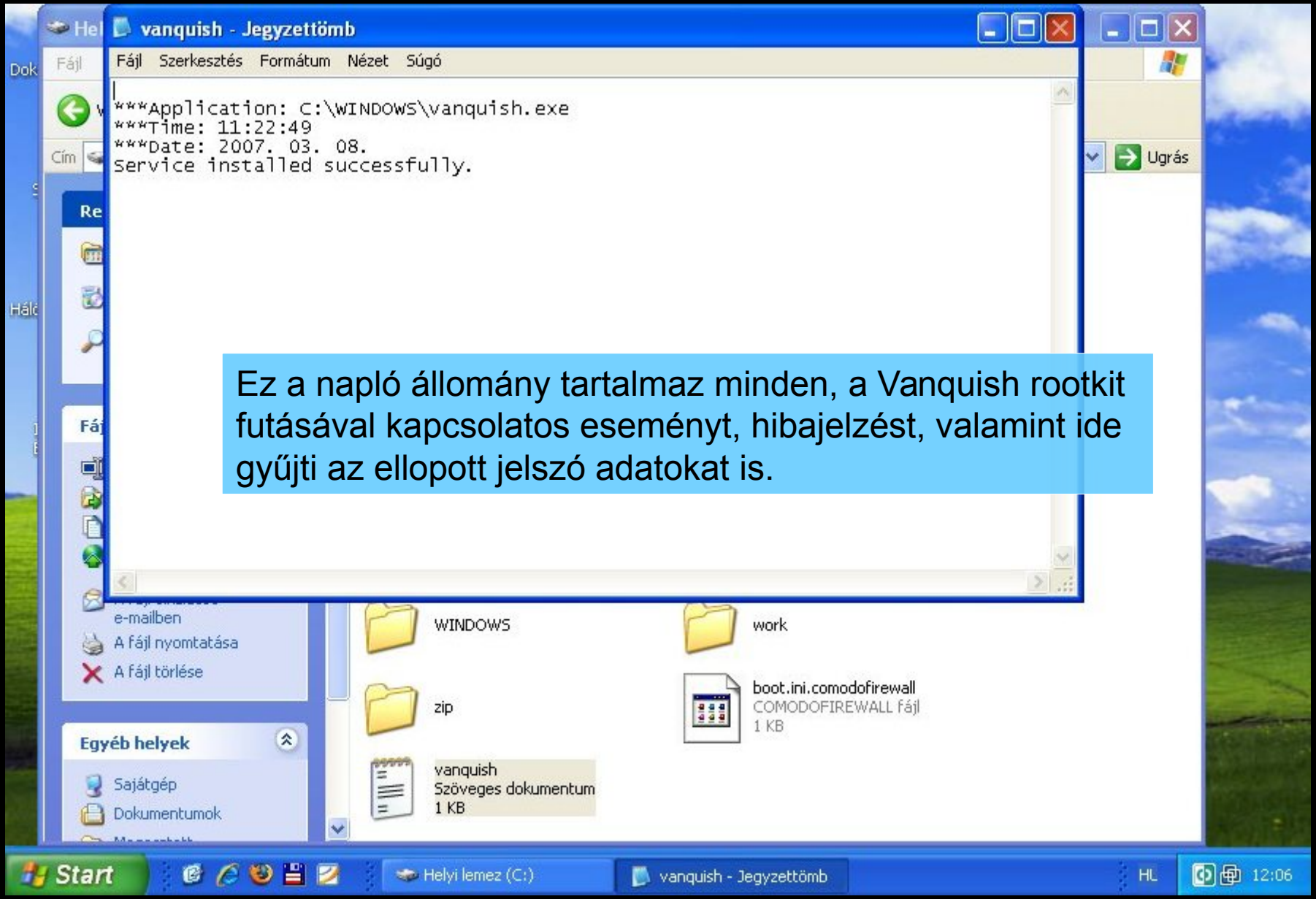

Helyi lemez (C:)
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Cím C:\
Ugrás
Újraindítás után ismét látszanak a mappáink,
ez határozottan jó jel.
Rendszerműveletek
A meghajtó tartalmának elrejtése
Programok telepítése és törlése
Fájlok és mappák keresése
Fájl- és mappaművelet
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
Sajátgép
Dokumentumok
Megosztott dokumentumok
Hálózati helyek
Részletek
Documents and Settings
file_monitor
install
Program Files
regmonitor
totalcmd
vanquish
vanquish_a
vanquish_b
vanquish_c
WINDOWS
work
zip
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
vanquish
Szöveges dokumentum
1 KB
Start
Helyi lemez (C:)
HL
12:06

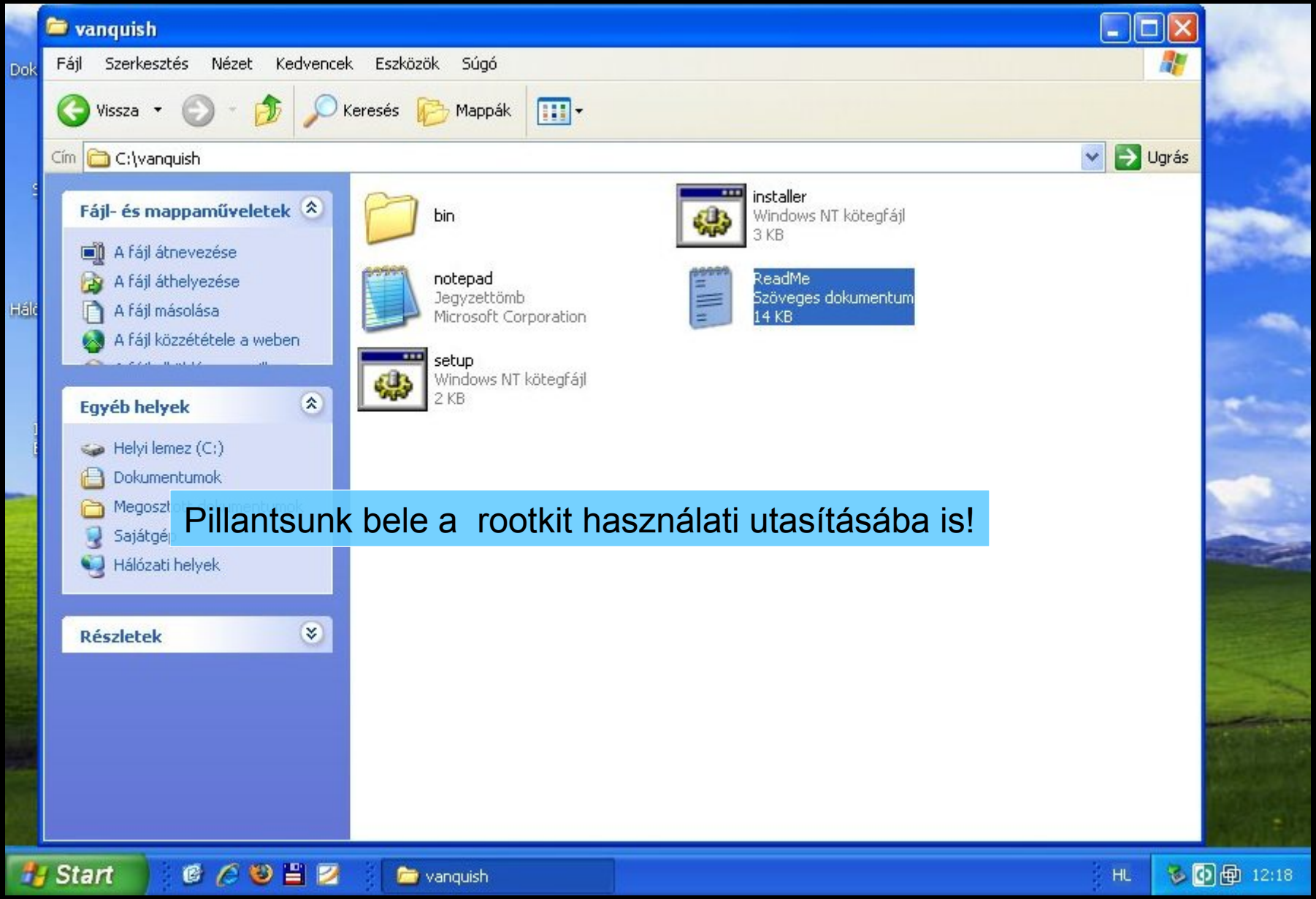

bin
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\vanquish\bin
Ugrás
Fájl- és mappaműveletek
Új mappa létrehozása
A mappa közzététele a weben
A mappa megosztása
Egyéb helyek
vanquish
Dokumentumok
Megosztott dokumentumok
Sajátgép
Hálózati helyek
Részletek
bind
Windows NT Image Binder
Microsoft Corporation
Láthatjuk, hogy a rejtett mappánkból az összes kártékony állomány ("vanquish.dll", "vanquish.exe") sikeresen eltávolításra került.
Start
bin
HL
12:06

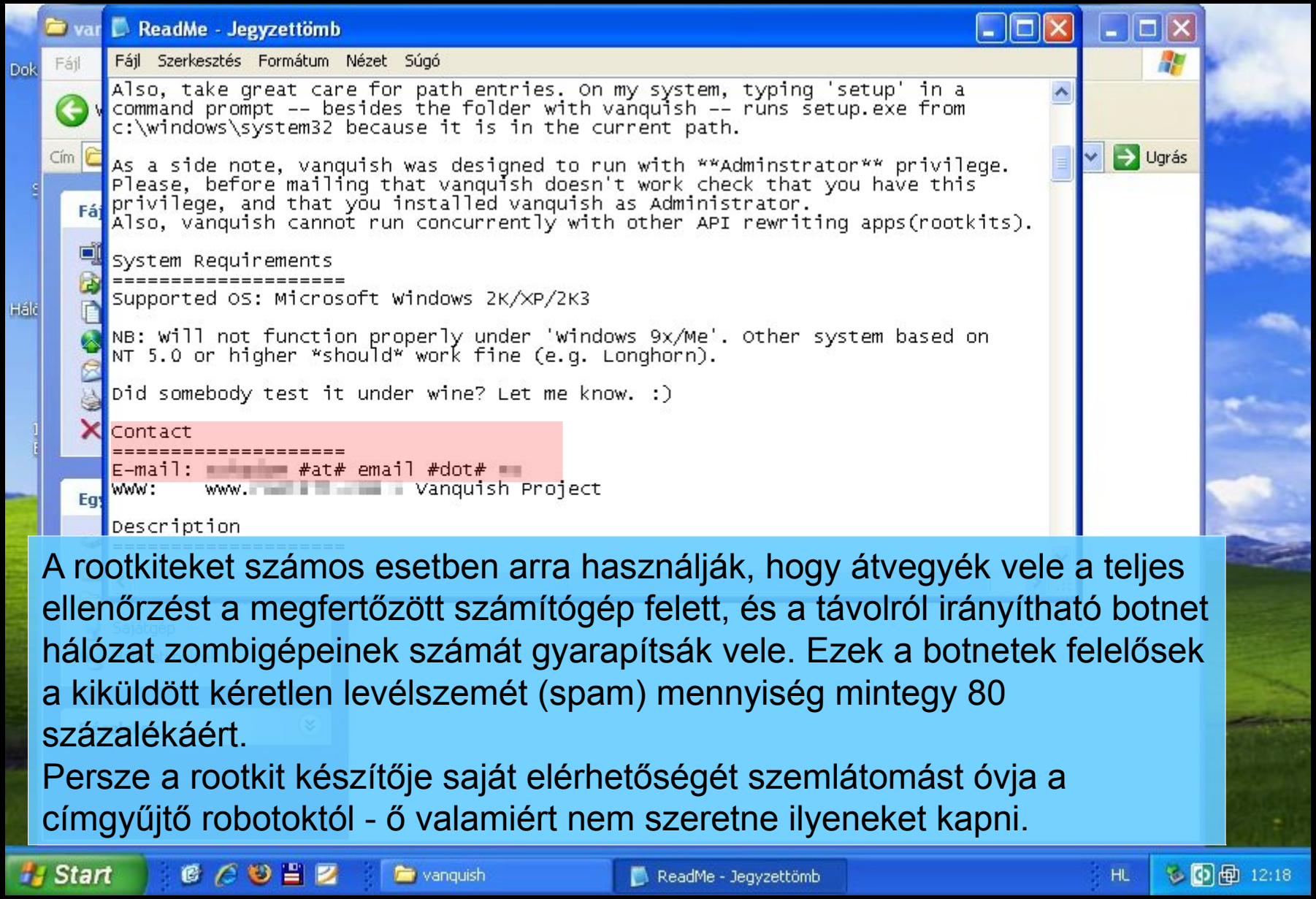


Újraindítás után azonban láthatunk egy új, korábban láthatatlan állományt is a főkönyvtárban: "vanquish.log"


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 fájl átnevezése
A fájl áthelyezése
A fájl másolása
A fájl közzététele a weben
A fájl elküldése e-mailben
A fájl nyomtatása
A fájl törlése
Egyéb helyek
Sajátgép
Dokumentumok
Documents and Settings
file_monitor
install
Program Files
regmonitor
totalcmd
vanquish
vanquish_a
vanquish_b
vanquish_c
WINDOWS
work
zip
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
vanquish
Szöveges dokumentum
1 KB
Start
Helyi lemez (C:)
HL
12:06

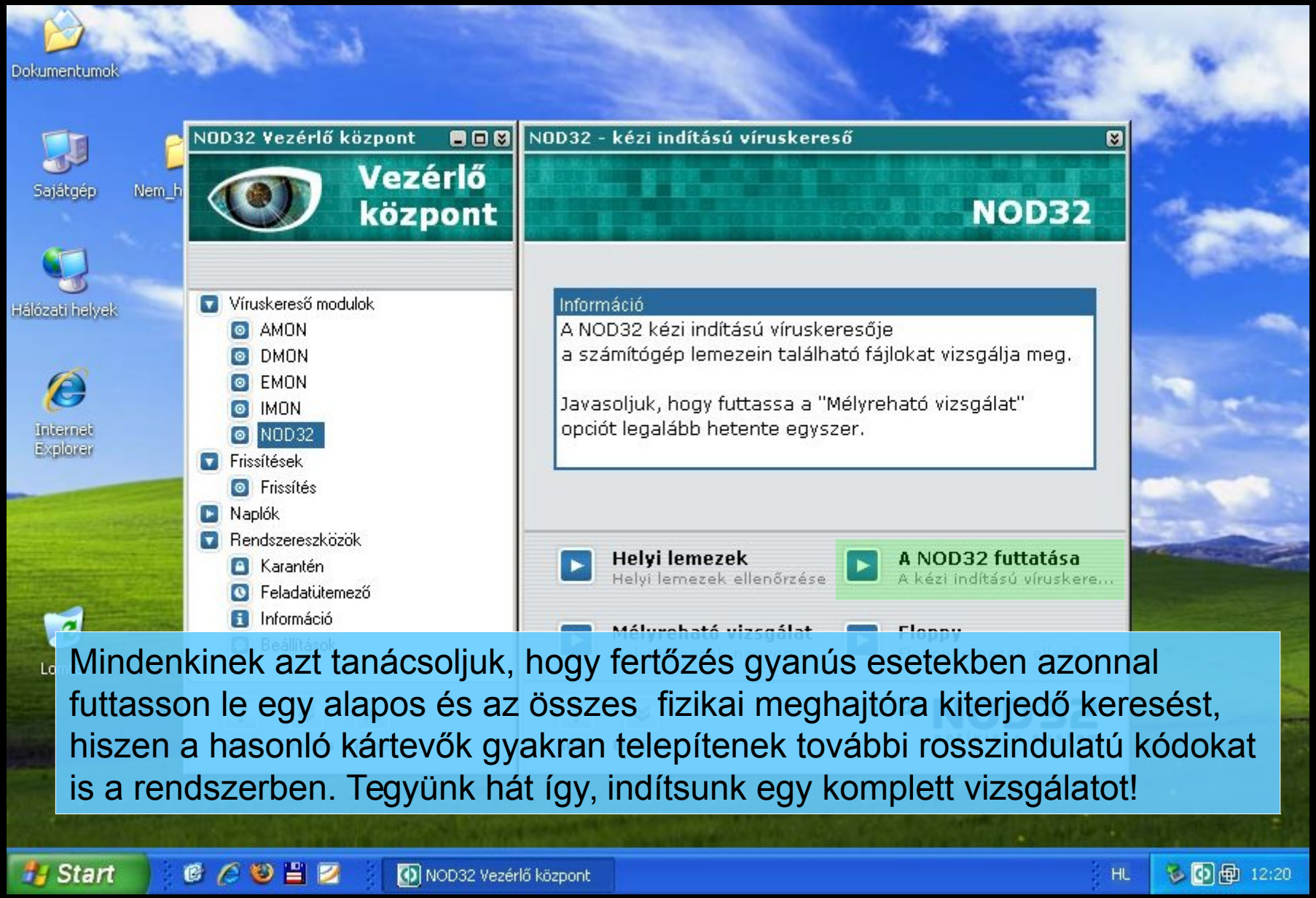

vanquish - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó
***Application: C:\WINDOWS\vanquish.exe
***Time: 11:22:49
***Date: 2007. 03. 08.
Service installed successfully.
Ez a napló állomány tartalmaz minden, a Vanquish rootkit futásával kapcsolatos eseményt, hibajelzést, valamint ide gyűjti az ellopott jelszó adatokat is.
WINDOWS
work
zip
boot.ini.comodofirewall
COMODOFIREWALL fájl
1 KB
vanquish
Szöveges dokumentum
1 KB
e-mailben
A fájl nyomtatása
A fájl törlése
Egyéb helyek
Sajátgép
Dokumentumok
Start
Helyi lemez (C:)
vanquish - Jegyzettömb
HL
12:06


vanquish
Fájl Szerkesztés Nézet Kedvencek Eszközök Súgó
Vissza
Keresés
Mappák
Cím C:\vanquish
Ugrás
Fájl- és mappaműveletek
A fájl átnevezése
A fájl áthelyezése
A fájl másolása
A fájl közzététele a weben
Egyéb helyek
Helyi lemez (C:)
Dokumentumok
Hálózati helyek
Részletek
bin
notepad
Jegyzettömb
Microsoft Corporation
setup
Windows NT kötegfájl
2 KB
installer
Windows NT kötegfájl
3 KB
ReadMe
Szöveges dokumentum
14 KB
Pillantsunk bele a rootkit használati utasításába is!
Start
vanquish
HL
12:18

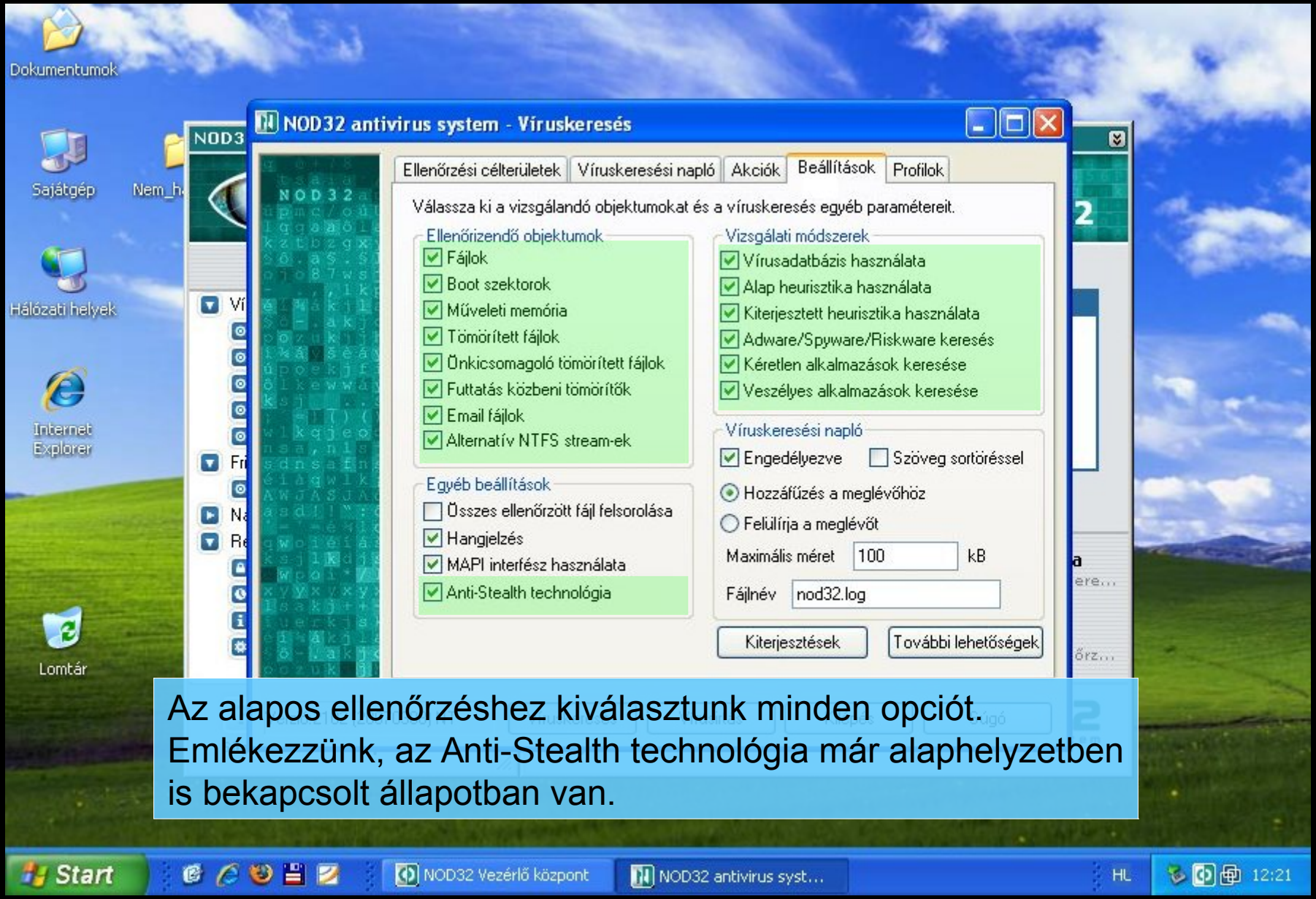


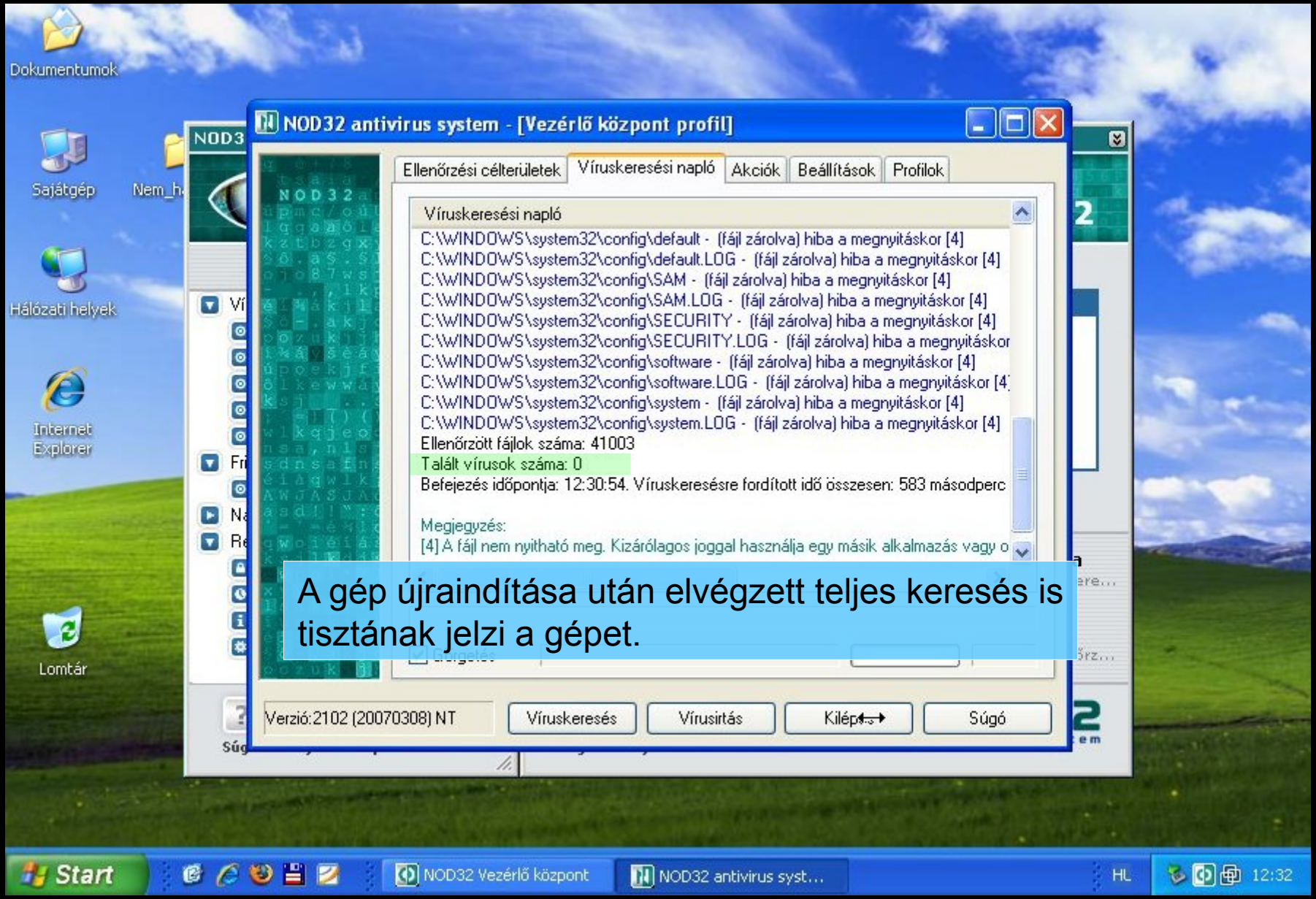
A rootkiteket számos esetben arra használják, hogy átvegyék vele a teljes ellenőrzést a megfertőzött számítógép felett, és a távolról irányítható botnet hálózat zombigépeinek számát gyarapítsák vele. Ezek a botnetek felelősek a kiküldött kéretlen levélszemét (spam) mennyiség mintegy 80 százalékáért.

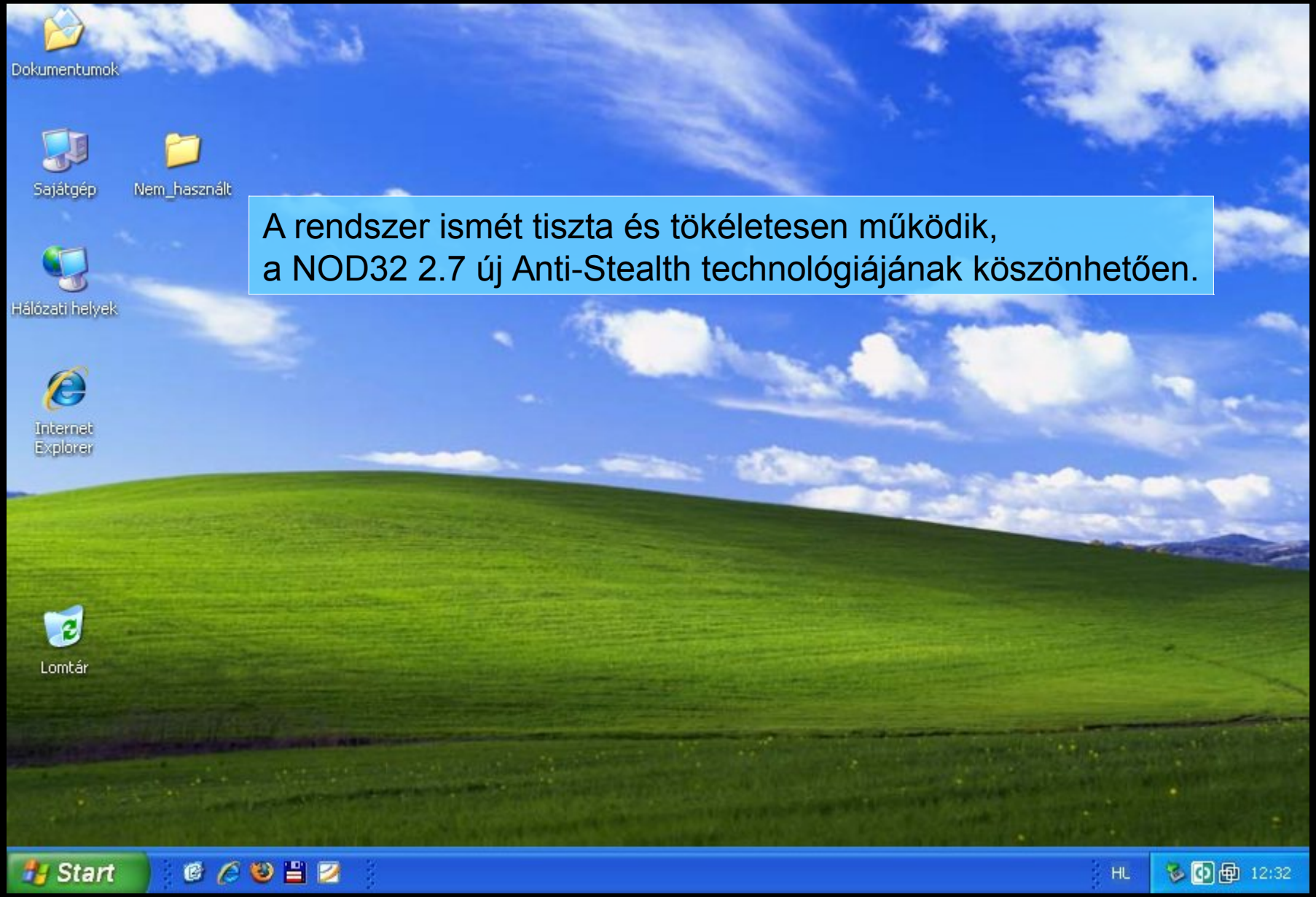
Persze a rootkit készítője saját elérhetőségét szemlátomást óvja a címgyűjtő robotoktól - ő valamiért nem szeretne ilyeneket kapni.

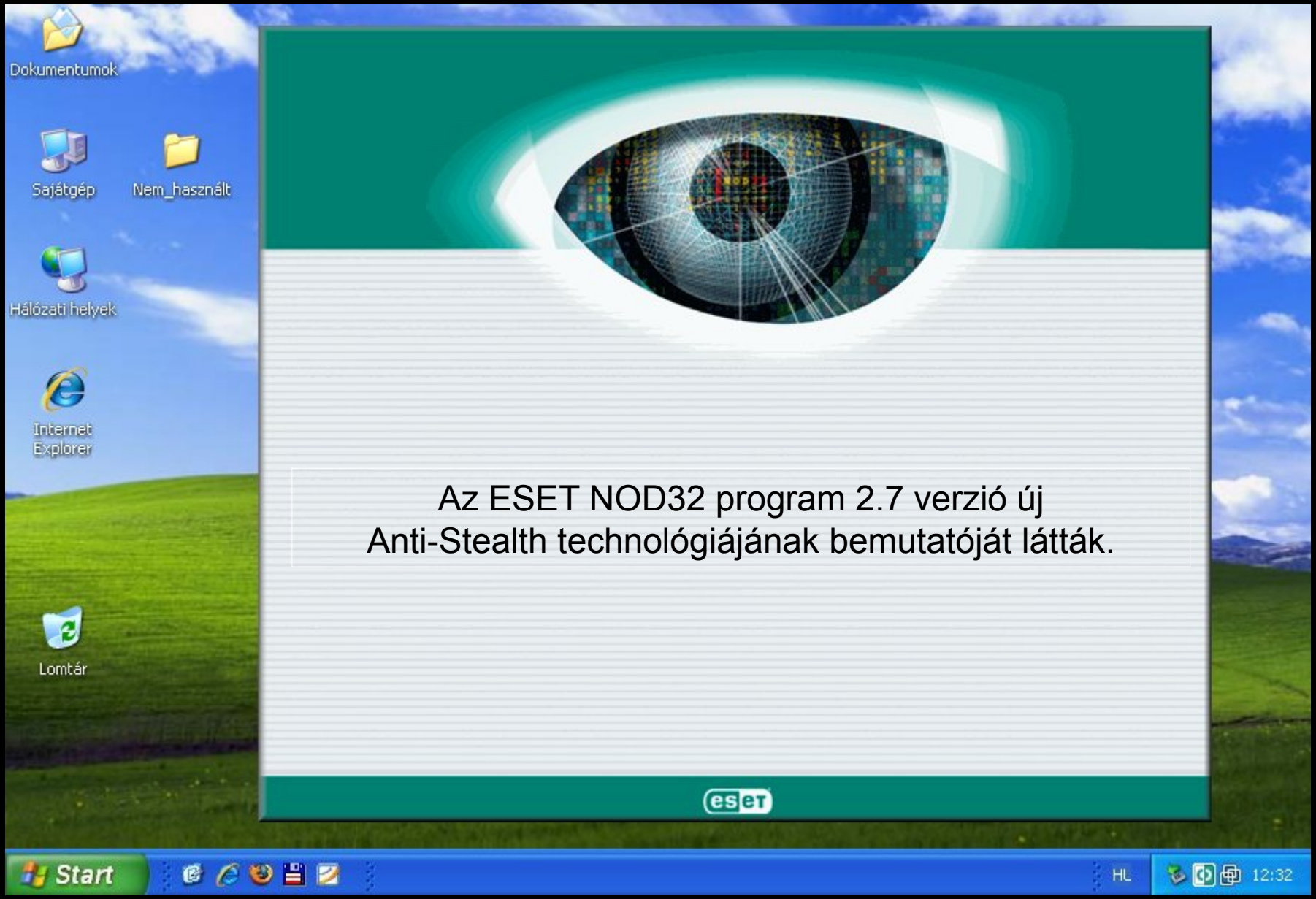


Mindenkinek azt tanácsoljuk, hogy fertőzés gyanús esetekben azonnal futtasson le egy alapos és az összes fizikai meghajtóra kiterjedő keresést, hiszen a hasonló kártevők gyakran telepítenek további rosszindulatú kódokat is a rendszerben. Tegyünk hát így, indítsunk egy komplett vizsgálatot!


Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
NOD32 antivirus system - Víruskeresés
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
Az alapos ellenőrzéshez kiválasztunk minden opciót. Emlékezzünk, az Anti-Stealth technológia már alaphelyzetben is bekapcsolt állapotban van.
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HL
12:21


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: 41003
Talált vírusok száma: 0
Befejezés időpontja: 12:30:54. Víruskeresésre fordított idő összesen: 583 másodperc
Megjegyzés:
[4] A fájl nem nyitható meg. Kizárólagos joggal használja egy másik alkalmazás vagy o
Verzió:2102 (20070308) NT
Víruskeresés
Vírusirtás
Kilépés
Súgó
A gép újraindítása után elvégzett teljes keresés is tisztának jelzi a gépet.
Dokumentumok
Sajátgép
Hálózati helyek
Internet Explorer
Lomtár
Start
NOD32 Vezérlő központ
NOD32 antivirus syst...
HU
12:32


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
12:32


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
12:32