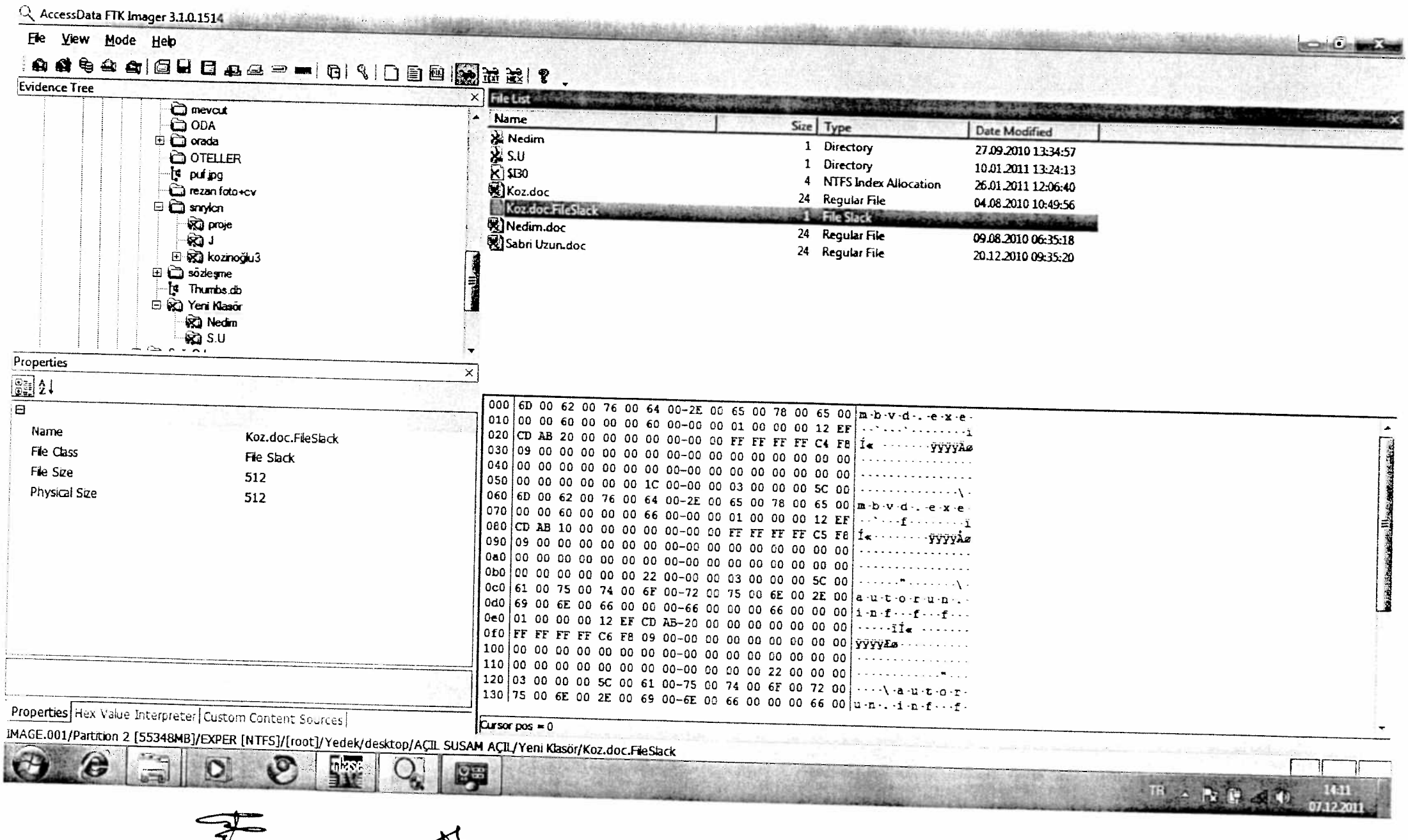

AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
mevcut
ODA
orada
OTELLER
puf.jpg
rezan foto+cv
snrylcn
proje
J
kozinoğlu3
sözleşme
Thumbs.db
Yeni Klasör
Nedim
S.U
File List
Name
Size
Type
Date Modified
Nedim 1 Directory 27.09.2010 13:34:57
S.U 1 Directory 10.01.2011 13:24:13
$I30 4 NTFS Index Allocation 26.01.2011 12:06:40
Koz.doc 24 Regular File 04.08.2010 10:49:56
Koz.doc.FileSlack 1 File Slack
Nedim.doc 24 Regular File 09.08.2010 06:35:18
Sabri Uzun.doc 24 Regular File 20.12.2010 09:35:20
Properties
Name Koz.doc.FileSlack
File Class File Slack
File Size 512
Physical Size 512
Properties
Hex Value Interpreter
Custom Content Sources
Cursor pos = 0
IMAGE.001/Partition 2 [55348MB]/EXPER [NTFS]/[root]/Yedek/desktop/AÇIL SUSAM AÇIL/Yeni Klasör/Koz.doc.FileSlack
TR
14:11
07.12.2011

webroot Prevx Research Division

Google Translate
Select Language
Google Gadgets powered by Google

"MBVD.EXE"

WORM

FREE PC CLEANUP FROM WEBROOT

Use Webroot SecureAnywhere to remove **MBVD.EXE.**

"Just when you thought it couldn't get any better or faster. The Webroot scanning engine is 'high octane' with a hidden nitrous oxide system. Bravo!!!"

W. LODZİNSKİ, SECUREANYWHERE USER

Get Free PC Cleanup

ASSOCİATED MALWARE GROUPS

The filename is associated with the malware group:

- Worm

FİLE BEHAVİOR

MBVD.EXE has been seen to perform the following behavior:

- The Process is packed and/or encrypted using a software packing process
- Adds a Registry Key (RUN) to auto start Programs on system start up
- Writes to another Process's Virtual Memory (Process Hijacking)
- Executes a Process
- This process creates other processes on disk
- Modifies the Windows Host File which could be used to stop you visiting specific web sites by redirecting you to alternative addresses without you knowing
- This Process Deletes Other Processes From Disk
- Creates new folders on the system
- Injects code into other processes
- Copies files

MBVD.EXE has been the subject of the following behavior:

- Executed as a Process
- Created as a process on disk
- Has code inserted into its Virtual Memory space by other programs
- Deleted as a process from disk

COUNTRY OF ORİGİN

The filename MBVD.EXE was first seen on Dec 2 2009 in the following geographical regions of the Webroot community:

- Turkey on Dec 2 2009

EK-2

- Vietnam on Dec 3 2009
- Slovenia on Dec 3 2009
- The United Kingdom on Mar 17 2010
- Mexico on Jul 28 2010
- Thailand on Jun 26 2011

FİLE NAME ALİASES

MBVD.EXE can also use the following file names:

- HERSS.EXE
- DC14.EXE
- DCS.EXE

FİLESİZES

The following file size has been seen:

- 3,316,864 bytes
- 184,494 bytes
- 113,792 bytes
- 113,972 bytes
- 335,156 bytes

FİLE TYPE

The filename MBVD.EXE is used by multiple object types including executable programs,objects.

HELP THE WEBROOT COMMUNİTY TO FİGHT CYBER CRİME

We are always looking for ways to improve the quality and speed of research to help us protect you from malicious software and cyber crime.

The filename referred to in this report is often associated with PC infections. If you have a program of this name on your PC and would like to help our research please tell us what you know in the form below:

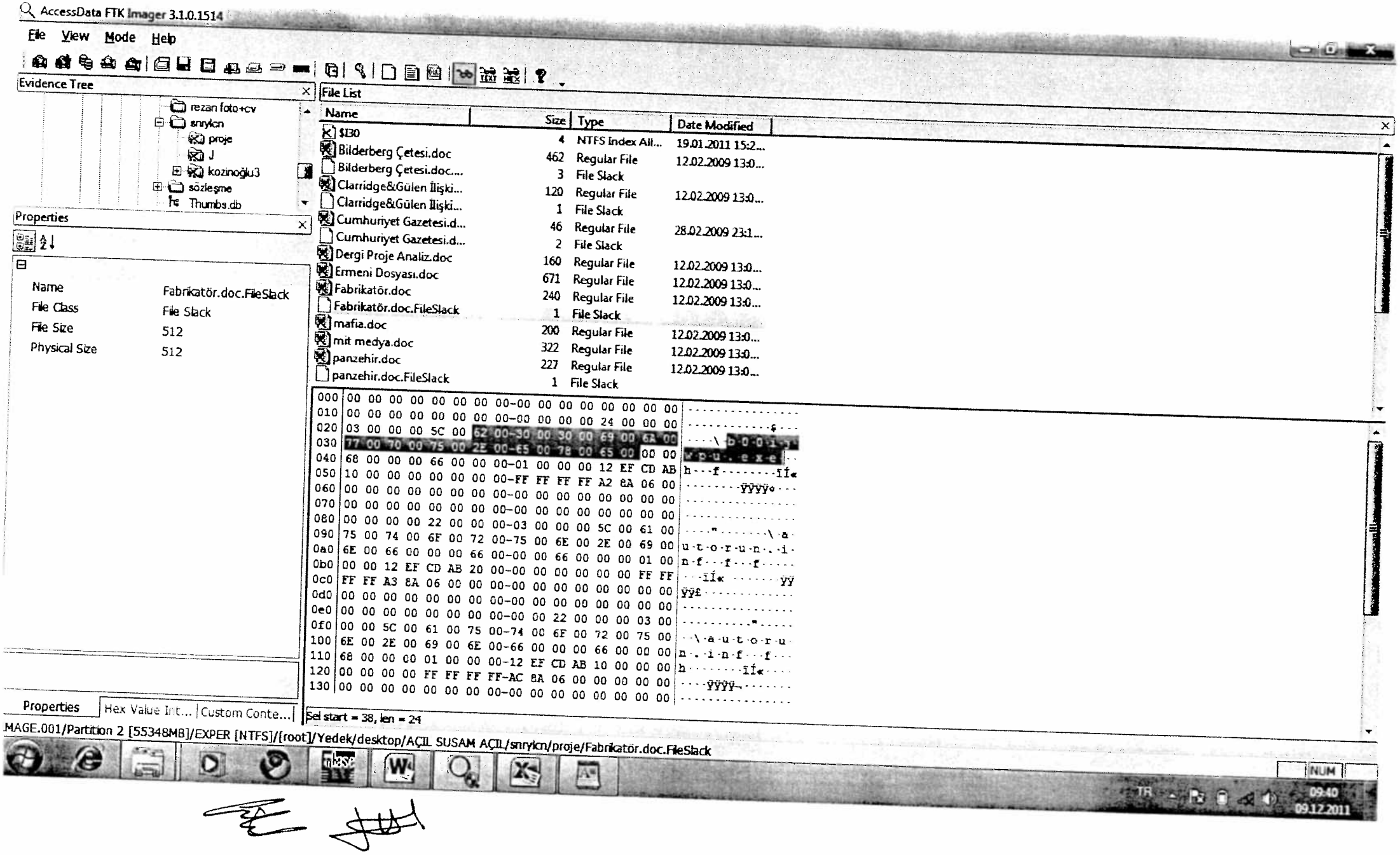
- I have this file on my PC and believe it is an infection
- I have this file on my PC and think it has made my PC slower
- My firewall asked if I wanted to let this file have access to the Internet
- My PC will not work since I noticed this file on it
- My antivirus detected this file but won't remove it
- I know what this file is and believe it is a Safe program
- I am the author of this file and would like to discuss how to have it reclassified as safe

Further Comments or information you'd like to share: *(optional)*

Your email address if you would like us to contact you about this file and any concerns you may have. *(optional)*

Send information »

EK-2


AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
rezan foto+cv
snrylcn
proje
J
kozinoğlu3
sözleşme
Thumbs.db
File List
Name
Size
Type
Date Modified
$I30 4 NTFS Index All... 19.01.2011 15:2...
Bilderberg Çetesi.doc 462 Regular File 12.02.2009 13:0...
Bilderberg Çetesi.doc... 3 File Slack
Clarridge&Gülen İlişki... 120 Regular File 12.02.2009 13:0...
Clarridge&Gülen İlişki... 1 File Slack
Cumhuriyet Gazetesi.d... 46 Regular File 28.02.2009 23:1...
Cumhuriyet Gazetesi.d... 2 File Slack
Dergi Proje Analiz.doc 160 Regular File 12.02.2009 13:0...
Ermeni Dosyası.doc 671 Regular File 12.02.2009 13:0...
Fabrikatör.doc 240 Regular File 12.02.2009 13:0...
Fabrikatör.doc.FileSlack 1 File Slack
mafia.doc 200 Regular File 12.02.2009 13:0...
mit medya.doc 322 Regular File 12.02.2009 13:0...
panzehir.doc 227 Regular File 12.02.2009 13:0...
panzehir.doc.FileSlack 1 File Slack
Properties
Name Fabrikatör.doc.FileSlack
File Class File Slack
File Size 512
Physical Size 512
Properties
Hex Value Int...
Custom Conte...
Sel start = 38, len = 24
IMAGE.001/Partition 2 [55348MB]/EXPER [NTFS]/[root]/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/proje/Fabrikatör.doc.FileSlack
NUM
TR
09:40
09.12.2011

webroot Prevx Research Division

Google Translate
Select Language
Google Gadgets powered by Google

"B00IJWPU.EXE"

MALICIOUS SOFTWARE

FREE PC CLEANUP FROM WEBROOT

Use Webroot SecureAnywhere to remove **B00IJWPU.EXE.**

"Just when you thought it couldn't get any better or faster. The Webroot scanning engine is 'high octane' with a hidden nitrous oxide system. Bravo!!!"

W. LODZINSKI, SECUREANYWHERE USER

Get Free PC Cleanup

ASSOCIATED MALWARE GROUPS

The filename is associated with the malware group:

- Malicious Software

FILE BEHAVIOR

B00IJWPU.EXE has been seen to perform the following behavior:

- The Process is packed and/or encrypted using a software packing process
- Adds a Registry Key (RUN) to auto start Programs on system start up
- This process creates other processes on disk
- Writes to another Process's Virtual Memory (Process Hijacking)
- The process hooks code into all running processes which could allow it to take control of the system or record keyboard input, mouse activity and screen contents
- Violates Windows/Vista Physical Memory Protection allowing it to look inside the data areas of other programs
- This Process Deletes Other Processes From Disk
- Executes a Process
- Copies files
- Injects code into other processes
- Hooks the WININET.DLL function allowing it to read or copy Http and Https web page content and session information
- Registers a Dynamic Link Library File

B00IJWPU.EXE has been the subject of the following behavior:

- Created as a process on disk
- Executed as a Process
- Has code inserted into its Virtual Memory space by other programs
- Added as a Registry auto start to load Program on Boot up
- Deleted as a process from disk
- Copied to multiple locations on the system

COUNTRY OF ORIGIN

The filename **B00IJWPU.EXE** was first seen on Oct 24 2009 in the following geographical regions of the Webroot community:

- Georgia on Oct 24 2009
- The United Kingdom on Nov 18 2009
- Turkey on Nov 18 2009
- Saudi Arabia on Nov 21 2009
- Morocco on Apr 3 2010
- Egypt on Nov 10 2010

FILE NAME ALIASES

B00IJWPU.EXE can also use the following file names:

- HERSS.EXE
- WCGSWA.EXE
- DPLYIM~1.EXE

FILESIZES

The following file size has been seen:

- 292,318 bytes
- 381,584 bytes
- 150,543 bytes
- 292,308 bytes
- 146,447 bytes

FILE TYPE

The filename B00IJWPU.EXE refers to many versions of an executable program.

HELP THE WEBROOT COMMUNITY TO FIGHT CYBER CRIME

We are always looking for ways to improve the quality and speed of research to help us protect you from malicious software and cyber crime.

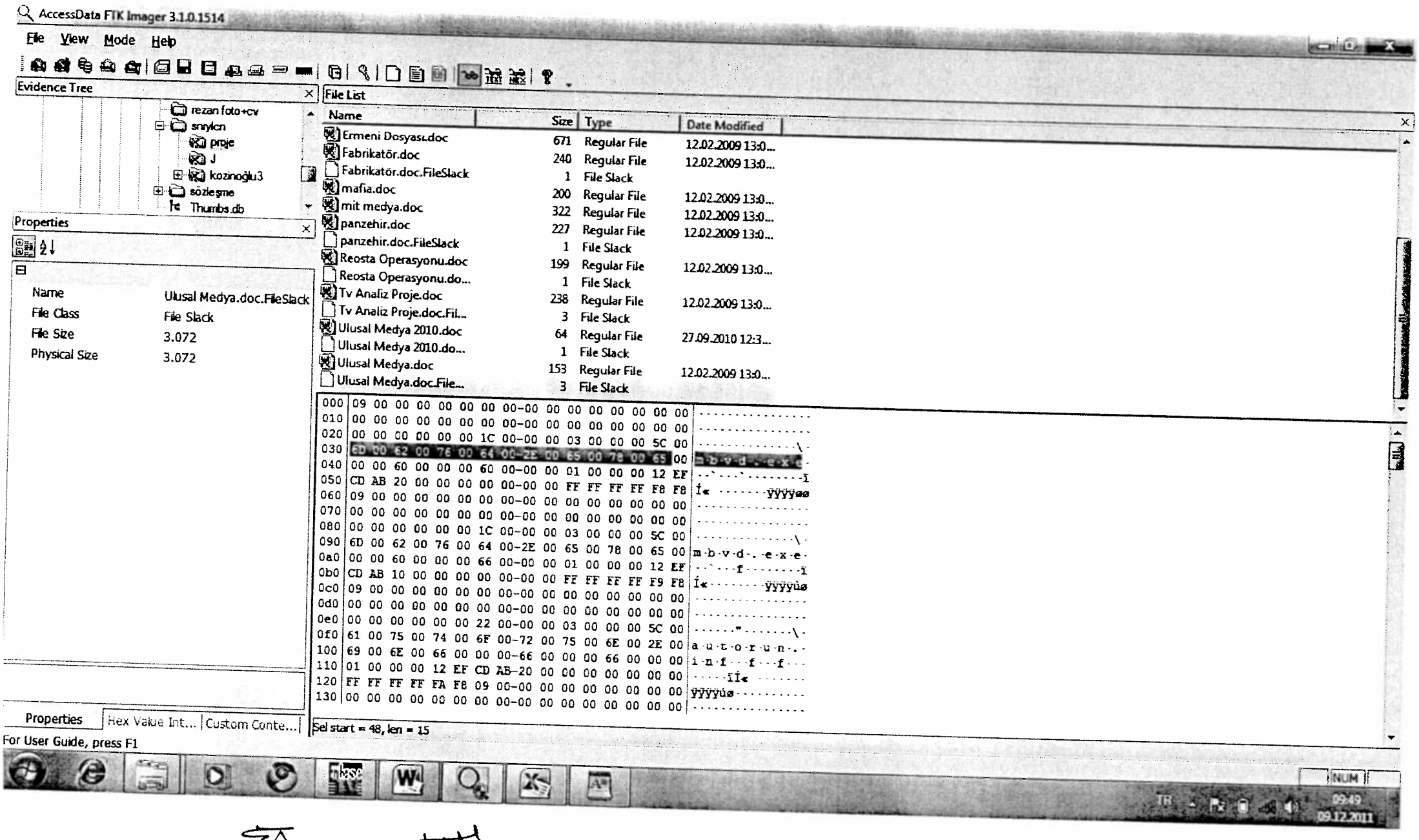
The filename referred to in this report is often associated with PC infections. If you have a program of this name on your PC and would like to help our research please tell us what you know in the form below:

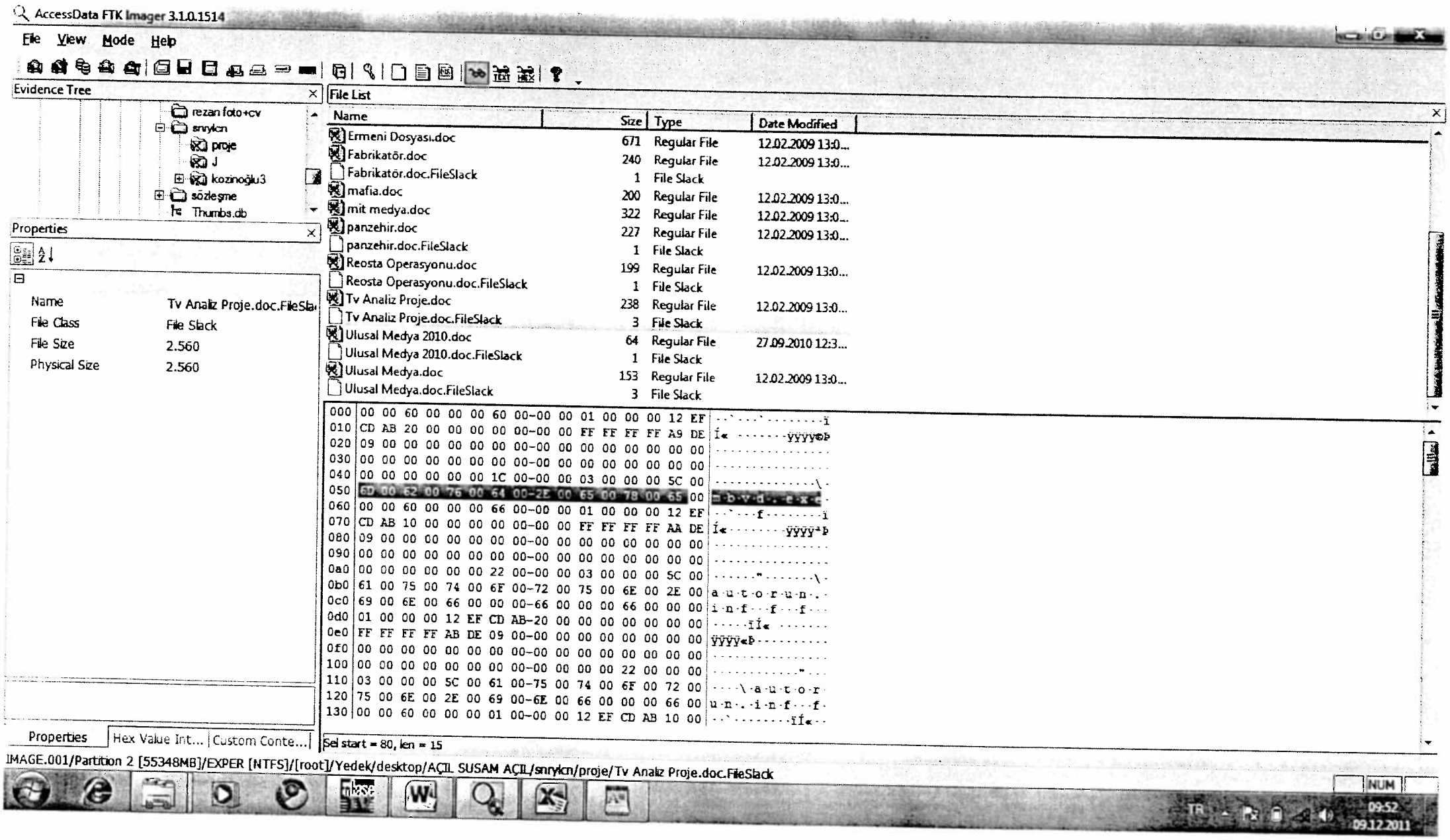
- I have this file on my PC and believe it is an infection
- I have this file on my PC and think it has made my PC slower
- My firewall asked if I wanted to let this file have access to the Internet
- My PC will not work since I noticed this file on it
- My antivirus detected this file but won't remove it
- I know what this file is and believe it is a Safe program
- I am the author of this file and would like to discuss how to have it reclassified as safe

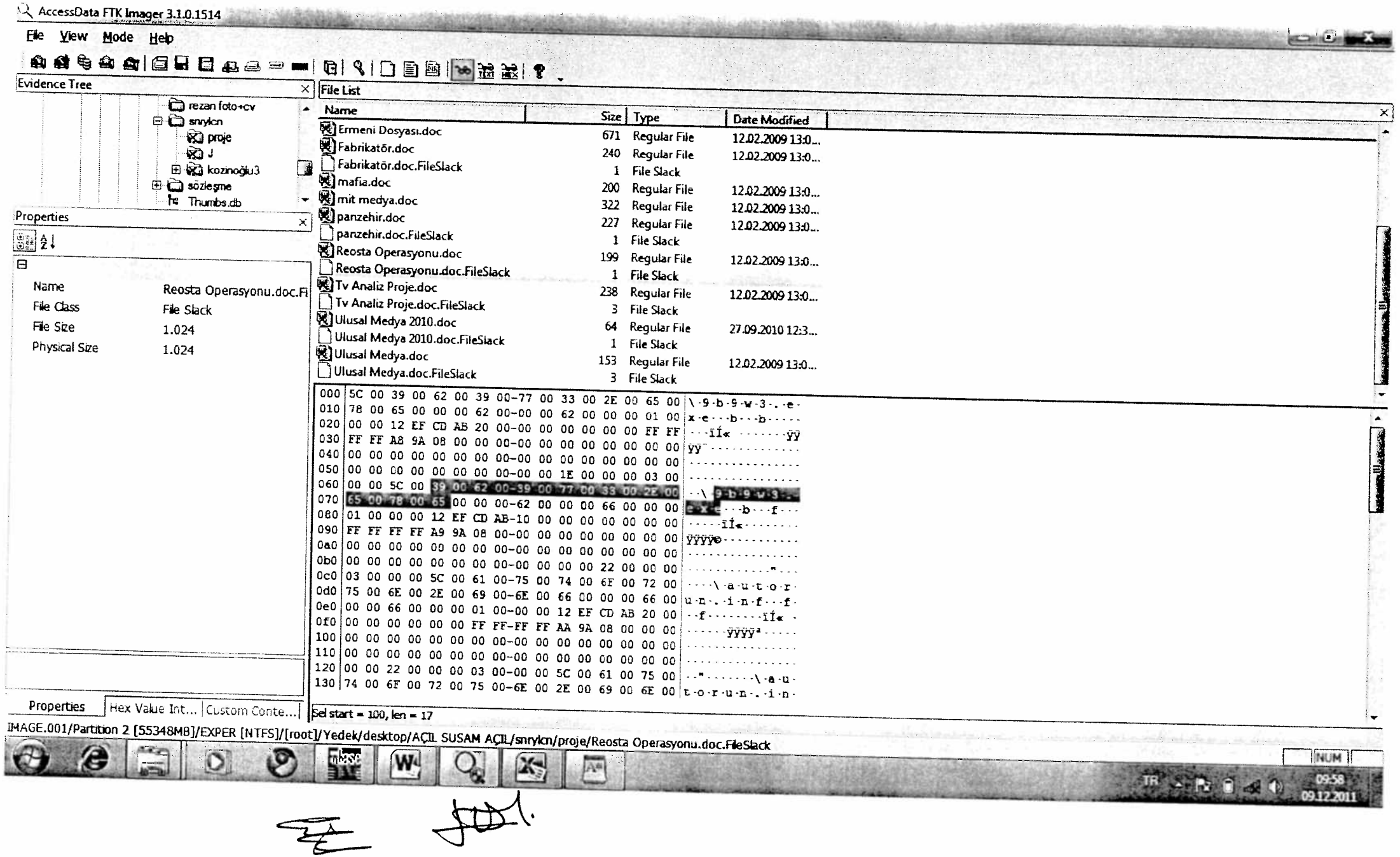
Further Comments or information you'd like to share: *(optional)*

Your email address if you would like us to contact you about this file and any concerns you may have: *(optional)*

Send Information »


AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
rezan foto+cv
snylcn
proje
J
kozinoğlu3
sözleşme
Thumbs.db
File List
Name
Size
Type
Date Modified
Ermeni Dosyası.doc 671 Regular File 12.02.2009 13:0...
Fabrikatör.doc 240 Regular File 12.02.2009 13:0...
Fabrikatör.doc.FileSlack 1 File Slack
mafia.doc 200 Regular File 12.02.2009 13:0...
mit medya.doc 322 Regular File 12.02.2009 13:0...
panzehir.doc 227 Regular File 12.02.2009 13:0...
panzehir.doc.FileSlack 1 File Slack
Reosta Operasyonu.doc 199 Regular File 12.02.2009 13:0...
Reosta Operasyonu.do... 1 File Slack
Tv Analiz Proje.doc 238 Regular File 12.02.2009 13:0...
Tv Analiz Proje.doc.Fil... 3 File Slack
Ulusal Medya 2010.doc 64 Regular File 27.09.2010 12:3...
Ulusal Medya 2010.do... 1 File Slack
Ulusal Medya.doc 153 Regular File 12.02.2009 13:0...
Ulusal Medya.doc.File... 3 File Slack
Properties
Name Ulusal Medya.doc.FileSlack
File Class File Slack
File Size 3.072
Physical Size 3.072
Properties
Hex Value Int...
Custom Conte...
Sel start = 48, len = 15
For User Guide, press F1
NUM
TR
09:49
09.12.2011


AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
rezan foto+cv
snrykcn
proje
J
kozinoğlu3
sözleşme
Thumbs.db
Properties
Name Tv Analiz Proje.doc.FileSla
File Class File Slack
File Size 2.560
Physical Size 2.560
Properties
Hex Value Int...
Custom Conte...
File List
Name Size Type Date Modified
Ermeni Dosyası.doc 671 Regular File 12.02.2009 13:0...
Fabrikatör.doc 240 Regular File 12.02.2009 13:0...
Fabrikatör.doc.FileSlack 1 File Slack
mafia.doc 200 Regular File 12.02.2009 13:0...
mit medya.doc 322 Regular File 12.02.2009 13:0...
panzehir.doc 227 Regular File 12.02.2009 13:0...
panzehir.doc.FileSlack 1 File Slack
Reosta Operasyonu.doc 199 Regular File 12.02.2009 13:0...
Reosta Operasyonu.doc.FileSlack 1 File Slack
Tv Analiz Proje.doc 238 Regular File 12.02.2009 13:0...
Tv Analiz Proje.doc.FileSlack 3 File Slack
Ulusal Medya 2010.doc 64 Regular File 27.09.2010 12:3...
Ulusal Medya 2010.doc.FileSlack 1 File Slack
Ulusal Medya.doc 153 Regular File 12.02.2009 13:0...
Ulusal Medya.doc.FileSlack 3 File Slack
000 00 00 60 00 00 00 60 00-00 00 01 00 00 00 12 EF
010 CD AB 20 00 00 00 00 00-00 00 FF FF FF FF A9 DE
020 09 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
040 00 00 00 00 00 00 1C 00-00 00 03 00 00 00 5C 00
050 6D 00 62 00 76 00 64 00-2E 00 65 00 78 00 65 00
060 00 00 60 00 00 00 66 00-00 00 01 00 00 00 12 EF
070 CD AB 10 00 00 00 00 00-00 00 FF FF FF FF AA DE
080 09 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0a0 00 00 00 00 00 00 22 00-00 00 03 00 00 00 5C 00
0b0 61 00 75 00 74 00 6F 00-72 00 75 00 6E 00 2E 00
0c0 69 00 6E 00 66 00 00 00-66 00 00 00 66 00 00 00
0d0 01 00 00 00 12 EF CD AB-20 00 00 00 00 00 00 00
0e0 FF FF FF FF AB DE 09 00-00 00 00 00 00 00 00 00
0f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
100 00 00 00 00 00 00 00 00-00 00 00 00 22 00 00 00
110 03 00 00 00 5C 00 61 00-75 00 74 00 6F 00 72 00
120 75 00 6E 00 2E 00 69 00-6E 00 66 00 00 00 66 00
130 00 00 60 00 00 00 01 00-00 00 12 EF CD AB 10 00
Sel start = 80, len = 15
IMAGE.001/Partition 2 [55348MB]/EXPER [NTFS]/[root]/Yedek/desktop/AÇIL SUSAM AÇIL/snrykcn/proje/Tv Analiz Proje.doc.FileSlack
NUM
TR
09:52
09.12.2011


AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
rezan foto+cv
snrylcn
proje
J
kozinoğlu3
sözleşme
Thumbs.db
Properties
Name Reosta Operasyonu.doc.Fi
File Class File Slack
File Size 1.024
Physical Size 1.024
Properties
Hex Value Int...
Custom Conte...
File List
Name
Size
Type
Date Modified
Ermeni Dosyası.doc 671 Regular File 12.02.2009 13:0...
Fabrikatör.doc 240 Regular File 12.02.2009 13:0...
Fabrikatör.doc.FileSlack 1 File Slack
mafia.doc 200 Regular File 12.02.2009 13:0...
mit medya.doc 322 Regular File 12.02.2009 13:0...
panzehir.doc 227 Regular File 12.02.2009 13:0...
panzehir.doc.FileSlack 1 File Slack
Reosta Operasyonu.doc 199 Regular File 12.02.2009 13:0...
Reosta Operasyonu.doc.FileSlack 1 File Slack
Tv Analiz Proje.doc 238 Regular File 12.02.2009 13:0...
Tv Analiz Proje.doc.FileSlack 3 File Slack
Ulusal Medya 2010.doc 64 Regular File 27.09.2010 12:3...
Ulusal Medya 2010.doc.FileSlack 1 File Slack
Ulusal Medya.doc 153 Regular File 12.02.2009 13:0...
Ulusal Medya.doc.FileSlack 3 File Slack
000 5C 00 39 00 62 00 39 00-77 00 33 00 2E 00 65 00
010 78 00 65 00 00 00 62 00-00 00 62 00 00 00 01 00
020 00 00 12 EF CD AB 20 00-00 00 00 00 00 00 FF FF
030 FF FF A8 9A 08 00 00 00-00 00 00 00 00 00 00 00
040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
050 00 00 00 00 00 00 00 00-00 00 1E 00 00 00 03 00
060 00 00 5C 00 39 00 62 00-39 00 77 00 33 00 2E 00
070 65 00 78 00 65 00 00 00-00 62 00 00 00 66 00 00 00
080 01 00 00 00 12 EF CD AB-10 00 00 00 00 00 00 00 00
090 FF FF FF FF A9 9A 08 00-00 00 00 00 00 00 00 00 00
0a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
0b0 00 00 00 00 00 00 00 00-00 00 00 00 22 00 00 00
0c0 03 00 00 00 5C 00 61 00-75 00 74 00 6F 00 72 00
0d0 75 00 6E 00 2E 00 69 00-6E 00 66 00 00 00 66 00
0e0 00 00 66 00 00 00 01 00-00 00 12 EF CD AB 20 00
0f0 00 00 00 00 00 00 FF FF-FF FF AA 9A 08 00 00 00
100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
120 00 00 22 00 00 00 03 00-00 00 5C 00 61 00 75 00
130 74 00 6F 00 72 00 75 00-6E 00 2E 00 69 00 6E 00
Sel start = 100, len = 17
IMAGE.001/Partition 2 [55348MB]/EXPER [NTFS]/[root]/Yedek/desktop/AÇIL SUSAM AÇIL/snrylcn/proje/Reosta Operasyonu.doc.FileSlack
NUM
TR
09:58
09.12.2011

webroot Prevx Research Division

Google Translate
Select Language

"9B9W3.EXE"

CLOAKED MALWARE

FREE PC CLEANUP FROM WEBROOT

Use Webroot SecureAnywhere to remove **9B9W3.EXE.**

"Just when you thought it couldn't get any better or faster. The Webroot scanning engine is 'high octane' with a hidden nitrous oxide system. Bravo!!!"

W. LODZINSKI, SECUREANYWHERE USER

Get Free PC Cleanup

ASSOCIATED MALWARE GROUPS

The filename is associated with the malware groups:

- Cloaked Malware
- Malicious Software

FILE BEHAVIOR

9B9W3.EXE has been seen to perform the following behavior:

- The Process is packed and/or encrypted using a software packing process
- Executes a Process

9B9W3.EXE has been the subject of the following behavior:

- Created as a process on disk
- Executed as a Process

COUNTRY OF ORIGIN

The filename 9B9W3.EXE was first seen on Mar 7 2010 in the following geographical regions of the Webroot community:

- Poland on Mar 7 2010
- The United Kingdom on Mar 7 2010

FILESIZES

The following file size has been seen:

- 115,127 bytes
- 286,720 bytes
- 126,351 bytes
- 274,498 bytes

FILE TYPE

The filename 9B9W3.EXE refers to many versions of an executable program.

EK-8

HELP THE WEBROOT COMMUNITY TO FIGHT CYBER CRIME

We are always looking for ways to improve the quality and speed of research to help us protect you from malicious software and cyber crime.

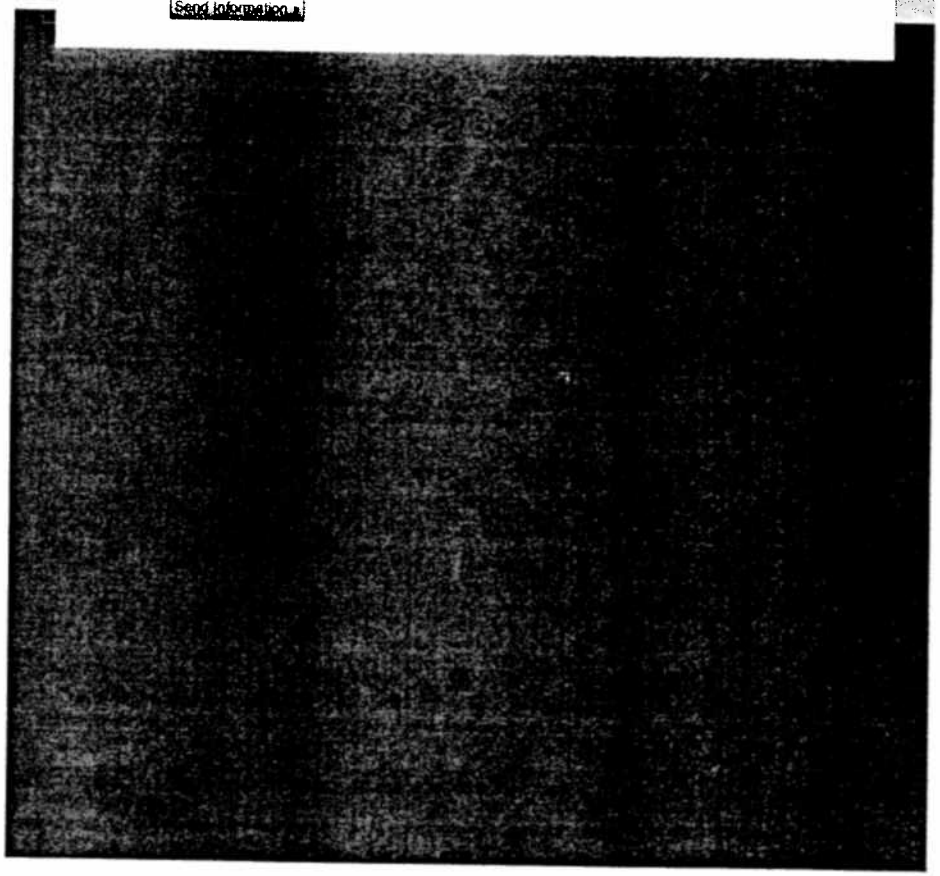
The filename referred to in this report is often associated with PC infections. If you have a program of this name on your PC and would like to help our research please tell us what you know in the form below:

- I have this file on my PC and believe it is an infection
- I have this file on my PC and think it has made my PC slower
- My firewall asked if I wanted to let this file have access to the Internet
- My PC will not work since I noticed this file on it
- My antivirus detected this file but won't remove it
- I know what this file is and believe it is a Safe program
- I am the author of this file and would like to discuss how to have it reclassified as safe

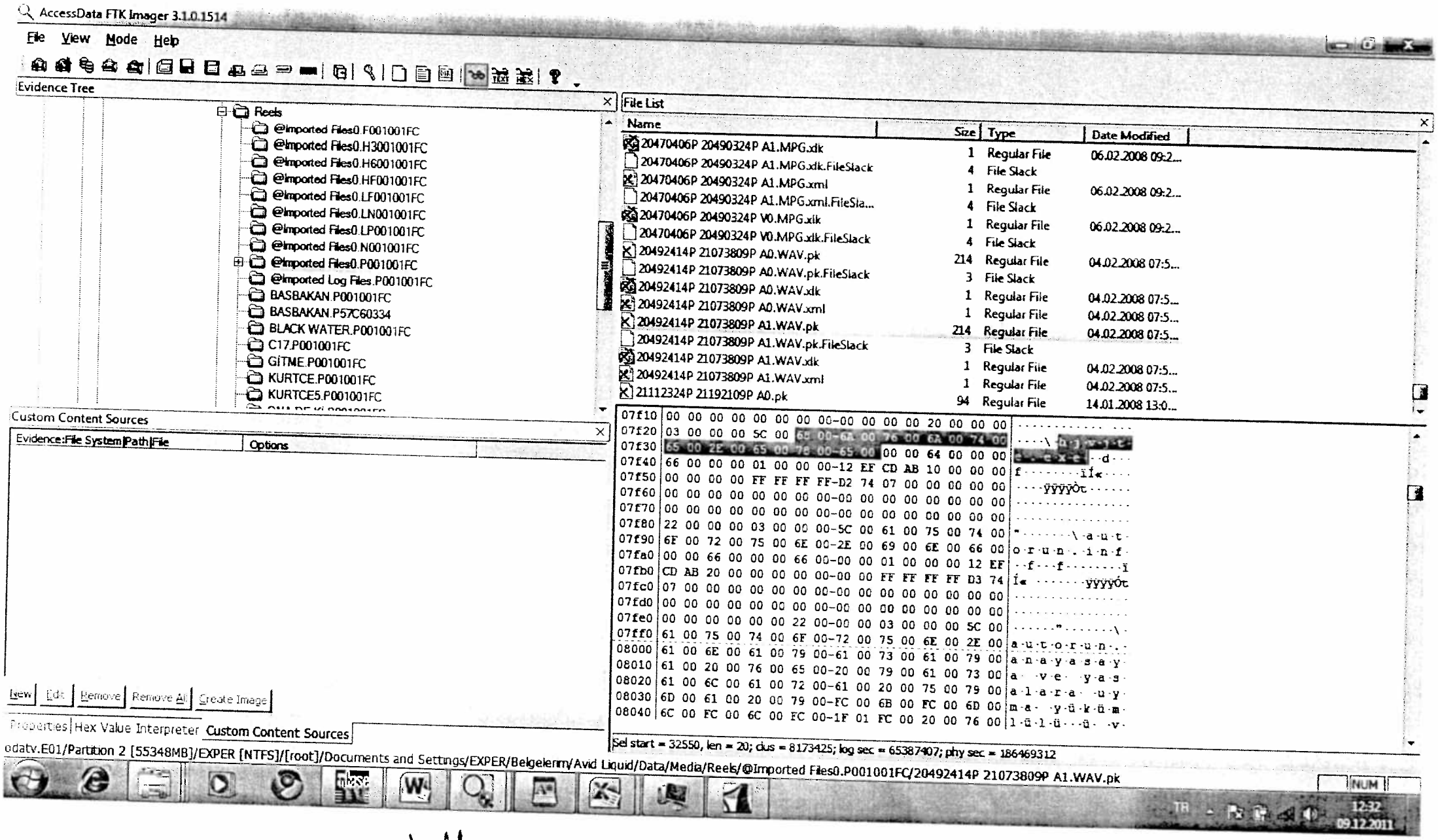
Further Comments or information you'd like to share: *(optional)*

Your email address if you would like us to contact you about this file and any concerns you may have: *(optional)*

Send Information



EK-8


AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
Reels
@Imported Files0.F001001FC
@Imported Files0.H3001001FC
@Imported Files0.H6001001FC
@Imported Files0.HF001001FC
@Imported Files0.LF001001FC
@Imported Files0.LN001001FC
@Imported Files0.LP001001FC
@Imported Files0.N001001FC
@Imported Files0.P001001FC
@Imported Log Files.P001001FC
BASBAKAN.P001001FC
BASBAKAN.P57C60334
BLACK WATER.P001001FC
C17.P001001FC
GİTME.P001001FC
KURTCE.P001001FC
KURTCE5.P001001FC
File List
Name
Size
Type
Date Modified
20470406P 20490324P A1.MPG.xdk 1 Regular File 06.02.2008 09:2...
20470406P 20490324P A1.MPG.xdk.FileSlack 4 File Slack
20470406P 20490324P A1.MPG.xml 1 Regular File 06.02.2008 09:2...
20470406P 20490324P A1.MPG.xml.FileSla... 4 File Slack
20470406P 20490324P V0.MPG.xdk 1 Regular File 06.02.2008 09:2...
20470406P 20490324P V0.MPG.xdk.FileSlack 4 File Slack
20492414P 21073809P A0.WAV.pk 214 Regular File 04.02.2008 07:5...
20492414P 21073809P A0.WAV.pk.FileSlack 3 File Slack
20492414P 21073809P A0.WAV.xdk 1 Regular File 04.02.2008 07:5...
20492414P 21073809P A0.WAV.xml 1 Regular File 04.02.2008 07:5...
20492414P 21073809P A1.WAV.pk 214 Regular File 04.02.2008 07:5...
20492414P 21073809P A1.WAV.pk.FileSlack 3 File Slack
20492414P 21073809P A1.WAV.xdk 1 Regular File 04.02.2008 07:5...
20492414P 21073809P A1.WAV.xml 1 Regular File 04.02.2008 07:5...
21112324P 21192109P A0.pk 94 Regular File 14.01.2008 13:0...
Custom Content Sources
Evidence:File System|Path|File
Options
New Edit Remove Remove All Create Image
Properties Hex Value Interpreter Custom Content Sources
Sel start = 32550, len = 20; clus = 8173425; log sec = 65387407; phy sec = 186469312
odatv.E01/Partition 2 [55348MB]/EXPER [NTFS]/[root]/Documents and Settings/EXPER/Belgelerim/Avid Liquid/Data/Media/Reels/@Imported Files0.P001001FC/20492414P 21073809P A1.WAV.pk
NUM
TR
12:52
09.12.2011

webroot Prevx Research Division

GoogleTranslate Select Language

"HJVJTE.EXE"

CLOAKED MALWARE

FREE PC CLEANUP FROM WEBROOT

Use Webroot SecureAnywhere to remove **HJVJTE.EXE.**

"Just when you thought it couldn't get any better or faster. The Webroot scanning engine is 'high octane' with a hidden nitrous oxide system. Bravo!!!"

W. LODZINSKI, SECUREANYWHERE USER

Get Free PC Cleanup

ASSOCIATED MALWARE GROUPS

The unsafe files using this name are associated with the malware groups:

- Cloaked Malware
- Malicious Software

FILE BEHAVIOR

HJVJTE.EXE has been seen to perform the following behavior:

- The Process is packed and/or encrypted using a software packing process
- Writes to another Process's Virtual Memory (Process Hijacking)
- Adds a Registry Key (RUN) to auto start Programs on system start up
- This process creates other processes on disk
- The process hooks code into all running processes which could allow it to take control of the system or record keyboard input, mouse activity and screen contents
- Violates Windows/Vista Physical Memory Protection allowing it to look inside the data areas of other programs
- This Process Deletes Other Processes From Disk
- Executes a Process
- Copies files
- Injects code into other processes
- Registers a Dynamic Link Library File

HJVJTE.EXE has been the subject of the following behavior:

- Executed as a Process
- Created as a process on disk
- Has code inserted into its Virtual Memory space by other programs
- Added as a Registry auto start to load Program on Boot up
- Deleted as a process from disk
- Copied to multiple locations on the system

COUNTRY OF ORIGIN

The filename HJVJTE.EXE was first seen on Oct 27 2009 in the following geographical regions of the Webroot community:

- India on Oct 27 2009
- The United Kingdom on Nov 18 2009
- Turkey on Nov 18 2009
- Brazil on Nov 30 2009
- Vietnam on Dec 24 2009

FILE NAME ALIASES

HJVJTE.EXE can also use the following file names:

- EM YEU 2 WEBSITE.EXE
- PHUONG TH WEBSITE.EXE
- HERSS.EXE
- (x-x).EXE
- 43117082.DAT
- LAN PHU WEBSITE.EXE
- HOT GIRL XUAN DINH.EXE
- DPLUQA~1.EXE
- 45296211.EXE
- 10151236.DAT

FILESIZES

The following file size has been seen:

- 292,822 bytes
- 113,953 bytes
- 292,826 bytes
- 101,164 bytes
- 137,726 bytes
- 147,328 bytes

FILE TYPE

The filename HJVJTE.EXE refers to many versions of an executable program.

HELP THE WEBROOT COMMUNITY TO FIGHT CYBER CRIME

We are always looking for ways to improve the quality and speed of research to help us protect you from malicious software and cyber crime.

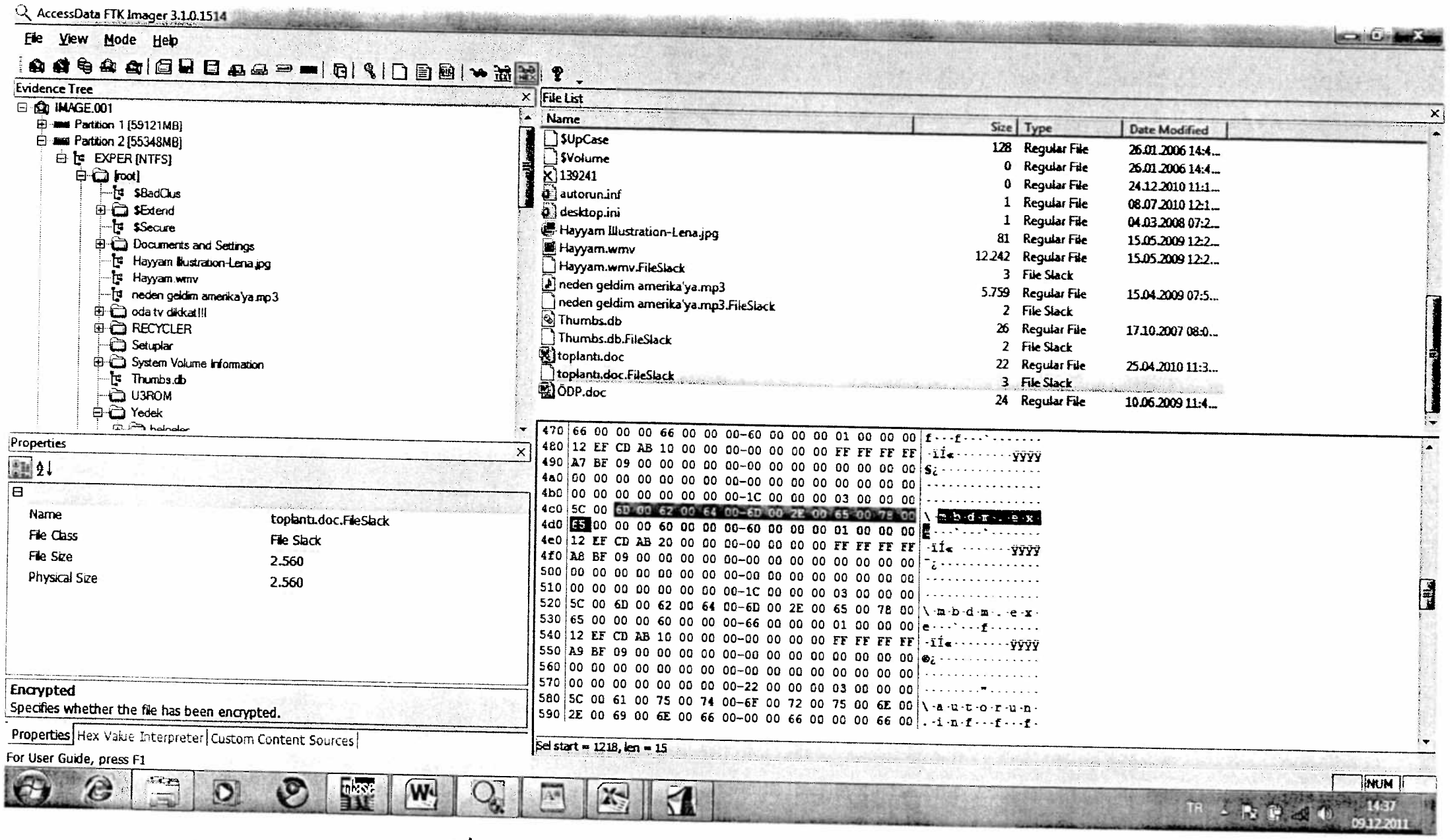
The filename referred to in this report is often associated with PC infections. If you have a program of this name on your PC and would like to help our research please tell us what you know in the form below:

- I have this file on my PC and believe it is an infection
- I have this file on my PC and think it has made my PC slower
- My firewall asked if I wanted to let this file have access to the Internet
- My PC will not work since I noticed this file on it
- My antivirus detected this file but won't remove it
- I know what this file is and believe it is a Safe program
- I am the author of this file and would like to discuss how to have it reclassified as safe

Further Comments or information you'd like to share: *(optional)*

Your email address if you would like us to contact you about this file and any concerns you may have: *(optional)*

Send Information »


AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
IMAGE.001
Partition 1 [59121MB]
Partition 2 [55348MB]
EXPER [NTFS]
[root]
$BadClus
$Extend
$Secure
Documents and Settings
Hayyam Illustration-Lena.jpg
Hayyam.wmv
neden geldim amerika'ya.mp3
oda tv dikkat!!!
RECYCLER
Setuplar
System Volume Information
Thumbs.db
U3ROM
Yedek
File List
Name Size Type Date Modified
$UpCase 128 Regular File 26.01.2006 14:4...
$Volume 0 Regular File 26.01.2006 14:4...
139241 0 Regular File 24.12.2010 11:1...
autorun.inf 1 Regular File 08.07.2010 12:1...
desktop.ini 1 Regular File 04.03.2008 07:2...
Hayyam Illustration-Lena.jpg 81 Regular File 15.05.2009 12:2...
Hayyam.wmv 12.242 Regular File 15.05.2009 12:2...
Hayyam.wmv.FileSlack 3 File Slack
neden geldim amerika'ya.mp3 5.759 Regular File 15.04.2009 07:5...
neden geldim amerika'ya.mp3.FileSlack 2 File Slack
Thumbs.db 26 Regular File 17.10.2007 08:0...
Thumbs.db.FileSlack 2 File Slack
toplantı.doc 22 Regular File 25.04.2010 11:3...
toplantı.doc.FileSlack 3 File Slack
ÖDP.doc 24 Regular File 10.06.2009 11:4...
Properties
Name toplantı.doc.FileSlack
File Class File Slack
File Size 2.560
Physical Size 2.560
Encrypted
Specifies whether the file has been encrypted.
Properties Hex Value Interpreter Custom Content Sources
For User Guide, press F1
Sel start = 1218, len = 15
NUM
TR
14:37
09.12.2011

webroot Prevx Research Division

Google Translate
Select Language
Google Gadgets powered by Google

MBDM.EXE

MALICIOUS SOFTWARE

FREE PC CLEANUP FROM WEBROOT

Use Webroot SecureAnywhere to remove **MBDM.EXE.**

"Just when you thought it couldn't get any better or faster. The Webroot scanning engine is 'high octane' with a hidden nitrous oxide system. Bravo!!!"

W. LODZINSKI, SECUREANYWHERE USER

Get Free PC Cleanup

ASSOCIATED MALWARE GROUPS

The unsafe files using this name are associated with the malware group:

- Malicious Software

FILE BEHAVIOR

MBDM.EXE has been seen to perform the following behavior:

- The Process is packed and/or encrypted using a software packing process
- Executes a Process
- Adds a Registry Key (RUN) to auto start Programs on system start up
- Writes to another Process's Virtual Memory (Process Hijacking)
- This process creates other processes on disk
- This Process Deletes Other Processes From Disk
- Copies files
- Injects code into other processes
- Creates a new Background Service on the machine
- Adds products to the system registry
- Automatically changes your firewall settings to allow itself or other programs to communicate over the internet
- Modifies Windows Security Policies to restrict/expand User Privileges on the machine
- Violates Windows/Vista Physical Memory Protection allowing it to look inside the data areas of other programs
- Disables the Notification Balloon for the Windows Security Center
- Disables Access to the Windows Registry Editor
- Disables Access to the Task Manager built into Windows

MBDM.EXE has been the subject of the following behavior:

- Created as a new Background Service on the machine
- Created as a process on disk
- Executed as a Process
- Added as a Registry auto start to load Program on Boot up
- Has code inserted into its Virtual Memory space by other programs
- Deleted as a process from disk
- Copied to multiple locations on the system

EK-12

COUNTRY OF ORIGIN

The filename MBDM.EXE was first seen on Sep 20 2008 in the following geographical regions of the Webroot community:

- on Sep 20 2008
- The United Kingdom on Dec 22 2009
- Philippines on Dec 22 2009
- Thailand on Aug 18 2010
- Peru on Sep 15 2010
- Chile on Jul 1 2011

FILE NAME ALIASES

MBDM.EXE can also use the following file names:

- HERSS.EXE
- 4993DC~1.EXE

FILESIZES

The following file size has been seen:

- 327,680 bytes
- 386,241 bytes
- 397,312 bytes
- 208,384 bytes
- 364,544 bytes
- 231,076 bytes

FILE TYPE

The filename MBDM.EXE is used by multiple object types including objects,executable programs.

HELP THE WEBROOT COMMUNITY TO FIGHT CYBER CRIME

We are always looking for ways to improve the quality and speed of research to help us protect you from malicious software and cyber crime.

The filename referred to in this report is often associated with PC infections. If you have a program of this name on your PC and would like to help our research please tell us what you know in the form below:

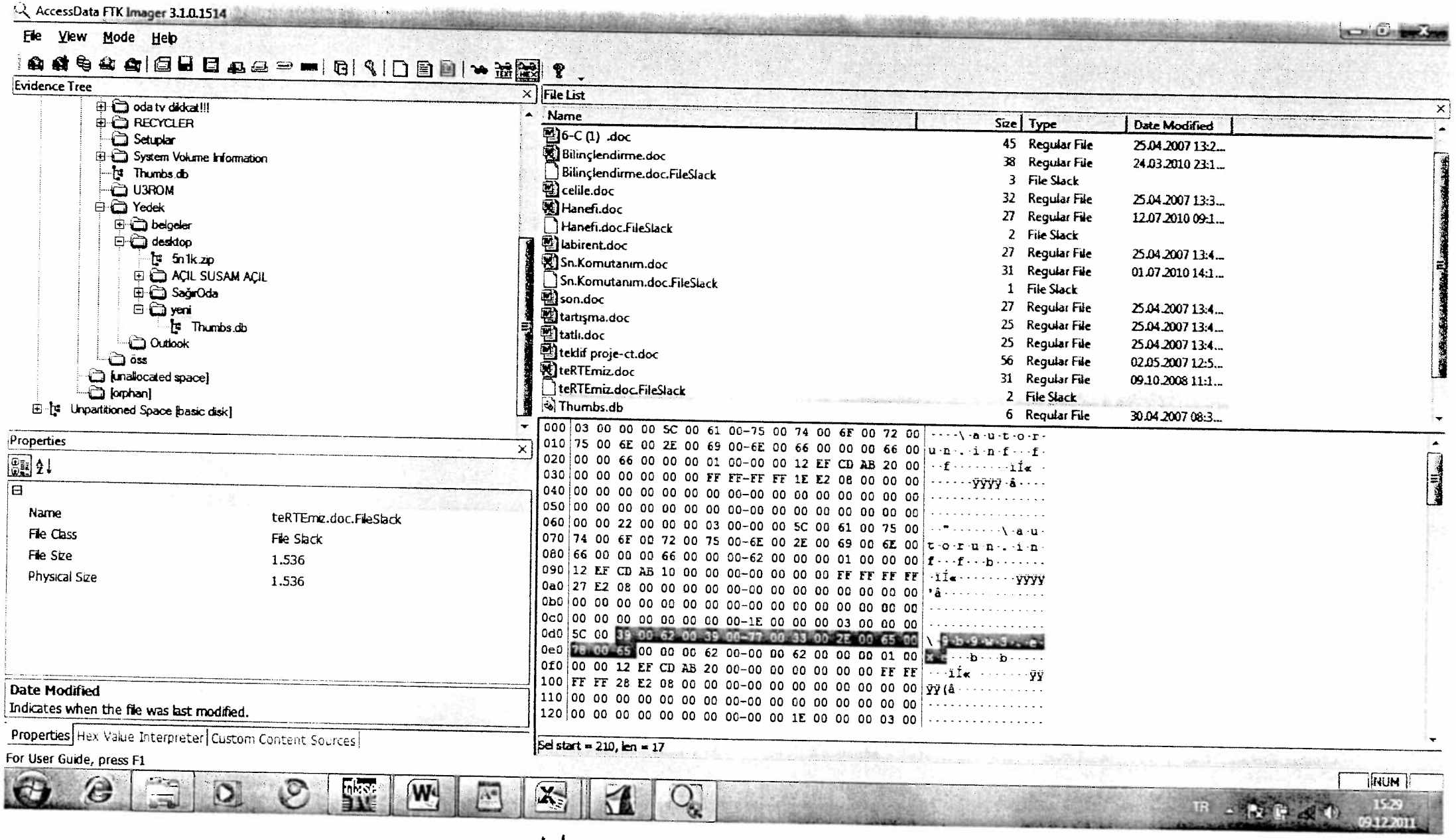
- I have this file on my PC and believe it is an infection
- I have this file on my PC and think it has made my PC slower
- My firewall asked if I wanted to let this file have access to the Internet
- My PC will not work since I noticed this file on it
- My antivirus detected this file but won't remove it
- I know what this file is and believe it is a Safe program
- I am the author of this file and would like to discuss how to have it reclassified as safe

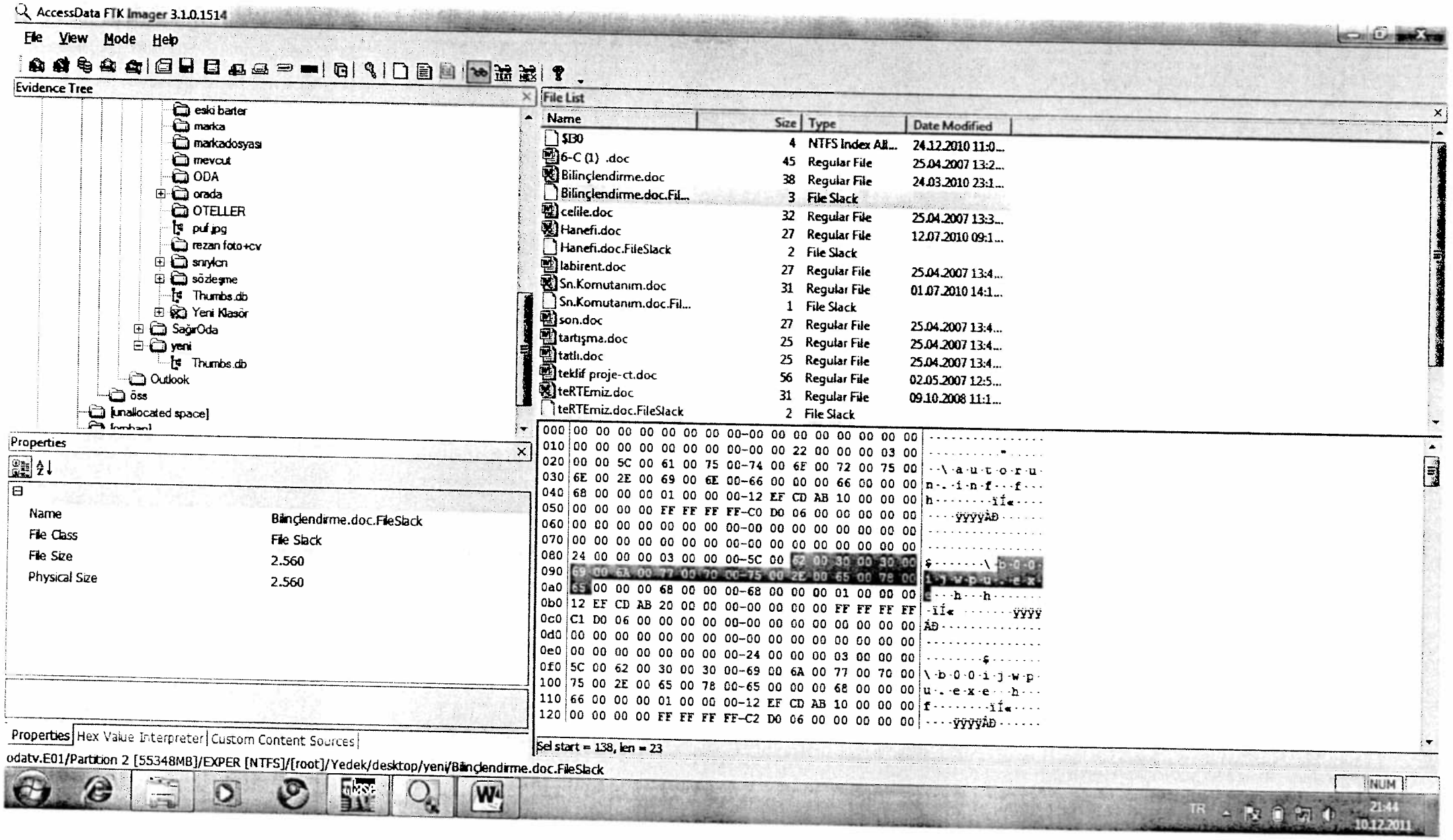
Further Comments or information you'd like to share: *(optional)*

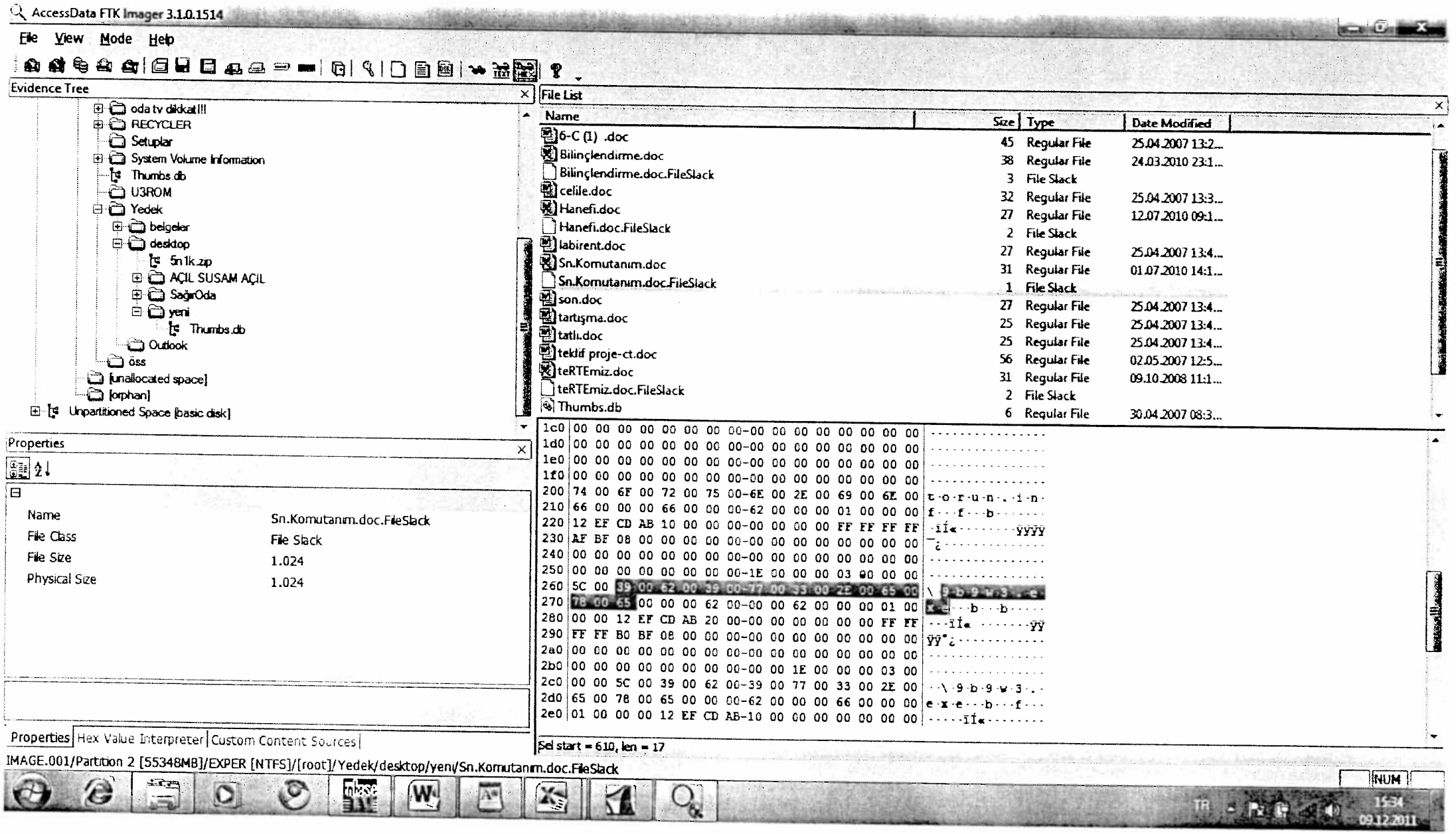
Your email address if you would like us to contact you about this file and any concerns you may have: *(optional)*

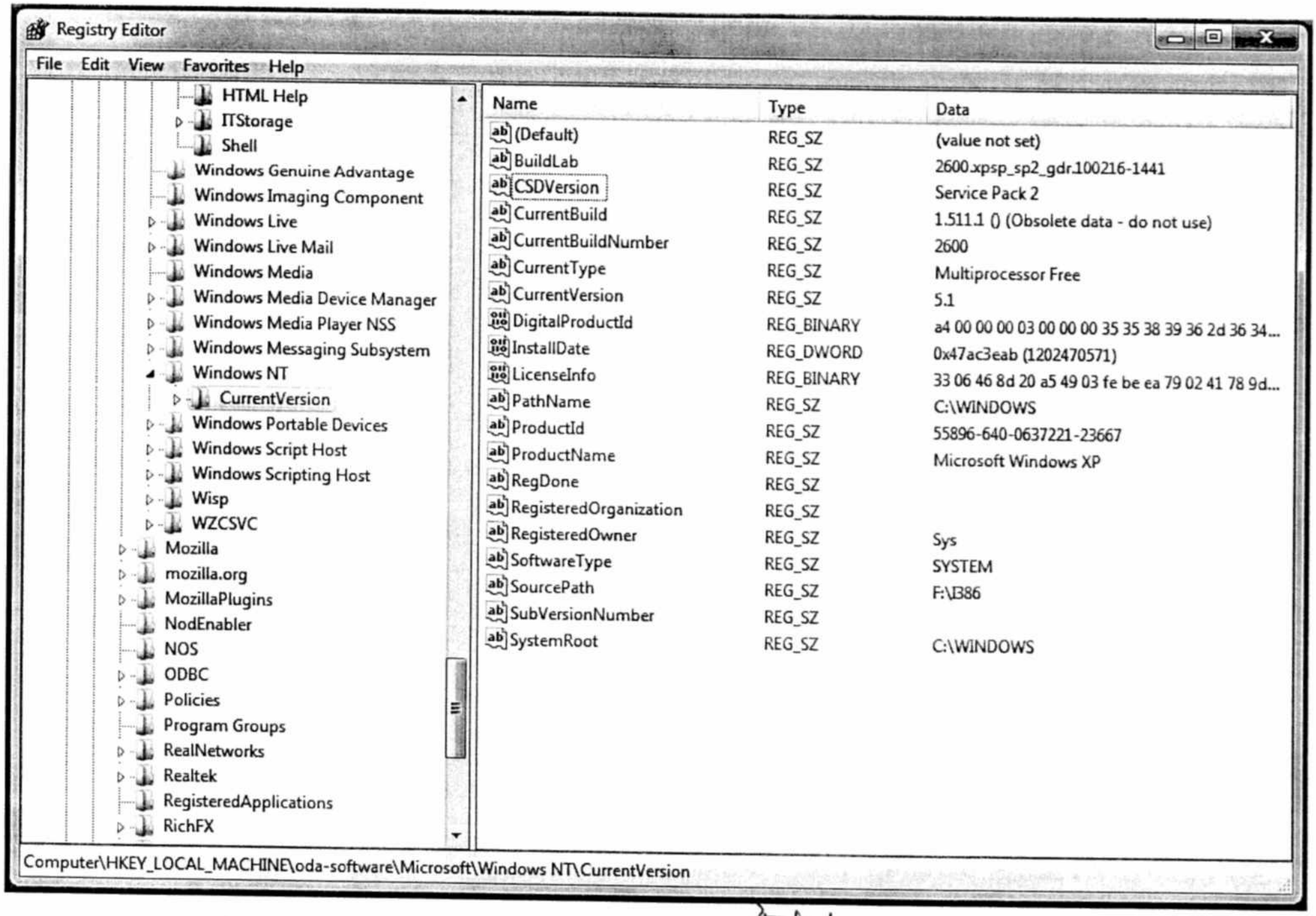
Send Information »

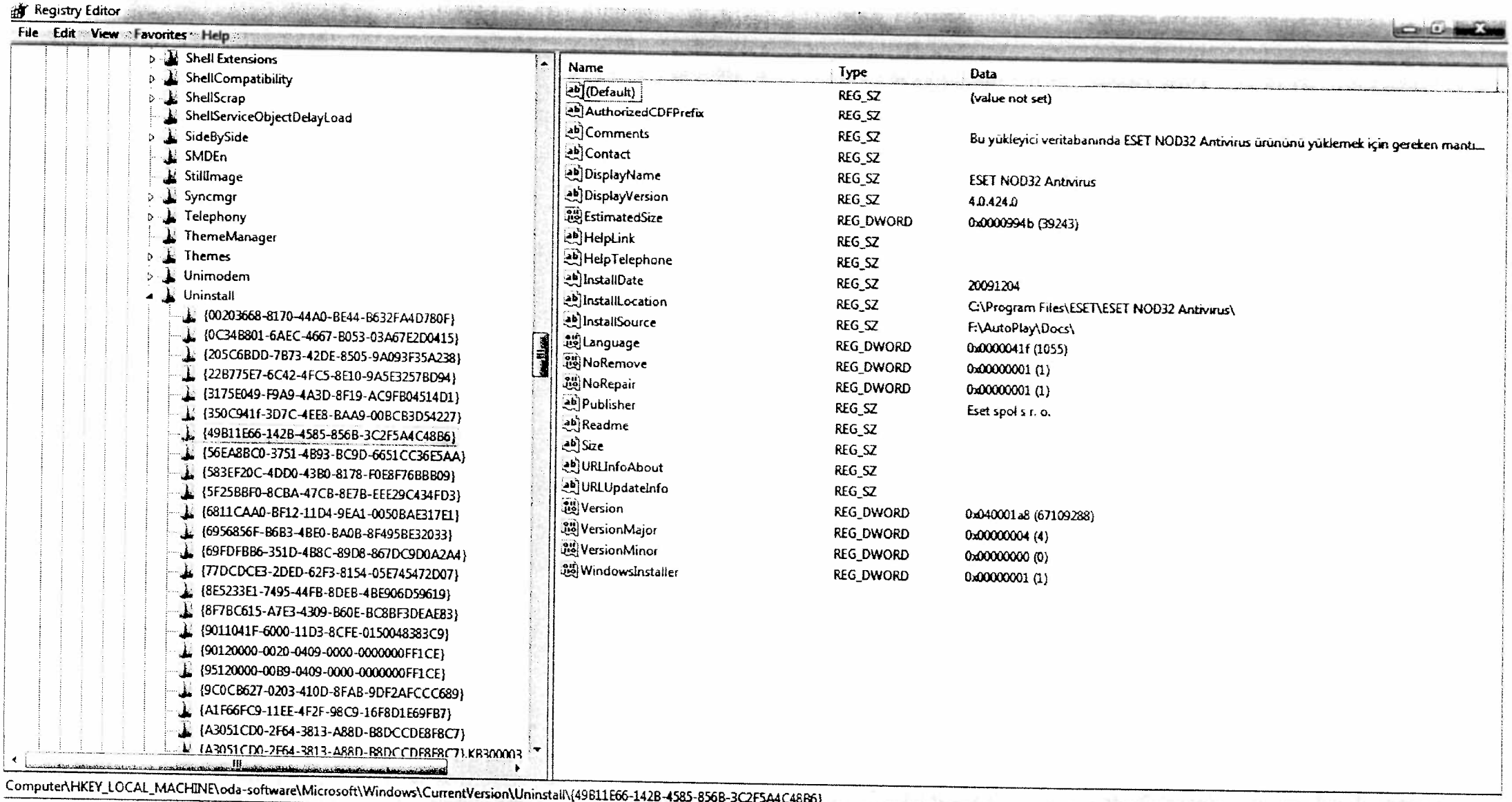
EK-12

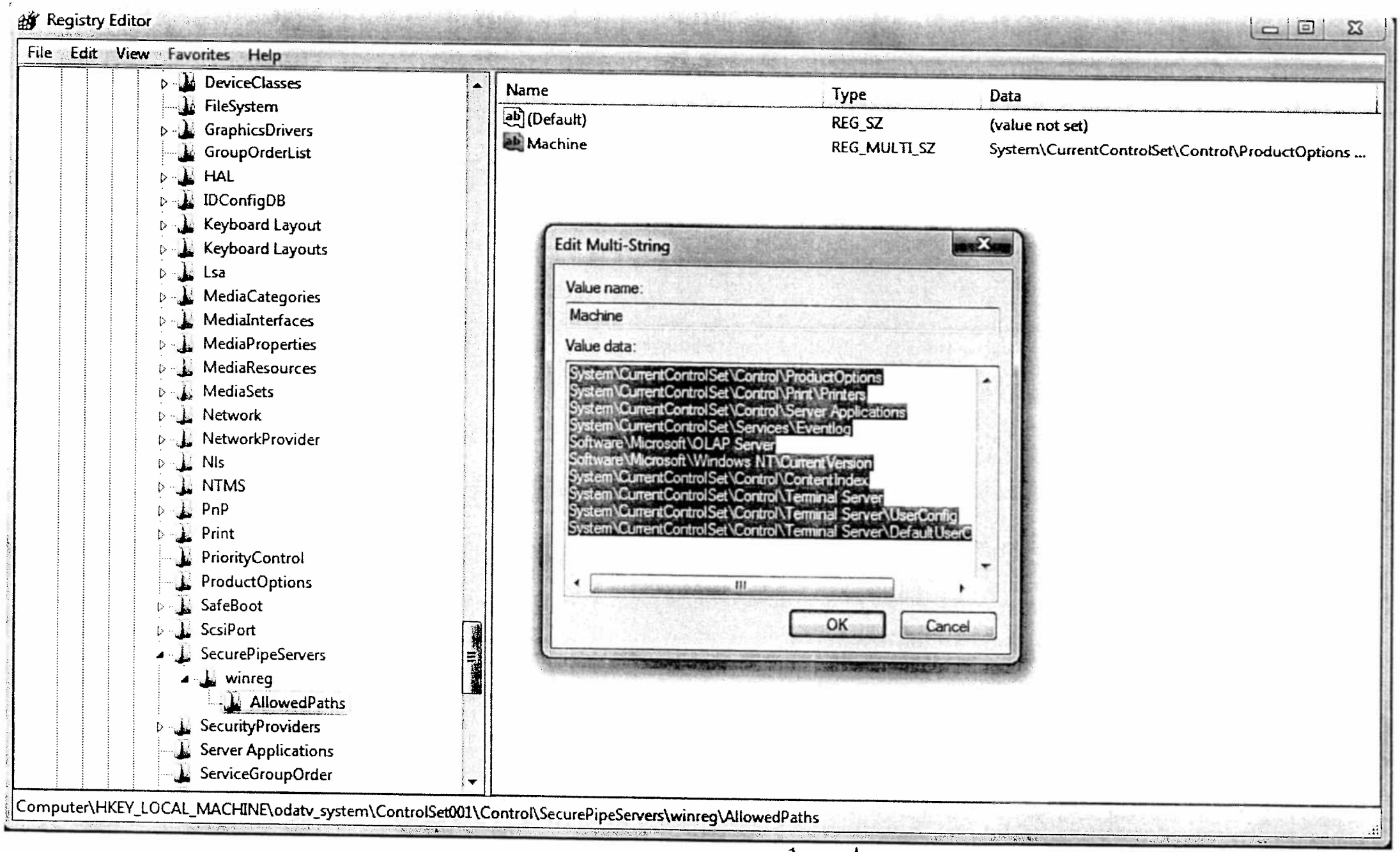

AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
oda tv dikkat!!!
RECYCLER
Setuplar
System Volume Information
Thumbs.db
U3ROM
Yedek
belgeler
desktop
5n1k.zip
AÇIL SUSAM AÇIL
SağırOda
yeni
Thumbs.db
Outlook
oss
[unallocated space]
[orphan]
Unpartitioned Space [basic disk]
File List
Name Size Type Date Modified
6-C (1) .doc 45 Regular File 25.04.2007 13:2...
Bilinçlendirme.doc 38 Regular File 24.03.2010 23:1...
Bilinçlendirme.doc.FileSlack 3 File Slack
celile.doc 32 Regular File 25.04.2007 13:3...
Hanefi.doc 27 Regular File 12.07.2010 09:1...
Hanefi.doc.FileSlack 2 File Slack
labirent.doc 27 Regular File 25.04.2007 13:4...
Sn.Komutanım.doc 31 Regular File 01.07.2010 14:1...
Sn.Komutanım.doc.FileSlack 1 File Slack
son.doc 27 Regular File 25.04.2007 13:4...
tartışma.doc 25 Regular File 25.04.2007 13:4...
tatlı.doc 25 Regular File 25.04.2007 13:4...
teklif proje-ct.doc 56 Regular File 02.05.2007 12:5...
teRTEmiz.doc 31 Regular File 09.10.2008 11:1...
teRTEmiz.doc.FileSlack 2 File Slack
Thumbs.db 6 Regular File 30.04.2007 08:3...
Properties
Name teRTEmiz.doc.FileSlack
File Class File Slack
File Size 1.536
Physical Size 1.536
Date Modified
Indicates when the file was last modified.
Properties Hex Value Interpreter Custom Content Sources
For User Guide, press F1
Sel start = 210, len = 17
NUM
TR
15:29
09.12.2011

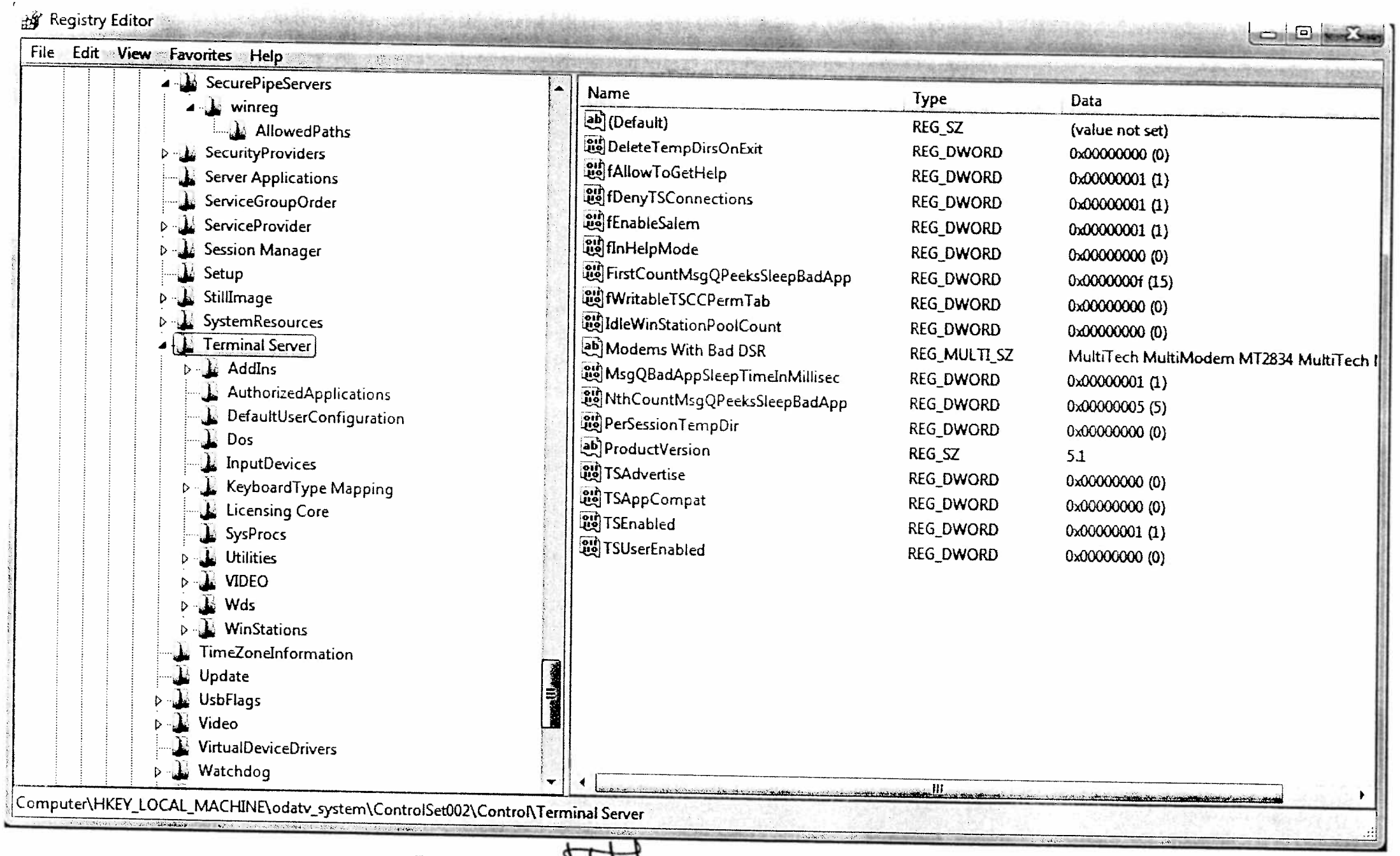

AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
eski bater
marka
markadosyası
mevcut
ODA
orada
OTELLER
puf.jpg
rezan foto+cv
sınıvlcn
sözleşme
Thumbs.db
Yeni Klasör
SağırOda
yeni
Thumbs.db
Outlook
öss
[unallocated space]
File List
Name
Size
Type
Date Modified
$I30 4 NTFS Index All... 24.12.2010 11:0...
6-C (1) .doc 45 Regular File 25.04.2007 13:2...
Bilinçlendirme.doc 38 Regular File 24.03.2010 23:1...
Bilinçlendirme.doc.Fil... 3 File Slack
celile.doc 32 Regular File 25.04.2007 13:3...
Hanefi.doc 27 Regular File 12.07.2010 09:1...
Hanefi.doc.FileSlack 2 File Slack
labirent.doc 27 Regular File 25.04.2007 13:4...
Sn.Komutanım.doc 31 Regular File 01.07.2010 14:1...
Sn.Komutanım.doc.Fil... 1 File Slack
son.doc 27 Regular File 25.04.2007 13:4...
tartışma.doc 25 Regular File 25.04.2007 13:4...
tatlı.doc 25 Regular File 25.04.2007 13:4...
teklif proje-ct.doc 56 Regular File 02.05.2007 12:5...
teRTEmiz.doc 31 Regular File 09.10.2008 11:1...
teRTEmiz.doc.FileSlack 2 File Slack
Properties
Name Bilinçlendirme.doc.FileSlack
File Class File Slack
File Size 2.560
Physical Size 2.560
Properties Hex Value Interpreter Custom Content Sources
Sel start = 138, len = 23
odatv.E01/Partition 2 [55348MB]/EXPER [NTFS]/[root]/Yedek/desktop/yeni/Bilinçlendirme.doc.FileSlack
NUM
TR
21:44
10.12.2011


AccessData FTK Imager 3.1.0.1514
File View Mode Help
Evidence Tree
oda tv dikkat!!!
RECYCLER
Setuplar
System Volume Information
Thumbs.db
U3ROM
Yedek
belgeler
desktop
5n1k.zip
AÇIL SUSAM AÇIL
SağırOda
yeni
Thumbs.db
Outlook
öss
[unallocated space]
[orphan]
Unpartitioned Space [basic disk]
File List
Name Size Type Date Modified
6-C (1) .doc 45 Regular File 25.04.2007 13:2...
Bilinçlendirme.doc 38 Regular File 24.03.2010 23:1...
Bilinçlendirme.doc.FileSlack 3 File Slack
celile.doc 32 Regular File 25.04.2007 13:3...
Hanefi.doc 27 Regular File 12.07.2010 09:1...
Hanefi.doc.FileSlack 2 File Slack
labirent.doc 27 Regular File 25.04.2007 13:4...
Sn.Komutanım.doc 31 Regular File 01.07.2010 14:1...
Sn.Komutanım.doc.FileSlack 1 File Slack
son.doc 27 Regular File 25.04.2007 13:4...
tartışma.doc 25 Regular File 25.04.2007 13:4...
tatlı.doc 25 Regular File 25.04.2007 13:4...
teklif proje-ct.doc 56 Regular File 02.05.2007 12:5...
teRTEmiz.doc 31 Regular File 09.10.2008 11:1...
teRTEmiz.doc.FileSlack 2 File Slack
Thumbs.db 6 Regular File 30.04.2007 08:3...
Properties
Name Sn.Komutanım.doc.FileSlack
File Class File Slack
File Size 1.024
Physical Size 1.024
Properties Hex Value Interpreter Custom Content Sources
Sel start = 610, len = 17
IMAGE.001/Partition 2 [55348MB]/EXPER [NTFS]/[root]/Yedek/desktop/yeni/Sn.Komutanım.doc.FileSlack
NUM
TR
15:34
09.12.2011


Registry Editor
File Edit View Favorites Help
HTML Help
ITStorage
Shell
Windows Genuine Advantage
Windows Imaging Component
Windows Live
Windows Live Mail
Windows Media
Windows Media Device Manager
Windows Media Player NSS
Windows Messaging Subsystem
Windows NT
CurrentVersion
Windows Portable Devices
Windows Script Host
Windows Scripting Host
Wisp
WZCSVC
Mozilla
mozilla.org
MozillaPlugins
NodEnabler
NOS
ODBC
Policies
Program Groups
RealNetworks
Realtek
RegisteredApplications
RichFX
Name Type Data
(Default) REG_SZ (value not set)
BuildLab REG_SZ 2600.xpsp_sp2_gdr.100216-1441
CSDVersion REG_SZ Service Pack 2
CurrentBuild REG_SZ 1.511.1 () (Obsolete data - do not use)
CurrentBuildNumber REG_SZ 2600
CurrentType REG_SZ Multiprocessor Free
CurrentVersion REG_SZ 5.1
DigitalProductId REG_BINARY a4 00 00 00 03 00 00 00 35 35 38 39 36 2d 36 34...
InstallDate REG_DWORD 0x47ac3eab (1202470571)
LicenseInfo REG_BINARY 33 06 46 8d 20 a5 49 03 fe be ea 79 02 41 78 9d...
PathName REG_SZ C:\WINDOWS
ProductId REG_SZ 55896-640-0637221-23667
ProductName REG_SZ Microsoft Windows XP
RegDone REG_SZ
RegisteredOrganization REG_SZ
RegisteredOwner REG_SZ Sys
SoftwareType REG_SZ SYSTEM
SourcePath REG_SZ F:\I386
SubVersionNumber REG_SZ
SystemRoot REG_SZ C:\WINDOWS
Computer\HKEY_LOCAL_MACHINE\oda-software\Microsoft\Windows NT\CurrentVersion


Registry Editor
File Edit View Favorites Help
Shell Extensions
ShellCompatibility
ShellScrap
ShellServiceObjectDelayLoad
SideBySide
SMDEn
StillImage
Syncmgr
Telephony
ThemeManager
Themes
Unimodem
Uninstall
{00203668-8170-44A0-BE44-B632FA4D780F}
{0C34B801-6AEC-4667-B053-03A67E2D0415}
{205C6BDD-7B73-42DE-8505-9A093F35A238}
{22B775E7-6C42-4FC5-8E10-9A5E3257BD94}
{3175E049-F9A9-4A3D-8F19-AC9FB04514D1}
{350C941f-3D7C-4EE8-BAA9-00BCB3D54227}
{49B11E66-142B-4585-856B-3C2F5A4C48B6}
{56EA8BC0-3751-4B93-BC9D-6651CC36E5AA}
{583EF20C-4DD0-43B0-8178-F0E8F76BBB09}
{5F25BBF0-8CBA-47CB-8E7B-EEE29C434FD3}
{6811CAA0-BF12-11D4-9EA1-0050BAE317E1}
{6956856F-B6B3-4BE0-BA0B-8F495BE32033}
{69FDFBB6-351D-4B8C-89D8-867DC9D0A2A4}
{77DCDCE3-2DED-62F3-8154-05E745472D07}
{8E5233E1-7495-44FB-8DEB-4BE906D59619}
{8F7BC615-A7E3-4309-B60E-BC8BF3DEAE83}
{9011041F-6000-11D3-8CFE-0150048383C9}
{90120000-0020-0409-0000-0000000FF1CE}
{95120000-00B9-0409-0000-0000000FF1CE}
{9C0CB627-0203-410D-8FAB-9DF2AFCCC689}
{A1F66FC9-11EE-4F2F-98C9-16F8D1E69FB7}
{A3051CD0-2F64-3813-A88D-B8DCCDE8F8C7}
Name
Type
Data
(Default)
REG_SZ
(value not set)
AuthorizedCDFPrefix
REG_SZ
Comments
REG_SZ
Bu yükleyici veritabanında ESET NOD32 Antivirus ürününü yüklemek için gereken mantı...
Contact
REG_SZ
DisplayName
REG_SZ
ESET NOD32 Antivirus
DisplayVersion
REG_SZ
4.0.424.0
EstimatedSize
REG_DWORD
0x0000994b (39243)
HelpLink
REG_SZ
HelpTelephone
REG_SZ
InstallDate
REG_SZ
20091204
InstallLocation
REG_SZ
C:\Program Files\ESET\ESET NOD32 Antivirus\
InstallSource
REG_SZ
F:\AutoPlay\Docs\
Language
REG_DWORD
0x0000041f (1055)
NoRemove
REG_DWORD
0x00000001 (1)
NoRepair
REG_DWORD
0x00000001 (1)
Publisher
REG_SZ
Eset spol s r. o.
Readme
REG_SZ
Size
REG_SZ
URLInfoAbout
REG_SZ
URLUpdateInfo
REG_SZ
Version
REG_DWORD
0x040001a8 (67109288)
VersionMajor
REG_DWORD
0x00000004 (4)
VersionMinor
REG_DWORD
0x00000000 (0)
WindowsInstaller
REG_DWORD
0x00000001 (1)
Computer\HKEY_LOCAL_MACHINE\oda-software\Microsoft\Windows\CurrentVersion\Uninstall\{49B11E66-142B-4585-856B-3C2F5A4C48B6}


Registry Editor
File Edit View Favorites Help
DeviceClasses
FileSystem
GraphicsDrivers
GroupOrderList
HAL
IDConfigDB
Keyboard Layout
Keyboard Layouts
Lsa
MediaCategories
MediaInterfaces
MediaProperties
MediaResources
MediaSets
Network
NetworkProvider
Nls
NTMS
PnP
Print
PriorityControl
ProductOptions
SafeBoot
ScsiPort
SecurePipeServers
winreg
AllowedPaths
SecurityProviders
Server Applications
ServiceGroupOrder
Name
Type
Data
(Default)
REG_SZ
(value not set)
Machine
REG_MULTI_SZ
System\CurrentControlSet\Control\ProductOptions ...
Edit Multi-String
Value name:
Machine
Value data:
System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Control\Server Applications
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion
System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal Server\UserConfig
System\CurrentControlSet\Control\Terminal Server\DefaultUserC
OK
Cancel
Computer\HKEY_LOCAL_MACHINE\odatv_system\ControlSet001\Control\SecurePipeServers\winreg\AllowedPaths


Registry Editor
File Edit View Favorites Help
SecurePipeServers
winreg
AllowedPaths
SecurityProviders
Server Applications
ServiceGroupOrder
ServiceProvider
Session Manager
Setup
StillImage
SystemResources
Terminal Server
AddIns
AuthorizedApplications
DefaultUserConfiguration
Dos
InputDevices
KeyboardType Mapping
Licensing Core
SysProcs
Utilities
VIDEO
Wds
WinStations
TimeZoneInformation
Update
UsbFlags
Video
VirtualDeviceDrivers
Watchdog
Name
Type
Data
(Default) REG_SZ (value not set)
DeleteTempDirsOnExit REG_DWORD 0x00000000 (0)
fAllowToGetHelp REG_DWORD 0x00000001 (1)
fDenyTSConnections REG_DWORD 0x00000001 (1)
fEnableSalem REG_DWORD 0x00000001 (1)
fInHelpMode REG_DWORD 0x00000000 (0)
FirstCountMsgQPeeksSleepBadApp REG_DWORD 0x0000000f (15)
fWritableTSCCPermTab REG_DWORD 0x00000000 (0)
IdleWinStationPoolCount REG_DWORD 0x00000000 (0)
Modems With Bad DSR REG_MULTI_SZ MultiTech MultiModem MT2834 MultiTech I
MsgQBadAppSleepTimeInMillisec REG_DWORD 0x00000001 (1)
NthCountMsgQPeeksSleepBadApp REG_DWORD 0x00000005 (5)
PerSessionTempDir REG_DWORD 0x00000000 (0)
ProductVersion REG_SZ 5.1
TSAdvertise REG_DWORD 0x00000000 (0)
TSAppCompat REG_DWORD 0x00000000 (0)
TSEnabled REG_DWORD 0x00000001 (1)
TSUserEnabled REG_DWORD 0x00000000 (0)
Computer\HKEY_LOCAL_MACHINE\odatv_system\ControlSet002\Control\Terminal Server

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
834707 (http://support.microsoft.com/kb/834707/)	MS04-038: Internet Explorer için toplu güvenlik güncelleştirmesi
841356 (http://support.microsoft.com/kb/841356/)	MS04-037: Windows Kabuğu Güvenlik açığı uzaktan kod yürütülmesine izin verebilir
867282 (http://support.microsoft.com/kb/867282/)	MS05-014: Internet Explorer için toplu güvenlik güncelleştirmesi
871250 (http://support.microsoft.com/kb/871250/)	MS05-003: Dizin Oluşturma Hizmeti'ndeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
873333 (http://support.microsoft.com/kb/873333/)	MS05-012: OLE ve COM'DAKI güvenlik açığı uzaktan kod yürütülmesine izin verebilir
873339 (http://support.microsoft.com/kb/873339/)	MS04-043: HyperTerminal'deki güvenlik açığı kod yürütülmesine izin verebilir
883939 (http://support.microsoft.com/kb/883939/)	MS05-025: Internet Explorer için toplu güvenlik güncelleştirmesi
885250 (http://support.microsoft.com/kb/885250/)	MS05-011: Sunucu ileti bloğu güvenlik açığı uzaktan kod yürütülmesine izin verebilir
885492 (http://support.microsoft.com/kb/885492/)	Microsoft, Microsoft Windows Media Player 9 için bir güvenlik güncelleştirmesi yayımladı
885835 (http://support.microsoft.com/kb/885835/)	MS04-044: Windows Çekirdeği ve LSASS'DEKI güvenlik açıkları ayrıcalık yükselmesine izin
885836 (http://support.microsoft.com/kb/885836/)	MS04-041: WordPad'deki Güvenlik açığı kod yürütülmesine izin verebilir
887219 (http://support.microsoft.com/kb/887219/)	MS05-004: ASP.NET Yol doğrulama güvenlik açığı yetkisiz erişime izin verebilir
887472 (http://support.microsoft.com/kb/887472/)	Microsoft, Microsoft Windows Messenger için bir güvenlik güncelleştirmesi yayımladı
888113 (http://support.microsoft.com/kb/888113/)	MS05-015: Köprü Nesnesi Kitaplığı Güvenlik açığı Windows Server 2003'te uzaktan kod yürütülmesine izin verebilir
888302 (http://support.microsoft.com/kb/888302/)	MS05-007: Windows'taki güvenlik açığı bilginin açığa çıkmasına neden olabilir
890046 (http://support.microsoft.com/kb/890046/)	MS05-032: Microsoft Aracısı'ndaki güvenlik açığı sahtekarlığa olanak tanıyabilir
890047 (http://support.microsoft.com/kb/890047/)	MS05-008: Windows Kabuğu Güvenlik açığı uzaktan kod yürütülmesine izin verebilir
890067 (http://support.microsoft.com/kb/890067/)	MS-DOS--tabanlı programlar, Windows Server 2003, Windows XP veya Windows 2000 çalıştıran bir bilgisayarda beklendiği gibi çalışmıyor
890175 (http://support.microsoft.com/kb/890175/)	MS05-001: HTML Yardımı güvenlik açığı kod yürütülmesine izin verebilir
890261 (http://support.microsoft.com/kb/890261/)	MS05-009: PNG işlemedeki güvenlik açığı için arabellek taşmasına neden olabilir

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
890859 (http://support.microsoft.com/kb/890859/)	MS05-018: Windows Çekirdeğindeki Güvenlik Açıkları Ayrıcalık Yükselmesine ve hizmet reddine izin verebilir
890923 (http://support.microsoft.com/kb/890923/)	MS05-020: Internet Explorer için toplu güvenlik güncelleştirmesi
891711 (http://support.microsoft.com/kb/891711/)	MS05-002: Güvenlik açığı işaretçi ve simge biçimi işleme uzaktan kod yürütülmesine izin verebilir
891781 (http://support.microsoft.com/kb/891781/)	MS05-013: DHTML düzenleme bileşeni ActiveX denetimindeki güvenlik açığı kod yürütülmesine izin verebilir
893066 (http://support.microsoft.com/kb/893066/)	MS05-019: TCP / ıp'deki güvenlik açıkları uzaktan kod yürütülmesine ve hizmet reddine izin verebilir
893086 (http://support.microsoft.com/kb/893086/)	MS05-016: Uzaktan kod yürütülmesine olanak sağlayan Windows Kabuğu Güvenlik Açığı
893756 (http://support.microsoft.com/kb/893756/)	MS05-040: Telefon hizmeti güvenlik açığı uzaktan kod yürütülmesine izin verebilir
896358 (http://support.microsoft.com/kb/896358/)	MS05-026: HTML Yardımı'ndaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
896422 (http://support.microsoft.com/kb/896422/)	MS05-027: Sunucu ileti bloğu'ndaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
896423 (http://support.microsoft.com/kb/896423/)	MS05-043: Yazdırma biriktiricisi hizmetindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
896424 (http://support.microsoft.com/kb/896424/)	Microsoft Güvenlik Bülteni MS05-053: Grafik işleme altyapısındaki güvenlik açıkları kod yürütülmesine izin verebilir
896426 (http://support.microsoft.com/kb/896426/)	MS05-028: Web istemcisi hizmetindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
896428 (http://support.microsoft.com/kb/896428/)	MS05-033: Telnet istemcisindeki güvenlik açığı bilginin açığa çıkmasına neden olabilir
896597 (http://support.microsoft.com/kb/896597/)	MS05-022: MSN Messenger'daki güvenlik açığı uzaktan kod yürütülmesine neden olabilir
896688 (http://support.microsoft.com/kb/896688/)	MS05-052: Internet Explorer için toplu güvenlik güncelleştirmesi
896727 (http://support.microsoft.com/kb/896727/)	MS05-038: Internet Explorer için toplu güvenlik güncelleştirmesi
897715 (http://support.microsoft.com/kb/897715/)	MS05-030: Outlook Express'teki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
899587 (http://support.microsoft.com/kb/899587/)	MS05-042: Kerberos Güvenlik Açıkları Hizmet, bilginin açığa çıkması ve sızdırma reddine neden olabilir
899588 (http://support.microsoft.com/kb/899588/)	MS05-039: Tak ve Kullan'daki güvenlik açığı uzaktan kod yürütülmesine ve ayrıcalık yükselmesine izin verebilir
899589 (http://support.microsoft.com/kb/899589/)	MS05-046: NetWare için istemci Hizmeti'ndeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
899591 (http://support.microsoft.com/kb/899591/)	MS05-041: Uzak Masaüstü Protokolü güvenlik açığı hizmet reddine olanak
900725 (http://support.microsoft.com/kb/900725/)	MS05-049: Windows kabuğundaki güvenlik açıkları uzaktan kod yürütülmesine izin verebilir
901190 (http://support.microsoft.com/kb/901190/)	MS06-009: Kore Dili Giriş Yöntemi Düzenleyicisi'ndeki IME güvenlik açığı ayrıcalık yükselmesine izin verebilir
901214 (http://support.microsoft.com/kb/901214/)	MS05-036: Microsoft Renk Yönetimi Modülü güvenlik açığı uzaktan kod yürütülmesine izin verebilir
902400 (http://support.microsoft.com/kb/902400/)	MS05-051: MS DTC ve COM + hizmetlerindeki güvenlik açıkları uzaktan kod yürütülmesine izin verebilir
903235 (http://support.microsoft.com/kb/903235/)	MS05-037: JView Profil Oluşturucusu Güvenlik açığı uzaktan kod yürütülmesine izin verebilir
903675 (http://support.microsoft.com/kb/903675/)	Algılama ve dağıtım kılavuzunu, 12 Temmuz 2005 güvenlik için bırakın
904706 (http://support.microsoft.com/kb/904706/)	MS05-050: DirectShow Güvenlik açığı uzaktan kod yürütülmesine izin verebilir
905414 (http://support.microsoft.com/kb/905414/)	MS05-045: Ağ Bağlantısı Yöneticisi'ndeki güvenlik açığı hizmet reddine olanak
905495 (http://support.microsoft.com/kb/905495/)	MS05-044: Windows FTP istemcisindeki güvenlik açığı dosya aktarım olanak verebilecek konumu müdahale
905749 (http://support.microsoft.com/kb/905749/)	MS05-047: Tak ve Kullan'daki güvenlik açığı uzaktan kod yürütülmesine ve ayrıcalık yükselmesine izin verebilir
905915 (http://support.microsoft.com/kb/905915/)	MS05-054: Internet Explorer için toplu güvenlik güncelleştirmesi
907245 (http://support.microsoft.com/kb/907245/)	MS05-048: Microsoft birlikte çalışma Veri Nesneleri'ndeki güvenlik açığı kod yürütülmesine izin verebilir
908519 (http://support.microsoft.com/kb/908519/)	MS06-002: Katıştırılmış Web yazı tipi güvenlik açığı uzaktan kod yürütülmesine izin verebilir
908531 (http://support.microsoft.com/kb/908531/)	MS06-015: Windows Gezgini'ndeki güvenlik açığı uzaktan kod yürütülmesine neden olabilir
910620 (http://support.microsoft.com/kb/910620/)	MS06-004: Internet Explorer için toplu güvenlik güncelleştirmesi
911280 (http://support.microsoft.com/kb/911280/)	MS06-025: Yönlendirme ve Uzaktan Erişim'deki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
911562 (http://support.microsoft.com/kb/911562/)	MS06-014: Microsoft Data Access Components (MDAC) işlevindeki güvenlik açığı kod yürütülmesine izin verebilir
911564 (http://support.microsoft.com/kb/911564/)	MS06-006: Windows Media Player ile Microsoft dışındaki internet tarayıcıları eklentisindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
911565 (http://support.microsoft.com/kb/911565/)	MS06-005: Windows Media Player'daki güvenlik açığı uzaktan kod yürütülmesine izin verebilir

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
911567 (http://support.microsoft.com/kb/911567/)	MS06-016: Outlook Express için toplu güvenlik güncelleştirmesi
911927 (http://support.microsoft.com/kb/911927/)	MS06-008: WebClient'ndaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
912812 (http://support.microsoft.com/kb/912812/)	MS06-013: Internet Explorer için toplu güvenlik güncelleştirmesi
912919 (http://support.microsoft.com/kb/912919/)	MS06-001: Grafik işleme altyapısındaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
913433 (http://support.microsoft.com/kb/913433/)	MS06-020: Adobe Macromedia Flash Player güvenlik açıkları uzaktan kod yürütülmesine izin verebilir
913446 (http://support.microsoft.com/kb/913446/)	MS06-007: TCP / ıp'deki güvenlik açığı hizmet reddine olanak
913580 (http://support.microsoft.com/kb/913580/)	MS06-018: Microsoft Distributed Transaction Coordinator güvenlik açığı hizmet reddine olanak
914388 (http://support.microsoft.com/kb/914388/)	MS06-036: DHCP istemcisi hizmetindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
914389 (http://support.microsoft.com/kb/914389/)	MS06-030: Sunucu ileti bloğu'ndaki güvenlik açığı ayrıcalık yükselmesine izin
914798 (http://support.microsoft.com/kb/914798/)	MS06-011: İzin veren Windows hizmet DACL'leri ayrıcalık yükselmesine neden olabilir
916281 (http://support.microsoft.com/kb/916281/)	MS06-021: Internet Explorer için toplu güvenlik güncelleştirmesi
917159 (http://support.microsoft.com/kb/917159/)	MS06-035: Sunucu hizmetindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
917283 (http://support.microsoft.com/kb/917283/)	MS06-033: ASP.NET'teki güvenlik açığı bilginin açığa çıkmasına neden olabilir
917344 (http://support.microsoft.com/kb/917344/)	MS06-023: Microsoft JScript'teki Güvenlik açığı uzaktan kod yürütülmesine izin verebilir
917422 (http://support.microsoft.com/kb/917422/)	MS06-051: Windows çekirdeğindeki güvenlik açığı uzaktan kod yürütülmesine neden olabilir
917537 (http://support.microsoft.com/kb/917537/)	MS06-034: Active Server Pages kullanan ınternet ınformation Services güvenlik açığı uzaktan kod yürütülmesine izin verebilir
917953 (http://support.microsoft.com/kb/917953/)	MS06-032: TCP / ıp'deki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
918118 (http://support.microsoft.com/kb/918118/)	MS07-013: Microsoft RichEdit Güvenlik açığı uzaktan kod yürütülmesine izin verebilir
918439 (http://support.microsoft.com/kb/918439/)	MS06-022: ART resim işleme güvenlik açığı uzaktan kod yürütülmesine izin verebilir
918899 (http://support.microsoft.com/kb/918899/)	MS06-042: Internet Explorer için toplu güvenlik güncelleştirmesi

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
919007 (http://support.microsoft.com/kb/919007/)	MS06-052: Pragmatik genel çok noktaya yayın (PGM) güvenlik açığı uzaktan kod yürütülmesine neden olabilir
920213 (http://support.microsoft.com/kb/920213/)	MS06-068: Microsoft Agent'taki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
920214 (http://support.microsoft.com/kb/920214/)	MS06-043: Microsoft Windows'taki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
920670 (http://support.microsoft.com/kb/920670/)	MS06-050: Microsoft Windows Köprü Nesnesi Kitaplığı'ndaki güvenlik açıkları uzaktan kod yürütülmesine izin verebilir
920683 (http://support.microsoft.com/kb/920683/)	MS06-041: DNS Çözümlemesi'ndaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
920685 (http://support.microsoft.com/kb/920685/)	MS06-053: Dizin Oluşturma Hizmeti'ndeki Güvenlik Açığı Siteler arası komut dosyası çalıştırmaya izin verebilir
921398 (http://support.microsoft.com/kb/921398/)	MS06-045: Windows Gezgini'ndeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
921503 (http://support.microsoft.com/kb/921503/)	MS07-043: OLE Otomasyonu'ndaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
921883 (http://support.microsoft.com/kb/921883/)	MS06-040: Sunucu hizmetindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
922616 (http://support.microsoft.com/kb/922616/)	MS06-046: HTML Yardımı güvenlik açığı uzaktan kod yürütülmesine izin verebilir
922760 (http://support.microsoft.com/kb/922760/)	MS06-067: Internet Explorer için toplu güvenlik güncelleştirmesi
922770 (http://support.microsoft.com/kb/922770/)	MS06-056: ASP.NET 2. 0'daki güvenlik açığı bilginin açığa çıkması için izin verebilir
922819 (http://support.microsoft.com/kb/922819/)	MS06-064: TCP/IP ıpv6 güvenlik açıkları hizmet reddine olanak
923191 (http://support.microsoft.com/kb/923191/)	MS06-057: Windows Gezgini'ndeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
923414 (http://support.microsoft.com/kb/923414/)	MS06-063: Sunucu Hizmeti'ndeki güvenlik açığı hizmet reddine olanak
923561 (http://support.microsoft.com/kb/923561/)	Windows WordPad Dönüştürücü Güncelleştirmesi, MS09-010: Açıklama: 14 Nisan 2009
923694 (http://support.microsoft.com/kb/923694/)	MS06-076: Outlook Express için toplu güvenlik güncelleştirmesini
923810 (http://support.microsoft.com/kb/923810/)	MS07-055: Kodak Resim Görüntüleyicisi'nde güvenlik açığı uzaktan kod yürütülmesine izin verebilir
923980 (http://support.microsoft.com/kb/923980/)	MS06-066: İstemcisi hizmetindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
924191 (http://support.microsoft.com/kb/924191/)	MS06-061: Microsoft XML Çekirdek Hizmetleri'ndeki güvenlik açıkları uzaktan kod yürütülmesine izin verebilir

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
924270 (http://support.microsoft.com/kb/924270/)	MS06-070: İş istasyonu Hizmeti'ndeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
924496 (http://support.microsoft.com/kb/924496/)	MS06-065: Windows Nesne Paketleyici'deki Güvenlik açığı uzaktan kod yürütülmesine izin verebilir
924667 (http://support.microsoft.com/kb/924667/)	MS07-012: Microsoft Foundation Classes'daki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
925454 (http://support.microsoft.com/kb/925454/)	MS06-072: Internet Explorer için toplu güvenlik güncelleştirmesi
925486 (http://support.microsoft.com/kb/925486/)	MS06-055: Vektör işaretleme dilindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
925902 (http://support.microsoft.com/kb/925902/)	MS07-017: GDI'daki güvenlik açığı uzaktan kod yürütülmesine olanak verebilir
926121 (http://support.microsoft.com/kb/926121/)	MS06-077: Uzaktan Yükleme Hizmetleri'nin güvenlik açığı uzaktan kod yürütülmesine izin verebilir
926247 (http://support.microsoft.com/kb/926247/)	MS06-074: Basit Ağ Yönetimi Protokolü (SNMP), güvenlik açığı uzaktan kod yürütülmesine izin verebilir
926255 (http://support.microsoft.com/kb/926255/)	MS06-075: Windows'taki güvenlik açığı ayrıcalık yükselmesine izin
926436 (http://support.microsoft.com/kb/926436/)	MS07-011: Microsoft OLE iletişim kutusu'ndaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
927779 (http://support.microsoft.com/kb/927779/)	MS07-009: Microsoft Data Access Components'taki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
927802 (http://support.microsoft.com/kb/927802/)	MS07-007: Windows Resim Alma Hizmetindeki Güvenlik açığı ayrıcalık yükselmesine izin
927977 (http://support.microsoft.com/kb/927977/)	MS06-071: Microsoft XML Çekirdek Hizmetleri 6.0 güvenlik güncelleştirmesi
927978 (http://support.microsoft.com/kb/927978/)	MS06-071: Microsoft XML Çekirdek Hizmetleri 4.0 güvenlik güncelleştirmesi
928090 (http://support.microsoft.com/kb/928090/)	MS07-016: Internet Explorer için toplu güvenlik güncelleştirmesi
928255 (http://support.microsoft.com/kb/928255/)	MS07-006: Windows Kabuğu Güvenlik açığı ayrıcalık yükselmesine izin
928843 (http://support.microsoft.com/kb/928843/)	MS07-008: HTML Yardımı ActiveX denetimindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
929123 (http://support.microsoft.com/kb/929123/)	MS07-034: Windows Mail ve Outlook Express için toplu güvenlik güncelleştirmesi
929969 (http://support.microsoft.com/kb/929969/)	MS07-004: Vektör işaretleme dilindeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
930178 (http://support.microsoft.com/kb/930178/)	MS07-021: Windows CSRSS'deki güvenlik açığı uzaktan kod yürütülmesine izin verebilir

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
930494 (http://support.microsoft.com/kb/930494/)	Windows XP Media Center ve Windows XP Tablet PC için .NET Framework 1.0 Service Pack 3 için güvenlik güncelleştirmesi: 10 Temmuz 2007'in açıklaması
931261 (http://support.microsoft.com/kb/931261/)	MS07-019: UPnP'deki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
931768 (http://support.microsoft.com/kb/931768/)	MS07-027: Internet Explorer için toplu güvenlik güncelleştirmesi
931784 (http://support.microsoft.com/kb/931784/)	MS07-022: Windows çekirdeğindeki güvenlik açığı ayrıcalık yükselmesine izin
932168 (http://support.microsoft.com/kb/932168/)	MS07-020: Microsoft Agent'taki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
933566 (http://support.microsoft.com/kb/933566/)	MS07-033: Internet Explorer için toplu güvenlik güncelleştirmesi
933579 (http://support.microsoft.com/kb/933579/)	Microsoft XML Çekirdek Hizmetleri 6.0 için güvenlik güncelleştirmesi MS07-042: Açıklama: 14 Ağustos 2007'in açıklaması
933729 (http://support.microsoft.com/kb/933729/)	MS07-058: RPC güvenlik açıkları hizmet reddine olanak
935839 (http://support.microsoft.com/kb/935839/)	MS07-035: Win32 API güvenlik açığı uzaktan kod yürütülmesine izin verebilir
935840 (http://support.microsoft.com/kb/935840/)	MS07-031: Schannel güvenlik açığı uzaktan kod yürütülmesine izin verebilir
936021 (http://support.microsoft.com/kb/936021/)	Microsoft XML Core Services 3.0 için güvenlik güncelleştirmesi: 14 Ağustos 2007'in açıklaması
936782 (http://support.microsoft.com/kb/936782/)	MS07-047: Windows Media Player'daki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
937143 (http://support.microsoft.com/kb/937143/)	MS07-045: Internet Explorer için toplu güvenlik güncelleştirmesi
937894 (http://support.microsoft.com/kb/937894/)	MS07-065: Message Queuing hizmeti güvenlik açığı uzaktan kod yürütülmesine neden olabilecek Windows XP ve Windows 2000'de izin verebilir
938464 (http://support.microsoft.com/kb/938464/)	MS08-052: Tüm Windows XP, Windows Vista, Windows Server 2003 ve Windows Server 2008 sürümleri ve Internet Explorer 6 SP1 içeren Windows Server 2000 için GDI+ güvenlik güncelleştirmesinin açıklaması
938829 (http://support.microsoft.com/kb/938829/)	MS07-046: Gdi'daki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
939373 (http://support.microsoft.com/kb/939373/)	MS07-041: Internet Information Services'taki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
939653 (http://support.microsoft.com/kb/939653/)	MS07-057: Internet Explorer için toplu güvenlik güncelleştirmesi
939778 (http://support.microsoft.com/kb/939778/)	MS07-053: Windows Services for UNIX'TEKI güvenlik açığı ayrıcalık yükselmesine izin
941202 (http://support.microsoft.com/kb/941202/)	MS07-056: Outlook Express ve Windows Mail güvenlik güncelleştirmesi

EK-18

Windows XP Service Pack 3 Güvenlik Güncelleştirmeleri

Microsoft güncelleme makale numarası	Microsoft güncelleme makale başlığı
941568 (http://support.microsoft.com/kb/941568/)	MS07-064: DirectX güvenlik açıkları uzaktan kod yürütülmesine izin verebilir
941644 (http://support.microsoft.com/kb/941644/)	MS08-001: TCP / ıp'deki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
941693 (http://support.microsoft.com/kb/941693/)	MS08-025: Windows çekirdeğindeki güvenlik açığı ayrıcalık yükselmesine izin
942099 (http://support.microsoft.com/kb/942099/)	MS07-054: MSN Messenger ve Windows Live Messenger'daki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
942615 (http://support.microsoft.com/kb/942615/)	MS07-069: Internet Explorer için toplu güvenlik güncelleştirmesi
942830 (http://support.microsoft.com/kb/942830/)	MS08-006: Internet Information Services'taki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
942831 (http://support.microsoft.com/kb/942831/)	MS08-005: Internet Information Services'taki güvenlik açığı ayrıcalık yükselmesine izin verebilir
943055 (http://support.microsoft.com/kb/943055/)	MS08-008: Windows 2000, Windows XP, Windows Server 2003 ve Windows Vista güvenlik güncelleştirmesi: 12 Şubat 2008'in açıklaması
943460 (http://support.microsoft.com/kb/943460/)	MS07-061: Windows URI İşlemedeki güvenlik açığı uzaktan kod yürütülmesine olanak verebilir
943485 (http://support.microsoft.com/kb/943485/)	MS08-002: LSASS Güvenlik açığı ayrıcalık yükselmesine izin verebilir
944338 (http://support.microsoft.com/kb/944338/)	MS08-022: VBScript ve JScript komut dosyası altyapılarındaki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
944533 (http://support.microsoft.com/kb/944533/)	MS08-010: Internet Explorer için toplu güvenlik güncelleştirmesi
944653 (http://support.microsoft.com/kb/944653/)	MS07-067: Macrovision sürücüsündeki güvenlik açığı ayrıcalık yükselmesine izin verebilir
945553 (http://support.microsoft.com/kb/945553/)	MS07-020: DNS istemcisindeki güvenlik açığı sahtekarlığa olanak tanıyabilir
946026 (http://support.microsoft.com/kb/946026/)	MS08-007: WebDAV Mini Yeniden Yönlendiricisi'ndeki güvenlik açığı uzaktan kod yürütülmesine izin verebilir
947864 (http://support.microsoft.com/kb/947864/)	MS06-024: Internet Explorer için toplu güvenlik güncelleştirmesi
948590 (http://support.microsoft.com/kb/948590/)	MS07-021: GDI'daki güvenlik açığı uzaktan kod yürütülmesine olanak verebilir
948881 (http://support.microsoft.com/kb/948881/)	MS08-023: ActiveX kill bitleri için kritik güvenlik güncelleştirmesi
950749 (http://support.microsoft.com/kb/950749/)	MS08-028: Microsoft Jet Veritabanı Altyapısındaki Güvenlik açığı uzaktan kod yürütülmesine izin verebilir

Ek-19

19 İncelenen hard diskteki dosya ve e-postalarda tespit edilen virüs ve trojan tipindeki zararlı yazılımların listesi

Sıra No	Dosya Adı	Trojan/Virüs Adı	Tipi
1	7E801F16-0000032B.eml	W32/Netsky.p.eml!exe	Virus
2	mammolo.exe	W32/PEPatcher	Trojan
3	nodenabler.exe	Generic.dx!vyt	Trojan
4	ctext5_cw.rar	W32/PEPatcher	Trojan
5	tdtdb.1.v2.1.8.af.rar	Generic.dx!suu	Trojan
6	_B3846296[4]6.htm	Exploit-ObscuredHtml	Trojan
7	Packmatronic 1.0 tev.exe	Generic.dx!wad	Trojan
8	37464F4E-00008C3D.eml	JS/Redirector.z	Trojan
9	39B32D12-00008262.eml	JS/Downloader.gen	Trojan
10	3A5D4A2E-0000AF7E.eml	JS/Redirector	Trojan
11	3A8A3BD1-0000B3D4.eml	Generic.dx!ucn	Trojan
12	3A9E797D-00006D03.eml	Bredolab.gen.c	Trojan
13	3A9E797D-00006E7B.eml	Generic.FakeAlert.c	Trojan
14	3A9E797D-0000761C.eml	Generic.FakeAlert!ht	Trojan
15	3B082FA0-00008903.eml	Generic.dx!tbw	Trojan
16	3B31505A-0000ADE8.eml	JS/Downloader.gen	Trojan
17	3B357B28-0000A0BF.eml	JS/Redirector	Trojan
18	3B862D72-000095ED.eml	Bredolab.gen.x	Trojan
19	3B974027-000047FD.eml	W32/Rimecud.gen.al	Trojan
20	3C1121B2-0000ADDC.eml	JS/Downloader.gen	Trojan
21	3C596FBC-00009846.eml	Bredolab.gen.c	Trojan
22	3C94215C-00009861.eml	Bredolab.gen.c	Trojan
23	3D1F37DB-0000AF90.eml	JS/Redirector	Trojan
24	3DF144FA-0000AF7D.eml	JS/Redirector	Trojan
25	3E121A49-00008FB7.eml	FakeAlert-JQ	Trojan
26	3E204D0E-0000025A.eml	W32.Netsky.p@MM!zip	Virus
27	3EF60822-00005B48.eml	Generic.Dropper.lr	Trojan
28	401D71F0-00009BE6.eml	Generic.Dropper.p	Trojan
29	40535C5C-0000ADE2.eml	JS/Downloader.gen	Trojan
30	42307EB7-0000784F.eml	DNSChanger.as	Trojan
31	43467A36-00005C87.eml	Generic.Dropper.lr	Trojan
32	44160E71-00005747.eml	Generic.Dropper.lr	Trojan
33	44C53D41-0000008D.eml	Exploit-MIME.gen.c	Exploit
34	45C53960-00009C06.eml	PWS-Zbot.gen.bn	Trojan
35	46CB0954-00008F14.eml	Cutwail!env.b	Trojan
36	487D6FB0-00007F0D.eml	BackDoor-DKI.gen.cj	Trojan
37	48DA2552-00000453.eml	Spy-Agent.cf.dr	Trojan
38	49090B0D-00006C6C.eml	W32/IRCbot.gen.a	Virus
39	494A0677-00009BE8.eml	Generic.Dropper.p	Trojan
40	494A0677-0000AD4D.eml	JS/Redirector	Trojan
41	49F7442B-00007FC3.eml	DNSChanger.bu	Trojan
42	4A8B6C7F-00008C86.eml	JS/Redirector.z	Trojan
43	4AC71A2F-0000AF6E.eml	JS/Redirector	Trojan
44	4B405878-00008274.eml	JS/Downloader.gen	Trojan
45	4B405878-00008FB5.eml	FakeAlert-JQ	Trojan
46	4B4E72FF-0000A0DA.eml	JS/Redirector	Trojan
47	4B991FDE-0000B026.eml	JS/Redirector	Trojan

Ek-19

19 İncelenen hard diskteki dosya ve e-postalarda tespit edilen virüs ve trojan tipindeki zararlı yazılımların listesi

Sıra No	Dosya Adı	Trojan/Virüs Adı	Tipi
48	4C2C1874-00000043.eml	Spy-Agent.cf.dr	Trojan
49	4C4628E2-00008C6B.eml	JS/Downloader.gen	Trojan
50	4CAD314F-00007F8F.eml	DNSChanger.bu	Trojan
51	4D95269E-00008C3B.eml	JS/Redirector.z	Trojan
52	4E0B152E-00008C6A.eml	JS/Downloader.gen	Trojan
53	4E45323B-00009B47.eml	Generic.Dropper.p	Trojan
54	4F8A5F7D-0000A0DE.eml	JS/Redirector	Trojan
55	504C5AB0-0000AD76.eml	JS/Downloader.gen	Trojan
56	50781481-00009626.eml	PWS-Zbot.gen.di	Trojan
57	50F018B2-00008CAA.eml	JS/Redirector.z	Trojan
58	51704757-0000984B.eml	Bredolab.gen.c	Trojan
59	519C3800-00007677.eml	Generic.FakeAlert!hu	Trojan
60	520B68F5-00007726.eml	Generic.Dropper.lr	Trojan
61	520B68F5-00007FD5.eml	DNSChanger.bu	Trojan
62	524F0F8C-0000B060.eml	JS/Redirector	Trojan
63	52B267E3-00009090.eml	FakeAlert-DefCnt.a.dldr	Trojan
64	5402557A-00008C93.eml	JS/Redirector.z	Trojan
65	54757336-000068F7.eml	Bredolab!env.a	Trojan
66	552E2745-0000A0CA.eml	JS/Redirector	Trojan
67	553169FA-0000036A.eml	Spy-Agent.bw	Trojan
68	55CA093C-00009C38.eml	PWS-Zbot.gen.bn	Trojan
69	55D6042F-00009781.eml	FakeAlert-SecurityTool.ag	Trojan
70	56275383-00000360.eml	Spy-Agent.bw	Trojan
71	56AE0732-0000ECAD.eml	BackDoor-Spyeye	Trojan
72	56CE2350-0000A0DF.eml	JS/Redirector	Trojan
73	57A961CA-00008C57.eml	JS/Redirector.z	Trojan
74	58B026CA-00008D34.eml	JS/Redirector.z	Trojan
75	58DA2607-000095FA.eml	Bredolab.gen.x	Trojan
76	59082A86-00008C8D.eml	JS/Redirector.z	Trojan
77	5991409D-00006D0C.eml	Bredolab.gen.c	Trojan
78	5B4B48AB-00009C3D.eml	PWS-Zbot.gen.bn	Trojan
79	5BAF0B6D-00008C78.eml	JS/Downloader.gen	Trojan
80	5C111017-00000366.eml	Spy-Agent.bw	Trojan
81	5C673CD6-0000936A.eml	PWS-Zbot.gen.bg	Trojan
82	5C673CD6-00009BD8.eml	Generic.Dropper.p	Trojan
83	5DA946D4-0000977E.eml	FakeAlert-SecurityTool.ag	Trojan
84	5E70506D-00008C54.eml	JS/Redirector.z	Trojan
85	5ED04EE57-00009BE.eml	PWS-Zbot.gen.bn	Trojan
86	5F323BF6-00008277.eml	JS/Downloader.gen	Trojan
87	5F323BF6-00008D2A.eml	JS/Redirector.z	Trojan
88	5F3D3979-00006240.eml	Generic.dx!ozg	Trojan
89	5F490DDC-00008FBA.eml	FakeAlert-JQ	Trojan
90	5F851ECA-00009814.eml	Generic.Downloader.z	Trojan
91	600322C3B-000076E7.eml	Generic.Dropper.lr	Trojan
92	600322C3B-00008D30.eml	JS/Redirector.z	Trojan
93	600322C3B-00009BC8.eml	Generic.Dropper.p	Trojan
94	612B406D-0000A0D3.eml	JS/Redirector	Trojan

Ek-19

19 İncelenen hard diskteki dosya ve e-postalarda tespit edilen virüs ve trojan tipindeki zararlı yazılımların listesi

Sıra No	Dosya Adı	Trojan/Virüs Adı	Tipi
95	613938DA-00008C59.eml	JS/Redirector.z	Trojan
96	619D3B8A-0000AF88.eml	JS/Redirector	Trojan
97	62214884-00009600.eml	Bredolab.gen.x	Trojan
98	62CC253A-00005AA2.eml	Generic.Dropper.lr	Trojan
99	63CB6BFC-0000826B.eml	JS/Downloader.gen	Trojan
100	641A13A5-0000ED6F.eml	Backdoor-Spyeye	Trojan
101	662A7346-00007739.eml	Generic.Dropper.lr	Trojan
102	6635570E-0000B034.eml	JS/Redirector	Trojan
103	67567114-0000ADE3.eml	JS/Downloader.gen	Trojan
104	68993CD5-00008D38.eml	JS/Redirector.z	Trojan
105	69D07AC2-00007BD9.eml	Spy-Agent.br	Trojan
106	6A895590-0000A0D1.eml	JS/Redirector	Trojan
107	6AD6047E-0000936C.eml	PWS-Zbot.gen.bg	Trojan
108	6AD6047E-00009FAC.eml	Downloader-CEW.a	Trojan
109	6B365CFD-00008FB6.eml	FakeAlert-JQ	Trojan
110	6B7232E6-00007FB3.eml	DNSChanger.bu	Trojan
111	6B7C41D6-00008C7C.eml	JS/Downloader.gen	Trojan
112	6B8E1311-00009C57.eml	PWS-Zbot.gen.bn	Trojan
113	6C7E4313-0000985D.eml	Bredolab.gen.c	Trojan
114	6CF45F45-0000545B.eml	W32/Rimecud.gen.al	Virus
115	6D0F49CB-00009826.eml	Generic.Downloader.z	Trojan
116	6E5D1AD4-0000826A.eml	JS/Downloader.gen	Trojan
117	6E9C61B0-0000A0E0.eml	JS/Redirector	Trojan
118	6EA14C66-0000AC99.eml	Downloader-AWM.gen.c	Trojan
119	6FEA0A26-00009784.eml	FakeAlert-SecurityTool.ag	Trojan
120	701F5D03-00009013.eml	Spam-Mailbot.m	Trojan
121	710D7BCE-00009847.eml	Bredolab.gen.c	Trojan
122	712956D4-00009C2D.eml	PWS-Zbot.gen.bn	Trojan
123	716317BF-0000A0DB-eml	JS/Redirector	Trojan
124	71A8710A-0000ADDF.eml	JS/Downloader.gen	Trojan
125	727561E6-0000ADD3.eml	JS/Downloader.gen	Trojan
126	72966512-0000592A.eml	Generic.Dropper.lr	Trojan
127	72D71D8F-00008E66.eml	Bredolab.gen.c	Trojan
128	733E5E46-00008C4B.eml	JS/Redirector.z	Trojan
129	73487583-0000A0B4.eml	JS/Redirector	Trojan
130	737D0D9F-0000AD09.eml	JS/Redirector	Trojan
131	73B12780-0000AD78.eml	JS/Downloader.gen	Trojan
132	745E3A4C-0000AD0B.eml	JS/Redirector	Trojan
133	74CD0288-00009822.eml	Generic.Downloader.z	Trojan
134	752F2732-00008C9E.eml	JS/Redirector.z	Trojan
135	766A3FA8-0000AF7C.eml	JS/Redirector	Trojan
136	76F41E05-00000021.eml	W32/Netsky.p@MM!zip	Virus
137	77A51798-00009094.eml	FakeAlert-DefCnt.a.dldr	Trojan
138	794937D6-0000766E.eml	Generic.FakeAlert!hu	Trojan
139	798375EF-00009FAE.eml	Downloader-CEW.a	Trojan
140	79877020-0000AD11.eml	JS/Redirector	Trojan
141	7A5A767D-00008267.eml	JS/Downloader.gen	Trojan

Ek-19

19 İncelenen hard diskteki dosya ve e-postalarda tespit edilen virüs ve trojan tipindeki zararlı yazılımların listesi

Sıra No	Dosya Adı	Trojan/Virüs Adı	Tipi
142	7A5A767D-00009014.eml	Spam-Mailbot.m	Trojan
143	7AC327BA-00009091.eml	FakeAlert-DefCnt.a.dldr	Trojan
144	7B495ACD-0000EC20.eml	PWS-Banker!gpr	Trojan
145	7B8E0436-00005A6F.eml	Generic.Dropper.lr	Trojan
146	7BB95772-00008D35.eml	JS/Redirector.z	Trojan
147	7DD1261E-00007FB0.eml	DNSChanger.bu	Trojan
148	7F8D7523-00008C9A.eml	JS/Redirector.z	Trojan
149	7F967FF5-0000826C.eml	JS/Downloader.gen	Trojan
150	ctext5_cw.rar	W32/PEPatcher	Trojan
151	tdtdb.1.v2.1.8.af.rar	Generic.dx!suu	Trojan
152	_B3846296[9]1.htm	JS/Redirector	Trojan
153	_wbk1007.tmp	JS/Downloader.gen	Trojan
154	001F1866-00008E30.eml	JS/Downloader.gen	Trojan
155	002C425F-0000AF74.eml	JS/Redirector	Trojan
156	003507CF-00009BF4.eml	Generic.Dropper.p	Trojan
157	0120759A-00005C31.eml	Generic.Dropper.lr	Trojan
158	0120759A-00008272.eml	JS/Downloader.gen	Trojan
159	0120759A-00008FB3.eml	FakeAlert-JQ	Trojan
160	01406185-00008E29.eml	JS/Downloader.gen	Trojan
161	01852B81-0000000D.eml	Spy-Agent.cf.dr	Trojan
162	03847F4F-0000AD4C.eml	JS/Redirector	Trojan
163	04E63569-00008CA4.eml	JS/Redirector.z	Trojan
164	05D7522D-0000AF8F.eml	JS/Redirector	Trojan
165	064D475E-00009845.eml	Bredolab.gen.c	Trojan
166	071C1D1C-00005CAD.eml	Generic.Dropper.lr	Trojan
167	074D4DC8-00009010.eml	Spam-Mailbot.m	Trojan
168	07F6092F-000075B3.eml	Generic.Dropper!ddg	Trojan
169	09A15B31-0000B3C1.eml	Generic.dx!ucn	Trojan
170	09ED75A6-0000B3CB.eml	Generic.dx!ucn	Trojan
171	0A2809CE-00003FDA.eml	W32/Rimecud.gen.al	Virus
172	0D1A41E1-00008C46.eml	JS/Redirector.z	Trojan
173	0D851DDE-0000AF7F.eml	JS/Redirector	Trojan
174	0E125F1E-00005B32.eml	Generic.Dropper.lr	Trojan
175	0F3E0099-00009B44.eml	Generic.Dropper.p	Trojan
176	0F901AC3-000095F6.eml	Bredolab.gen.x	Trojan
177	0FBF2F14-00007636.eml	Generic.FakeAlert!ht	Trojan
178	12E33A70-00009C58.eml	PWS-Zbot.gen.bn	Trojan
179	131F0A93-00000318.eml	W32/Netsky.p@MM!zip	Virus
180	132A1E6D-00008CB7.eml	JS/Redirector.z	Trojan
181	13661CD0-00007F92.eml	DNSChanger.bu	Trojan
182	13661CD0-00009BC5.eml	Generic.Dropper.p	Trojan
183	14642F87-00008C42.eml	JS/Redirector.z	Trojan
184	15A15422-00009BC9.eml	Generic.Dropper.p	Trojan
185	17A62C2D-0000A0C3.eml	JS/Redirector	Trojan
186	17DE628E-00009859.eml	Bredolab.gen.c	Trojan
187	182D2EF4-0000B3C6.eml	Generic.dx!ucn	Trojan
188	183A1FB4-0000EA9A.eml	PWS-Zbot.gen.ab	Trojan

Ek-19

19 İncelenen hard diskteki dosya ve e-postalarda tespit edilen virüs ve trojan tipindeki zararlı yazılımların listesi

Sıra No	Dosya Adı	Trojan/Virüs Adı	Tipi
189	187E16C5-00009FA3.eml	Downloader-CEW.a	Trojan
190	194D13F4-0000AD0E.eml	JS/Redirector	Trojan
191	19653E44-0000AF73.eml	JS/Redirector	Trojan
192	1A5C5B36-00009815.eml	Generic.Downloader.z	Trojan
193	1B1D4DBE-0000983F.eml	Bredolab.gen.c	Trojan
194	1B4D76A8-0000A0BB.eml	JS/Redirector	Trojan
195	1C04765F-00008FA8.eml	JS/Redirector	Trojan
196	1C902875-0000B031.eml	JS/Redirector	Trojan
197	1D327A99-000090DF.eml	FakeAlert-DefCnt.a.dldr	Trojan
198	1DFC0DF1-0000B023.eml	JS/Redirector	Trojan
199	1F3E1866-0000C752.eml	PWS-Banker!qpj	Trojan
200	1FC61419-0000B021.eml	JS/Redirector	Trojan
201	2059127E-00008D44.eml	JS/Redirector.z	Trojan
202	216757BE-00009825.eml	Generic.Downloader.z	Trojan
203	2213260D-0000826E.eml	JS/Downloader.gen	Trojan
204	2213260D-00008D15.eml	JS/Redirector.z	Trojan
205	222247DF-00008CA2.eml	JS.Redirector.z	Trojan
206	22421871-0000C7AA.eml	Generic.PWS.y!cvh	Trojan
207	22937D19-0000B221.eml	Downloader-CEW.g	Trojan
208	23321295-0000EA10.eml	PWS-Zbot.gen.ab	Trojan
209	23C948CC-00009BD7.eml	Generic.Dropper.p	Trojan
210	24417B55-0000A0D5.eml	JS/Redirector	Trojan
211	246264E0-00006BF9.eml	Bredolab.gen.c	Trojan
212	249D62F1-0000B3AA.eml	Generic.dx!ucn	Trojan
213	25687613-0000AD07.eml	JS/Redirector	Trojan
214	258B5326-00009C35.eml	PWS-Zbot.gen.bn	Trojan
215	25AD5AB7-0000B022.eml	JS/Redirector	Trojan
216	266878D4-00007BDA.eml	Spy-Agent.br	Trojan
217	26BF527F-0000B02A.eml	JS/Redirector	Trojan
218	26E901EB-00007145.eml	Generic.FakeAlert!hh	Trojan
219	27D37F0D-0000AD0A.eml	JS/Redirector	Trojan
220	283C668C-0000B027.eml	JS/Redirector	Trojan
221	284830C8-0000A0D4.eml	JS/Redirector	Trojan
222	285248DB-00009C02.eml	PWS-Zbot.gen.bn	Trojan
223	289A1D72-00009095.eml	FakeAlert-DefCnt.a.dldr	Trojan
224	2906049C-00008FA9.eml	JS/Redirector	Trojan
225	29731BD1-00009C3F.eml	PWS-Zbot.gen.bn	Trojan
226	29A6598D-00009823.eml	Generic.Downloader.z	Trojan
227	2BD560B7-000005F6.eml	Generic.dx	Trojan
228	2C4C333D-00008C64.eml	JS/Redirector.z	Trojan
229	2C6C2E53-0000ADDA.eml	JS/Downloader.gen	Trojan
230	2D326965-00009824.eml	Generic.Downloader.z	Trojan
231	2D943CF9-0000AF7B.eml	JS/Redirector	Trojan
232	2DEA4AA7-00006A70.eml	Downloader-CEW	Trojan
233	2F640D5A-00009C3C.eml	PWS-Zbot.gen.bn	Trojan
234	2FE0164E-0000ED70.eml	Backdoor-Spyeye	Trojan
235	30177300-0000B070.eml	JS/Redirector	Trojan

Ek-19

19 İncelenen hard diskteki dosya ve e-postalarda tespit edilen virüs ve trojan tipindeki zararlı yazılımların listesi

Sıra No	Dosya Adı	Trojan/Virüs Adı	Tipi
236	301C0BDB-000057A4.eml	Generic.Dropper.Ir	Trojan
237	301C0BDB-00008270.eml	JS/Downloader.gen	Trojan
238	304E354E-000067CF.eml	DNSChanger.bf	Trojan
239	30814E30-0000ADDD.eml	JS/Downloader.gen	Trojan
240	32237E64-0000EA1F.eml	PWS-Zbot.gen.ab	Trojan
241	33201BAD-0000B072.eml	JS/Redirector	Trojan
242	3459263D-0000E3BD.eml	W32/Rimecud.gen.al	Virus
243	349219DA-00008D4B.eml	Cutwail!env.b	Trojan
244	356E785C-0000B078.eml	JS/Redirector	Trojan
245	362C0C29-00009C50.eml	PWS-Zbot.gen.bn	Trojan
246	36514255-00008E2E.eml	JS/Downloader.gen	Trojan
247	366B66C4-00008D2E.eml	JS/Redirector.z	Trojan
248	368E0D66-00006952.eml	Bredolab!env.a	Trojan
249	368E0D66-00007FAA.eml	DNSChanger.bu	Trojan
250	368E0D66-00009FAD.eml	Downloader-CEW.a	Trojan
251	36990902-00007CA7.eml	Spy-Agent.br	Trojan