

# **Vba32 AntiRootkit vs TDL 4**

Dmitry Varshavsky  
Nikolay Moskalenko



**VirusBlokAda**

# 1. Detection

## a) Forged Master Boot Record

Name	Device Object	Media Type	Sector Size (Bytes)	Access Type	Partition Style	Type	Status
\Device\Harddisk0\DR0 Partition0 [ 0x00000800 - 0x3A395800 ]	0x86308A88	FixedMedia	512	Controller Direct Access (IDE)	MBR	Basic	Forged

Total: 1

## b) Additional hidden in memory atapi instance ( depending on configuration it may also be iastor/scsiport/etc. )

DriverObject	Name	Base	Entry Point	Size	Full Path	Description	Company Name	Information
		0xF7A03000	0xF7A04872	0x3000	C:\WINDOWS\system32\BOOTVID.dll	VGA Boot Driver	Microsoft Corp...	Signed
		0xF760F000	0xF761AC05	0xD000	C:\WINDOWS\system32\DRIVERS\1394BUS...	1394 Bus Devic...	Microsoft Corp...	Signed
0x863E26E0	\Driver\ACPI	0xF74C0000	0xF74E9059	0x2E0...	C:\WINDOWS\system32\Drivers\ACPI.sys	ACPI драйвер д...	Корпорация ...	Signed
0x860FFF38	\Driver\AFD	0xF2C0D000	0xF2C2AF40	0x22000	C:\WINDOWS\system32\drivers\afd.sys	Ancillary Functi...	Microsoft Corp...	Signed
0x8626CAC0	\Driver\atapi	0xF7452000	0xF74675F7	0x18000	C:\WINDOWS\system32\Drivers\atapi.sys	IDE/ATAPI Port...	Microsoft Corp...	Signed
0x8634D478	\Driver\atapi	0xF7452000	0xF74675F7	0x18000	C:\WINDOWS\system32\Drivers\atapi.sys	IDE/ATAPI Port...	Microsoft Corp...	Signed Hidden in memory
0x86313748	\Driver\Aud...	0xF7CA7000	0xF7CA7600	0x1000	C:\WINDOWS\system32\DRIVERS\audstub.sys	AudStub Driver	Microsoft Corp...	Signed
0x8621D3A8	\Driver\Beep	0xF7AF7000	0xF7AF766C	0x2000	C:\WINDOWS\system32\Drivers\Beep.SYS	BEEP Driver	Microsoft Corp...	Signed
		0xF7937000	0xF7937000	0x5000	C:\WINDOWS\system32\Drivers\CdAudio.SYS	CD-ROM Audio ...	Microsoft Corp...	Signed Unloaded modul...
0x86295A40	\FileSystem...	0xF368B000	0xF3698A85	0x10000	C:\WINDOWS\system32\Drivers\Cdfs.SYS	CD-ROM File Sy...	Microsoft Corp...	Signed
0x863C7360	\Driver\Cdr...	0xF780F000	0xF78196DA	0xD000	C:\WINDOWS\system32\DRIVERS\cdrom.sys	SCSI CD-ROM ...	Microsoft Corp...	Signed
		0xF764F000	0xF7659E8F	0xD000	C:\WINDOWS\system32\DRIVERS\CLASSP...	SCSI Class Syst...	Microsoft Corp...	Signed
0x8637BA08	\Driver\Disk	0xF763F000	0xF76468AB	0x9000	C:\WINDOWS\system32\Drivers\disk.sys	PnP Disk Driver	Microsoft Corp...	Signed
0x862D6F38	\Driver\dmio	0xF746A000	0xF748BF05	0x26000	C:\WINDOWS\system32\Drivers\dmio.sys	Драйвер ввода...	Корпорация ...	Signed
0x86384340	\Driver\Admi...	0xF7AF1000	0xF7AF1BF6	0x2000	C:\WINDOWS\system32\Drivers\dmload.sys	NT Disk Manag...	Microsoft Corp...	Signed
		0xF2B39000	0xF2B4E5F7	0x18000	C:\WINDOWS\system32\Drivers\dump_atapi...			File doesn't exist
		0xF7AFF000	0xF7AFFB80	0x2000	C:\WINDOWS\system32\Drivers\dump_WML...			File doesn't exist
		0xF31B8000	0xF31B7E80	0x3000	C:\WINDOWS\system32\drivers\dxapi.sys	DirectX API Driver	Microsoft Corp...	Signed
		0x8F9C1000	0x8F9D1090	0x12000	C:\WINDOWS\system32\drivers\dxg.sys	DirectX Graphic...	Microsoft Corp...	Signed
		0xF384C000	0xF384C359	0x1000	C:\WINDOWS\system32\drivers\dxgthk.sys	DirectX Graphic...	Microsoft Corp...	Signed
0x863D0DE0	\Driver\Fdc	0xF79DF000	0xF79E494A	0x7000	C:\WINDOWS\system32\DRIVERS\Fdc.sys	Floppy Disk Con...	Microsoft Corp...	Signed
0x86125698	\Driver\Fips	0xF36CB000	0xF36CFF2B	0x9000	C:\WINDOWS\system32\DRIVERS\Fips.SYS	Драйвер FIPS ...	Корпорация ...	Signed
		0xF7987000	0xF7987000	0x5000	C:\WINDOWS\system32\Drivers\Flypndisk.SYS	Floppy Driver	Microsoft Corp...	Signed Unloaded modul...
0x862CF280	\FileSystem...	0xF7433000	0xF744ED6A	0x1F000	C:\WINDOWS\system32\Drivers\ftm.sys	Microsoft Filesys...	Microsoft Corp...	Signed
0x86114C08	\FileSystem...	0xF7AF5000	0xF7AF65E4	0x2000	C:\WINDOWS\system32\Drivers\Fs_Rec.SYS	File System Rec...	Microsoft Corp...	Signed
0x863E56D0	\Driver\Ftd...	0xF7490000	0xF74AB4E2	0x1F000	C:\WINDOWS\system32\Drivers\ftdisk.sys	Драйвер систе...	Корпорация ...	Signed
0x86114980	\Driver\Hd...	0xF2420000	0xF2444006	0x28000	C:\WINDOWS\system32\drivers\h43agg5.sys	Yba32 AntiRoot...	VirusBlokAda ...	YBA32 Signed
0x860FABE0	\Driver\HTT...	0xF24C0000	0xF24FAF57	0x41000	C:\WINDOWS\system32\Drivers\HTTP.sys	HTTP Protocol ...	Microsoft Corp...	Signed
0x861DC308	\Driver\I80...	0xF769F000	0xF76A8385	0xE000	C:\WINDOWS\system32\DRIVERS\i8042prt.sys	Драйвер порта...	Корпорация ...	Signed
0x863C7258	\Driver\Imapi	0xF77F0000	0xF78079FB	0x8000	C:\WINDOWS\system32\DRIVERS\imapi.sys	IMAPI Kernel Dri...	Microsoft Corp...	Signed
0x86106340	\Driver\IpN...	0xF2851000	0xF28BF59C	0x21000	C:\WINDOWS\system32\DRIVERS\ipnat.sys	IP Network Addr...	Microsoft Corp...	Signed
0x860E9790	\Driver\IPSec	0xF2CAF000	0xF2C8F885	0x13000	C:\WINDOWS\system32\DRIVERS\ipsec.sys	IPSec Driver	Microsoft Corp...	Signed
0x8637E2A0	\Driver\Nisa...	0xF75E0000	0xF75F63E4	0x9000	C:\WINDOWS\system32\Drivers\isapnp.sys	Драйвер шинны...	Корпорация ...	Signed
0x861D9270	\Driver\Kb...	0xF79EF000	0xF79F361D	0x7000	C:\WINDOWS\system32\DRIVERS\kbdclass	Драйвер класс...	Корпорация ...	Signed

File Information: C:\WINDOWS\system32\ntldr.dll  
 Size: 712192 Bytes (695.50 KB)    Attributes: rsha    Created: 16:00:00 18.08.2004    Modified: 16:00:00 18.08.2004    Accessed: 20:52:00 20.11.2011  
 MD5: a0c4b8baeebedb02853d134017e2d607    SHA1: 1c07feb13d877fc310d91447b19e54923bce17b

Total: 103

c) "\\Device\HardDisk0\DR0" device stack

Device Object	Name	Upper Device	Lower Device	Driver Object	Driver	Information
0x8629B0C0			0x8629B030	0x8629D530	C:\WINDOWS\system32\DRIVERS\redb...	Signed
0x8629B030	\Device\CdRom0	0x8629B0C0	0x8629A020	0x863C7360	C:\WINDOWS\system32\DRIVERS\vdco...	Signed
0x8629A020		0x8629B030	0x862FE968	0x863C7258	C:\WINDOWS\system32\DRIVERS\ima...	Signed
0x862FE968	\Device\00000063	0x8629A020	0x862D4D98	0x863E26E0	C:\WINDOWS\System32\Drivers\ACPI.sys	Signed
0x862D4D98	\Device\Ide\IdeDevic...	0x862FE968		0x8626CAC0	C:\WINDOWS\System32\Drivers\atapi.sys	Signed
<b>( 4 devices )</b>						
0x8626C150			0x86308AB8	0x862D6158	C:\WINDOWS\System32\Drivers\PartMg...	Signed
0x86308AB8	\Device\Harddisk0\DR0	0x8626C150	0x8632FF18	0x8637BA08	C:\WINDOWS\System32\Drivers\disk.sys	Signed
0x8632FF18	\Device\00000062	0x86308AB8	0x862FED98	0x863E26E0	C:\WINDOWS\System32\Drivers\ACPI.sys	Signed
0x862FED98	\	0x8632FF18		0x8634D478	C:\WINDOWS\System32\Drivers\atapi.sys	Signed Hidden in memory
<b>\Device\Ide\IdeDeviceP4T0L0-9 ( 4 device...)</b>						
0x8626C150			0x86308AB8	0x862D6158	C:\WINDOWS\System32\Drivers\PartMg...	Signed
0x86308AB8	\Device\Harddisk0\DR0	0x8626C150	0x8632FF18	0x8637BA08	C:\WINDOWS\System32\Drivers\disk.sys	Signed
0x8632FF18	\Device\00000062	0x86308AB8	0x862FED98	0x863E26E0	C:\WINDOWS\System32\Drivers\ACPI.sys	Signed
0x862D5D58	\Device\Ide\IdeDevic...	0x8632FF18		0x8626CAC0	C:\WINDOWS\System32\Drivers\atapi.sys	Signed
<b>\Device\Ide\PciIdeChannel1-3 ( 3 devices )</b>						
0x8630A030	\Device\Ide\IdePort3		0x863E37F0	0x8626CAC0	C:\WINDOWS\System32\Drivers\atapi.sys	Signed
0x863E37F0	\Device\0000005d	0x8630A030	0x863E3A20	0x863E26E0	C:\WINDOWS\System32\Drivers\ACPI.sys	Signed
0x863E3A20	\Device\Ide\PciIdeC...	0x863E37F0		0x863BF780	C:\WINDOWS\System32\Drivers\pciide....	Signed
<b>\Device\NTPNP_PCI0014 ( 3 devices )</b>						
0x8634DAC8			0x86300F18	0x863C28A0	C:\WINDOWS\System32\Drivers\pci.sys	Signed
0x86300F18	\Device\0000004f	0x8634DAC8	0x86399E50	0x863E26E0	C:\WINDOWS\System32\Drivers\ACPI.sys	Signed
0x86399E50	\Device\NTPNP_PCI0...	0x86300F18		0x863C28A0	C:\WINDOWS\System32\Drivers\pci.sys	Signed
<b>\Device\Ide\PciIde2Channel0-4 ( 3 devices )</b>						
0x8632F030	\Device\Ide\IdePort4		0x86384D48	0x8626CAC0	C:\WINDOWS\System32\Drivers\atapi.sys	Signed
0x86384D48	\Device\0000005e	0x8632F030	0x8634D278	0x863E26E0	C:\WINDOWS\System32\Drivers\ACPI.sys	Signed
0x8634D278	\Device\Ide\PciIde2C...	0x86384D48		0x863BF780	C:\WINDOWS\System32\Drivers\pciide....	Signed
<b>\Device\NTPNP_PCI0007 ( 3 devices )</b>						
0x8637D030	\Device\Ide\PciIde1		0x8626D770	0x863BF780	C:\WINDOWS\System32\Drivers\pciide....	Signed
0x8626D770	\Device\00000049	0x8637D030	0x8637F688	0x863E26E0	C:\WINDOWS\System32\Drivers\ACPI.sys	Signed

Total: 264 device forming 59 device stacks

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

Type	Address	Driver	Addition	Information
LoadImage	0x86010170	Vba32 AntiRootKit Handler		VBA32
<b>LoadImage</b>	<b>0x8634D903</b>	<b>[Unknown Handler]</b>		
Shutdown	0xF3D0BC74	C:\WINDOWS\system32\DRIVERS\Cdfs.SYS	DeviceObject = 0x8617E328	Signed
PostAcquireForCcFlush	0xF74411EA	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PostAcquireForModifi...	0xF74411EA	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PostAcquireForSectio...	0xF74411EA	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PostReleaseForCcFlu...	0xF74411EA	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PostReleaseForModifi...	0xF74411EA	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PostReleaseForSecti...	0xF74411EA	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PreAcquireForCcFlush	0xF7441118	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PreAcquireForModifi...	0xF7441118	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PreAcquireForSection...	0xF7441118	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PreReleaseForCcFlush	0xF7441118	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PreReleaseForModifi...	0xF7441118	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
PreReleaseForSectio...	0xF7441118	C:\WINDOWS\System32\Drivers\fltMgr.sys	FsFilterCallbacks = 0x863CF2F8...	Signed
Shutdown	0xF7B015BE	C:\WINDOWS\System32\Drivers\Fs_Rec.SYS	DeviceObject = 0x8614DBB0	Signed
Shutdown	0xF7B015BE	C:\WINDOWS\System32\Drivers\Fs_Rec.SYS	DeviceObject = 0x861F7F08	Signed
Shutdown	0xF7B015BE	C:\WINDOWS\System32\Drivers\Fs_Rec.SYS	DeviceObject = 0x86272E30	Signed
Shutdown	0xF7B015BE	C:\WINDOWS\System32\Drivers\Fs_Rec.SYS	DeviceObject = 0x8617FF08	Signed
Shutdown	0xF7B015BE	C:\WINDOWS\System32\Drivers\Fs_Rec.SYS	DeviceObject = 0x861AC7B0	Signed
Shutdown	0xF74912BE	C:\WINDOWS\System32\Drivers\fdisk.sys	DeviceObject = 0x863CAE60	Signed
Shutdown	0xF761F73A	C:\WINDOWS\System32\Drivers\MountMgr.sys	DeviceObject = 0x863CB408	Signed
SeFileSystem	0xF32251EB	C:\WINDOWS\system32\DRIVERS\mrxmb.sys		Signed
BugCheckReason	0xF7AA3A30	C:\WINDOWS\system32\DRIVERS\mssmbios.sys	CallbackRecord = 0xF7AA4AA0	Signed
BugCheckReason	0xF7AA3A78	C:\WINDOWS\system32\DRIVERS\mssmbios.sys	CallbackRecord = 0xF7AA4A60	Signed
BugCheckReason	0xF7AA3AC0	C:\WINDOWS\system32\DRIVERS\mssmbios.sys	CallbackRecord = 0xF7AA4A80	Signed
PreAcquireForCcFlush	0xF7347B3F	C:\WINDOWS\System32\Drivers\Mup.sys	FsFilterCallbacks = 0x863CD618...	Signed
PreAcquireForModifi...	0xF7347B3F	C:\WINDOWS\System32\Drivers\Mup.sys	FsFilterCallbacks = 0x863CD618...	Signed
PreAcquireForSection...	0xF7347A4F	C:\WINDOWS\System32\Drivers\Mup.sys	FsFilterCallbacks = 0x863CD618...	Signed
PreReleaseForCcFlush	0xF7347B3F	C:\WINDOWS\System32\Drivers\Mup.sys	FsFilterCallbacks = 0x863CD618...	Signed

Total: 43

e) All of major IRP Handlers points to the same memory address

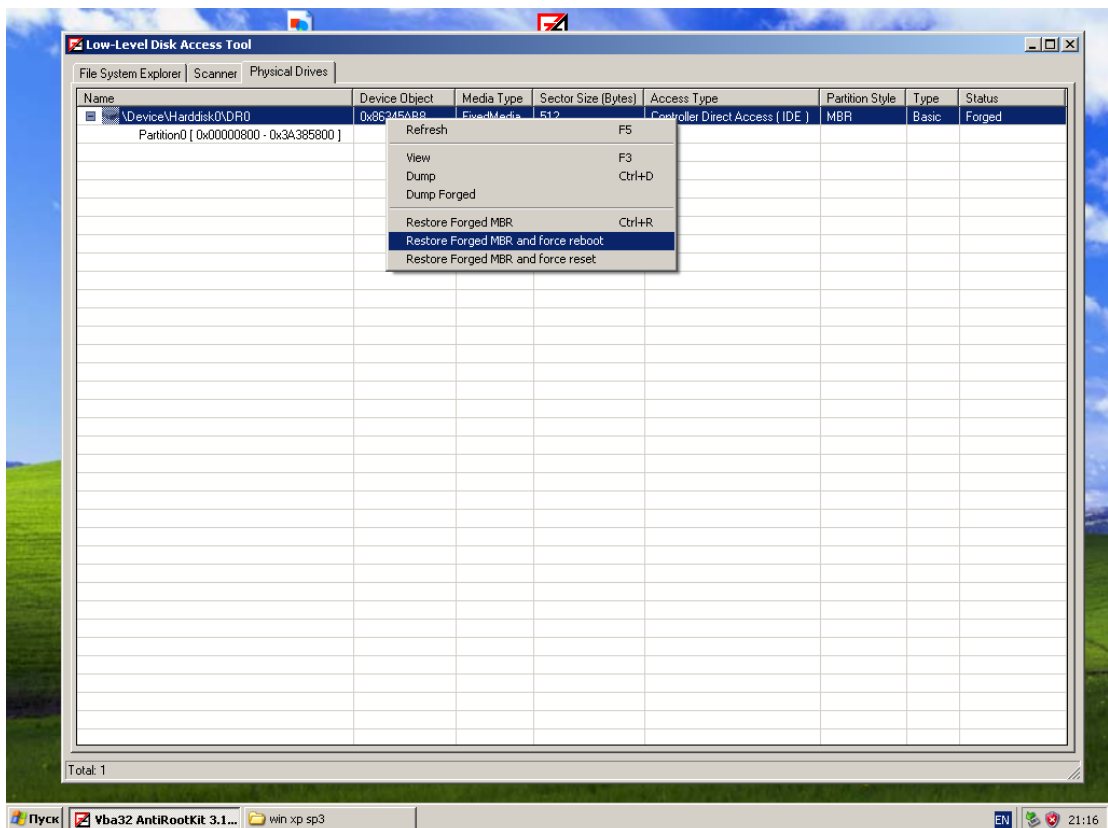
Driver Object	Handler Name	Current Address	Driver	Information
\Driver\atapi	DriverStartIo	0x8634E31B	[Unknown Handler]	
\Driver\atapi	IRP_MJ_PNP	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_SET_QUOTA	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_QUERY_QUOTA	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_DEVICE_CHANGE	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_SYSTEM_CONTROL	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_POWER	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_SET_SECURITY	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_QUERY_SECURITY	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_CREATE_MAILSLLOT	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_CLEANUP	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_LOCK_CONTROL	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_SHUTDOWN	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_INTERNAL_DEVICE_CONTROL	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_DEVICE_CONTROL	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_FILE_SYSTEM_CONTROL	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_DIRECTORY_CONTROL	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_SET_VOLUME_INFORMATION	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_QUERY_VOLUME_INFORMA...	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_FLUSH_BUFFERS	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_SET_EA	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_QUERY_EA	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_SET_INFORMATION	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_QUERY_INFORMATION	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_WRITE	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_READ	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_CLOSE	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_CREATE_NAMED_PIPE	0x8634E4D0	[Unknown Handler]	
\Driver\atapi	IRP_MJ_CREATE	0x8634E4D0	[Unknown Handler]	

Total: 29

f) Note that some additional anomalies, such as injected .dlls or remote threads, which are not shown in this document, may be present in infected system

## 2. Removal

- a) To fully disinfect the operating system select "Restore Forged MBR and force reboot" option



- b) After reboot Vba32 AntiRootkit will start automatically

