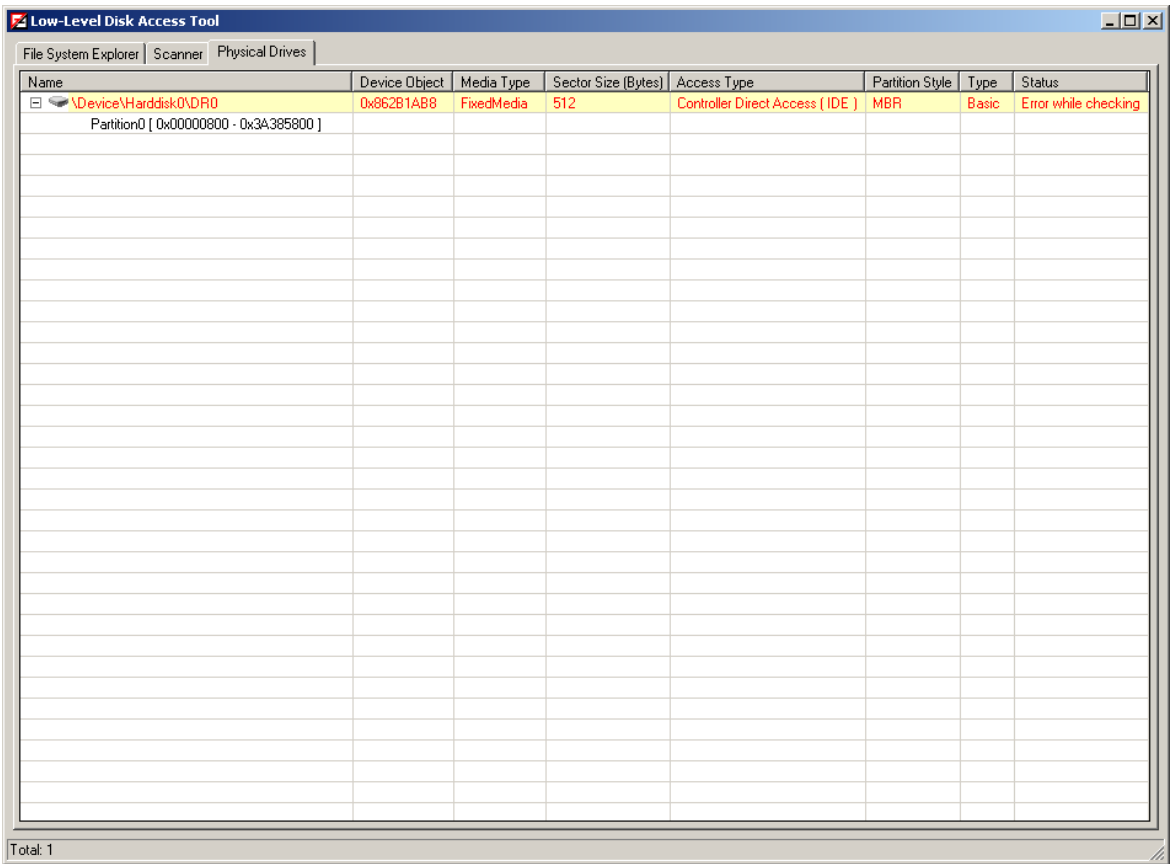
Vba32 AntiRootkit vs TDL 2

Dmitry Varshavsky
Nikolay Moskalenko

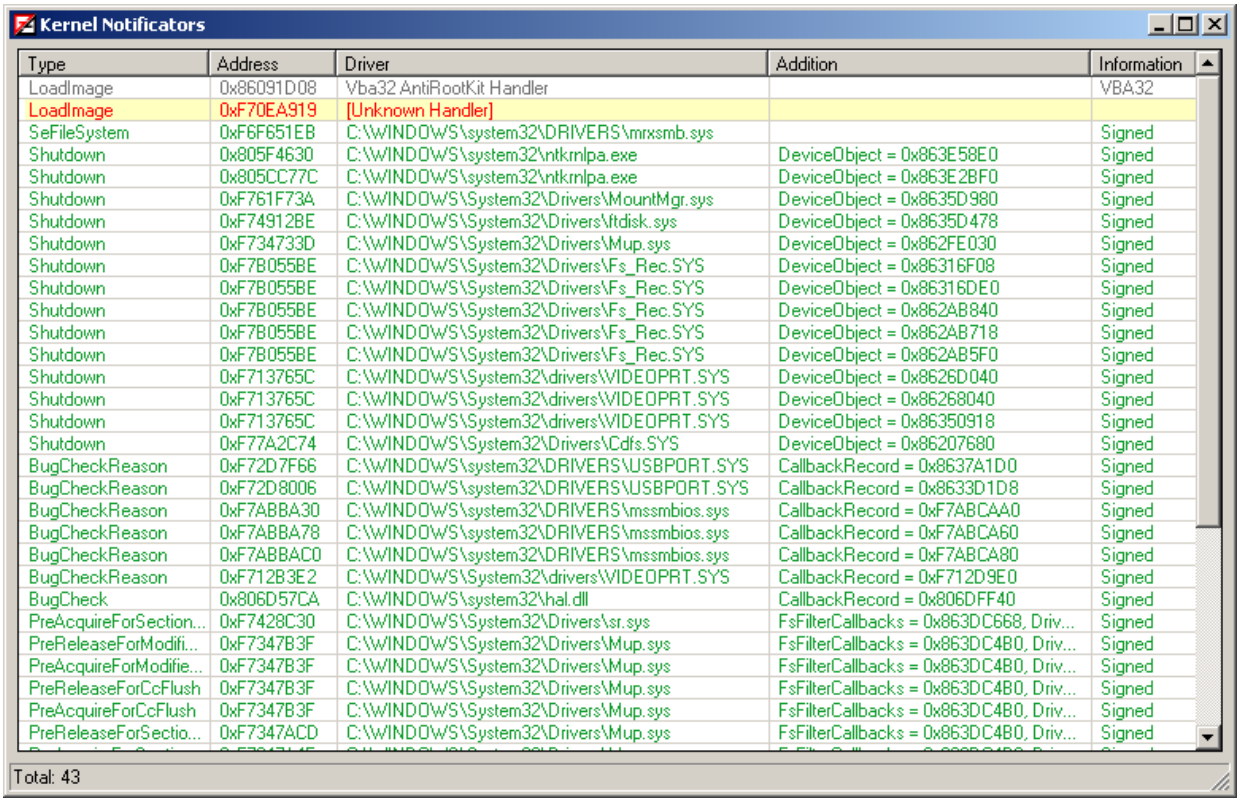
VirusBlokAda

1.Detection

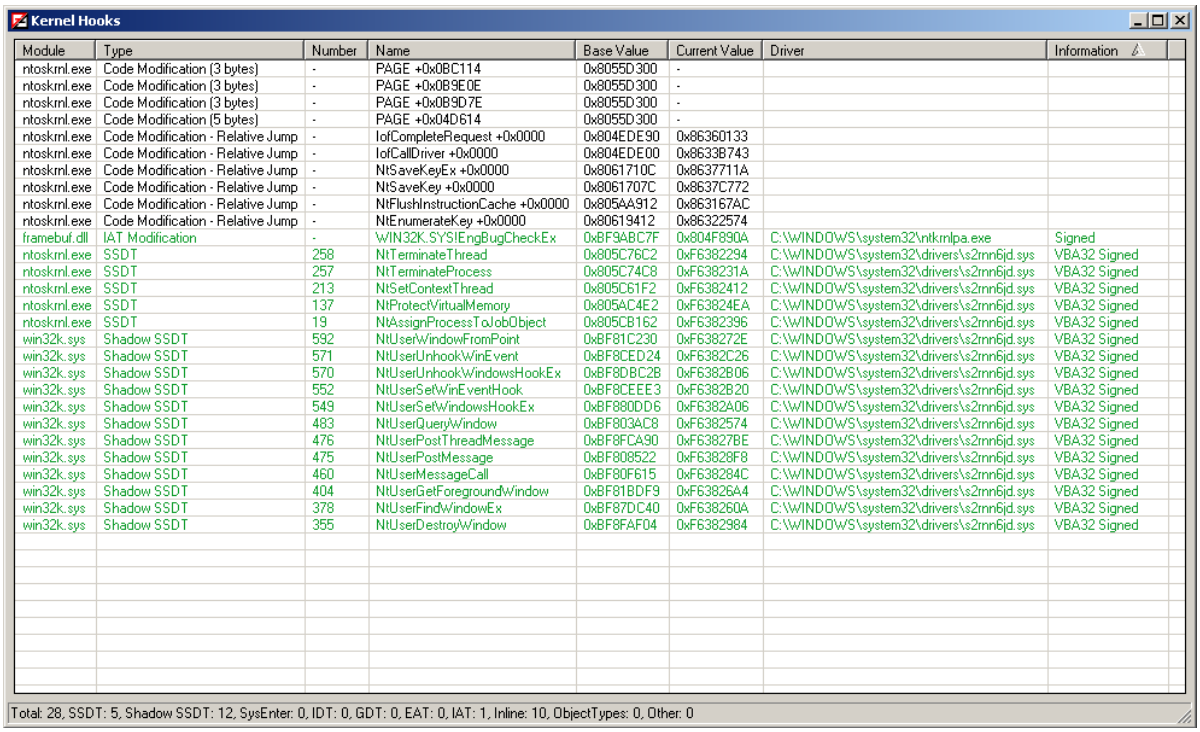
a) TDL2 rootkit prevents opening hard drive ("\Device\HardDisk0\DR0") from user-mode (Status: Error while checking)



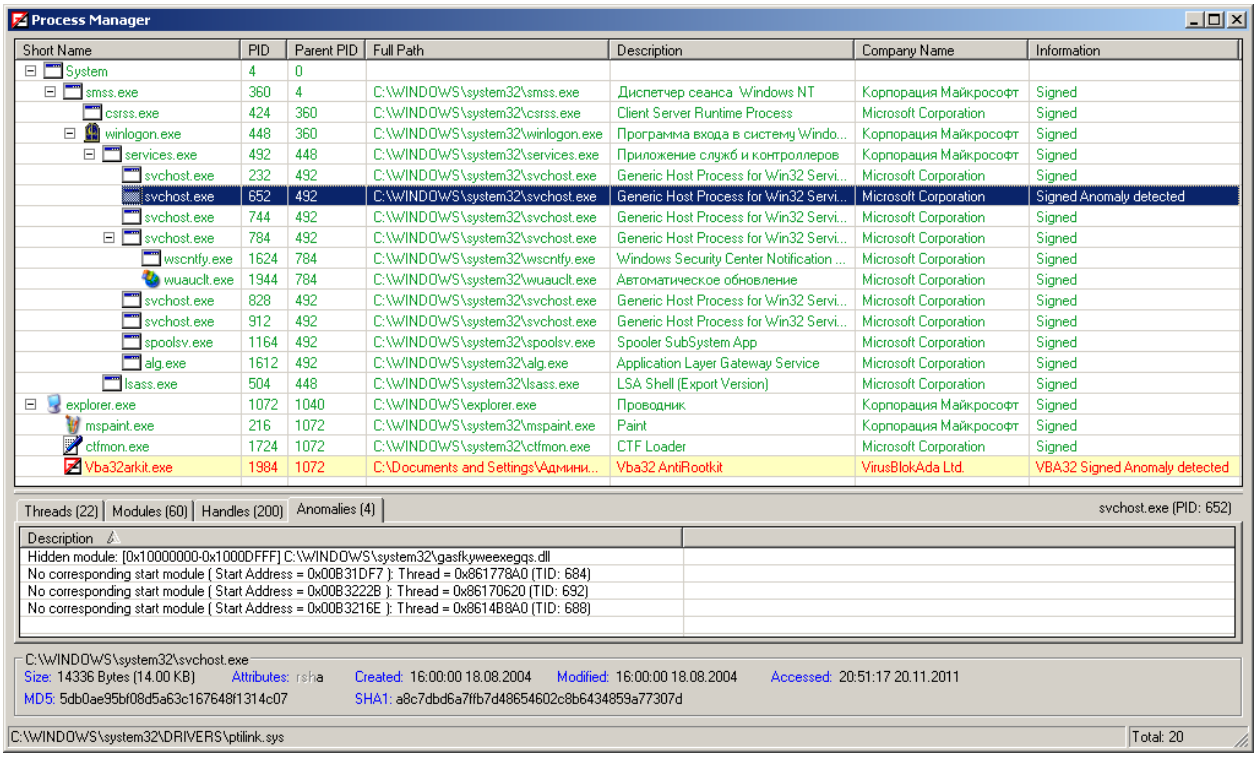
b) LoadImage handler doesn't belong to any loaded kernel module



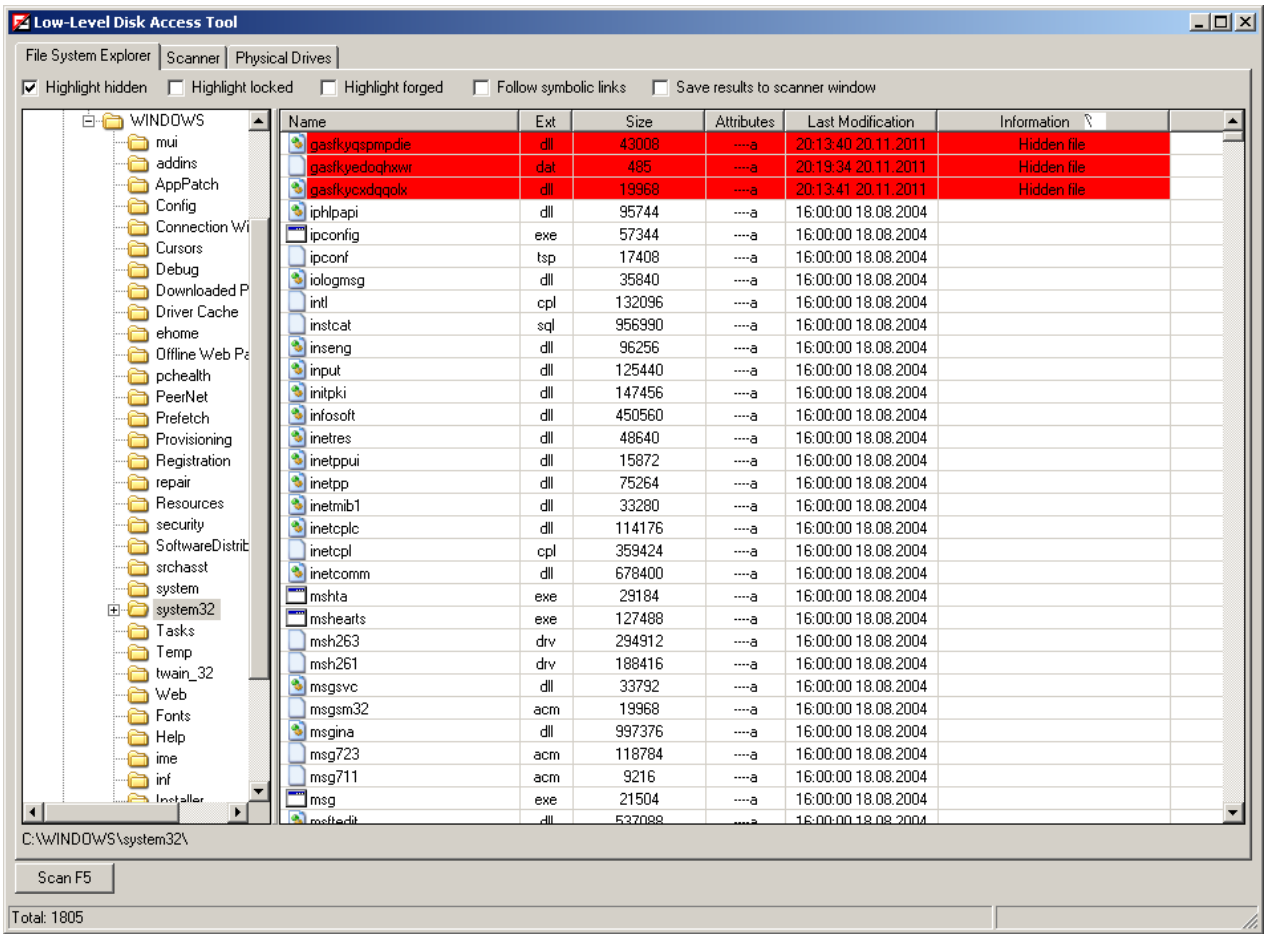
c) Rootkit sets several kernel-mode hooks (IofCompleteRequest and IofCallDriver hooks used to filter disk operations; NtEnumerateKey, NtSaveKey and NtSaveKeyEx hooks protect malicious service from enumeration and deletion; NtFlushInstructionCache hook designed for user/kernel mode parts interaction). Rootkit periodically checks presence of these hooks and restores them if needed



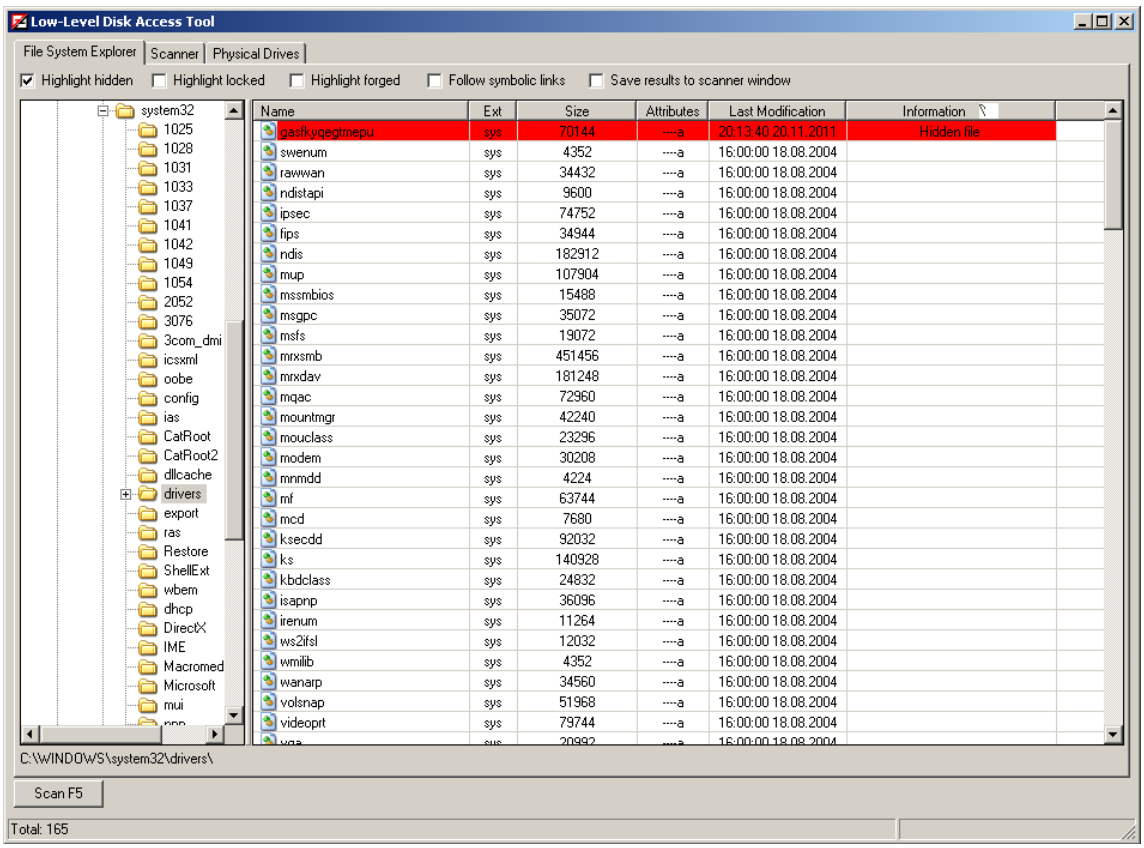
d) Rootkit injects .dlls into system (such as svchost.exe) and user processes (such as explorer.exe/iexplore.exe/etc. – not shown here); it also creates remote threads in those processes



e) Rootkit's payload stored on disk in "\SystemRoot\System32" directory

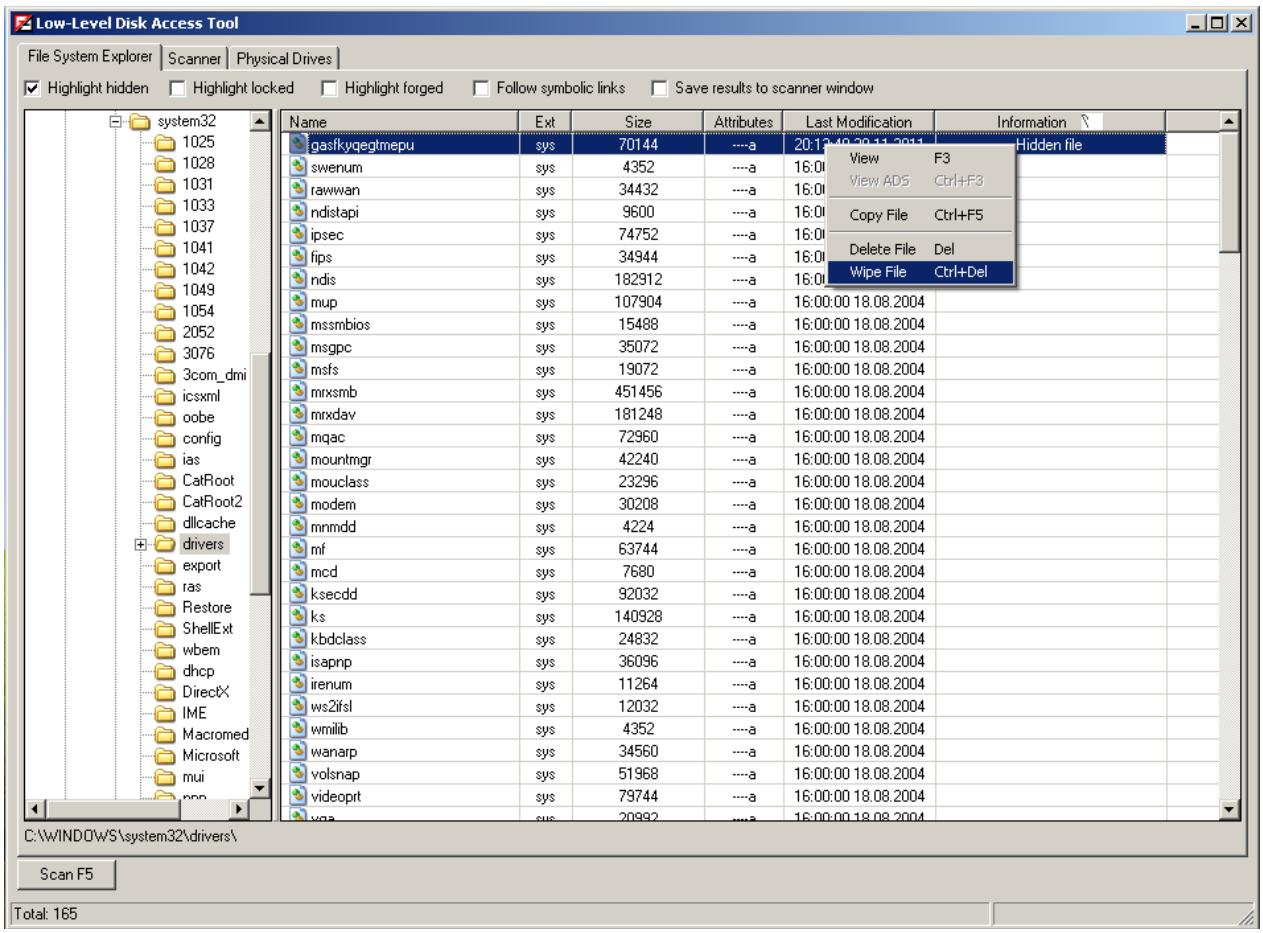


f) Malicious driver itself

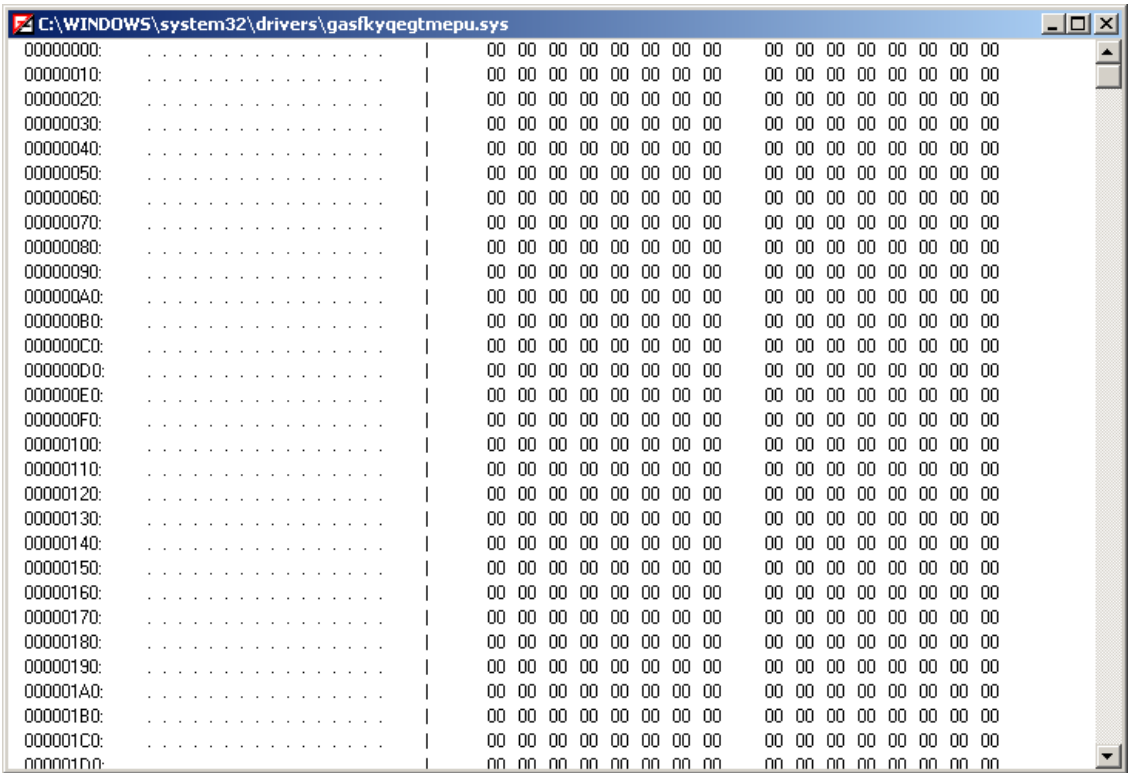


2.Removal

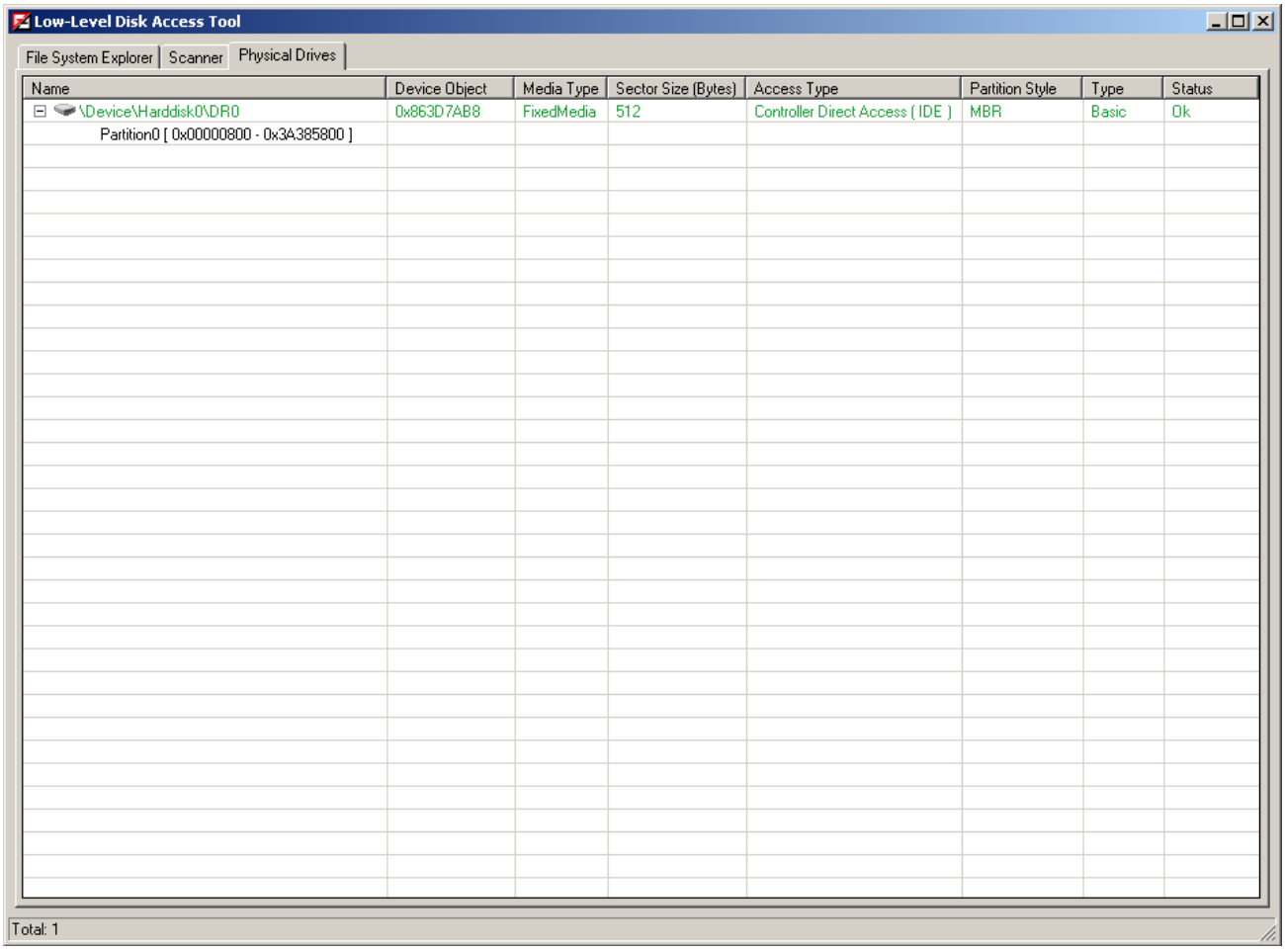
a) Wipe malicious driver

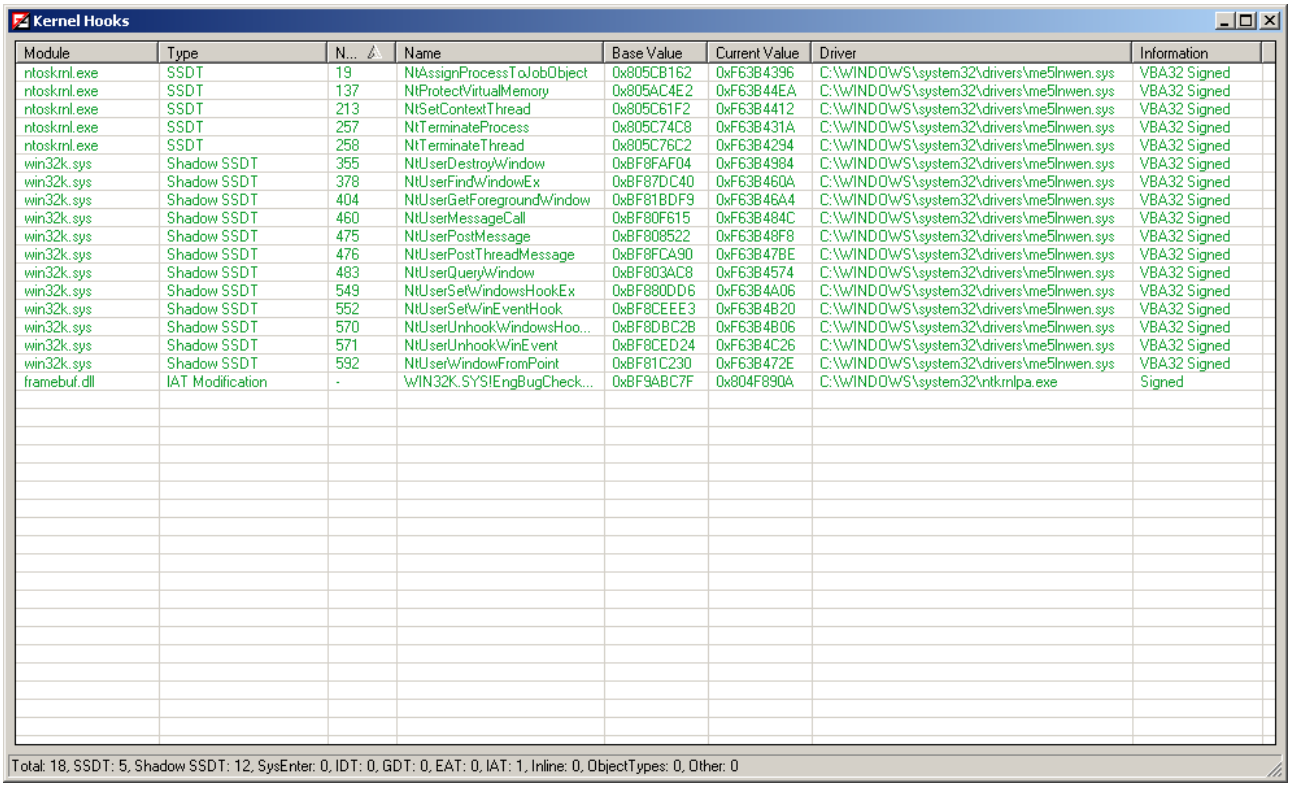


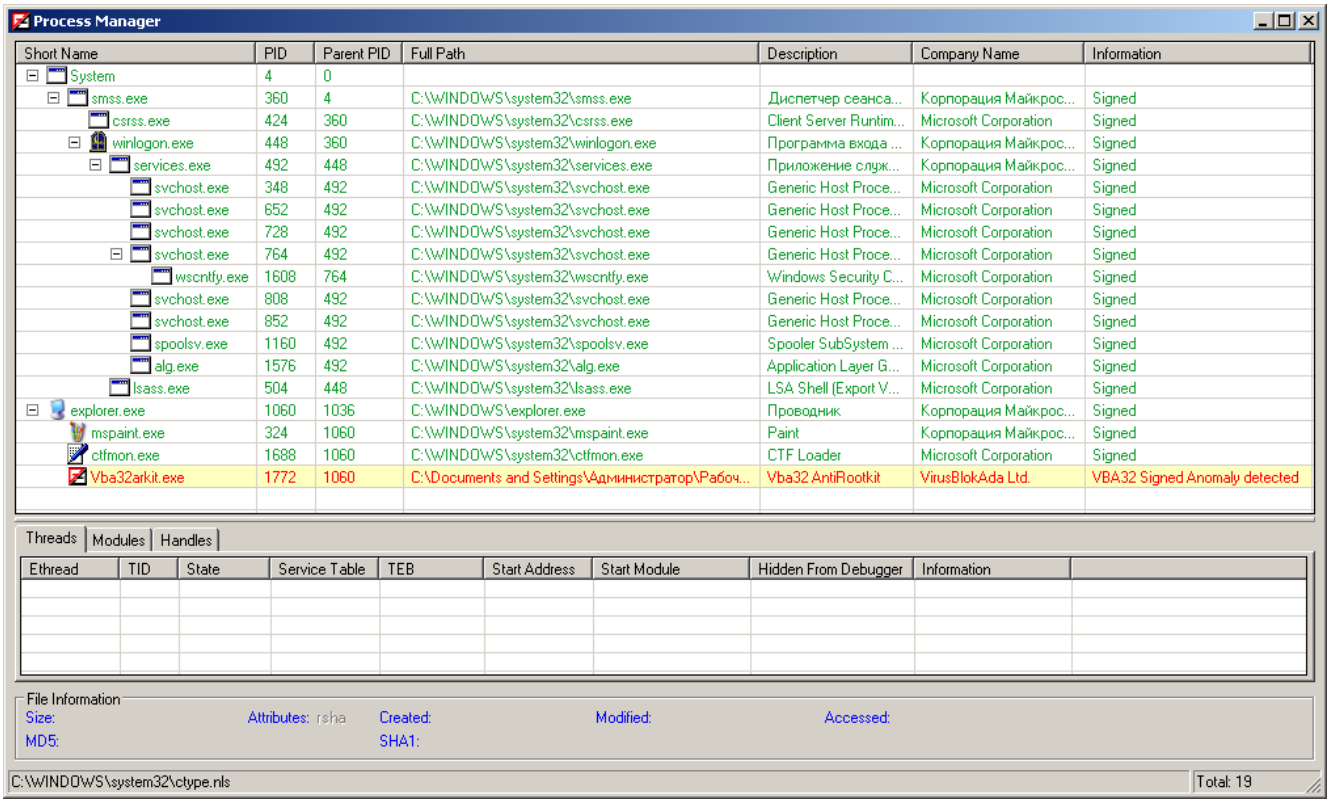
b) Ensure that file's content zeroed



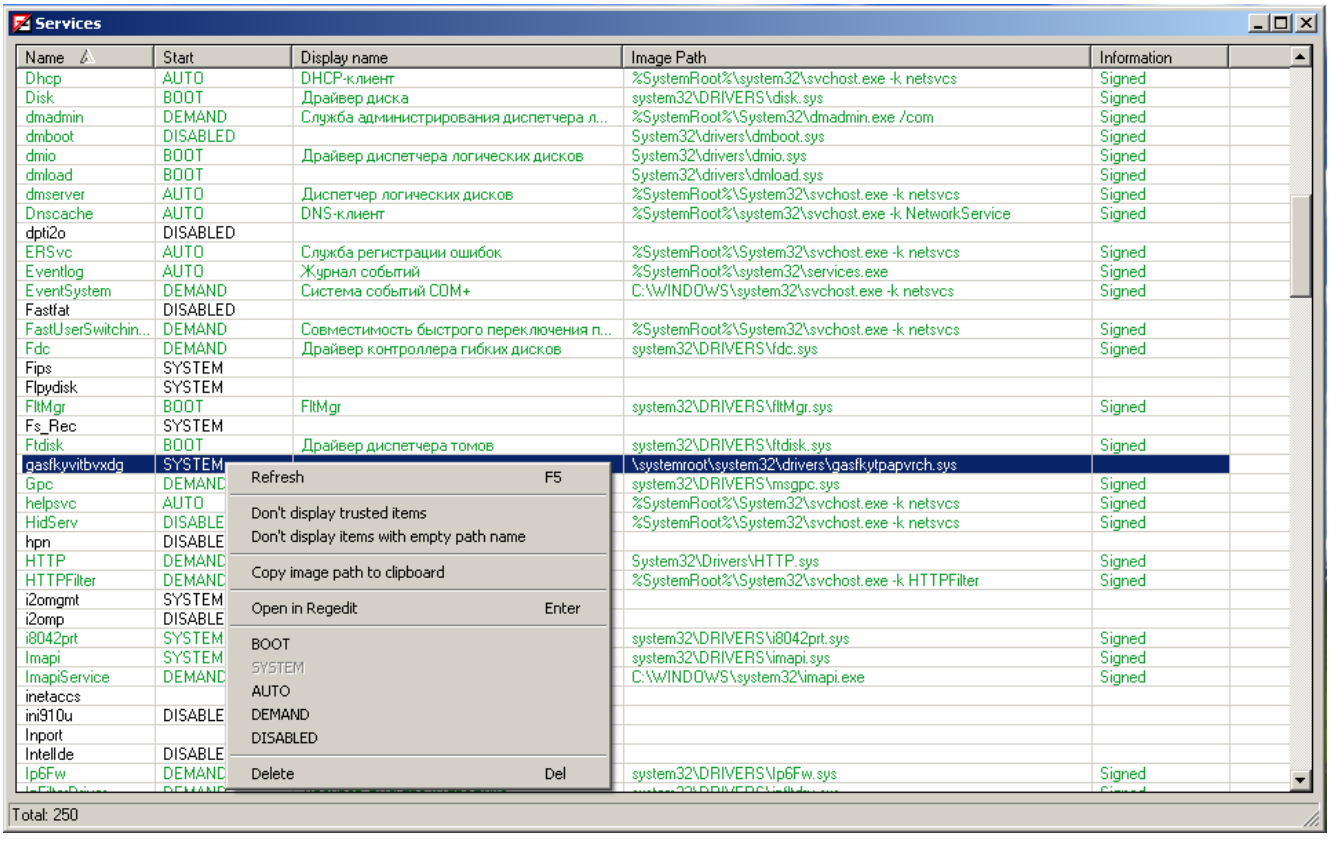
c) Restart the system and make sure that system is clean (MBR is fine, there is no unknown LoadImage handler, no any suspicious hooks and injected modules)


Low-Level Disk Access Tool
File System Explorer
Scanner
Physical Drives
Name
Device Object
Media Type
Sector Size (Bytes)
Access Type
Partition Style
Type
Status
\Device\Harddisk0\DR0
0x863D7AB8
FixedMedia
512
Controller Direct Access (IDE)
MBR
Basic
Ok
Partition0 [0x00000800 - 0x3A385800]
Total: 1


Kernel Hooks
Module
Type
N...
Name
Base Value
Current Value
Driver
Information
ntoskrnl.exe SSDT 19 NtAssignProcessToJobObject 0x805CB162 0xF63B4396 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
ntoskrnl.exe SSDT 137 NtProtectVirtualMemory 0x805AC4E2 0xF63B44EA C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
ntoskrnl.exe SSDT 213 NtSetContextThread 0x805C61F2 0xF63B4412 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
ntoskrnl.exe SSDT 257 NtTerminateProcess 0x805C74C8 0xF63B431A C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
ntoskrnl.exe SSDT 258 NtTerminateThread 0x805C76C2 0xF63B4294 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 355 NtUserDestroyWindow 0xBF8FAF04 0xF63B4984 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 378 NtUserFindWindowEx 0xBF87DC40 0xF63B460A C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 404 NtUserGetForegroundWindow 0xBF81BDF9 0xF63B46A4 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 460 NtUserMessageCall 0xBF80F615 0xF63B484C C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 475 NtUserPostMessage 0xBF808522 0xF63B48F8 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 476 NtUserPostThreadMessage 0xBF8FCA90 0xF63B47BE C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 483 NtUserQueryWindow 0xBF803AC8 0xF63B4574 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 549 NtUserSetWindowsHookEx 0xBF880DD6 0xF63B4A06 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 552 NtUserSetWinEventHook 0xBF8CEEE3 0xF63B4B20 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 570 NtUserUnhookWindowsHoo... 0xBF8DBC2B 0xF63B4B06 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 571 NtUserUnhookWinEvent 0xBF8CED24 0xF63B4C26 C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
win32k.sys Shadow SSDT 592 NtUserWindowFromPoint 0xBF81C230 0xF63B472E C:\WINDOWS\system32\drivers\me5lnwen.sys VBA32 Signed
framebuf.dll IAT Modification - WIN32K.SYS!EngBugCheck... 0xBF9ABC7F 0x804F890A C:\WINDOWS\system32\ntkrnlpa.exe Signed
Total: 18, SSDT: 5, Shadow SSDT: 12, SysEnter: 0, IDT: 0, GDT: 0, EAT: 0, IAT: 1, Inline: 0, ObjectTypes: 0, Other: 0



d) Delete malicious service from registry (manual permissions modification in Regedit may be needed)



e) Finally delete rootkit file and its payload