

Windows ME – Vista

Microsoft

Windows,

?

?

.

,

,

.

,

,

.

.

—

.

—

.

!

1.

,

1.

2.

Host Intrusion Prevention System

3.

2.

1.

UPS (Uninterruptible Power Supply)

DEP (Data Execution Prevention)

2.

Internet Explorer

Mozilla Firefox

Opera

3.

1.

2.

1. ,

1.

(malware, malicious

software) – ,

. malware

, ,

– (Trojan),

(Worm) (Virus). .

Trojan – ,

: ,

, – .

– ,

, ,

. ,

.

.

Worm –

,

: ,

, – ,

. , .

:

, .

, /

, .

Virus —

malware

Virus

Начало файла изменяется так, чтобы внедренный код вируса получал управление при исполнении программы	В середину файла внедряется фрагмент вредоносного кода. Используется компрессия, так что размер файла не меняется.	Конец файла не затрагивается.
--	--	-------------------------------

« »,

(malware). «Virus»,

malware, -

« ».

« »

malware Virus.

Trojan Worm

100%,

« »

« »

« ? ».

« », — « », .

« (AdWare), - (Hoax), (SpamTool , VirTool)

BackDoor —

RootKit —

(Spyware) - « »

malware

1)

Flash-

2)

3)

4)

5)

20

2.

- malware,
- 1)
 - 2) (ZIP RAR).
 - 3)

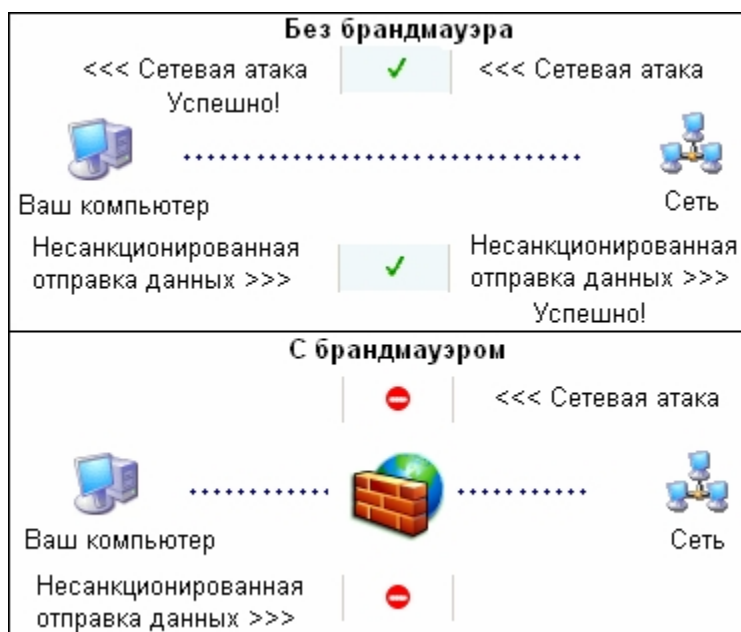
newvirus@company.com, virus@company.com

- 4)
- (on-access),
(on-demand),

(firewalls),

1)

2)



– ZoneAlarm, Outpost

Firewall, Sunbelt Kerio Personal Firewall, COMODO Personal Firewall

.

Internet Security,

,

.

.

BitDefender Internet Security

Kaspersky Internet Security.

:

, . .

,

,

.

,

.

:

,

().

,

.

, ,

,

.

.

—

,

.

,

.

—

• ,

•

•

•

,

,

,

—

•

– Ad-Aware, Spybot – Search and Destroy, AVG Anti-Spyware .

Host Intrusion Prevention Systems (HIPS),

, -

•

,

HIPS

—

HIPS

100%

,

,

,

•

HIPS –

,

HIPS

HIPS

Sandbox.

HIPS –

,

HIPS

/

•

,

•

HIPS

HIPS

HIPS

Sandbox

HIPS

Windows

s

HIPS -

System Safety Monitor

AntiHook.

HIPS –

CyberHawk.

HIPS

Sandbox –

DefenseWall HIPS

Sandboxie.

3.

Documents and Settings, WINDOWS

WINDOWS\system32.

(. .

C:\rose.exe),

Program Files WINDOWS\system.

_____ — ,
.

Windows – Registry Editor (C:\Windows\regedit.exe).
malware,

.
—
.

Autoruns sysinternals.com —

, .

malware

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services,](#)
[HKEY_LOCAL_MACHINE\System\ControlSet00*\Services.](#)

. ,

Internet Explorer.

_____ — ,
.

NT-

Windows Vista. Malware

, ,

, - ,

. ,

.

— « ».

—

-

-

.

,

,

, ,

,

.

:

:

— — cmd.exe - OK: 'netstat -a' — Enter.

ESTABLISHED —

TIME_WAIT (CLOSE_WAIT) —

LISTENING —

LISTENING

Internet Explorer;

— JavaScript.

— ActiveX.

Microsoft,

ActiveX

— , Browser Helper Objects. Internet Explorer

.

,

.

—

;

.

DEP (Data Execution Prevention)

—

.

,

.

,

DEP,

Windows.

.

DEP

,

;

DEP

.

2.

,

:

,

,

.

,
 .
 (
).
 -
 ,
 .
 _____,
 (ICQ),

,
 (
),
).

,

.

.

.

2000, XP Pro, 2003:

- — 'gpedit.msc' - OK -

-

-

(,).

'gpupdate'

XP Home

,

:

1) - — 'regedit' – OK.

2) HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies.

3)

4) Explorer

5)

NoDriveTypeAutoRun

_____ :

0x1 -

0x4 -

0x8 -

0x10 -

0x20 - CD-

0x40 - RAM-

0x80 -

0xFF - .

_____ :

0x95 - Windows 2000 2003 (,)

0x91 - Windows XP ()
: XP Home (Explorer), .

, , .
,

:

:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

: NoDriveAutoRun

: 0x0–0x3FFFFFFF

" " -

() ,

- B

: 0x0

« ».

(

picture.jpg.vbs,

picture.jpg).

– – ‘regedit’ - OK.

– – ‘NeverShowExt’ – Enter.

- F3, /

:

readme.txt readmenot.txt,

.

readme.txt

readmenot,

.

_____.

.

- :

, , Inbound Connection, Server Rights

.

(FTP, P2P, ICQ-

)

—

.

,

,

(

).

,

,

.

Windows —

.

.

ICQ

_____.

.

_____ ICQ- (

, QIP, Miranda) -

Internet Explorer Firefox Opera.

,

;

,

,

.

(_____). -

.

_____.

.

(_____) -

.

.

_____ « »

_____ ,

_____ (

_____) ,

.

.

1) _____ (,).

2) _____ .

3) _____ .

4) _____ (18).

Microsoft – _____ .

Flash-

: Windows, Nero BackItUp, Norton Ghost

.

.

,

.

,

—

,

.

,

.

Norton GoBack.

.

,

.

,

,

.

Windows

Worms

Doors

Cleaner

(<http://www.firewallleaktester.com/wwdc.htm>),

.

,

,

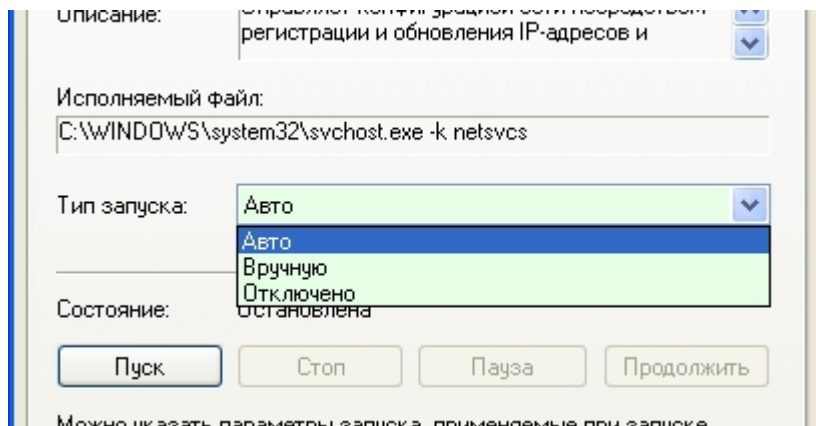
!

() —

,

—

.



Windows XP

(

.)

!!!

!

Dial-Up

ADSL.

(Manual).

(Disabled)

(

):

DNS- [DNS Client]

Machine Debug Manager

NetMeeting Remote Desktop Sharing

_____ [Automatic Updates] (_____
Windows)

_____ [Wireless Zero Configuration]

_____ [Secondary Logon] (_____
_____)

_____ DDE [Network DDE DSDM]

_____ [Remote Desktop Help Session Manager]

_____ HID-_____ [Human Interface Device Access]

_____ NetBIOS _____ TCP/IP [TCP/IP NetBIOS

Helper Service]

_____ [ClipBook]

_____ [System Restore Service]

_____ [Indexing Service]

_____ SSDP [SSDP Discovery Service]

_____ DDE [Network DDE]

_____ [Application Layer

Gateway Service] (_____ Windows XP SP2)

_____ IPSEC [IPSEC Services]

_____ [Terminal Services]

_____ [Fast User Switching Compatibility] (_____
_____).

_____ [Remote Registry]

_____ (BITS)

[Background Intelligent Transfer Service] (_____
Windows – _____)

(, ,):

ASP.NET State Service

InstallDriver Table Manager

MS Software Shadow Copy Provider

Office Source Engine

QoS RSVP

Windows Installer

WMI [WMI Performance

Adapter]

Windows/ (ICS)

[Windows Firewall/Internet Connection Sharing]

- [Web Client]

- [Remote

Access Auto Connection Manager]

[Logical Disk Manager]

[Remote

Access Connection Manager]

[Performance

Logs and Alerts]

[Uninterruptible Power

Supply]

[Distributed

Transaction Coordinator]

[Routing and Remote

Access]

[Task Scheduler] (

)

HTTP SSL [HTTP SSL]

_____ [Network Connections]
 _____ COM+ [COM+ Event System]
 _____ COM+ [COM+ System Application]
 _____ COM - IMAPI [IMAPI CD-
 Burning COM Service]

 [Logical Disk Manager Administrative Service]
 _____ Windows [Windows Time]
 _____ (WIA) [Windows Image
 Acquisition]
 _____ [Network Provisioning Service]
 _____ [Error Reporting Service]

 _____ [Portable Media Serial Number Service]
 _____ (NLA) [Network Location
 Awareness]
 _____ - [Smart Card]
 _____ [Help and Support]
 _____ [Removable Storage]
 _____ [Volume Shadow Copy]
 _____ PnP- [Universal Plug and Play
 Device Host]
 _____ [Application Management]

 (-):
 _____ [Telephony]
 _____ (RPC) [Remote Procedure Call]
 DHCP- [DHCP Client] ()
 Plug and Play

Windows Audio

Windows User Mode Driver Framework

_____ [Print Spooler]

_____ [Security Accounts

Manager]

_____ [Event Log]

_____ DCOM [DCOM Server Process

Launcher]

_____ [Protected Storage]

_____ Windows [Windows

Management Instrumentation]

_____ [Distributed Link

Tracking Client]

_____ [Shell Hardware

Detection]

_____ [Cryptographic Services]

_____ [Themes]

_____ [System Event

Notification]

_____ [Security Center] (
)

(DNS-

—

DNS,

IP-

.

.

(Machine Debug Manager — .
 , .

(NetMeeting Remote Desktop Sharing —
NetMeeting. ,

(— ,
Windows. ,
.

(— .
.
 , .

(— , ,
.
 , .

(DDE — ,
(shared) .
DDE .

(— .
 .

(HID- — ,
.

(NetBIOS TCP/IP — LMHOSTS,
NetBIOS.
LMHOSTS, NetBIOS.

(— ,
.

(System Restore —
Windows. System
Restore ,

(
Windows .

(SSDP PnP-
.
PnP- .

(DDE
().

(

Windows. Windows XP SP2

(

IPSEC

IP-

(

—

(

),

(

(

—

(ASP.NET State Service – .NET Framework.
 , .

(InstallDriver Table Manager –
InstallShield. .

(MS Software Shadow Copy Provider - ,
(. .
,).
 .

(Office Source Engine –
/
 .

(QoS RSVP – .
 .

(Windows Installer – Windows.
 .

(WMI –
 . ,
 .

(Windows/ (ICS) —
Windows. ,
.

(- — , Windows
.
.

(- — ,
 , -
 .
.

(—
 .
.

(—
 .
 - .

(—
 ,
 ,
 .

(COM+ - , .

(COM+ - , COM+

(COM - IMAPI -

Windows, - .

().

(

(Windows

((WIA)

()

(
.
.
(
, ,
Microsoft.
.
(
(-).
((NLA)
().
(- -
/
.
(- Windows.
().
,
.

(— .

.

(— , .

(PnP- — PnP .

(— .

((BITS) — Windows, . ; .

(— , — , IP- .

((RPC) - Windows.

RPC , .
Machine Debug Manager, MS Software Shadow Copy Provider, QoS
RSVP, Windows Audio, Windows Installer, Windows User Mode Driver
Framework, WMI,

, ,
, ,
HID-
Windows,

, ,
COM+, COM+,

, ,
(WIA),
IPSEC,
(BITS),

(DHCP- — .
ADSL.

(Plug and Play - « ».

, *Windows Audio*,

,
- .

(*Windows Audio* — ,

.

(*Windows User Mode Driver Framework* — ,

,

(

).

(— ,

.

.

(— ,

.

.

(— ,

.

(*DCOM*

DCOM-

.

,

.

(

(, . .),

Windows.

(Windows — ,

Windows/ (ICS)

(— ,

NTFS.

(—

(

(— Windows.

(—

COM+.

(

Windows Vista (

www.thevista.ru),

Windows XP

Desktop Window Manager Session Manager /

DWM: Desktop Window Manager.
Aero Glass,

IP Helper : IPv6

IPv4- IPv6,

Offline Files / - :

- -
- ,

Program Compatibility Assistant Service /

:
Program Compatibility Assistant.
Program Compatibility Assistant,

ReadyBoost : ReadyBoost.

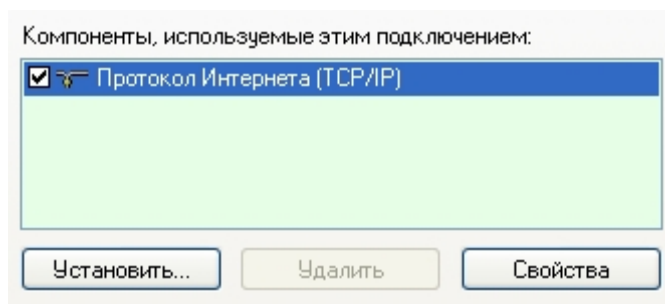
USB- Flash-
,
USB-
,
.

Tablet PC Input Service /

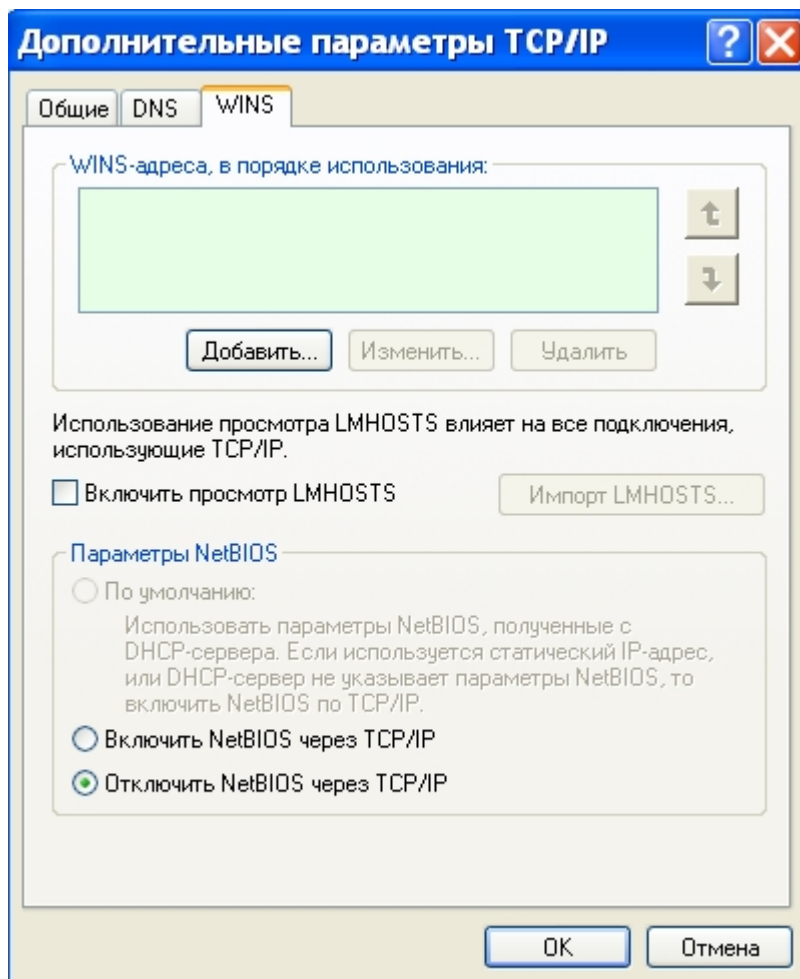
TabletPC: Tablet PC. Tablet
PC,

Windows Defender :

(spyware adware),



WINS.



LMHOSTS

NetBIOS TCP/IP.

OK.

ActiveX.

Internet Explorer

Internet Explorer,

Internet Explorer;

Internet Explorer;

.NET Framework

OK.

Cookies

Internet Explorer,

—

Cookie.

Cookies —

Internet Explorer

Internet Explorer,

—

Internet

Explorer.

IE.

(, -
). ,
 .

Mozilla Firefox

Firefox

Firefox

NoScript ,

: <https://addons.mozilla.org/firefox/722/>.

NoScript

.

,

.

, Tools – Options,
Enable Java Enable JavaScript.

Content.

Cookies

, Tools – Options,

Privacy.

Cookies.

Allow sites to set Cookies.

Cookies,

unless I have removed cookies set by the site.

Cookies

,

Cookies.

Opera

Opera – – – –
JavaScript (, :
- - - -
- , , , :
- ,
).

Cookies

Opera – – – –
Cookies –
cookies (, Cookies :
Cookies – – Cookies
- , , :
- ,
).

Cookies

(Outlook Express)

OE – C – – –

«

»,

«

»;

- « ,
» , «
 ,
» «
HTML».

3.

,
 ,
 .

1.

AVZ

AVZ –
 .

AVZ
HTM.

AVZ:

AVZGuard –
 .

AVZ
AVZPM –
 ,

_____ ,

_____ ,

■

1

■

Hijack This

;

■

■

Autoruns

,
,
.

FileMonitor

,
.
,
.
— .

RegMonitor

, File Monitor;
.

Process Explorer

,

Windows.

PE —

.

Drop My Rights

‘ ‘

“Drop My Rights”,
Microsoft (Michael Howard).

,

.

Drop My Rights

,

.

,

IE Firefox

.

IE

:

c:\ _ _ \dropmyrights.exe "C:\Program Files\Internet
Explorer\iexplore.exe" C

IE,

C, “Constrained user” («
»).

-

, ,

,

.

:

N – normal user ()

C – constrained user ()

U – untrusted user ()

,

.

« »

,

“Shortcut” (« »)

“Target” (« »),

DropMyRights.exe, , C:\windows\dropmyrights.exe "C:\Program
Files\Mozilla Firefox\firefox.exe" N.

, , ,
,
(
).

: <http://msdn2.microsoft.com/en-us/library/ms972827.aspx>

2.

-

Anti-Malware.Ru :

<http://www.anti-malware.ru>

— — ,
:

<http://virusinfo.info>

Microsoft Windows —

OSZone:

<http://oszone.net/>

— :
<http://viruslist.com>

Trojan-

PSW.Win32.LdPinch.

ICQ

Exploit (,),

AVZ.

p2u,

:

~nOn sTop~ (Kaspersky Lab Forum)

dey (Kaspersky Lab Forum)

Serega_I (Kaspersky Lab Forum)

Ego1st (Kaspersky Lab Forum)

ANDYBOND (Kaspersky Lab Forum)

Umnik (Kaspersky Lab Forum)

(VirusInfo)

RiC (VirusInfo)

pig (VirusInfo)

Xen (VirusInfo)

Minos (VirusInfo)

ALEX(XX) (VirusInfo)

Shu_b (VirusInfo)

SuperBrat (Anti-Malware forum community)

(Anti-Malware forum community)

JIABP (Kaspersky Lab Forum)

rav (VirusInfo)

© , 2007.

<http://security-advisory.newmail.ru> –