

# **Vba32 AntiRootkit vs TDL 2**

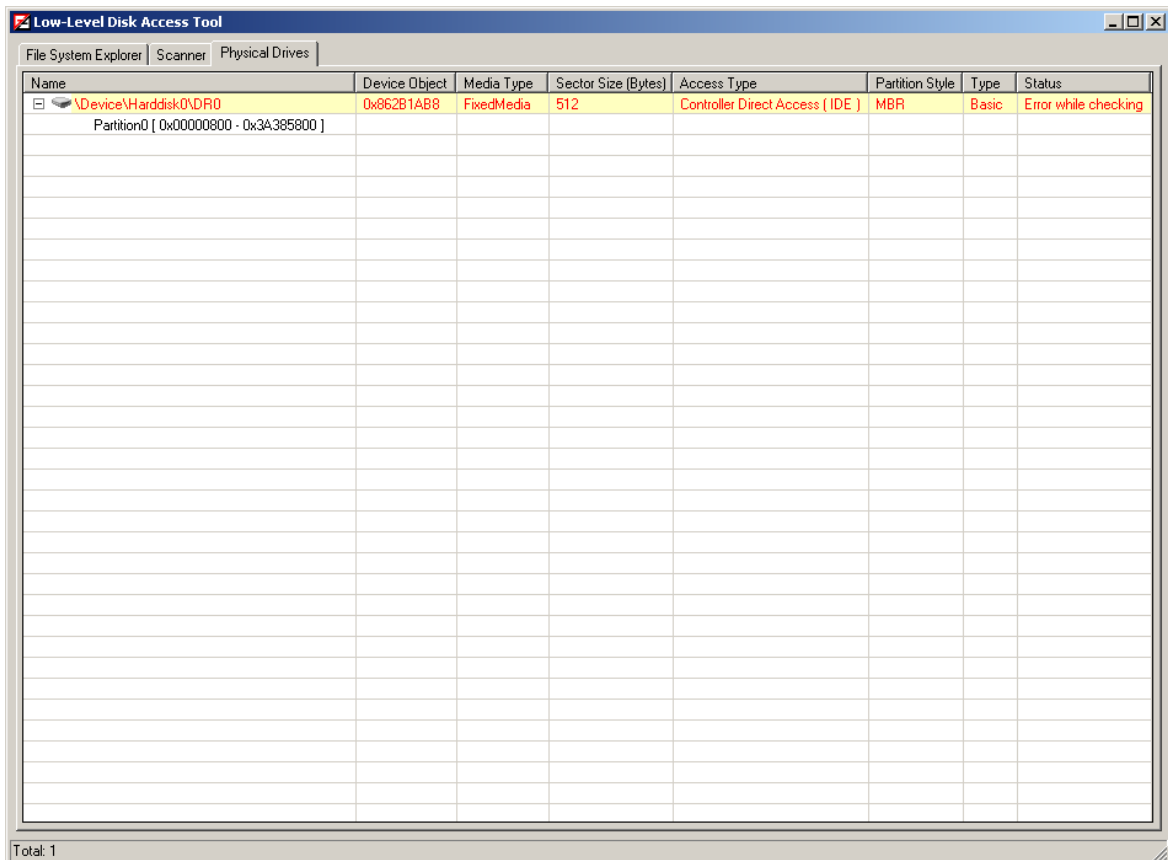
Dmitry Varshavsky  
Nikolay Moskalenko



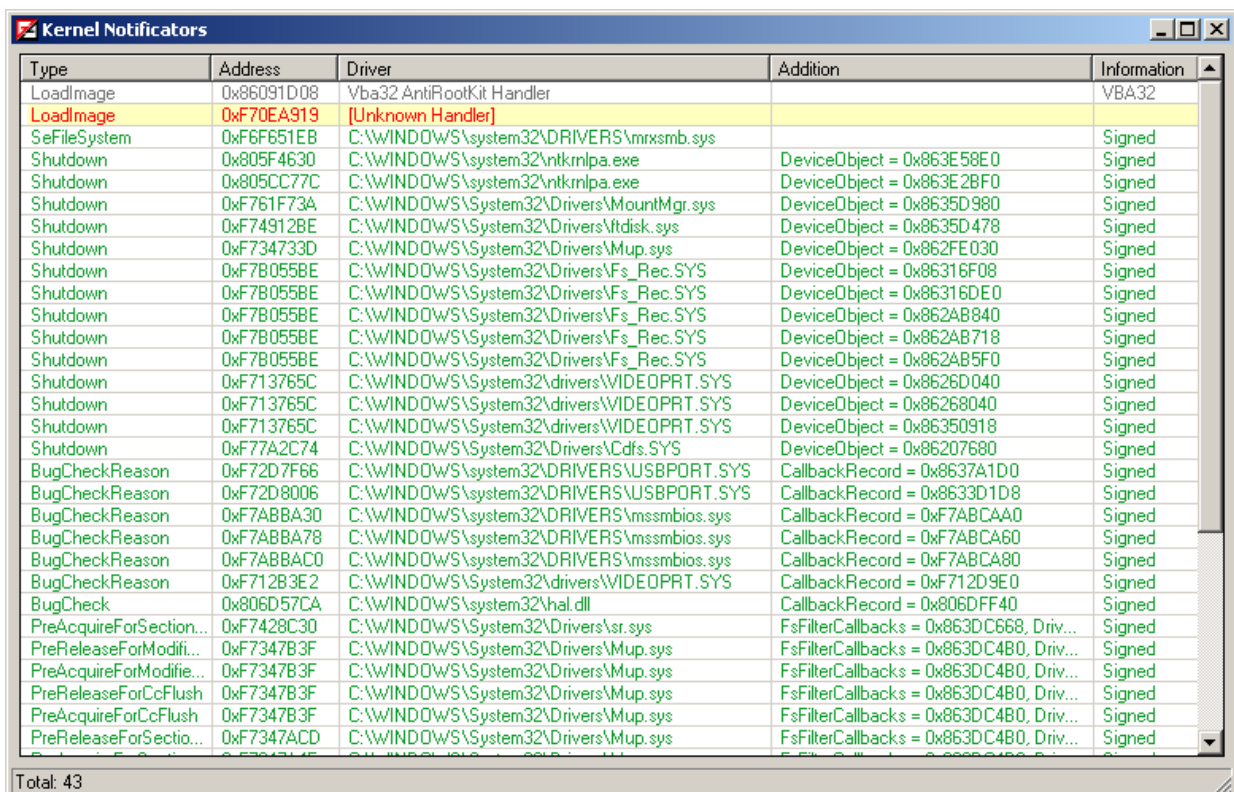
**VirusBlokAda**

# 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 ( IoCompleteRequest and IoCallDriver 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

Module	Type	Number	Name	Base Value	Current Value	Driver	Information
ntoskrnl.exe	Code Modification (3 bytes)	-	PAGE +0x0BC114	0x8055D300	-		
ntoskrnl.exe	Code Modification (3 bytes)	-	PAGE +0x0B9E0E	0x8055D300	-		
ntoskrnl.exe	Code Modification (3 bytes)	-	PAGE +0x0B9D7E	0x8055D300	-		
ntoskrnl.exe	Code Modification (5 bytes)	-	PAGE +0x04D614	0x8055D300	-		
ntoskrnl.exe	Code Modification - Relative Jump	-	IoCompleteRequest +0x0000	0x804EDE90	0x86360133		
ntoskrnl.exe	Code Modification - Relative Jump	-	IoCallDriver +0x0000	0x804EDE00	0x86338743		
ntoskrnl.exe	Code Modification - Relative Jump	-	NtSaveKeyEx +0x0000	0x8061710C	0x8637711A		
ntoskrnl.exe	Code Modification - Relative Jump	-	NtSaveKey +0x0000	0x8061707C	0x8637C772		
ntoskrnl.exe	Code Modification - Relative Jump	-	NtFlushInstructionCache +0x0000	0x805AA912	0x863167AC		
ntoskrnl.exe	Code Modification - Relative Jump	-	NtEnumerateKey +0x0000	0x80619412	0x86322574		
framebuf.dll	IAT Modification	-	WIN32K.SYS!EngBugCheckEx	0xBF9ABC7F	0x804F890A	C:\WINDOWS\system32\ntkrnlpa.exe	Signed
ntoskrnl.exe	SSDT	258	NtTerminateThread	0x805C76C2	0xF6382294	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
ntoskrnl.exe	SSDT	257	NtTerminateProcess	0x805C74C8	0xF638231A	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
ntoskrnl.exe	SSDT	213	NtSetContextThread	0x805C61F2	0xF6382412	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
ntoskrnl.exe	SSDT	137	NtProtectVirtualMemory	0x805AC4E2	0xF63824EA	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
ntoskrnl.exe	SSDT	19	NtAssignProcessToJobObject	0x805C8162	0xF6382396	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	592	NtUserWindowFromPoint	0xBF81C230	0xF638272E	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	571	NtUserUnhookWinEvent	0xBF8CED24	0xF6382C25	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	570	NtUserUnhookWindowsHookEx	0xBF8DBCB2B	0xF6382B06	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	552	NtUserSetWinEventHook	0xBF8CEEE3	0xF6382B20	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	549	NtUserSetWindowsHookEx	0xBF89DD6	0xF6382A06	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	483	NtUserQueryWindow	0xBF803AC8	0xF6382574	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	476	NtUserPostThreadMessage	0xBF8FCA90	0xF63827BE	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	475	NtUserPostMessage	0xBF808522	0xF63828F8	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	460	NtUserMessageCall	0xBF80F615	0xF638284C	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	404	NtUserGetForegroundWindow	0xBF818DF9	0xF63826A4	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	378	NtUserFindWindowEx	0xBF87DC40	0xF638260A	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed
win32k.sys	Shadow SSDT	355	NtUserDestroyWindow	0xBF8FAF04	0xF6382984	C:\WINDOWS\system32\drivers\2mn6jd.sys	VBA32 Signed

Total: 28, SSDT: 5, Shadow SSDT: 12, SysEnter: 0, IDT: 0, GDT: 0, EAT: 0, IAT: 1, Inline: 10, ObjectTypes: 0, Other: 0

- 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

Short Name	PID	Parent PID	Full Path	Description	Company Name	Information
System	4	0				
smss.exe	360	4	C:\WINDOWS\system32\smss.exe	Диспетчер сеанса Windows NT	Корпорация Майкрософт	Signed
csrss.exe	424	360	C:\WINDOWS\system32\csrss.exe	Client Server Runtime Process	Microsoft Corporation	Signed
winlogon.exe	448	360	C:\WINDOWS\system32\winlogon.exe	Программа входа в систему Windows	Корпорация Майкрософт	Signed
services.exe	492	448	C:\WINDOWS\system32\services.exe	Приложение служб и контроллеров	Корпорация Майкрософт	Signed
svchost.exe	232	492	C:\WINDOWS\system32\svchost.exe	Generic Host Process for Win32 Servi...	Microsoft Corporation	Signed
svchost.exe	652	492	C:\WINDOWS\system32\svchost.exe	Generic Host Process for Win32 Servi...	Microsoft Corporation	Signed Anomaly detected
svchost.exe	744	492	C:\WINDOWS\system32\svchost.exe	Generic Host Process for Win32 Servi...	Microsoft Corporation	Signed
svchost.exe	784	492	C:\WINDOWS\system32\svchost.exe	Generic Host Process for Win32 Servi...	Microsoft Corporation	Signed
wscntfy.exe	1624	784	C:\WINDOWS\system32\wscntfy.exe	Windows Security Center Notification ...	Microsoft Corporation	Signed
wuauclt.exe	1944	784	C:\WINDOWS\system32\wuauclt.exe	Автоматическое обновление	Microsoft Corporation	Signed
svchost.exe	828	492	C:\WINDOWS\system32\svchost.exe	Generic Host Process for Win32 Servi...	Microsoft Corporation	Signed
spoolsv.exe	912	492	C:\WINDOWS\system32\spoolsv.exe	Spooler SubSystem App	Microsoft Corporation	Signed
alg.exe	1164	492	C:\WINDOWS\system32\alg.exe	Application Layer Gateway Service	Microsoft Corporation	Signed
lsass.exe	504	448	C:\WINDOWS\system32\lsass.exe	LSA Shell (Export Version)	Microsoft Corporation	Signed
explorer.exe	1072	1040	C:\WINDOWS\explorer.exe	Проводник	Корпорация Майкрософт	Signed
mspaint.exe	216	1072	C:\WINDOWS\system32\mspaint.exe	Paint	Корпорация Майкрософт	Signed
ctfmon.exe	1724	1072	C:\WINDOWS\system32\ctfmon.exe	CTF Loader	Microsoft Corporation	Signed
Vba32arokit.exe	1984	1072	C:\Documents and Settings\Админист...	Vba32 AntiRootkit	VirusBlokAde Ltd.	VBA32 Signed Anomaly detected

Threads (22) | Modules (60) | Handles (200) | Anomalies (4) | svchost.exe (PID: 652)

Description: Hidden module: [0x10000000-0x10000FFF] C:\WINDOWS\system32\gasfkyweeegqs.dll  
 No corresponding start module ( Start Address = 0x00831DF7 ): Thread = 0x861778A0 (TID: 684)  
 No corresponding start module ( Start Address = 0x0083222B ): Thread = 0x86170620 (TID: 692)  
 No corresponding start module ( Start Address = 0x0083216E ): Thread = 0x8614B8A0 (TID: 688)

C:\WINDOWS\system32\svchost.exe  
 Size: 14336 Bytes (14.00 KB) | Attributes: rsha | Created: 16:00:00 18.08.2004 | Modified: 16:00:00 18.08.2004 | Accessed: 20:51:17 20.11.2011  
 MD5: 5eb0ae95bf08d5a63c167648f1314c07 | SHA1: a8c7dbd6a7fb7d48654602c8b6434859a77307d

C:\WINDOWS\system32\DRIVERS\ipitlink.sys | Total: 20

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

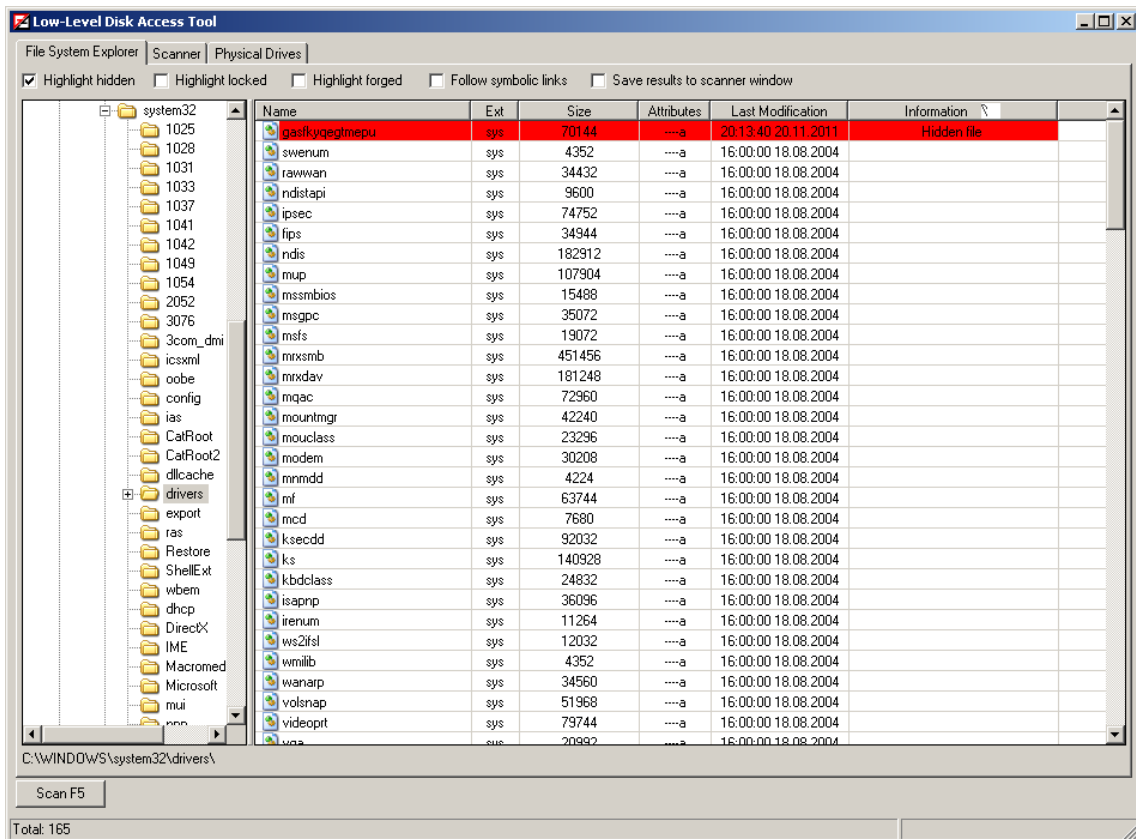
Name	Ext	Size	Attributes	Last Modification	Information
gasfkyqspmpde	dll	43008	---a	20:13:40 20.11.2011	Hidden file
gasfkyedqghwr	dat	485	---a	20:19:34 20.11.2011	Hidden file
gasfkycxdqgqolx	dll	19968	---a	20:13:41 20.11.2011	Hidden file
iphlpapi	dll	95744	---a	16:00:00 18.08.2004	
ipconfig	exe	57344	---a	16:00:00 18.08.2004	
ipconf	tsp	17408	---a	16:00:00 18.08.2004	
iologmsg	dll	35840	---a	16:00:00 18.08.2004	
intl	cpl	132096	---a	16:00:00 18.08.2004	
instcat	sql	956990	---a	16:00:00 18.08.2004	
inseng	dll	96256	---a	16:00:00 18.08.2004	
input	dll	125440	---a	16:00:00 18.08.2004	
initpki	dll	147456	---a	16:00:00 18.08.2004	
infosoft	dll	450560	---a	16:00:00 18.08.2004	
inetres	dll	48640	---a	16:00:00 18.08.2004	
inetppui	dll	15872	---a	16:00:00 18.08.2004	
inetpp	dll	75264	---a	16:00:00 18.08.2004	
inetmb1	dll	33280	---a	16:00:00 18.08.2004	
inetplc	dll	114176	---a	16:00:00 18.08.2004	
inetcpl	cpl	359424	---a	16:00:00 18.08.2004	
inetcomm	dll	678400	---a	16:00:00 18.08.2004	
mshata	exe	29184	---a	16:00:00 18.08.2004	
msharts	exe	127488	---a	16:00:00 18.08.2004	
msh263	drv	294912	---a	16:00:00 18.08.2004	
msh261	drv	188416	---a	16:00:00 18.08.2004	
msgsvc	dll	33792	---a	16:00:00 18.08.2004	
msgsm32	acm	19968	---a	16:00:00 18.08.2004	
msgina	dll	997376	---a	16:00:00 18.08.2004	
msg723	acm	118784	---a	16:00:00 18.08.2004	
msg711	acm	9216	---a	16:00:00 18.08.2004	
msg	exe	21504	---a	16:00:00 18.08.2004	
msgdt	dll	537088	---a	16:00:00 18.08.2004	

C:\WINDOWS\system32\

Scan F5

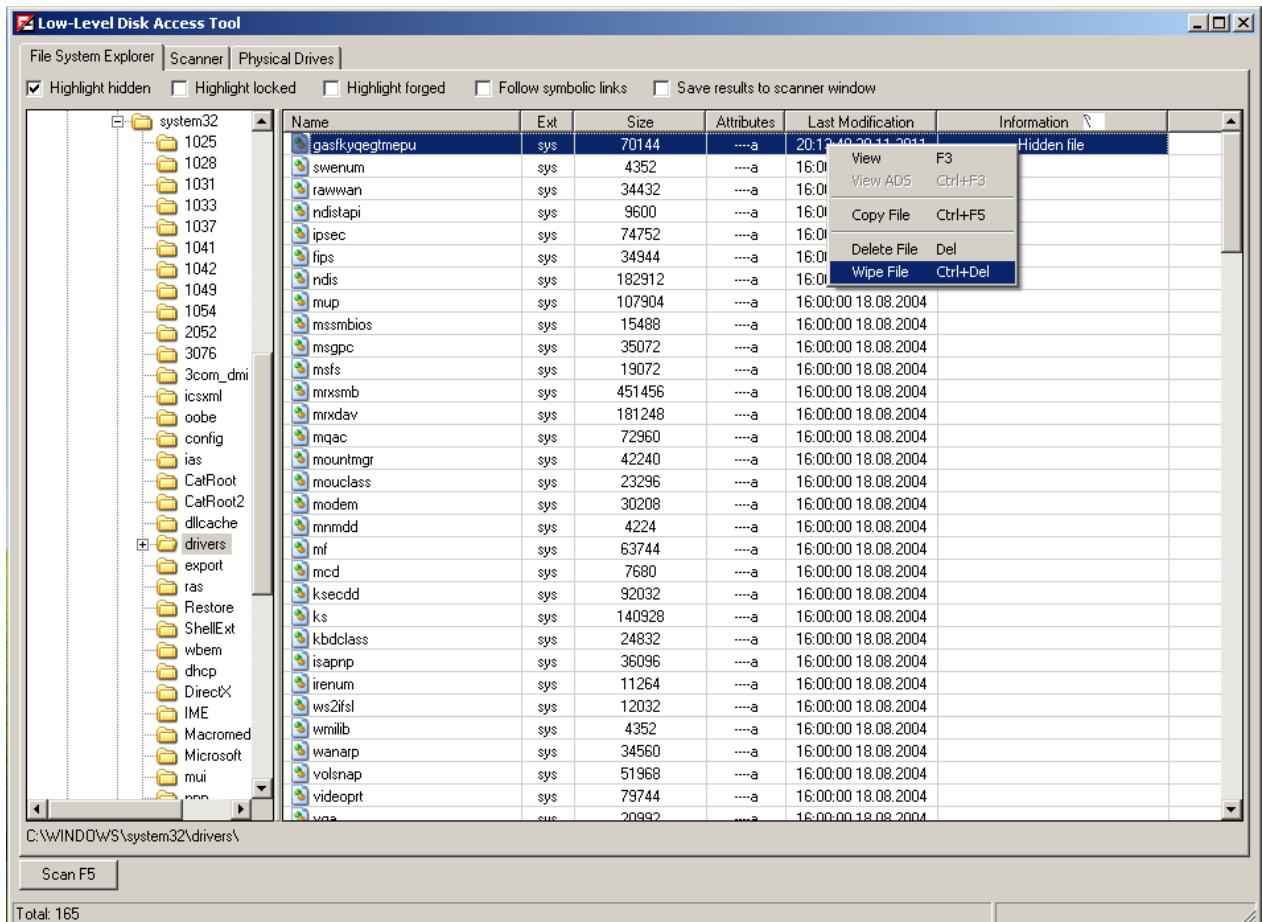
Total: 1805

f) Malicious driver itself

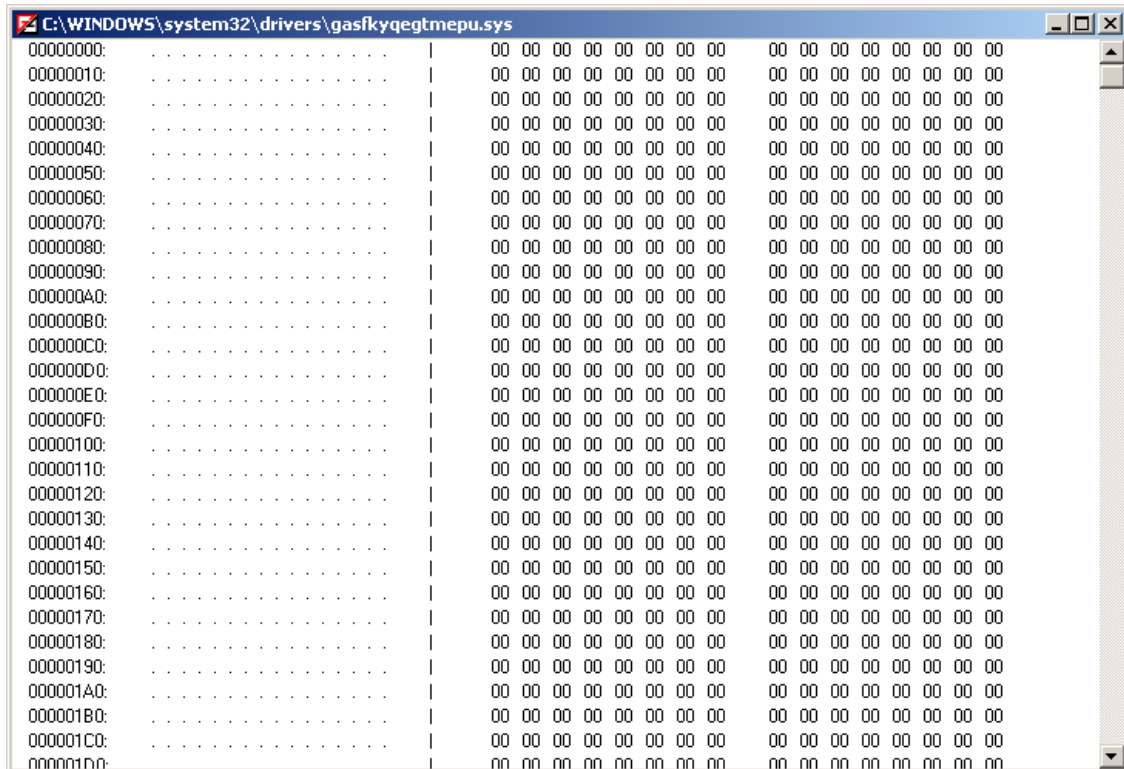


## 2. Removal

### 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 )



Short Name	PID	Parent PID	Full Path	Description	Company Name	Information
System	4	0				
smss.exe	360	4	C:\WINDOWS\system32\smss.exe	Диспетчер сеанса...	Корпорация Майкрос...	Signed
csrss.exe	424	360	C:\WINDOWS\system32\csrss.exe	Client Server Runtim...	Microsoft Corporation	Signed
winlogon.exe	448	360	C:\WINDOWS\system32\winlogon.exe	Программа входа ...	Корпорация Майкрос...	Signed
services.exe	492	448	C:\WINDOWS\system32\services.exe	Приложение служ...	Корпорация Майкрос...	Signed
svchost.exe	348	492	C:\WINDOWS\system32\svchost.exe	Generic Host Proce...	Microsoft Corporation	Signed
svchost.exe	652	492	C:\WINDOWS\system32\svchost.exe	Generic Host Proce...	Microsoft Corporation	Signed
svchost.exe	728	492	C:\WINDOWS\system32\svchost.exe	Generic Host Proce...	Microsoft Corporation	Signed
svchost.exe	764	492	C:\WINDOWS\system32\svchost.exe	Generic Host Proce...	Microsoft Corporation	Signed
wscntfy.exe	1608	764	C:\WINDOWS\system32\wscntfy.exe	Windows Security C...	Microsoft Corporation	Signed
svchost.exe	808	492	C:\WINDOWS\system32\svchost.exe	Generic Host Proce...	Microsoft Corporation	Signed
svchost.exe	852	492	C:\WINDOWS\system32\svchost.exe	Generic Host Proce...	Microsoft Corporation	Signed
spoolsv.exe	1160	492	C:\WINDOWS\system32\spoolsv.exe	Spooler SubSystem...	Microsoft Corporation	Signed
alg.exe	1576	492	C:\WINDOWS\system32\alg.exe	Application Layer G...	Microsoft Corporation	Signed
lsass.exe	504	448	C:\WINDOWS\system32\lsass.exe	LSA Shell (Export V...	Microsoft Corporation	Signed
explorer.exe	1060	1036	C:\WINDOWS\explorer.exe	Проводник	Корпорация Майкрос...	Signed
mspaint.exe	324	1060	C:\WINDOWS\system32\mspaint.exe	Paint	Корпорация Майкрос...	Signed
ctfmon.exe	1688	1060	C:\WINDOWS\system32\ctfmon.exe	CTF Loader	Microsoft Corporation	Signed
Vba32arikit.exe	1772	1060	C:\Documents and Settings\Администратор\Рабоч...	Vba32 AntiRootkit	VirusBlokAda Ltd.	VBA32 Signed Anomaly detected

Ethread	TID	State	Service Table	TEB	Start Address	Start Module	Hidden From Debugger	Information

File Information  
Size: Attributes: rsha Created: Modified: Accessed:  
MD5: SHA1:

C:\WINDOWS\system32\ctypes.nls Total: 19

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

Name	Start	Display name	Image Path	Information
Dhcp	AUTO	DHCP-клиент	%SystemRoot%\system32\svchost.exe -k netsvcs	Signed
Disk	BOOT	Драйвер диска	system32\DRIVERS\disk.sys	Signed
dmadmin	DEMAND	Служба администрирования диспетчера л...	%SystemRoot%\system32\dmadmin.exe /com	Signed
dmboot	DISABLED		System32\drivers\dmboot.sys	Signed
dmio	BOOT	Драйвер диспетчера логических дисков	System32\drivers\dmio.sys	Signed
dmload	BOOT		System32\drivers\dmload.sys	Signed
dmserver	AUTO	Диспетчер логических дисков	%SystemRoot%\system32\svchost.exe -k netsvcs	Signed
Dnscache	AUTO	DNS-клиент	%SystemRoot%\system32\svchost.exe -k NetworkService	Signed
dpti2o	DISABLED			
ERSvc	AUTO	Служба регистрации ошибок	%SystemRoot%\system32\svchost.exe -k netsvcs	Signed
Eventlog	AUTO	Журнал событий	%SystemRoot%\system32\services.exe	Signed
EventSystem	DEMAND	Система событий COM+	C:\WINDOWS\system32\svchost.exe -k netsvcs	Signed
Fastfat	DISABLED			
FastUserSwitchin...	DEMAND	Совместимость быстрого переключения п...	%SystemRoot%\system32\svchost.exe -k netsvcs	Signed
Fdc	DEMAND	Драйвер контроллера гибких дисков	system32\DRIVERS\fdc.sys	Signed
Fips	SYSTEM			
Flydisk	SYSTEM			
FltMgr	BOOT	FltMgr	system32\DRIVERS\fltMgr.sys	Signed
Fs_Rec	SYSTEM			
Ftdisk	BOOT	Драйвер диспетчера томов	system32\DRIVERS\ftdisk.sys	Signed
gasfkyvbtvxdg	SYSTEM		%systemroot%\system32\drivers\gasfkytpapvrch.sys	
Gpc	DEMAND	Refresh F5	system32\DRIVERS\msgpc.sys	Signed
helpsvc	AUTO		%SystemRoot%\system32\svchost.exe -k netsvcs	Signed
HidServ	DISABLE	Don't display trusted items	%SystemRoot%\system32\svchost.exe -k netsvcs	Signed
hpn	DISABLE	Don't display items with empty path name		
HTTP	DEMAND		System32\Drivers\HTTP.sys	Signed
HTTPFilter	DEMAND	Copy image path to clipboard	%SystemRoot%\system32\svchost.exe -k HTTPFilter	Signed
i2omgmt	SYSTEM			
i2omp	DISABLE	Open in Regedit Enter		
i8042prt	SYSTEM		system32\DRIVERS\i8042prt.sys	Signed
Imapi	SYSTEM		system32\DRIVERS\imapi.sys	Signed
ImapiService	DEMAND		C:\WINDOWS\system32\imapi.exe	Signed
inetaccs	AUTO			
ini910u	DISABLE			
Inport	DISABLED			
Intellde	DISABLE			
Ip6Fw	DEMAND	Delete Del	system32\DRIVERS\Ip6Fw.sys	Signed
IpFilter	DEMAND		system32\DRIVERS\IpFilter.sys	Signed

Total: 250



e) Finally delete rootkit file and its payload

