

TECHNICAL REPORT

15 / 01 / 2007

Contents

Computer: PC 1	3
Computer: PC 2	14
Computer: PC 3	21
Computer: PC 4	32
Computer: PC 5	43
Annex: Vulnerability description	59



Computer : PC1 - User : Domain1\user1

Audit start date

07 / 09 / 2006 13:20

Audit end date

07 / 09 / 2006 13:31

Items scanned 12496
 Files scanned 5932
 Messages scanned 6472

Malicious code discovered in the computer

- Active malicious code with a low danger level has been detected on your computer.
- The computer has 4 malicious code of which 2 are active.

Level of protection of the computer

- The computer is not adequately protected.

Malicious code detected

Active malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	0	0
Moderate	0	0
Low	2	51

Latent malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	0	0
Moderate	1	1
Low	1	44

Security failures

Security protection

Type of protection	Protection detected	Active	Updated
Antivirus	Symantec Antivirus Corporate Edition	Yes	Yes
Antispyware	Not available		
Personal firewall	Not available		
HIPS	Not available		

Vulnerabilities

0 vulnerabilities have been detected on the computer



Active malicious code

Highly dangerous malicious code

No highly dangerous active malicious code has been found

Rest of active malicious code

Name	Application/MyWebSearch
Items detected	46
Type	PUP
Hidden	No
Danger level	Low
Known since	29 / 09 / 2004

Details of the location

Running or marked to run

Name and location	Hidden
c:\documents and settings\all users\start menu\programs\startup\MyWebSearch Email Plugin.lnk	No
C:\PROGRA~1\MYWEBS~1\bar\1.bin\F3HISTSW.DLL	No
C:\Program Files\MyWebSearch\SrchAstt\1.bin\MWSSRCAS.DLL	No

In Registry

Location	Hidden
hkey_classes_root\clsid\{00A6FAF1-072E-44cf-8957-5838F569A31D}	No
hkey_classes_root\clsid\{07B18EA1-A523-4961-B6BB-170DE4475CCA}	No
hkey_classes_root\clsid\{07B18EA3-A523-4961-B6BB-170DE4475CCA}	No
hkey_classes_root\clsid\{07B18EA9-A523-4961-B6BB-170DE4475CCA}	No
hkey_classes_root\clsid\{07B18EAB-A523-4961-B6BB-170DE4475CCA}	No
hkey_classes_root\clsid\{147A976E-EEE1-4377-8EA7-4716E4CDD239}	No

Location	Hidden
hkey_classes_root\clsid\{147A976F-EEE1-4377-8EA7-4716E4CDD239}	No
hkey_classes_root\clsid\{63D0ED2C-B45B-4458-8B3B-60C69BBBD83C}	No
hkey_classes_root\clsid\{7473D292-B7BB-4f24-AE82-7E2CE94BB6A9}	No
hkey_classes_root\clsid\{938AA51A-996C-4884-98CE-80DD16A5C9DA}	No
hkey_classes_root\clsid\{9AFB8248-617F-460d-9366-D71CDEDA3179}	No
hkey_classes_root\clsid\{A4730EBE-43A6-443e-9776-36915D323AD3}	No
hkey_classes_root\clsid\{A9571378-68A1-443d-B082-284F960C6D17}	No
hkey_classes_root\clsid\{ADB01E81-3C79-4272-A0F1-7B2BE7A782DC}	No
HKEY_CLASSES_ROOT\Interface\{6E74766C-4D93-4CC0-96D1-47B8E07F F9CA}	No
HKEY_CLASSES_ROOT\Interface\{bbabdc90-f3d5-4801-863a-ee6ae52986 2d}	No
HKEY_CLASSES_ROOT\Interface\{d6ff3684-ad3b-48eb-bbb4-b9e6c5a355c 1}	No
HKEY_CLASSES_ROOT\Interface\{eb9e5c1c-b1f9-4c2b-be8a-27d6446fdaf8 }	No
hkey_classes_root\MyWebSearch.OutlookAddin	No
hkey_classes_root\MyWebSearch.OutlookAddin.1	No
hkey_classes_root\MyWebSearchToolBar.SettingsPlugin	No
hkey_classes_root\MyWebSearchToolBar.SettingsPlugin.1	No
HKEY_CLASSES_ROOT\TypeLib\{29D67D3C-509A-4544-903F-C8C1B823 6554}	No
HKEY_CLASSES_ROOT\TypeLib\{7473D290-B7BB-4F24-AE82-7E2CE94B B6A9}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{00A6FAF1-072E-44cf-8 957-5838F569A31D}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{07B18EA1-A523-4961-B 6BB-170DE4475CCA}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{07B18EA3-A523-4961-B 6BB-170DE4475CCA}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{07B18EA9-A523-4961-B 6BB-170DE4475CCA}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{07B18EAB-A523-4961- B6BB-170DE4475CCA}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{147A976E-EEE1-4377-8 EA7-4716E4CDD239}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{147a976f-eee1-4377-8e a7-4716e4cdd239}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{63D0ED2C-B45B-4458- 8B3B-60C69BBBD83C}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{7473D292-B7BB-4f24-A E82-7E2CE94BB6A9}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{938AA51A-996C-4884-9 8CE-80DD16A5C9DA}	No

Location	Hidden
HKEY_LOCAL_MACHINE\software\classes\CLSID\{9AFB8248-617F-460d-9366-D71CDEDA3179}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{a4730ebe-43a6-443e-9776-36915d323ad3}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{A9571378-68A1-443d-B082-284F960C6D17}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{ADB01E81-3C79-4272-A0F1-7B2BE7A782DC}	No
hkey_local_machine\software\FocusInteractive	No
hkey_local_machine\software\microsoft\windows\currentversion\uninstall\MyWebSearch bar Uninstall	No
hkey_local_machine\software\MyWebSearch	No

In file

Name and location	Hidden
c:\program files\MyWebSearch	No
c:\windows\system32\3PSSavr.scr	No

Name	Application/MediaPipe
Items detected	5
Type	PUP
Hidden	No
Danger level	Low
Known since	16 / 02 / 2006

Details of the location

Running or marked to run

Name and location	Hidden
C:\PROGRA~1\P2PNET~1\P2PNET~1.EXE	No
c:\program files\p2pnetworks\mpp2pl.exe	No

In Registry

Location	Hidden
hkey_classes_root\clsid\{B3E19860-0CD5-4991-A066-4FCA2704DE59}	No
HKEY_CLASSES_ROOT\TypeLib\{AFDBB222-DEA9-4C12-B3A3-A13C2985E3EE}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{B3E19860-0CD5-4991-A066-4FCA2704DE59}	No

Latent malicious code

Highly dangerous malicious code

No highly dangerous latent malicious code has been found

Rest of latent malicious code

Name	Application/FunWeb
Items detected	44
Type	PUP
Hidden	No
Danger level	Low
Known since	21 / 02 / 2004

Details of the location

In Registry

Location	Hidden
hkey_classes_root\clsid\{00A6FAF6-072E-44cf-8957-5838F569A31D}	No
hkey_classes_root\clsid\{0F8ECF4F-3646-4C3A-8881-8E138FFCAF70}	No
hkey_classes_root\clsid\{3DC201FB-E9C9-499C-A11F-23C360D7C3F8}	No
hkey_classes_root\clsid\{8E6F1832-9607-4440-8530-13BE7C4B1D14}	No
hkey_classes_root\clsid\{98D9753D-D73B-42D5-8C85-4469CDA897AB}	No
hkey_classes_root\clsid\{9FF05104-B030-46FC-94B8-81276E4E27DF}	No
hkey_classes_root\clsid\{B813095C-81C0-4E40-AA14-67520372B987}	No
hkey_classes_root\clsid\{C9D7BE3E-141A-4C85-8CD6-32461F3DF2C7}	No
hkey_classes_root\clsid\{CFF4CE82-3AA2-451F-9B77-7165605FB835}	No
hkey_classes_root\FunWebProducts.HistoryKillerScheduler	No
hkey_classes_root\FunWebProducts.HistoryKillerScheduler.1	No
hkey_classes_root\FunWebProducts.HistorySwatterControlBar	No
hkey_classes_root\FunWebProducts.HistorySwatterControlBar.1	No
hkey_classes_root\FunWebProducts.HTMLMenu	No
hkey_classes_root\FunWebProducts.HTMLMenu.1	No
hkey_classes_root\FunWebProducts.HTMLMenu.2	No

Location	Hidden
hkey_classes_root\FunWebProducts.IECookiesManager	No
hkey_classes_root\FunWebProducts.IECookiesManager.1	No
hkey_classes_root\FunWebProducts.KillerObjManager	No
hkey_classes_root\FunWebProducts.KillerObjManager.1	No
hkey_classes_root\FunWebProducts.PopSwatterBarButton	No
hkey_classes_root\FunWebProducts.PopSwatterBarButton.1	No
hkey_classes_root\FunWebProducts.PopSwatterSettingsControl	No
hkey_classes_root\FunWebProducts.PopSwatterSettingsControl.1	No
HKEY_CLASSES_ROOT\Interface\{63D0ED2D-B45B-4458-8B3B-60C69BBBD83C}	No
HKEY_CLASSES_ROOT\Interface\{de38c398-b328-4f4c-a3ad-1b5e4ed93477}	No
hkey_classes_root\ScreenSaverControl.ScreenSaverInstaller	No
hkey_classes_root\ScreenSaverControl.ScreenSaverInstaller.1	No
HKEY_CLASSES_ROOT\TypeLib\{e47caee0-deea-464a-9326-3f2801535a4d}	No
HKEY_CLASSES_ROOT\TypeLib\{f42228fb-e84e-479e-b922-fbbd096e792c}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{00a6faf6-072e-44cf-8957-5838f569a31d}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{0f8ecf4f-3646-4c3a-8881-8e138ffcaf70}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{3DC201FB-E9C9-499C-A11F-23C360D7C3F8}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{8E6F1832-9607-4440-8530-13BE7C4B1D14}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{98D9753D-D73B-42D5-8C85-4469CDA897AB}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{9FF05104-B030-46FC-94B8-81276E4E27DF}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{b813095c-81c0-4e40-aa14-67520372b987}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{c9d7be3e-141a-4c85-8cd6-32461f3df2c7}	No
HKEY_LOCAL_MACHINE\software\classes\CLSID\{cff4ce82-3aa2-451f-9b77-7165605fb835}	No
hkey_local_machine\software\Fun Web Products	No
hkey_local_machine\software\FunWebProducts	No
HKEY_LOCAL_MACHINE\Software\Microsoft\Code Store Database\Distribution Units\{1D4DB7D2-6EC9-47A3-BD87-1E41684E07BB}	No

In file

Name and location	Hidden
c:\program files\FunWebProducts	No
c:\windows\downloaded program files\3initialsetup1.0.0.15.inf	No

Name	Adware/Weirdontheweb
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	10 / 06 / 2005

Details of the location

In Registry

Location	Hidden
HKEY_CLASSES_ROOT\AppID\{7911272A-A32A-404E-8A51-EE18B99B18C4}	No

Cookies

No cookies have been detected on the computer

Jokes

No jokes have been detected on the computer

Details of the protection and vulnerabilities

Details of the protection

Antivirus protection

Protection	Version	Enabled	Up-to-date
Symantec Antivirus Corporate Edition	10.0	Yes	Yes

Antispyware protection

The computer does not have anti-spyware

Firewall protection

The computer does not have a firewall

HIPS protection

The computer does not have HIPS

Details of the vulnerabilities

No vulnerabilities have been detected on the computer

Details of audited computer

Computer name	PC 1
User name	Domain1\user1
Domain:	Domain1
Group:	Administrators,Users
IP:	172.16.51.131

Operating system:	Windows XP Professional
Service Pack:	Service Pack 2
IE version:	6.0.2900.2180
Outlook version:	11.0.5510.0
Outlook Express version:	6.0.2900.2180
Default browser:	Internet Explorer
Default mail client:	Microsoft Office Outlook

Computer : PC 2 - User : Domain2\user2

Audit start date

07 / 09 / 2006 13:23

Audit end date

07 / 09 / 2006 13:38

Items scanned 2188
 Files scanned 2176
 Messages scanned 0

Malicious code discovered in the computer

- Active malicious code with a moderate danger level has been detected on your computer.
- The computer has 3 malicious code of which 3 are active.

Level of protection of the computer

- The computer is not adequately protected.

Malicious code detected

Active malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	0	0
Moderate	3	22
Low	0	0

Latent malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	0	0
Moderate	0	0
Low	0	0

Security failures

Security protection

Type of protection	Protection detected	Active	Updated
Antivirus	Symantec Antivirus Corporate Edition	No	No
Antispyware	Not available		
Personal firewall	Not available		
HIPS	Not available		

Vulnerabilities

50 vulnerabilities have been detected on the computer



Active malicious code

Highly dangerous malicious code

No highly dangerous active malicious code has been found

Rest of active malicious code

Name	Adware/Gator
Items detected	14
Type	Adware
Hidden	No
Danger level	Moderate
Known since	11 / 09 / 2003

Details of the location

Running or marked to run

Name and location	Hidden
C:\Documents and Settings\All Users\Start Menu\Programs\Startup\GStartup.Ink	No
C:\Program Files\Common Files\CMEII\CMEIIAPI.dll	No
c:\program files\common files\cmeii\cmesys.exe	No
c:\program files\common files\cmeii\gappmgr.dll	No
C:\Program Files\Common Files\CMEII\Glocl.dll	No
C:\Program Files\Common Files\CMEII\GStore.dll	No
c:\program files\common files\cmeii\gstoreserver.dll	No
C:\Program Files\Common Files\GMT\GMT.exe	No
C:\Program Files>Date Manager\DateManager.exe	No



In file

Name and location	Hidden
c:\documents and settings\all users\start menu\programs\GAIN	No
c:\program files\common files\CMEII	No
c:\program files\common files\GMT	No
c:\winnt\GatorPdpPlugin.log	No
c:\winnt\GatorPdpSetup.log	No

Name	Adware/Xupiter
Items detected	4
Type	Adware
Hidden	No
Danger level	Moderate
Known since	30 / 01 / 2004

Details of the location

Running or marked to run

Name and location	Hidden
C:\Program Files\Xupiter\XTUpdate.dll	No

In file

Name and location	Hidden
c:\program files\Xupiter	No
c:\winnt\downloaded program files\XupiterToolbarLoader.inf	No
C:\WINNT\TEMP\XupiterToolbarInstaller.exe	No

Name	Adware/Gator.PTime
Items detected	4
Type	Adware

Hidden	No
Danger level	Moderate
Known since	16 / 09 / 2005

Details of the location

Running or marked to run

Name and location	Hidden
c:\documents and settings\all users\start menu\programs\startup\PrecisionTime.lnk	No
C:\Program Files\PrecisionTime\PrecisionTime.exe	No

In file

Name and location	Hidden
c:\documents and settings\all users\start menu\programs\PrecisionTime	No
c:\program files\PrecisionTime	No



Details of the protection and vulnerabilities

Details of the protection

Antivirus protection

Protection	Version	Enabled	Up-to-date
Symantec Antivirus Corporate Edition	10.1	No	No

Antispyware protection

The computer does not have anti-spyware

Firewall protection

The computer does not have a firewall

HIPS protection

The computer does not have HIPS

Details of the vulnerabilities

Vulnerabilities detected:

[MS03-039](#) [MS04-011](#) [MS04-012](#) [MS04-013](#) [MS04-018](#) [MS04-040](#) [MS05-014](#) [MS05-020](#)
[MS05-025](#) [MS05-037](#) [MS05-038](#) [MS05-039](#) [MS05-040](#) [MS05-042](#) [MS05-043](#) [MS05-044](#)
[MS05-045](#) [MS05-046](#) [MS05-047](#) [MS05-048](#) [MS05-049](#) [MS05-050](#) [MS05-051](#) [MS05-052](#)
[MS05-053](#) [MS05-054](#) [MS05-055](#) [MS06-001](#) [MS06-002](#) [MS06-006](#) [MS06-013](#) [MS06-015](#)
[MS06-016](#) [MS06-018](#) [MS06-021](#) [MS06-025](#) [MS06-030](#) [MS06-031](#) [MS06-032](#) [MS06-035](#)
[MS06-036](#) [MS06-040](#) [MS06-041](#) [MS06-042](#) [MS06-044](#) [MS06-045](#) [MS06-046](#) [MS06-049](#)
[MS06-050](#) [MS06-051](#)

Details of audited computer

Computer name	PC 2
User name	Domain2\user2
Domain:	Domain2
Group:	
IP:	172.16.1.11
Operating system:	Windows 2000
Service Pack:	Service Pack 4
IE version:	6.0.2800.1106
Outlook version:	9.0.0.2416
Outlook Express version:	6.0.2800.1106
Default browser:	Internet Explorer
Default mail client:	Outlook Express

Computer : PC 3 - User : Domain3\user3

Audit start date

07 / 09 / 2006 13:26

Audit end date

07 / 09 / 2006 13:40

Items scanned 11275
 Files scanned 6446
 Messages scanned 4810

Malicious code discovered in the computer

- Active malicious code with a low danger level has been detected on your computer.
- The computer has 12 malicious code of which 1 is active.

Level of protection of the computer

- The computer is not adequately protected.

Malicious code detected

Active malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	0	0
Moderate	0	0
Low	1	2

Latent malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	0	0
Moderate	6	8
Low	5	10

Security failures

Security protection

Type of protection	Protection detected	Active	Updated
Antivirus	Symantec Antivirus Corporate Edition	No	No
Antispyware	Not available		
Personal firewall	Not available		
HIPS	Not available		

Vulnerabilities

31 vulnerabilities have been detected on the computer

Active malicious code

Highly dangerous malicious code

No highly dangerous active malicious code has been found

Rest of active malicious code

Name	Adware/Idonate
Items detected	2
Type	Adware
Hidden	No
Danger level	Low
Known since	05 / 04 / 2006

Details of the location

Running or marked to run

Name and location	Hidden
C:\WINNT\iDonate.dll	No

In file

Name and location	Hidden
c:\winnt\iDonate.dll	No

Latent malicious code

Highly dangerous malicious code

No highly dangerous latent malicious code has been found

Rest of latent malicious code

Name	Application/MyWay
Items detected	2
Type	PUP
Hidden	No
Danger level	Low
Known since	11 / 09 / 2003

Details of the location

In Registry

Location	Hidden
hkey_classes_root\typelib\{0494D0D0-F8E0-41AD-92A3-14154ECE70AC}	No

In file

Name and location	Hidden
c:\program files\MyWay	No

Name	Application/FunWeb
Items detected	2
Type	PUP
Hidden	No

Danger level	Low
Known since	21 / 02 / 2004

Details of the location

In file

Name and location	Hidden
c:\program files\FunWebProducts	No
c:\winnt\downloaded program files\3initialsetup1.0.0.6.inf	No

Name		Adware/WinTools
Items detected	2	
Type	Adware	
Hidden	No	
Danger level	Moderate	
Known since	18 / 03 / 2004	

Details of the location

In Registry

Location	Hidden
hkey_local_machine\system\controlset001\enum\root\LEGACY_WINTOOLS SVC	No

In file

Name and location	Hidden
C:\WINNT\TEMP\msiein	No

Name		Adware/VirtualBouncer
Items detected	2	



Type	Adware
Hidden	No
Danger level	Moderate
Known since	22 / 03 / 2004

Details of the location

In file

Name and location	Hidden
c:\program files\VBouncer	No
c:\winnt\system32\INNERADINSTALL.LOG	No

Name	Adware/NavHelper
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	03 / 06 / 2004

Details of the location

In file

Name and location	Hidden
c:\program files\NavExcel	No

Name	Adware/MyDailyHoroscope
Items detected	1
Type	Adware
Hidden	No

Danger level	Moderate
Known since	22 / 07 / 2004

Details of the location

In file

Name and location	Hidden
c:\program files\My Daily Horoscope	No

Name	Adware/Twain-Tech
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	02 / 08 / 2004

Details of the location

In file

Name and location	Hidden
C:\WINNT\TEMP\THI138.tmp	No

Name	Application/MyWebSearch
Items detected	1
Type	PUP
Hidden	No
Danger level	Low
Known since	29 / 09 / 2004

Details of the location

In file

Name and location	Hidden
c:\program files\MyWebSearch	No

Name	Adware/Gator.PTime
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	16 / 09 / 2005

Details of the location

In file

Name and location	Hidden
c:\documents and settings\all users\start menu\programs\PrecisionTime	No

Name	Application/Bestoffer
Items detected	1
Type	PUP
Hidden	No
Danger level	Low
Known since	26 / 09 / 2005

Details of the location



In file

Name and location	Hidden
c:\winnt\smdat32a.sys	No

Name	Application/RegClean32
Items detected	4
Type	PUP
Hidden	No
Danger level	Low
Known since	03 / 10 / 2005

Details of the location

In Registry

Location	Hidden
hkey_local_machine\software\microsoft\windows\currentversion\uninstall\Registry Cleaner (Trial)_is1	No

In file

Name and location	Hidden
c:\documents and settings\all users\start menu\programs\RegistryCleaner	No
c:\program files\Registry Cleaner Trial	No
c:\program files\TPT Registry_Cleaner (Trial)	No

Cookies

No cookies have been detected on the computer

Jokes

No jokes have been detected on the computer

Details of the protection and vulnerabilities

Details of the protection

Antivirus protection

Protection	Version	Enabled	Up-to-date
Symantec Antivirus Corporate Edition	10.0	No	No

Antispyware protection

The computer does not have anti-spyware

Firewall protection

The computer does not have a firewall

HIPS protection

The computer does not have HIPS

Details of the vulnerabilities

Vulnerabilities detected:

[MS04-013](#) [MS04-018](#) [MS04-040](#) [MS05-014](#) [MS05-020](#) [MS05-025](#) [MS05-037](#) [MS05-038](#)
[MS05-044](#) [MS05-052](#) [MS05-054](#) [MS06-013](#) [MS06-015](#) [MS06-016](#) [MS06-018](#) [MS06-021](#)
[MS06-025](#) [MS06-030](#) [MS06-031](#) [MS06-032](#) [MS06-035](#) [MS06-036](#) [MS06-040](#) [MS06-041](#)
[MS06-042](#) [MS06-044](#) [MS06-045](#) [MS06-046](#) [MS06-049](#) [MS06-050](#) [MS06-051](#)

Details of audited computer

Computer name	PC 3
User name	Domain3\user3
Domain:	Domain3
Group:	
IP:	172.16.51.101
Operating system:	Windows 2000
Service Pack:	Service Pack 4
IE version:	6.0.2800.1106
Outlook version:	11.0.5510.0
Outlook Express version:	6.0.2800.1106
Default browser:	Avant Browser
Default mail client:	Microsoft Office Outlook

Computer : PC 4 - User : Domain4\user4

Audit start date

07 / 09 / 2006 13:27

Audit end date

07 / 09 / 2006 13:49

Items scanned

6933

Files scanned

6922

Messages scanned

0

Malicious code discovered in the computer

- Active malicious code with a high danger level has been detected on your computer.
- The computer has 10 malicious code of which 6 are active.

Level of protection of the computer

- The computer is not adequately protected.

Malicious code detected

Active malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	1	1
Moderate	5	13
Low	0	0

Latent malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	0	0
Moderate	4	8
Low	0	0

Security failures

Security protection

Type of protection	Protection detected	Active	Updated
Antivirus	Symantec Antivirus Corporate Edition	No	Yes
Antispyware	Not available		
Personal firewall	Not available		
HIPS	Not available		

Vulnerabilities

0 vulnerabilities have been detected on the computer

Active malicious code

Highly dangerous malicious code

No highly dangerous active malicious code has been found

Rest of active malicious code

Name	Adware/PurityScan
Items detected	2
Type	Adware
Hidden	No
Danger level	Moderate
Known since	20 / 11 / 2003

Details of the location

Running or marked to run

Name and location	Hidden
C:\WINDOWS\system32\ecirzplt.dll	No
C:\WINDOWS\system32\logonui.dll	No

Name	Adware/Sqwire
Items detected	6
Type	Adware

Hidden	No
Danger level	Moderate
Known since	06 / 04 / 2004

Details of the location

Running or marked to run

Name and location	Hidden
C:\PROGRA~1\COMMON~1\ukfz\ukfza.exe	No
C:\PROGRA~1\COMMON~1\ukfz\ukfzd\ukfzc.dll	No
c:\progra~1\common~1\ukfz\ukfzm.exe	No

In Registry

Location	Hidden
hkey_local_machine\software\microsoft\windows\currentversion\app management\arpcache\TSA	No
hkey_local_machine\software\microsoft\windows\currentversion\uninstall\TSA	No

In file

Name and location	Hidden
c:\windows\system32\tsuninst.exe	No

Name	Adware/Maxifiles
Items detected	1
Type	Adware
Hidden	No
Danger level	High
Known since	31 / 05 / 2005

Details of the location

Running or marked to run

Name and location	Hidden
c:\windows\system32\swinkqex.exe	No

Name	Adware/Qoologic
Items detected	3
Type	Adware
Hidden	No
Danger level	Moderate
Known since	05 / 09 / 2005

Details of the location

Running or marked to run

Name and location	Hidden
C:\Documents and Settings\All Users\Start Menu\Programs\Startup\plcgi.exe	No
C:\WINDOWS\system32\elpfsw.dll	No
c:\windows\system32\xeqfco.exe	No

Name	Adware/Zenosearch
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	08 / 11 / 2005



Details of the location

Running or marked to run

Name and location	Hidden
c:\windows\system32\pjsdrego.exe	No

Name	Trj/Qoologic.J
Items detected	1
Type	Trojan
Hidden	No
Danger level	Moderate
Known since	20 / 03 / 2006

Details of the location

Running or marked to run

Name and location	Hidden
C:\WINDOWS\system32\onhjc.exe	No



Latent malicious code

Highly dangerous malicious code

No highly dangerous latent malicious code has been found

Rest of latent malicious code

Name	Adware/Exact.BargainBuddy
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	11 / 09 / 2003

Details of the location

In Registry

Location	Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{F4E04583-354E-4076-BE7D-ED6A80FD66DA}	No

Name	Adware/Exact.SearchBar
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	12 / 08 / 2004

Details of the location

In Registry

Location	Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{AEECBFDA-12FA-4881-BDCE-8C3E1CE4B344}	No

Name	Adware/CommAd
Items detected	4
Type	Adware
Hidden	No
Danger level	Moderate
Known since	27 / 10 / 2005

Details of the location

In Registry

Location	Hidden
hkey_local_machine\system\controlset001\enum\root\LEGACY_CMDSERVICE	No
hkey_local_machine\system\controlset001\enum\root\LEGACY_NETWORK_MONITOR	No
hkey_local_machine\system\currentcontrolset\enum\root\LEGACY_CMDSERVICE	No
hkey_local_machine\system\currentcontrolset\enum\root\LEGACY_NETWORK_MONITOR	No

Name	Adware/DropSpam
Items detected	2
Type	Adware



Hidden	No
Danger level	Moderate
Known since	18 / 12 / 2005

Details of the location

In Registry

Location	Hidden
hkey_current_user\software\dropspam	No
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{2DEA8791-C2B7-48E1-8992-8E8E6A6FE789}	No

Cookies

Location	C:\Documents and Settings\LocalService\Cookies
Number of cookies	5

Jokes

No jokes have been detected on the computer

Details of the protection and vulnerabilities

Details of the protection

Antivirus protection



Protection	Version	Enabled	Up-to-date
Symantec Antivirus Corporate Edition	8.0	No	Yes

Antispyware protection

The computer does not have anti-spyware

Firewall protection

The computer does not have a firewall

HIPS protection

The computer does not have HIPS

Details of the vulnerabilities

No vulnerabilities have been detected on the computer

Details of audited computer

Computer name	PC 4
User name	Domain4\user4
Domain:	Domain4
Group:	
IP:	172.16.1.5
Operating system:	Windows XP Professional
Service Pack:	Service Pack 2
IE version:	6.0.2900.2180
Outlook version:	11.0.8010.0
Outlook Express version:	6.0.2900.2180
Default browser:	Internet Explorer

Default mail client:

Microsoft Office Outlook

Computer : PC 5 - User : Domain5\user5

Audit start date

07 / 09 / 2006 13:27

Audit end date

07 / 09 / 2006 23:10

Items scanned 3718
 Files scanned 3630
 Messages scanned 0

Malicious code discovered in the computer

- Active malicious code with a high danger level has been detected on your computer.
- The computer has 18 malicious code of which 2 are active.

Level of protection of the computer

- The computer is not adequately protected.

Malicious code detected

Active malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	1	1
Moderate	0	0
Low	1	28

Latent malicious code

Danger level	Malicious code	Items discovered
Very High	0	0
High	2	5
Moderate	13	18
Low	1	33

Security failures

Security protection

Type of protection	Protection detected	Active	Updated
Antivirus	Not available		
Antispyware	Not available		
Personal firewall	Not available		
HIPS	Not available		

Vulnerabilities

15 vulnerabilities have been detected on the computer

Active malicious code

Highly dangerous malicious code

No highly dangerous active malicious code has been found

Rest of active malicious code

Name	Application/MyWebSearch
Items detected	28
Type	PUP
Hidden	No
Danger level	Low
Known since	29 / 09 / 2004

Details of the location

Running or marked to run

Name and location	Hidden
C:\PROGRA~1\MYWEBS~1\bar\1.bin\MWSBAR.DLL	No
c:\progra~1\mywebs~1\bar\1.bin\mwsoemon.exe	No
C:\PROGRA~1\MYWEBS~1\bar\1.bin\mwsoestb.dll	No
C:\Program Files\MyWebSearch\bar\1.bin\F3HTMLMU.DLL	No
C:\Program Files\MyWebSearch\bar\1.bin\M3OUTLCN.DLL	No
C:\Program Files\MyWebSearch\bar\1.bin\MWSBAR.DLL	No

In Registry

Location	Hidden
hkey_classes_root\clsid\{00A6FAF1-072E-44cf-8957-5838F569A31D}	No
hkey_classes_root\clsid\{07B18EA1-A523-4961-B6BB-170DE4475CCA}	No
hkey_classes_root\clsid\{07B18EA3-A523-4961-B6BB-170DE4475CCA}	No
hkey_classes_root\clsid\{07B18EA9-A523-4961-B6BB-170DE4475CCA}	No



Location	Hidden
hkey_classes_root\clsid\{07B18EAB-A523-4961-B6BB-170DE4475CCA}	No
hkey_classes_root\clsid\{147A976F-EEE1-4377-8EA7-4716E4CDD239}	No
hkey_classes_root\clsid\{63D0ED2C-B45B-4458-8B3B-60C69BBBD83C}	No
hkey_classes_root\clsid\{7473D292-B7BB-4f24-AE82-7E2CE94BB6A9}	No
hkey_classes_root\clsid\{938AA51A-996C-4884-98CE-80DD16A5C9DA}	No
hkey_classes_root\clsid\{9AFB8248-617F-460d-9366-D71CDEDA3179}	No
hkey_classes_root\clsid\{A4730EBE-43A6-443e-9776-36915D323AD3}	No
hkey_classes_root\clsid\{A9571378-68A1-443d-B082-284F960C6D17}	No
hkey_classes_root\clsid\{ADB01E81-3C79-4272-A0F1-7B2BE7A782DC}	No
hkey_classes_root\MyWebSearch.OutlookAddin	No
hkey_classes_root\MyWebSearch.OutlookAddin.1	No
hkey_classes_root\MyWebSearchToolBar.SettingsPlugin	No
hkey_classes_root\MyWebSearchToolBar.SettingsPlugin.1	No
hkey_local_machine\software\microsoft\office\outlook\addins\MyWebSearch.OutlookAddin	No
hkey_local_machine\software\microsoft\office\word\addins\MyWebSearch.OutlookAddin	No
hkey_local_machine\software\microsoft\windows\currentversion\uninstall\MyWebSearch bar Uninstall	No

In file

Name and location	Hidden
c:\program files\MyWebSearch	No
c:\winnt\system32\3PSSavr.scr	No

Name	Bck/Afcore.AS
Items detected	1
Type	Bakcdoor
Hidden	No
Danger level	High
Known since	25 / 07 / 2006

Details of the location

Running or marked to run

Name and location	Hidden
C:\WINNT\system32\iasaccz.dll	No



Latent malicious code

Highly dangerous malicious code

No highly dangerous latent malicious code has been found

Rest of latent malicious code

Name	Exploit/iFrame
Items detected	2
Type	Hacking Tool
Hidden	No
Danger level	Moderate
Known since	23 / 04 / 2002

Details of the location

In mail

Location
Mailbox - Karen Walker\Inbox\Delivery Status Notification (Failure)\Mail Delivery (failure nhenderson@uses.org)
Mailbox - Karen Walker\Inbox\Mail Delivery (failure kwalker@rcc.mass.edu)

Name	Adware/eZula
Items detected	2
Type	Adware
Hidden	No
Danger level	Moderate

Known since	11 / 09 / 2003
--------------------	----------------

Details of the location

In Registry

Location	Hidden
hkey_classes_root\typelib\{E0D3B292-A0B0-4640-975C-2F882E039F52}	No
hkey_local_machine\software\classes\typelib\{E0D3B292-A0B0-4640-975C-2F882E039F52}	No

Name	Adware/Exact.BargainBuddy
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	11 / 09 / 2003

Details of the location

In file

Name and location	Hidden
c:\program files\Bargain Buddy	No

Name	Adware/KeenValue
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	02 / 01 / 2004

Details of the location

In file

Name and location	Hidden
C:\WINNT\TEMP\IncrediFindBHOLog.tmp	No

Name	Application/FunWeb
Items detected	33
Type	PUP
Hidden	No
Danger level	Low
Known since	21 / 02 / 2004

Details of the location

In Registry

Location	Hidden
hkey_classes_root\clsid\{00A6FAF6-072E-44cf-8957-5838F569A31D}	No
hkey_classes_root\clsid\{0F8ECF4F-3646-4C3A-8881-8E138FFCAF70}	No
hkey_classes_root\clsid\{3DC201FB-E9C9-499C-A11F-23C360D7C3F8}	No
hkey_classes_root\clsid\{8E6F1832-9607-4440-8530-13BE7C4B1D14}	No
hkey_classes_root\clsid\{98D9753D-D73B-42D5-8C85-4469CDA897AB}	No
hkey_classes_root\clsid\{9FF05104-B030-46FC-94B8-81276E4E27DF}	No
hkey_classes_root\clsid\{B813095C-81C0-4E40-AA14-67520372B987}	No
hkey_classes_root\clsid\{C9D7BE3E-141A-4C85-8CD6-32461F3DF2C7}	No
hkey_classes_root\clsid\{CFF4CE82-3AA2-451F-9B77-7165605FB835}	No
hkey_classes_root\FunWebProducts.DataControl	No
hkey_classes_root\FunWebProducts.DataControl.1	No
hkey_classes_root\FunWebProducts.HistoryKillerScheduler	No
hkey_classes_root\FunWebProducts.HistoryKillerScheduler.1	No
hkey_classes_root\FunWebProducts.HistorySwatterControlBar	No
hkey_classes_root\FunWebProducts.HistorySwatterControlBar.1	No
hkey_classes_root\FunWebProducts.HTMLMenu	No
hkey_classes_root\FunWebProducts.HTMLMenu.1	No
hkey_classes_root\FunWebProducts.HTMLMenu.2	No



Location	Hidden
hkey_classes_root\FunWebProducts.IECookiesManager	No
hkey_classes_root\FunWebProducts.IECookiesManager.1	No
hkey_classes_root\FunWebProducts.KillerObjManager	No
hkey_classes_root\FunWebProducts.KillerObjManager.1	No
hkey_classes_root\FunWebProducts.PopSwatterBarButton	No
hkey_classes_root\FunWebProducts.PopSwatterBarButton.1	No
hkey_classes_root\FunWebProducts.PopSwatterSettingsControl	No
hkey_classes_root\FunWebProducts.PopSwatterSettingsControl.1	No
hkey_classes_root\FunWebProducts.ShellViewControl	No
hkey_classes_root\FunWebProducts.ShellViewControl.1	No
hkey_classes_root\ScreenSaverControl.ScreenSaverInstaller	No
hkey_classes_root\ScreenSaverControl.ScreenSaverInstaller.1	No
hkey_local_machine\software\FunWebProducts	No

In file

Name and location	Hidden
c:\program files\FunWebProducts	No
c:\winnt\downloaded program files\3initialsetup1.0.0.15.inf	No

Name	Adware/WinTools
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	18 / 03 / 2004

Details of the location

In Registry

Location	Hidden
hkey_local_machine\system\currentcontrolset\enum\root\LEGACY_WINTOO LSSVC	No

Name		Adware/AdDestroyer
Items detected	2	
Type	Adware	
Hidden	No	
Danger level	Moderate	
Known since	22 / 03 / 2004	

Details of the location

In Registry

Location	Hidden
hkey_classes_root\SWLAD1.SWLAD	No
hkey_local_machine\software\classes\SWLAD1.SWLAD	No

Name		Adware/VirtualBouncer
Items detected	1	
Type	Adware	
Hidden	No	
Danger level	Moderate	
Known since	22 / 03 / 2004	

Details of the location

In file

Name and location	Hidden
c:\winnt\system32\INNERADINSTALL.LOG	No

Name		Adware/TVMedia
------	--	----------------



Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	15 / 04 / 2004

Details of the location

In Registry

Location	Hidden
hkey_local_machine\software\microsoft\windows\currentversion\uninstall\{5886A6DC-AAF4-45E9-979A-8E5E6DEE30E7}	No

Name	Adware/DealHelper
Items detected	2
Type	Adware
Hidden	No
Danger level	Moderate
Known since	22 / 06 / 2004

Details of the location

In Registry

Location	Hidden
hkey_local_machine\software\microsoft\windows\currentversion\uninstall\TimeSync	No

In file

Name and location	Hidden
c:\program files\TimeSync	No



Name	Adware/AdLogix
Items detected	2
Type	Adware
Hidden	No
Danger level	Moderate
Known since	16 / 07 / 2004

Details of the location

In Registry

Location	Hidden
hkey_classes_root\SWin32.SDWin32	No
hkey_local_machine\software\classes\SWin32.SDWin32	No

Name	Spyware/ClientMan
Items detected	4
Type	Spyware
Hidden	No
Danger level	High
Known since	27 / 07 / 2004

Details of the location

In Registry

Location	Hidden
hkey_classes_root\clsid\{CC905FF6-B553-496C-9DFA-CFF65ADCD0FC}	No
hkey_classes_root\searchrep.SearchRepPP	No
hkey_classes_root\searchrep.SearchRepPP.1	No
hkey_local_machine\software\classes\searchrep.SearchRepPP	No

Name		Adware/Twain-Tech
Items detected	1	
Type	Adware	
Hidden	No	
Danger level	Moderate	
Known since	02 / 08 / 2004	

Details of the location

In file

Name and location	Hidden
C:\WINNT\TEMP\THI2BC8.tmp	No

Name		Adware/ClockSync
Items detected	1	
Type	Adware	
Hidden	No	
Danger level	Moderate	
Known since	27 / 09 / 2004	

Details of the location

In file

Name and location	Hidden
c:\program files\ClockSync	No

Name		Spyware/Whazit
Items detected	1	

Type	Spyware
Hidden	No
Danger level	High
Known since	29 / 11 / 2004

Details of the location

In file

Name and location	Hidden
c:\winnt\system32\kyf.dat	No

Name	Adware/Transponder
Items detected	1
Type	Adware
Hidden	No
Danger level	Moderate
Known since	28 / 01 / 2005

Details of the location

In file

Name and location	Hidden
C:\WINNT\TEMP\dummy.htm	No

Cookies

No cookies have been detected on the computer

Jokes

No jokes have been detected on the computer

Details of the protection and vulnerabilities

Details of the protection

Antivirus protection

The computer does not have an antivirus

Antispyware protection

The computer does not have anti-spyware

Firewall protection

The computer does not have a firewall

HIPS protection

The computer does not have HIPS

Details of the vulnerabilities

Vulnerabilities detected:

[MS04-013](#) [MS04-018](#) [MS04-040](#) [MS05-014](#) [MS05-020](#) [MS05-025](#) [MS05-037](#) [MS05-038](#)
[MS05-044](#) [MS05-052](#) [MS05-054](#) [MS06-013](#) [MS06-016](#) [MS06-021](#) [MS06-042](#)

Details of audited computer

Computer name	PC 5
User name	Domain5\user5
Domain:	Domain5
Group:	
IP:	172.16.2.103
Operating system:	Windows 2000
Service Pack:	Service Pack 4
IE version:	6.0.2600.0
Outlook version:	11.0.5510.0
Outlook Express version:	6.0.2600.0
Default browser:	Internet Explorer
Default mail client:	Microsoft Office Outlook

Annex: Vulnerability description

Identifier	MS03-039
Description/Possible effects:	It is a group of critical vulnerabilities in the RPCSS service on Windows 2003/XP/2000/NT computers, which allows hackers to execute arbitrary code and to launch remote Denial of Service attacks against the computer.
Severity:	High
Appeared:	02 / 06 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSNT
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Blaster, Blaster.B, Blaster.C, Blaster.E, Blaster.F, Blaster.G, Blaster.H, Nachi.A, Nachi.B, Nachi.C, Nachi.D, Nachi.E, Nachi.F, Nachi.G, Nachi.H, Plexus.A, Plexus.B
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS04-011
Description/Possible effects:	It is a critical vulnerability in the LSASS service on Windows XP/2000 computers, which allows to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	04 / 03 / 05
Systems affected:	WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Sasser.A, Sasser.B, Sasser.C, Sasser.D, Sasser.E, Sasser.F, Sasser.G, Korgo.A, Korgo.B, Korgo.D, Korgo.E, Korgo.F, Korgo.G, Korgo.H, Korgo.I, Korgo.M, Korgo.N, Korgo.O, Korgo.P, Korgo.Q, Korgo.R, Korgo.S, Korgo.T, Korgo.U, Korgo.V, Korgo.X, Korgo.Z, Bobax.A, Bobax.B, Bobax.C, Bobax.D, Plexus.A, Plexus.B, Cycle.A

Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS04-012
Description/Possible effects:	It is a group of critical vulnerabilities in RPC-DCOM on Windows 2003/XP/2000/NT computers, which allows hackers to execute arbitrary code and to launch remote Denial of Service attacks and information to be disclosed.
Severity:	High
Appeared:	02 / 06 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSNT, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Blaster, Blaster.B, Blaster.C, Blaster.E, Blaster.F, Blaster.G, Blaster.H, Nachi.A, Nachi.B, Nachi.C, Nachi.D, Nachi.E, Nachi.F, Nachi.G, Nachi.H, Plexus.A, Plexus.B
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS04-013
Description/Possible effects:	It is a critical vulnerability in Windows 2003/XP/2000/NT/Me/98 computers, known as MHTML URL Processing Vulnerability, which allows to remotely execute arbitrary code in the vulnerable computer.
Severity:	Moderate
Appeared:	04 / 03 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSNT, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	MhtRedir.N, MhtRedir.S, DialogArg, Daol.A, Mimail, Mimail.B, Mimail.D, Sinala.A
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS04-018
Description/Possible effects:	It is a critical vulnerability in Windows 2003/XP/2000/NT computers, known as MHTML

	URL Processing Vulnerability, which allows to remotely execute arbitrary code in the vulnerable computer.
Severity:	Moderate
Appeared:	11 / 04 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSNT
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	MhtRedir.N, MhtRedir.S, DialogArg, Daol.A, Mimail, Mimail.B, Mimail.D, Sinala.A
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS04-040
Description/Possible effects:	It is a vulnerability in Internet Explorer v6.0 running on Windows XP/2000/NT/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged-on user.
Severity:	Moderate
Appeared:	03 / 12 / 04
Systems affected:	WINDOWSXP, WINDOWS2000, WINDOWSNT, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Bofra.B, Bofra.C
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-014
Description/Possible effects:	It is a set of four vulnerabilities that affect Internet Explorer 5.01, 5.5 and 6 running on Windows 2003/XP/2000/Me/98 computers. The vulnerabilities allow to take complete control of the computer.
Severity:	Moderate
Appeared:	09 / 02 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Bofra.B, Bofra.C
Can be fixed:	Yes

Link to solution:	http://update.microsoft.com/
-------------------	---

Identifier	MS05-020
Description/Possible effects:	It is a group of vulnerabilities in Internet Explorer on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	13 / 04 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Bofra.B, Bofra.C
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-025
Description/Possible effects:	It is a group of vulnerabilities in Internet Explorer on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	15 / 06 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Bofra.B, Bofra.C
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-037
Description/Possible effects:	It is a critical vulnerability in Internet Explorer versions 5.01, 5.5 and 6 on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate

Appeared:	13 / 07 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-038
Description/Possible effects:	It is a group of vulnerabilities in Internet Explorer versions 5.01, 5.5 and 6 on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	10 / 08 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-044
Description/Possible effects:	It is a vulnerability on Windows 2003/XP computers and Internet Explorer version 6 on Windows 2000, which allows hackers to save a file that the affected user tries to download via the Windows FTP client in a location where it could have unexpected effects.
Severity:	Moderate
Appeared:	14 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWSXP
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-052
------------	----------

Description/Possible effects:	It is a vulnerability in Internet Explorer versions 5.01, 5.5 and 6 on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	13 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-054
Description/Possible effects:	It is a group of vulnerabilities in Internet Explorer versions 5.01, 5.5 and 6 on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	14 / 12 / 05
Systems affected:	WINDOWS2003, WINDOWSP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-006
Description/Possible effects:	It is an important vulnerability in the Windows Media Player plug-in on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	15 / 02 / 06
Systems affected:	WINDOWS2003, WINDOWSP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	

Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-013
Description/Possible effects:	It is a group of vulnerabilities in Internet Explorer versions 5.01 and 6 on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	12 / 04 / 06
Systems affected:	WINDOWS2003, WINDOWSP, WINDOWS2000, WINDOWSP, WINDOWSP
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	CreatetxtRange
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-015
Description/Possible effects:	It is a critical vulnerability in Windows Explorer on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	12 / 04 / 06
Systems affected:	WINDOWS2003, WINDOWSP, WINDOWS2000, WINDOWSP, WINDOWSP
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-016
Description/Possible effects:	It is an important vulnerability in Outlook Express versions 5.5 and 6 running on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.

Severity:	Moderate
Appeared:	12 / 04 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-018
Description/Possible effects:	It is a group of vulnerabilities in the Distributed Transaction Coordinator on Windows 2003/XP/2000 computers, which allows Denial of Service attacks to be launched against vulnerable computers.
Severity:	Moderate
Appeared:	10 / 05 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-021
Description/Possible effects:	It is a group of vulnerabilities in Internet Explorer versions 5.01 and 6 on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	14 / 06 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-025
Description/Possible effects:	It is a group of critical vulnerabilities on Windows

	2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user or local privilege elevation.
Severity:	High
Appeared:	14 / 06 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-030
Description/Possible effects:	It is a group of vulnerabilities in Server Message Block (SMB) on Windows 2003/XP/2000 computers, which allows hackers to perform a local privilege escalation and denial of service attack in the vulnerable computer.
Severity:	High
Appeared:	14 / 06 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-031
Description/Possible effects:	It is a moderate vulnerability on Windows 2000 computers, which allows attacking users to pass themselves off as a valid RPC server.
Severity:	High
Appeared:	14 / 06 / 06
Systems affected:	WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-032
Description/Possible effects:	It is a vulnerability in the TCP/IP protocol driver on

	Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	High
Appeared:	14 / 06 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-035
Description/Possible effects:	It is a group of critical vulnerabilities in Server Service on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user or to disclose information.
Severity:	High
Appeared:	12 / 07 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-036
Description/Possible effects:	It is a vulnerability in the DHCP client service on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	High
Appeared:	12 / 07 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-040
Description/Possible effects:	It is a critical vulnerability in Server Service on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	High
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSEX, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Oscarbot.KD
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-041
Description/Possible effects:	It is a group of vulnerabilities in the DNS resolution on Windows 2003/XP/2000 computers, which allow hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	High
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSEX, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-042
Description/Possible effects:	It is a group of vulnerabilities in Internet Explorer versions 5.01 and 6 on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	High
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSEX, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-044
Description/Possible effects:	It is a critical vulnerability in Outlook Express 6 on Windows 2003/XP computers, which allows to remotely execute arbitrary code in the vulnerable computer.
Severity:	High
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-045
Description/Possible effects:	It is an important vulnerability in Windows Explorer on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-046
Description/Possible effects:	It is a critical vulnerability in HTML Help ActiveX control on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	High
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes

Link to solution:	http://update.microsoft.com/
-------------------	---

Identifier	MS06-049
Description/Possible effects:	It is a vulnerability in Windows Kernel on Windows 2000 computers, which allows hackers to gain local privilege escalation.
Severity:	Moderate
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-050
Description/Possible effects:	It is a group of important vulnerabilities in Hyperlink Object Library on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-051
Description/Possible effects:	It is a group of critical vulnerabilities in Windows kernel on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user or local privilege escalation.
Severity:	High
Appeared:	09 / 08 / 06
Systems affected:	WINDOWS2003, WINDOWSP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes

Link to solution:	http://update.microsoft.com/
-------------------	---

Identifier	MS05-039
Description/Possible effects:	It is a vulnerability in Plug and Play (PnP) on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user or local privilege elevation.
Severity:	Moderate
Appeared:	10 / 08 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Zotob.A, Zotob.B, Zotob.C, Zotob.D, Zotob.E, Zotob.F, Zotob.G, Zotob.H, Zotob.I, IRCbot.KC, IRCbot.KD
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-040
Description/Possible effects:	It is a vulnerability of the Telephony service on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user or local privilege elevation.
Severity:	Moderate
Appeared:	10 / 08 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-042
Description/Possible effects:	It is a group of vulnerabilities in the Kerberos protocol on Windows 2003/XP/2000 computers, which allows Denial of Service attacks to be launched, as well as information disclosure and spoofing.
Severity:	Moderate
Appeared:	10 / 08 / 05

Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-043
Description/Possible effects:	It is a vulnerability in the Print Spooler service on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	10 / 08 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-045
Description/Possible effects:	It is a moderate vulnerability in Network Connection Manager on Windows 2003/XP/2000 computers, which allows hackers to launch denial of service attacks.
Severity:	Moderate
Appeared:	14 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-046
Description/Possible effects:	It is an important vulnerability in the Client Service for Netware on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate

Appeared:	13 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-047
Description/Possible effects:	It is a vulnerability in Plug and Play (PnP) on Windows XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user or local privilege elevation.
Severity:	Moderate
Appeared:	13 / 10 / 05
Systems affected:	WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Zotob.A, Zotob.B, Zotob.C, Zotob.D, Zotob.E, Zotob.F, Zotob.G, Zotob.H, Zotob.I, IRCbot.KC, IRCbot.KD
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-048
Description/Possible effects:	It is a vulnerability in Collaboration Data Objects on Windows 2003/XP/2000 or Exchange 2000 Server computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	13 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-049
Description/Possible effects:	It is a group of important vulnerabilities on Windows 2003/XP/2000 computers, which allows hackers to

	gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	13 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-050
Description/Possible effects:	It is a vulnerability in DirectX versions 7.0, 8.0, 8.1, 8.2 and 9.0 on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	13 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-051
Description/Possible effects:	It is a group of vulnerabilities on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user, local privilege elevation or launch denial of service attacks.
Severity:	Moderate
Appeared:	13 / 10 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-053
Description/Possible effects:	It is a group of vulnerabilities on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user, or launch denial of service attacks.
Severity:	Moderate
Appeared:	09 / 11 / 05
Systems affected:	WINDOWS2003, WINDOWSWXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS05-055
Description/Possible effects:	It is a vulnerability in Windows Kernel on Windows 2000 computers, which allows hackers to gain local elevation of privilege.
Severity:	Moderate
Appeared:	14 / 12 / 05
Systems affected:	WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-001
Description/Possible effects:	It is a critical vulnerability in Graphics Rendering Engine on Windows 2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	09 / 01 / 06
Systems affected:	WINDOWS2003, WINDOWSWXP, WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Exploit/Metafire
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-002
Description/Possible effects:	It is a critical vulnerability in Embedded Web Fonts on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	11 / 01 / 06
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSME, WINDOWS98
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS03-026
Description/Possible effects:	It is a critical vulnerability in Windows 2003/XP/2000/NT computers, known as Buffer Overrun In RPC Interface, which allows to remotely execute arbitrary code in the vulnerable computer.
Severity:	Moderate
Appeared:	04 / 03 / 05
Systems affected:	WINDOWS2003, WINDOWSXP, WINDOWS2000, WINDOWSNT
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	Blaster, Blaster.B, Blaster.C, Blaster.E, Blaster.F, Blaster.G, Blaster.H, Nachi.A, Nachi.B, Nachi.C, Nachi.D, Nachi.E, Nachi.F, Nachi.G, Nachi.H, Plexus.A, Plexus.B
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/

Identifier	MS06-004
Description/Possible effects:	It is a critical vulnerability in the Graphics Rendering Engine on Windows 2003/XP/2000/Me/98 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged on user.
Severity:	Moderate
Appeared:	15 / 02 / 06

Systems affected:	WINDOWS2000
Threats discovered in the computer that exploit it:	
Other threats that exploit it:	
Can be fixed:	Yes
Link to solution:	http://update.microsoft.com/