ANTI-VIRUS ARTIFACTS II

// By ethereal__vx

Table of Contents

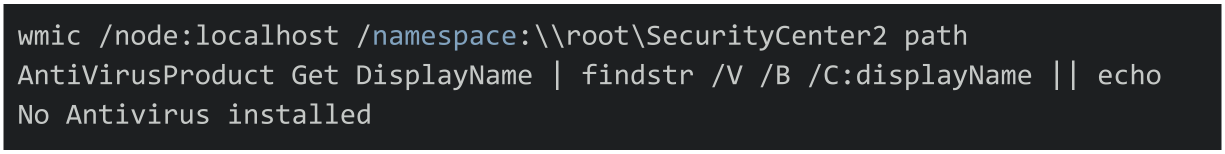
Welcome to Antivirus Artifacts II.

My initial release of Antivirus Artifacts saw quite a bit of positive feedback. Criticism I received revolved around minifilter driver documentation (or the lack thereof) and documenting the process I took to discover these artifacts. This subsequent 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.

Antivirus Artifacts I: Original text

As 2020 comes to end I have seen many anti-virus evasion methods come and go. Most notably there has been a resurgence of classic anti-hooking techniques (note the release date) which have proven to be effective against many AV and EDR systems. While this is effective a question still remains to be unanswered: if we are being hooked, who is hooking us? 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. In this paper I will document antiviral remnants: artifacts present on the machine which can indicate whether or not a security product is in place thus removing our dependency on the Windows Security Center namespace.

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

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

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
SymEvnt.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
bhdrvx64.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
BHDrvx64.sys	IRP_MJ_CREATE
BHDrvx64.sys	IRP_MJ_WRITE
BHDrvx64.sys	IRP_MJ_CLEANUP
BHDrvx64.sys	IRP_MJ_SET_INFORMATION
BHDrvx64.sys	IRP_MJ_SET_SECURITY
BHDrvx64.sys	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION
BHDrvx64.sys	IRP_MJ_FILE_SYSTEM_CONTROL
BHDrvx64.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	IRP_MJ_CREATE
SRTSP64.SYS	IRP_MJ_CLEANUP
SRTSP64.SYS	IRP_MJ_WRITE
SRTSP64.SYS	IRP_MJ_VOLUME_MOUNT
SRTSP64.SYS	IRP_MJ_PNP
SRTSP64.SYS	IRP_MJ_SET_INFORMATION
SRTSP64.SYS	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION
SRTSP64.SYS	IRP_MJ_RELEASE_FOR_SECTION_SYNCHRONIZATION
SRTSP64.SYS	IRP_MJ_FILE_SYSTEM_CONTROL
SRTSP64.SYS	IRP_MJ_SHUTDOWN
SRTSP64.SYS	IRP_MJ_DEVICE_CONTROL
SYMEFASI64.SYS	IRP_MJ_CREATE
SYMEFASI64.SYS	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION
SYMEFASI64.SYS	IRP_MJ_SHUTDOWN
SYMEFASI64.SYS	IRP_MJ_WRITE
SYMEFASI64.SYS	IRP_MJ_CLEANUP
SYMEFASI64.SYS	IRP_MJ_CLOSE
SYMEFASI64.SYS	IRP_MJ_FILE_SYSTEM_CONTROL
SYMEFASI64.SYS	IRP_MJ_DEVICE_CONTROL
SYMEFASI64.SYS	IRP_MJ_PNP
SYMEFASI64.SYS	IRP_MJ_SET_INFORMATION

Web Traffic:

Protocol	Remote Address	Local Port	Remote Port
TCP	52.234.240.1	59882	443

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	C:\Windows\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	IRP_MJ_CREATE
tmeyes.sys	IRP_MJ_READ
tmeyes.sys	IRP_MJ_WRITE
tmeyes.sys	IRP_MJ_CLEANUP
tmeyes.sys	IRP_MJ_SET_INFORMATION
tmeyes.sys	IRP_MJ_FILE_SYSTEM_CONTROL
tmeyes.sys	IRP_MJ_VOLUME_MOUNT
tmeyes.sys	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION
tmeyes.sys	IRP_MJ_SET_SECURITY

Web Traffic:

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

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	System32

DLL's present:

Name	Description	Path
WRusr.dll	Webroot SecureAnywhere	Windows\SysWOW64\WRusr.dll

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

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

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

NTDLL.DLL

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

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	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
atc.sys	IRP_MJ_CREATE_NAMED_PIPE
atc.sys	IRP_MJ_PNP
TRUFOS.SYS	IRP_MJ_CREATE
TRUFOS.SYS	IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION

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

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:
2a419d2ddf31ee89a8deda913abf1b25d45bb0dc59a93c606756cfa66acb0791