Scanning started at 20.07.2011 15:42:14
Database loaded: signatures - 290427, NN profile(s) - 2, malware removal microprograms - 56, signature database released 17.07.2011 16:00
Heuristic microprograms loaded: 388
PVS microprograms loaded: 9
Digital signatures of system files loaded: 287066
Heuristic analyzer mode: Medium heuristics mode
Malware removal mode: disabled
Windows version is: 5.1.2600, ; AVZ is run with administrator rights
System Restore: enabled
1. Searching for Rootkits and other software intercepting API functions
1.1 Searching for user-mode API hooks
Analysis: kernel32.dll, export table found in section .text
Analysis: ntdll.dll, export table found in section .text
Analysis: user32.dll, export table found in section .text
Analysis: advapi32.dll, export table found in section .text
Analysis: ws2_32.dll, export table found in section .text
Analysis: wininet.dll, export table found in section .text
Analysis: rasapi32.dll, export table found in section .text
Analysis: urlmon.dll, export table found in section .text
Analysis: netapi32.dll, export table found in section .text
1.2 Searching for kernel-mode API hooks
Driver loaded successfully
SDT found (RVA=074C00)
Kernel ntoskrnl.exe found in memory at address 804D0000
SDT = 80544C00
KiST = 804FC624 (284)
Functions checked: 284, intercepted: 0, restored: 0
1.3 Checking IDT and SYSENTER
Analyzing CPU 1
Checking IDT and SYSENTER - complete
1.4 Searching for masking processes and drivers
Checking not performed: extended monitoring driver (AVZPM) is not installed
1.5 Checking IRP handlers
Driver loaded successfully
Checking - complete
2. Scanning RAM
Number of processes found: 14
Number of modules loaded: 168
Scanning RAM - complete
3. Scanning disks
Direct reading: C:\Dokumente und Einstellungen\Jultta Lomenko\Lokale Einstellungen\Anwendungsdaten\Opera\Opera\vps\0000\wb.vx
4. Checking Winsock Layered Service Provider (SPI/LSP)
LSP settings checked. No errors detected
5. Searching for keyboard/mouse/windows events hooks (Keyloggers, Trojan DLLs)
C:\WINDOWS\System32\winspool.drv --> Suspicion for Keylogger or Trojan DLL
C:\WINDOWS\System32\winspool.drv>>> Behaviour analysis
Behaviour typical for keyloggers was not detected
Note: Do NOT delete suspicious files, send them for analysis (see FAQ for more details), because there are lots of useful hooking DLLs

6. Searching for opened TCP/UDP ports used by malicious software
Checking - disabled by user
7. Heuristic system check
>>> C:\WINDOWS\System32\qmgr.dll HSC: suspicion for File with suspicious name (high degree of probability)
Non-standard registry key for system service: BITS ImagePath=""
Non-standard registry key for system service: wuauserv ImagePath=""
>>> C:\WINDOWS\System32\alg.exe HSC: suspicion for File with suspicious name (CH) (high degree of probability)
>>> C:\WINDOWS\System32\dllcache\userinit.exe HSC: suspicion for File with suspicious name (CH)
Checking - complete
8. Searching for vulnerabilities
>> Services: potentially dangerous service allowed: Messenger (Nachrichtendienst)
>> Services: potentially dangerous service allowed: Alerter (Warndienst)
> Services: please bear in mind that the set of services depends on the use of the PC (home PC, office PC connected to corporate network, etc)!
>> Security: disk drives' autorun is enabled
>> Security: administrative shares (C$, D$ ...) are enabled
>> Security: anonymous user access is enabled
>>> Security: Internet Explorer allows automatic queries of ActiveX administrative elements
>> Security: terminal connections to the PC are allowed
>> Security: sending Remote Assistant queries is enabled
Checking - complete
9. Troubleshooting wizard
>> Abnormal EXE files association
>> Abnormal COM files association
>> Protocol prefixes are modified
>> Internet Explorer - automatic queries of ActiveX operating elements are allowed
>> HDD autorun is allowed
>> Network drives autorun is allowed
>> Removable media autorun is allowed
Checking - complete
Files scanned: 16208, extracted from archives: 10798, malicious software found 0, suspicions - 0
Scanning finished at 20.07.2011 15:45:13
Time of scanning: 00:03:02