

ANTI-VIRUS ARTIFACTS III

// By [ethereal_vx](#)



Table of Contents

Topic	Page
Introduction	3
Avira	4 - 7
F-Secure	8 - 10
Norton	11 - 15
TrendMicro	16 - 18
WebRoot	19 - 22
BitDefender	23 - 27
MalwareBytes	28 - 30
Adaware	31 - 32
AVAST	33 - 37
Dr. Web	38 - 40
Kaspersky	41 - 43
Conclusion	44

Welcome to Antivirus Artifacts III.

The Antivirus Artifacts series so far has focused exclusively on mnemonic artifacts: drivers, API hooks, or processes which may be present. This third entry identifies registry artifacts from the AV product as well as services. New AVs have been added to the collection: Adaware, Dr. Web, AVAST, Kaspersky.

Note: due to the size of the registry artifacts retrieved they will not be listed in this paper. Registry dumps for HKEY_LOCAL_MACHINE, HKEY_CURRENT_CONFIG, HKEY_CLASSES_ROOT, HKEY_USERS, and HKEY_CURRENT_USER can be viewed on my GitHub.

<https://github.com/D3VI5H4/Antivirus-Artifacts/tree/main/Registry%20Data>

Summary of Antivirus Artifacts I:

The most common method to determine if an anti-virus product or EDR system is in place is using the [WMIC](#) and performing a basic query against the [Windows Security Center namespace](#).

```
wmic /node:localhost /namespace:\\root\SecurityCenter2 path  
AntiVirusProduct Get DisplayName | findstr /V /B /C:displayName || echo  
No Antivirus installed
```

courtesy of [Sam Denty](#) from [StackOverflow](#)

This method will work in most scenarios. The problem presented here is that this will only return a string if the anti-virus product, or the EDR system, has chosen to register itself in the Windows Security Center namespace. If the product has not registered itself this query will fail. Knowing we are dependent on a security product to register itself I have decided to go down a different path.

Summary of Antivirus Artifacts II:

This release is to act as an amendment to the original paper by diving deeper into antivirus products and their operations by documenting drivers loaded into the Windows kernel as well as listing the [file system filters](#) in place.

Note: all data listed and found is the result of a clean installation with default configuration. As data from the antivirus were discovered there were fluctuations in web traffic. All web traffic listed was discovered from the antivirus at run-time. In the event you decide to review any of the products listed in this paper note you may get different results based on your geographical location or activity being performed by the antivirus product.

Avira

Parent Directory
C:\Program Files (x86)\Avira\

Binaries present:

Name	Description	Sub directory
Avira.ServiceHost.exe	Avira Service Host	Launcher
Avira.Systray.exe	Avira	Launcher
Avira.OptimizerHost.exe	Avira Optimizer Host	Optimizer Host
Avira.VpnService.exe	VpnService	VPN
Avira.SoftwareUpdater.ServiceHost.exe	Avira Updater Service Host	Software Updater
Avira.Spotlight.Service.exe	Avira Security	Launcher
avguard.exe	Antivirus Host Framework Service	Antivirus
avshadow.exe	Anti vir Shadow copy Service	Antivirus
protectedservice.exe	Avira Protected Antimalware Service	Antivirus
avipbb.sys	Avira Driver for Security Enhancement	C:\Windows\System32\Drivers\
avkmgr.sys	Avira Manager Driver	C:\Windows\System32\Drivers\
avgntflt.sys	Avira Minifilter Driver	C:\Windows\System32\Drivers\
avdevprot.sys	Avira USB Feature Driver	C:\Windows\System32\Drivers\
avusbflt.sys	Avira USB Filter Driver	C:\Windows\System32\Drivers\
avnetflt.sys	Avira WFP Network Driver	C:\Windows\System32\Drivers\

In-memory modules present:

Name	Description	Sub Directory
Avira.SystemSpeedUp.UI.ShellExtension.dll	Avira.SystemSpeedUp.UI.ShellExtension.dll	System SpeedUp

Functions Hooked:

N/A	N/A	N/A
-----	-----	-----

Minifilters Present:

Driver	Altitude	Type
avipbb.sys	367600	FSFilter Activity Monitor
avgntflt.sys	320500	FSFilter Anti-Virus

Antivirus Driver	Request
avgntflt.sys	IRP_MJ_CREATE
avgntflt.sys	IRP_MJ_CLEANUP
avgntflt.sys	IRP_MJ_WRITE
avgntflt.sys	IRP_MJ_SET_INFORMATION
avgntflt.sys	IRP_MJ_SET_SECURITY
avgntflt.sys	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION
avgntflt.sys	IRP_MJ_FLUSH_BUFFERS
avgntflt.sys	IRP_MJ_FILE_SYSTEM_CONTROL

[continued below]

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	35.157.123.32	64359	443
TCP	18.196.164.37	64546	443
TCP	35.186241.51	64536	443
TCP	18.157.205.1	64540	80
TCP	18.157.205.1	64541	443
TCP	104.19.148.8	64542	443
TCP	172.217.167.232	64543	443
TCP	13.35.221.216	64544	443
TCP	13.35.221.216	64545	443
TCP	172.217.167.206	64547	443
TCP	52.86.179.151	64548	443
TCP	74.125.24.157	64549	443
TCP	172.217.167.196	64550	443
TCP	172.217.167.195	64551	443

[continued below]

Services:

Name	Description	Startup Type	Path
Avira Service Host	Hosts multiple Avira Services within one Windows service.	Automatic	\Launcher\Avira.ServiceHost.exe
Avira Optimizer Host	Hosts multiple Avira optimization services within one Windows service.	Automatic	\Optimizer Host\Avira.OptimizerHost.exe
AviraPhantomVPN	Avira Phantom VPN	Automatic	\VPN\Avira.VpnService.exe
Avira Updater Service	Support service for Avira Software Updater	Automatic	\SoftwareUpdater\Avira.SoftwareUpdater.ServiceHost.exe
Avira Security	Avira Security	Automatic	\Security\Avira.Spotlight.Service.exe
Avira Mail Protection	Offers permanent protection against viruses and malware for email clients with the Avira search engine.	Automatic	\Antivirus\avmailc7.exe
Avira Protected Service	Launch Avira's anti-malware service as a protected service.	Automatic	\Antivirus\ProtectedService.exe
Avira Real Time Protection	Offers permanent protection against viruses and malware with the Avira search engine.	Automatic	\Antivirus\avguard.exe
Avira Scheduler	Service to schedule Avira Antivirus jobs & updates	Automatic	\Antivirus\sched.exe
Avira Web Protection	Offers permanent protection against viruses & malware for web browsers with the Avira Search Engine	Automatic	\Antivirus\avwebg7.exe

FSecure

Parent Directory
C:\Program Files(x86)\F-Secure\Anti-Virus\

Binaries present:

Name	Description	Sub directory
fshs.sys	DG 64-bit kernel module	Ultralight\ulcore\%ld\
fsulgk.sys	F-Secure Gatekeeper 64 bit	Ultralight\ulcore\%ld\
nif2s64.sys	F-Secure NIF2 Core Driver	N/A
fshoster32.exe	F-Secure plugin hosting service	N/A
fsorsp64.exe	F-Secure ORSP Service 32-bit (Release)	Ultralight\ulcore\%ld\
fshoster64.exe	F-Secure plugin hosting service	Ultralight\ulcore\%ld\
fsulprothoster.exe	F-Secure plugin hosting service	Ultralight\ulcore\%ld\

In-memory modules present:

Name	Description	Sub Directory
spapi64.dll	F-Secure Scanning API 64-bit	Ultralight\ulcore\%ld\
fsamsi64.dll	F-Secure AMSI Client	Ultralight\ulcore\%ld\
fs_ccf_ipc_64.dll	Inter-process communication library	Ultralight\ulcore\%ld\

Functions Hooked:

N/A	N/A	N/A
-----	-----	-----

Minifilters Present:

Driver	Altitude	Type
fshs.sys	388222	FSFilter Activity Monitor
fshs.sys	388221	FSFilter Activity Monitor
fsatp.sys	388220	FSFilter Activity Monitor
fsgk.sys	322000	FSFilter Anti-Virus

Antivirus Driver	Request
fsulgk.sys	IRP MJ CREATE
fsulgk.sys	IRP MJ CLEANUP
fsulgk.sys	IRP MJ WRITE
fsulgk.sys	IRP MJ SET INFORMATION
fsulgk.sys	IRP MJ SET SECURITY
fsulgk.sys	IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	34.240.57.157	50256	443
TCP	23.199.50.97	50264	443
TCP	18.210.194.134	50310	80
TCP	18.210.194.134	50311	80

Services:

Name	Description	Startup Type	Path
F-Secure Hoster	F-Secure DLL Hoster Service	Automatic	\Anti-Virus\fsloser32.exe
F-Secure Hoster Restricted	F-Secure DLL Hoster Service	Automatic	\Anti-Virus\fsloser32.exe --service --namespace default --id 2
F-Secure UltraLight Hoster	F-Secure UltraLight Hoster	Automatic	\Ultralight\ulcore\1607432682\fsloser64.exe --service --namespace ul_default
F-Secure UltraLight Network Hoster	-	Automatic	\Ultralight\ulcore\1607432682\fsloser64.exe --service --namespace ul_default --id 2
F-Secure UltraLight ORSP Client	F-Secure UltraLight ORSP Client	Automatic	\Ultralight\ulcore\1607432682\fsorsp64.exe
F-Secure UltraLight Protected Hoster	-	Automatic	\Ultralight\ulcore\1607432682\fsulprothoster.exe" --service --namespace ul_default --id 5

Norton

Parent Directory
C:\Program Files\Norton Internet Security\

Binaries present:

Name	Description	Sub directory
NortonSecurity.exe	NortonSecurity	Engine\%ld
nsWscSvc.exe	NortonSecurity WSC Service	Engine\%ld
SYMEFASI64.sys	Symantec Extended File Attributes	C:\Windows\System32\Drivers\NGCx64\%ld
SymEvt.sys	Symantec Eventing Platform	NortonData\%ld\SymPlatform
SYMEVENT64x86.sys	Symantec Event Library	C:\Windows\System32\Drivers\
SRTSPX64.sys	Symantec Auto Protect	C:\Windows\System32\Drivers\NGCx64\%ld
SRTSP.sys	Symantec Auto Protect	C:\Windows\System32\Drivers\NGCx64\%ld

In-memory modules present:

Name	Description	Sub Directory
symamsi.dll	Symantec AMSI Provider	Engine\%ld
ccVrTrst.dll	Symantec Trust Validation Engine 64bit	Engine\%ld
ccSet.dll	Symantec Settings Manager Engine	Engine\%ld
ccLib.dll	Symantec Library	Engine\%ld
EFACli64.dll	Symantec Extended File Attributes	Engine\%ld
ccIPC.dll	Symantec ccIPC Engine	Engine\%ld
IPSEng32.dll	IPS Script Engine DLL	ProgramFile\NortonSecurity\NortonData\..\

Functions Hooked

KERNELBASE.DLL

VirtualAllocEx	CreateFileMappingW	CreateFileMappingNumaW
CreateFileW	MapViewOfFile	VirtualProtect
HeapCreate	VirtualAlloc	MapViewOfFileEx
CreateRemoteThreadEx	WriteProcessMemory	VirtualProtectEx

NTDLL.DLL

RtlAddVectoredExceptionHandler	RtlRemoveVectoredExceptionHandler	LdrLoadDll
RtlCreateHeap	NtSetInformationProcess	NtMapViewOfSection
NtWriteVirtualMemory	NtCreateSection	NtProtectVirtualMemory
NtCreateFile	NtCreateProcess	NtCreateThreadEx
NtCreateUserProcess	KiUserExceptionDispatcher	N/A

KERNEL32.DLL

CreateFileMappingA	SetProcessDEPPolicy	VirtualAlloc
MapViewOfFile	CreateFileMappingW	VirtualProtect
HeapCreate	MapViewOfFileEx	CreateRemoteThread
VirtualAllocEx	VirtualProtectEx	WriteProcessMemory
WinExec	N/A	N/A

[continued below]

Minifilters Present:

Driver	Altitude	Type
symefasi.sys	260610	FSFilter Content Screener
SRTSP.sys	329000	FSFilter Anti-Virus
symevnt.sys	365090	FSFilter Activity Monitor
bhdrv64.sys	365100	FSFilter Activity Monitor
symevnt.sys	365090	FSFilter Activity Monitor

Antivirus Driver	Request
eeCtrl64.sys	IRP_MJ_CREATE
eeCtrl64.sys	IRP_MJ_CLEANUP
eeCtrl64.sys	IRP_MJ_SET_INFORMATION
BHDrv64.sys	IRP_MJ_CREATE
BHDrv64.sys	IRP_MJ_WRITE
BHDrv64.sys	IRP_MJ_CLEANUP
BHDrv64.sys	IRP_MJ_SET_INFORMATION
BHDrv64.sys	IRP_MJ_SET_SECURITY
BHDrv64.sys	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION
BHDrv64.sys	IRP_MJ_FILE_SYSTEM_CONTROL
BHDrv64.sys	IRP_MJ_DIRECTORY_CONTROL
SymEvnt.sys	IRP_MJ_CREATE
SymEvnt.sys	IRP_MJ_WRITE
SymEvnt.sys	IRP_MJ_SET_INFORMATION
SymEvnt.sys	IRP_MJ_FILE_SYSTEM_CONTROL
SymEvnt.sys	IRP_MJ_SHUTDOWN
SymEvnt.sys	IRP_MJ_LOCK_CONTROL

Antivirus Driver	Request
SRTSP64.SYS	<u>IRP MJ CREATE</u>
SRTSP64.SYS	<u>IRP MJ CLEANUP</u>
SRTSP64.SYS	<u>IRP MJ WRITE</u>
SRTSP64.SYS	<u>IRP MJ VOLUME MOUNT</u>
SRTSP64.SYS	<u>IRP MJ PNP</u>
SRTSP64.SYS	<u>IRP MJ SET INFORMATION</u>
SRTSP64.SYS	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
SRTSP64.SYS	<u>IRP MJ RELEASE FOR SECTION SYNCHRONIZATION</u>
SRTSP64.SYS	<u>IRP MJ FILE SYSTEM CONTROL</u>
SRTSP64.SYS	<u>IRP MJ SHUTDOWN</u>
SRTSP64.SYS	<u>IRP MJ DEVICE CONTROL</u>
SYMEFASI64.SYS	<u>IRP MJ CREATE</u>
SYMEFASI64.SYS	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
SYMEFASI64.SYS	<u>IRP MJ SHUTDOWN</u>
SYMEFASI64.SYS	<u>IRP MJ WRITE</u>
SYMEFASI64.SYS	<u>IRP MJ CLEANUP</u>
SYMEFASI64.SYS	<u>IRP MJ CLOSE</u>
SYMEFASI64.SYS	<u>IRP MJ FILE SYSTEM CONTROL</u>
SYMEFASI64.SYS	<u>IRP MJ DEVICE CONTROL</u>
SYMEFASI64.SYS	<u>IRP MJ PNP</u>
SYMEFASI64.SYS	<u>IRP MJ SET INFORMATION</u>

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	52.234.240.1	59882	443

Services:

Name	Description	Startup Type	Path
Norton Security	Norton Security	Automatic	\Engine\%ld\NortonSecurity.exe
Norton WSC Service	Norton WSC Service	Automatic	\Engine\%ld\nsWscSvc.exe

Trend Micro

Parent Directory
C:\Program Files\TrendMicro

Binaries present:

Name	Description	Sub directory
coreFrameworkHost.exe	Trend Micro Anti-Malware Solution	AMSP
uiWatchDog.exe	Trend Micro Client Session Agent Monitor	UniClient
uiSeAgnt.exe	Client Session Agent	UniClient
uiWinMgr.exe	Trend Micro Client Main Console	Titanium
Tmsalntance64.exe	Trend Micro Browser Exploit Detection Engine	AMSP
AMSPTelemetryService.exe	Trend Micro Anti-Malware Solution	AMSP
tmeyes.sys	TrendMicro Eyes driver Module	C:\Windows\System32\Drivers\
TMUMH.sys	Trend Micro UMH Driver x64	C:\Windows\System32\Drivers\
tmusa.sys	Trend Micro Osprey Scanner Driver	C:\Windows\System32\Drivers\
tmnciesc.sys	Trend Micro NCIE Scanner	C:\Windows\System32\Drivers\
TMEBC64.sys	Trend Micro early boot driver	C:\Windows\System32\Drivers\
tmeevw.sys	Trend Micro EagleEye Driver (VW)	C:\Windows\System32\Drivers\

In-memory modules present:

Name	Description	Sub Directory
TmUmEvt64.dll	Trend Micro User-Mode Hook Event Module	\System32\tmumh\20019\AddOn\8.55.0.1018
tmmon64.dll	Trend Micro UMH Monitor Engine	\System32\tmumh\20019
TmAMSIProvider64.dll	Trend Micro AMSI Provider Module	\System32\TmAMSI
TmOverlayIcon.dll	Trend Micro Folder Shield Shell Extension	Titanium

Functions Hooked

KERNELBASE.DLL

CreateFileA	CreateFileW	LoadLibraryExW
CreateFileMappingW	LoadLibraryExA	CreateRemoteThreadEx
VirtualAlloc	MapViewOfFile	VirtualProtect
HeapCreate	WriteProcessMemory	VirtualProtectEx
LoadLibraryA	LoadLibraryW	N/A

KERNEL32.DLL

CreateFileMappingA	N/A	N/A
------------------------------------	-----	-----

NTDLL.DLL

RtlCreateHeap	LdrUnloadDll	LdrUnloadDll
NtMapViewOfSection	NtUnmapViewOfSection	NtContinue
NtCreateSection	NtProtectVirtualMemory	NtCreateFile
NtSetContextThread	N/A	N/A

Minifilters Present:

Driver	Altitude	Type
tmeyes.sys	328520	FSFilter Anti-Virus

Antivirus Driver	Request
tmeyes.sys	<u>IRP MJ CREATE</u>
tmeyes.sys	<u>IRP MJ READ</u>
tmeyes.sys	<u>IRP MJ WRITE</u>
tmeyes.sys	<u>IRP MJ CLEANUP</u>
tmeyes.sys	<u>IRP MJ SET INFORMATION</u>
tmeyes.sys	<u>IRP MJ FILE SYSTEM CONTROL</u>
tmeyes.sys	<u>IRP MJ VOLUME MOUNT</u>
tmeyes.sys	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
tmeyes.sys	<u>IRP MJ SET SECURITY</u>

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	104.108.237.54	58495	443
TCP	23.35.33.60	58672	443

Services:

Name	Description	Startup Type	Path
Amsp	Trend Micro Solution Platform	Automatic	AMSP\coreServiceShell.exe
AMSPTLM	Trend Micro Activity Data Service	Automatic	AMSP\AMSPTelemetryService.exe

WebRoot

Parent Directory
C:\Program Files\WebRoot

Binaries present:

Name	Description	Sub directory
WRSA.exe	WebRoot Secure Anywhere	WRSA.exe
WRSkyClient.x64.exe	WebRoot Secure Anywhere	Core
WRCoreService.x64.exe	WebRoot Secure Anywhere Core Service	Core
WRCore.x64.sys	WebRoot Secure Anywhere	Core
WRkrn.sys	WebRoot Secure Anywhere	Core

In-memory modules present:

Name	Description	Sub Directory
WRusr.dll	WebRoot Secure Anywhere	C:\Windows\System32\
WRusr.dll	Webroot SecureAnywhere	C:\Windows\SysWOW64\

Functions Hooked:

ADVAPI32.DLL

OpenSCManagerW	OpenServiceW	OpenSCManagerA
StartServiceW	ControlService	CreateServiceA
CreateServiceW	DeleteService	OpenServiceA
StartServiceA	WmiExecuteMethodW	N/A

USER32.DLL

PostThreadMessageA	PostMessageA	SendMessageA
SendMessageTimeoutA	SetWindowTextA	CreateWindowExA
SetWindowsHookExA	DrawTextExW	CreateWindowExW
PostMessageW	SendMessageW	SetWindowTextW
PostThreadMessageW	SendMessageTimeoutW	SetWindowsHookExW
SetWinEventHook	SendMessageCallbackW	SendNotifyMessageW
ExitWindowsEx	MessageBoxTimeoutW	SendMessageCallbackA

KERNELBASE.DLL

OutputDebugStringA	CreateProcessInternalW	N/A
------------------------------------	--	-----

NTDLL.DLL

NtWaitForSingleObject	NtDeviceIoControlFile	NtRequestWaitReplyPort
NtOpenProcess	NtMapViewOfSection	NtTerminateProcess
NtDelayExecution	NtWriteVirtualMemory	NtOpenEvent
NtAdjustPrivilegesToken	NtQueueApcThread	NtCreateEvent
NtCreateSection	NtCreateThread	NtProtectVirtualMemory
NtTerminateThread	NtWaitForMultipleObjects	NtSetValueKey
NtAlpcConnectPort	NtAlpcCreatePort	NtAlpcCreatePortSection
NtAlpcCreateSectionView	NtAlpcSendWaitReceivePort	NtAssignProcessToJobObject
NtConnectPort	NtCreateMutant	NtCreatePort
NtCreateSemaphore	NtCreateThreadEx	NtDeleteKey
NtDeleteValueKey	NtMakeTemporaryObject	NtOpenMutant
NtOpenSemaphore	NtOpenThread	NtQueueApcThreadEx
NtRequestPort	NtSecureConnectPort	NtSetContextThread
NtShutdownSystem	NtSystemDebugControl	CsrClientCallServer

URLMON.DLL

URLDownloadToFileW	URLDownloadToFileA	N/A
------------------------------------	------------------------------------	-----

WININET.DLL

InternetOpenA	InternetCloseHandle	InternetOpenUrlA
-------------------------------	-------------------------------------	----------------------------------

GDI32.DLL

BitBlt	TextOutW	N/A
------------------------	--------------------------	-----

KERNEL32.DLL

GetTickCount	N/A	N/A
------------------------------	-----	-----

RPCRT4.DLL

RpcSend	RpcSendReceive	NdrSendReceive
---------	----------------	----------------

Minifilters Present:

Driver	Altitude	Type
WRCORE.x64.sys	320110	FSFilter Anti-Virus
WRKrn.sys	320111	FSFilter Anti-Virus

Antivirus Driver	Request
WRCORE.x64.sys	IRP_MJ_CREATE
WRCORE.x64.sys	IRP_MJ_WRITE
WRKrn.sys	IRP_MJ_CREATE
WRKrn.sys	IRP_MJ_CLEANUP
WRKrn.sys	IRP_MJ_WRITE
WRKrn.sys	IRP_MJ_SET_INFORMATION

Services:

Name	Description	Startup Type	Path
WRSVC	WRSVC	Automatic	Webroot\WRSa.exe
WRSkyClient	WRSkyClient	Automatic	Webroot\Core\WRSkyClient.exe
WRCoreService	WRCoreService	Automatic	Webroot\Core\WRCoreService.exe

BitDefender

Parent Directory
C:\Program Files\Bitdefender Antivirus Free\

Binaries present:

Name	Description	Path
atc.sys	BitDefender Active Threat Controller	C:\Windows\System32\Drivers\
gemma.sys	BitDefender Generic Exploit Mitigation	C:\Windows\System32\Drivers\
fvevol.sys	BitDefender Drive Encryption Driver	C:\Windows\System32\Drivers\
bdredline.exe	BitDefender redline update	\
vsserv.exe	BitDefender Security Service	\
vsservppl.exe	BitDefender Correlation Service	\
updatesrv.exe	BitDefender Update Service	\
bdagent.exe	BitDefender bdagent.exe	\

In-memory modules present:

Name	Description	Path
bdhkm64.dll	BitDefender Hooking DLL	bdkdm\%ld\
atcuf64.dll	BitDefender Active Threat Controller	atcuf\%ld\

Functions Hooked:

KERNELBASE.DLL

DefineDosDeviceW	CreateProcessW	CreateProcessA
CreateProcessInternalA	CreateProcessInternalW	PeekConsoleInputW
CloseHandle	DeleteFileW	OpenThread
CreateRemoteThreadEx	GetProcAddress	MoveFileWithProgressW
MoveFileExW	GetModuleBaseNameW	GetModuleInformation
GetModuleFileNameExW	EnumProcessModules	SetEnvironmentVariableW
EnumDeviceDrivers	SetEnvironmentVariableA	QueueUserAPC
GetLogicalProcessorInformationEx	LoadLibraryA	LoadLibraryW
GetLogicalProcessorInformation	GetApplicationRecoveryCallback	EnumProcessModulesEx
PeekConsoleInputA	ReadConsoleInputA	ReadConsoleInputW
GenerateConsoleCtrlEvent	ReadConsoleA	ReadConsoleW
CreateRemoteThread	N/A	N/A

COMBASE.DLL

CoCreateInstance	CoGetClassObject	N/A
----------------------------------	----------------------------------	-----

KERNEL32.DLL

Process32NextW	CreateToolhelp32Snapshot	MoveFileExA
MoveFileWithProgressA	DefineDosDeviceA	N/A

GDI32.DLL

CreateDCW	BitBlt	CreateCompatibleDC
CreateBitmap	CreateDCA	CreateCompatibleBitmap

USER32.DLL

<u>SetWindowsHookExW</u>	<u>CallNextHookEx</u>	<u>FindWindowExA</u>
<u>SendMessageA</u>	<u>PeekMessageA</u>	<u>PeekMessageW</u>
<u>GetDesktopWindow</u>	<u>SendMessageW</u>	<u>SetWindowLongW</u>
<u>GetKeyState</u>	<u>PostMessageW</u>	<u>EnumDesktopWindows</u>
<u>EnumWindows</u>	<u>GetMessageW</u>	<u>SystemParametersInfoW</u>
<u>FindWindowW</u>	<u>GetAsyncKeyState</u>	<u>SetPropW</u>
<u>FindWindowExW</u>	<u>GetDC</u>	<u>GetMessageA</u>
<u>SystemParametersInfoA</u>	<u>SendNotifyMessageW</u>	<u>SetWinEventHook</u>
<u>PostMessageA</u>	<u>UnhookWindowsHookEx</u>	<u>GetClipboardData</u>
<u>SetWindowLongA</u>	<u>SetClipboardData</u>	<u>SendNotifyMessageA</u>
<u>GetDCEX</u>	<u>GetKeyboardState</u>	<u>GetRawInputData</u>
<u>GetWindowDC</u>	<u>RegisterRawInputDevices</u>	<u>SetWindowsHookExA</u>
<u>FindWindowA</u>	<u>SetPropA</u>	N/A

NTDLL.DLL

<u>RtlImageNtHeaderEx</u>	<u>NtSetInformationThread</u>	<u>NtClose</u>
<u>NtOpenProcess</u>	<u>NtMapViewOfSection</u>	<u>NtUnmapViewOfSection</u>
<u>NtTerminateProcess</u>	<u>NtWriteVirtualMemory</u>	<u>NtDuplicateObject</u>
<u>NtReadVirtualMemory</u>	<u>NtAdjustPrivilegesToken</u>	<u>NtQueueApcThread</u>
<u>NtCreateProcessEx</u>	<u>NtCreateThread</u>	<u>NtResumeThread</u>
<u>NtAlpcConnectPort</u>	<u>NtAlpcCreatePort</u>	<u>NtAlpcSendWaitReceivePort</u>
<u>NtCreateProcess</u>	<u>NtCreateThreadEx</u>	<u>NtCreateUserProcess</u>
<u>NtQuerySystemEnvironmentValueEx</u>	<u>NtRaiseHardError</u>	<u>NtSetContextThread</u>
<u>NtSetSystemEnvironmentValueEx</u>	<u>RtlWow64SetThreadContext</u>	<u>RtlReportException</u>

Minifilters Present:

Driver	Altitude	Type
vlflt.sys	320832	FSFilter Anti-Virus
gemma.sys	320782	FSFilter Anti-Virus
Atc.sys	320781	FSFilter Anti-Virus
TRUFOS.SYS	320770	FSFilter Anti-Virus

Antivirus Driver	Request
vlflt.sys	IRP MJ CREATE
vlflt.sys	IRP MJ CLEANUP
vlflt.sys	IRP MJ SET INFORMATION
vlflt.sys	IRP MJ WRITE
vlflt.sys	IRP MJ FILE SYSTEM CONTROL
vlflt.sys	IRP MJ VOLUME MOUNT
vlflt.sys	IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION
vlflt.sys	IRP MJ DIRECTORY CONTROL
gemma.sys	IRP MJ CREATE
gemma.sys	IRP MJ CLEANUP
gemma.sys	IRP MJ SET INFORMATION
gemma.sys	IRP MJ WRITE
gemma.sys	IRP MJ READ
gemma.sys	IRP MJ QUERY INFORMATION

Antivirus Driver	Request
atc.sys	<u>IRP MJ CREATE</u>
atc.sys	<u>IRP MJ WRITE</u>
atc.sys	<u>IRP MJ CLEANUP</u>
atc.sys	<u>IRP MJ READ</u>
atc.sys	<u>IRP MJ SET INFORMATION</u>
atc.sys	<u>IRP MJ QUERY INFORMATION</u>
atc.sys	<u>IRP MJ DIRECTORY CONTROL</u>
atc.sys	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
atc.sys	<u>IRP MJ QUERY EA</u>
atc.sys	<u>IRP MJ SET EA</u>
atc.sys	<u>IRP MJ FILE SYSTEM CONTROL</u>
atc.sys	<u>IRP MJ CREATE NAMED PIPE</u>
atc.sys	<u>IRP MJ PNP</u>
TRUFOS.SYS	<u>IRP MJ CREATE</u>
TRUFOS.SYS	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>

Services:

Name	Description	Startup Type	Path
ProductAgentService	Bitdefender Product Agent Service	Automatic	ProductAgentService.exe
vsserv	Bitdefender Security Service	Automatic	vsserv.exe
vsservppl	Bitdefender Correlation Service	Automatic	vsservppl.exe
updatesrv	Bitdefender Update Service	Automatic	updatesrv.exe

MalwareBytes

Parent Directory
C:\Program Files\MalwareBytes\

Binaries present:

Name	Description	Sub directory
mwac.sys	Malwarebytes Web Protection	C:\Windows\System32\Drivers\
mbamswissarmy.sys	Malwarebytes SwissArmy	C:\Windows\System32\Drivers\
mbam.sys	Malwarebytes Real-Time Protection	C:\Windows\System32\Drivers\
MbamChameleon.sys	Malwarebytes Chameleon	C:\Windows\System32\Drivers\
farflt.sys	Malwarebytes Anti-Ransomware Protection	C:\Windows\System32\Drivers\
mbae64.sys	Malwarebytes Anti-Exploit	C:\Windows\System32\Drivers\
MBAMService.exe	Malwarebytes Service	Anti-Malware
mbamtray.exe	Malwarebytes Tray Application	Anti-Malware
mbam.exe	Malwarebytes	Anti-Malware

In-memory modules present:

Name	Description	Sub Directory
mbae.dll	MalwareBytes Anti-exploit	AntiMalware

Functions Hooked:

MSCVRT.DLL

_wsystem	system	N/A
--------------------------	------------------------	-----

WSA_32.DLL

WSAStartup	N/A	N/A
----------------------------	-----	-----

SHELL32.DLL

ShellExecuteW	ShellExecuteExW	N/A
-------------------------------	---------------------------------	-----

NTDLL.DLL

ResolveDelayLoadedAPI	GetDllHandle	CreateProcessInternalW
NtAllocateVirtualMemory	NtProtectVirtualMemory	N/A

KERNELBASE.DLL

VirtualAllocEx	CreateProcessW	CreateProcessInternalW
GetModuleHandleW	CreateFileW	LoadLibraryExW
VirtualProtect	HeapCreate	VirtualAlloc
WriteProcessMemory	CreateFileA	VirtualProtectEx
CreateProcessA	CreateProcessInternalA	N/A

URLMON.DLL

URLDownloadToFileW	URLDownloadToCacheFileA	URLDownloadToCacheFileW
URLDownloadToFileA	URLOpenBlockingStreamA	URLOpenBlockingStreamW
URLOpenStreamA	URLOpenStreamW	N/A

WININET.DLL

InternetReadFile	InternetReadFileExW	HttpOpenRequestW
HttpSendRequestW	HttpSendRequestExW	HttpSendRequestA
HttpSendRequestExA	InternetOpenUrlA	InternetOpenUrlW
HttpOpenRequestA	N/A	N/A

KERNEL32.DLL

SetProcessDEPPolicy	CopyFileA	MoveFileA
MoveFileW	CopyFileW	WinExec

Minifilters Present:

Driver	Altitude	Type
mbam.sys	328800	FSFilter Anti-Virus
mbamwatchdog.sys	400900	FSFilter Top
farwflt.sys	268150	FSFilter Activity Monitor

Antivirus Driver	Request
mbamwatchdog.sys	IRP MJ CREATE
mbamwatchdog.sys	IRP MJ SET INFORMATION
mbamwatchdog.sys	IRP MJ SET SECURITY
mbam.sys	IRP MJ CREATE
mbam.sys	IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	13.226.202.2	50364	443

Adaware

Parent Directory
C:\Program Files(x86)\adaware\adaware antivirus

Binaries present:

Name	Description	Sub directory
AdawareDesktop.exe	Adaware Desktop	\adaware antivirus\12.10.111.0
AdawareTray.exe	Adaware Tray	\adaware antivirus\12.10.111.0
AdawareService.exe	Adaware service	\adaware antivirus\12.10.111.0
atc.sys	BitDefender Active Threat Control Filesystem Minifilter	C:\Windows\System32\Drivers\
gzflt.sys	Bit Defender Gonzales Filesystem Driver	C:\Windows\System32\Drivers\

In-memory modules present:

Name	Description	Path
N/A	N/A	N/A

Functions Hooked:

N/A	N/A	N/A
-----	-----	-----

Minifilters Present:

Driver	Altitude	Type
gzflt.sys	320820	FSFilter Anti-Virus
Atc.sys	320781	FSFilter Anti-Virus
TRUFOS.SYS	320770	FSFilter Anti-Virus

Antivirus Driver	Request
TRUFOS.SYS	IRP MJ CREATE
TRUFOS.SYS	IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION
gzflt.sys	IRP MJ CREATE
gzflt.sys	IRP MJ CLEANUP
gzflt.sys	IRP MJ SET INFORMATION
gzflt.sys	IRP MJ WRITE
gzflt.sys	IRP MJ FILE SYSTEM CONTROL
gzflt.sys	IRP MJ VOLUME MOUNT
gzflt.sys	IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION
atc.sys	IRP MJ CREATE
atc.sys	IRP MJ WRITE
atc.sys	IRP MJ CLEANUP
atc.sys	IRP MJ READ
atc.sys	IRP MJ SET INFORMATION
atc.sys	IRP MJ QUERY INFORMATION
atc.sys	IRP MJ DIRECTORY CONTROL
atc.sys	IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION
atc.sys	IRP MJ QUERY EA
atc.sys	IRP MJ SET EA
atc.sys	IRP MJ FILE SYSTEM CONTROL

Services:

Name	Description	Startup Type	Path
Adaware antivirus service	Helps protect users from Malware & other potentially unwanted software	Automatic	adaware antivirus\%ld\AdAwareService.exe

Avast

Parent Directory
C:\Program Files\AvastSoftware\Avast

Binaries present:

Name	Description	Sub directory
aswArPot.sys	Avast Anti Rootkit	C:\Windows\System32\Drivers\
aswbidsdriver.sys	Avast IDS Application Activity Monitor Driver.	C:\Windows\System32\Drivers\
aswbidsh.sys	Avast Application Activity Monitor Helper Driver	C:\Windows\System32\Drivers\
aswbuniv.sys	Avast Universal Driver	C:\Windows\System32\Drivers\
aswKbd.sys	Avast Keyboard Filter Driver	C:\Windows\System32\Drivers\
aswMonFlt.sys	Avast File System Filter	C:\Windows\System32\Drivers\
aswNetHub.sys	Avast Network Security Driver	C:\Windows\System32\Drivers\
aswRdr2.sys	Avast Antivirus	C:\Windows\System32\Drivers\
aswSnx.sys	Avast Antivirus	C:\Windows\System32\Drivers\
aswSP.sys	Avast Self Protection	C:\Windows\System32\Drivers\
aswStm.sys	Avast Stream Filter	C:\Windows\System32\Drivers\
aswVmm.sys	Avast VM Monitor	C:\Windows\System32\Drivers\
wsc_proxy.exe	Avast Remediation exe	/
AvastSvc.exe	Avast Service	/
aswEngSrv.exe	Avast Antivirus engine server	/
aswToolsSvc.exe	Avast Antivirus	/
aswidsagent.exe	Avast Software Analyzer	/
AvastUI.exe	Avast Antivirus	/

In-memory modules present:

Name	Description	Sub Directory
awshook.dll	Avast Hook Library	/x86
ashShell.dll	Avast Shell Extension	/

Functions Hooked:**ADVAPI32.DLL**

CryptImportKey	LogonUserW	CryptGenKey
CryptDuplicateKey	LogonUserA	LogonUserExA
LogonUserExW	N/A	N/A

USER32.DLL

GetClipboardData	SetWindowsHookExA	SetWindowsHookExW
----------------------------------	-----------------------------------	-----------------------------------

NTDLL.DLL

RtlQueryEnvironmentVariable	LdrLoadDll	NtQueryInformationProcess
NtMapViewOfSection	NtTerminateProcess	NtOpenSection
NtWriteVirtualMemory	NtOpenEvent	NtCreateEvent
NtCreateSection	NtProtectVirtualMemory	NtResumeThread
NtCreateMutant	NtCreateSemaphore	NtCreateUserProcess
NtOpenMutant	NtOpenSemaphore	NtOpenThread
NtSuspendProcess	RtlDecompressBuffer	N/A

Minifilters Present:

Driver	Altitude	Type
aswSP.sys	388401	FSFilter Activity Monitor
aswMonFlt.sys	320700	FSFilter Anti-Virus
aswSnx.sys	137600	FSFilter Virtualization

Antivirus Driver	Request
aswSP.sys	<u>IRP MJ CREATE</u>
aswSP.sys	<u>IRP MJ CREATE NAMED PIPE</u>
aswSP.sys	<u>IRP MJ SET INFORMATION</u>
aswSP.sys	<u>IRP MJ FILE SYSTEM CONTROL</u>
aswSP.sys	<u>IRP MJ LOCK CONTROL</u>
aswSP.sys	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
aswSP.sys	<u>IRP MJ SET SECURITY</u>
aswSP.sys	<u>IRP MJ WRITE</u>
aswSP.sys	<u>IRP MJ CLOSE</u>
aswMonFlt.sys	<u>IRP MJ CREATE</u>
aswMonFlt.sys	<u>IRP MJ WRITE</u>
aswMonFlt.sys	<u>IRP MJ CLEANUP</u>
aswMonFlt.sys	<u>IRP MJ CLOSE</u>
aswMonFlt.sys	<u>IRP MJ SET INFORMATION</u>
aswMonFlt.sys	<u>IRP MJ SET SECURITY</u>
aswMonFlt.sys	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
aswMonFlt.sys	<u>IRP MJ FILE SYSTEM CONTROL</u>
aswSnx.sys	<u>IRP MJ CREATE</u>
aswSnx.sys	<u>IRP MJ NETWORK QUERY OPEN</u>
aswSnx.sys	<u>IRP MJ WRITE</u>
aswSnx.sys	<u>IRP MJ DIRECTORY CONTROL</u>
aswSnx.sys	<u>IRP MJ CLEANUP</u>
aswSnx.sys	<u>IRP MJ QUERY INFORMATION</u>
aswSnx.sys	<u>IRP MJ SET INFORMATION</u>
aswSnx.sys	<u>IRP MJ FILE SYSTEM CONTROL</u>
aswSnx.sys	<u>IRP MJ QUERY VOLUME INFORMATION</u>

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	5.45.59.36	51910	80
TCP	5.62.54.29	51911	80
TCP	5.62.53.230	52459	443
TCP	5.62.53.230	52460	443
TCP	5.62.53.212	52461	443
TCP	5.62.53.212	52462	443

[continued below]

Services:

Name	Description	Startup Type	Path
Avast Antivirus	Manages & implements Avast Antivirus services for this computer. This includes real time shields , the virus chest & the scheduler.	Automatic	\AvastSvc.exe
Avast Browser Update Service	Keep your avast software upto date.	Automatic	C:\Program Files (x86)\AVAST Software\Browser\Update\AvastBrowserUpdate.exe /svc
Avast Browser Update Service	Keeps your avast software upto date	Manual	C:\Program Files (x86)\AVAST Software\Browser\Update\AvastBrowserUpdate.exe /medsvc
Avast Secure Browser Elevation Service	-	Manual	C:\Program Files (x86)\AVAST Software\Browser\Application\%ld\elevation_service.exe
Avast Tools	Manages & implements avast tools services for the computer	Automatic	C:\Program Files\Avast Software\Avast\aswToolsSvc.exe /runassvc
AvastWsc Reporter	-	Automatic	C:\Program Files\Avast Software\Avast\wsc_proxy.exe /runassvc /rpcserver

Dr.Web

Parent Directory
C:\Program Files\DrWeb

Binaries present:

Name	Description	Sub directory
dwdg.sys	Dr.Web device Guard for Windows	C:\Windows\System32\Drivers\
spiderg3.sys	Dr.Web File System Monitor	C:\Windows\System32\Drivers\
A4B1FF85CA.sys	Dr.Web Protection for Windows	C:\program files\kmspico\temp
dwprot.sys	Dr.Web Protection for Windows	C:\Windows\System32\Drivers\
dwnetfilter.exe	Dr. Web Net Filtering Service	\
dwservice.exe	Dr. Web Control Service	\
dwantisipam.exe	Dr. Web Anti Spam	\
dwarkdameon.exe	Dr. Web Anti-Rootkit Service	\
dwscanner.exe	Dr. Web Scanner SE	\

In-memory modules present:

Name	Description	Sub Directory
drwamsi64.dll	Dr. Web AMSI	/

Functions Hooked:

See remarks at bottom	N/A	N/A
-----------------------	-----	-----

Minifilters Present:

Driver	Altitude	Type
spider3g.sys	323600	FSFilter Anti-Virus
dwprot.sys	323610	FSFilter Anti-Virus

Antivirus Driver	Request
dwdg.sys	<u>IRP MJ CREATE</u>
dwprot.sys	<u>IRP MJ CREATE</u>
dwprot.sys	<u>IRP MJ CLEANUP</u>
dwprot.sys	<u>IRP MJ CLOSE</u>
dwprot.sys	<u>IRP MJ READ</u>
dwprot.sys	<u>IRP MJ WRITE</u>
dwprot.sys	<u>IRP MJ SET INFORMATION</u>
dwprot.sys	<u>IRP MJ DEVICE CONTROL</u>
dwprot.sys	<u>IRP MJ FILE SYSTEM CONTROL</u>
dwprot.sys	<u>IRP MJ SET EA</u>
dwprot.sys	<u>IRP MJ SET SECURITY</u>
dwprot.sys	<u>IRP MJ SET EA</u>
dwprot.sys	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
spiderg3.sys	<u>IRP MJ CREATE</u>
spiderg3.sys	<u>IRP MJ FILE SYSTEM CONTROL</u>
spiderg3.sys	<u>IRP MJ WRITE</u>
spiderg3.sys	<u>IRP MJ CLEANUP</u>
spiderg3.sys	<u>IRP MJ CLOSE</u>
spiderg3.sys	<u>IRP MJ SET INFORMATION</u>
spiderg3.sys	<u>IRP MJ ACQUIRE FOR SECTION SYNCHRONIZATION</u>
spiderg3.sys	<u>IRP MJ RELEASE FOR SECTION SYNCHRONIZATION</u>
spiderg3.sys	<u>IRP MJ SHUTDOWN</u>

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	162.159.134.234	50183	443

Services:

Name	Description	Startup Type	Path
Dr.Web Control Service	Dr.Web Control Service is an essential part of Dr.Web Anti-virus! Please do not stop and do not disable it	Automatic	C:\Program Files\DrWeb\dwservice.exe --logfile="C:\ProgramData\Doctor Web\Logs\dwservice.log"
Dr.Web Net Filtering Service	Dr.Web Net Filtering Service checks incoming and outgoing traffic.	Manual	"C:\Program Files\DrWeb\dwnetfilter.exe" --ats
Dr.Web Scanning Engine	Dr.Web Scanning Engine checks your files against viruses. It is an essential part of the Dr.Web Anti-Virus! Please do not stop and do not disable it.	Manual	"C:\Program Files\Common Files\Doctor Web\Scanning Engine\dwengine.exe"

Note: Dr Web hooks functions. The functions are hooked using reflective DLL loading. Process Explorer and Process Hacker do not detect the loaded / injected DLLs. Dr Web loads 3 additional DLLs including a modified NTDLL which has no header. The modified NTDLL variant is loaded from a kernel-side component. I have not inspected this further.

Kaspersky

Parent Directory
C:\Program Files(x86)\Kaspersky Lab

Binaries present:

Name	Description	Sub directory
klupd_klif_klark.sys	Kaspersky Lab Anti-Rootkit	C:\Windows\System32\Drivers\
klupd_klif_mark.sys	Kaspersky Lab Anti-Rootkit Memory Driver	C:\Windows\System32\Drivers\
klupd_klif_arkmon.sys	Kaspersky Lab Anti-Rootkit Monitor Driver	C:\ProgramData\Kaspersky Lab\AVP21.2\
avp.exe	Kaspersky Anti-Virus	\Kaspersky Security Cloud 21.2
avpui.exe	Kaspersky Anti-Virus	\Kaspersky Security Cloud 21.2
kpm.exe	Kaspersky Password Manager	\AVP21.2\Lab
ksdeui.exe	Kaspersky Secure Connection	\Kaspersky VPN 5.2
ksde.exe	Kaspersky Secure Connection	\Kaspersky VPN 5.2
kldisk.sys	Virtual Disk	C:\Windows\System32\Drivers\
klflt.sys	Filter Core	C:\Windows\System32\Drivers\
klgse.sys	Security Extender	C:\Windows\System32\Drivers\
klhk.sys	klhk	C:\Windows\System32\Drivers\
klids.sys	Network Processor	C:\Windows\System32\Drivers\
klif.sys	Core System Interceptors	C:\Windows\System32\Drivers\
klm6.sys	Packet Network Filter	C:\Windows\System32\Drivers\
klkbdflt2.sys	Light Keyboard Device Filter	C:\Windows\System32\Drivers\
klpd.sys	Format Recognizer	C:\Windows\System32\Drivers\
kltap.sys	TAP-Windows Virtual Network Driver	C:\Windows\System32\Drivers\
klupd_klif_kimul.sys	Kaspersky Lab Anti-Rootkit Monitor Driver	C:\Windows\System32\Drivers\

In-memory modules present:

Name	Description	Sub Directory
antimalware_provider.dll	Kaspersky AntiMalwareProvider Component	Kaspersky Total Security 21.2\x64

Functions Hooked:

N/A	N/A	N/A
-----	-----	-----

Minifilters Present:

Driver	Altitude	Type
klif.sys	323600	FSFilter Anti-Virus

Antivirus Driver	Request
klif.sys	IRP_MJ_CREATE
klif.sys	IRP_MJ_CREATE_NAMED_PIPE
klif.sys	IRP_MJ_READ
klif.sys	IRP_MJ_WRITE
klif.sys	IRP_MJ_SET_INFORMATION
klif.sys	IRP_MJ_DIRECTORY_CONTROL
klif.sys	IRP_MJ_FILE_SYSTEM_CONTROL
klif.sys	IRP_MJ_DEVICE_CONTROL
klif.sys	IRP_MJ_SHUTDOWN
klif.sys	IRP_MJ_CLEANUP
klif.sys	IRP_MJ_SET_SECURITY
klif.sys	IRP_MJ_PNP
klif.sys	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION
klif.sys	IRP_MJ_VOLUME_MOUNT

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	80.239.170.149	50719	80
TCP	67.27.99.250	50800	443
TCP	67.27.99.250	50801	443
TCP	38.113.165.138	51881	443
TCP	66.110.49.116	51875	443

Services:

Name	Description	Startup Type	Path
Kaspersky Anti-Virus Service 21.2	Provides computer protection against viruses and other malware, network attacks, Internet fraud and spam.	Automatic	"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Total Security 21.2\avp.exe" -r
Kaspersky Volume Shadow Copy Service Bridge 21.2	Kaspersky Volume Shadow Copy Service Bridge	Manual	"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Total Security 21.2\x64\vssbridge64.exe"
Kaspersky VPN Secure Connection Service 5.2	Protects confidential data that the user enters on websites (such as banking card numbers or passwords for access to online banking services) and prevents theft of funds during online transactions.	Automatic	"C:\Program Files (x86)\Kaspersky Lab\Kaspersky VPN 5.2\ksde.exe" -r

Note: Kaspersky also contains a Standard Filter for Keyboard I/O

Conclusion:

As this series has grown we are now starting to see anti-viruses use an array of different technologies which can be difficult for malware authors to see. Although many rely on archaic hooking techniques, and hook archaic functionality from well-known malware techniques, many also come equipped with fairly robust file system minifilters to capture data which escape the hooks. This is evident because in the original entry in the Antivirus Artifacts series F-Secure was able to detect the keylogger placed on the machine despite not using any API hooks and also being unfamiliar with the malicious binaries MD5 hash. This robust minifilter system, coupled with static binary analysis implementations (something YARA rule-like), could prove to be a challenging adversary for malware authors.

As a final note: in this series I was unable to test these anti-viruses against the ‘Undertaker’ malware written because after the release of Antivirus Artifacts 1 most antivirus companies had flagged the file hash as malicious. The homebrew malware proof-of-concept can be viewed on VirusTotal.

Previous paper proof-of-concept IOC:

[2a419d2ddf31ee89a8deda913abf1b25d45bb0dc59a93c606756cfa66ach0791](https://www.virustotal.com/file/2a419d2ddf31ee89a8deda913abf1b25d45bb0dc59a93c606756cfa66ach0791/analysis/1544444444/)