Hijack Execution Flow: DLL, Sub-technique T1574.001 - Enterprise

Archived: 2026-04-05 17:07:36 UTC

C0057 3CX Supply Chain Attack

During the 3CX Supply Chain Attack, AppleJeus splits functionally across multiple .dll files using export functions, such as DLLGetClassObject, to execute code from an embedded .dll file within another .dll file. AppleJeus has also used DLL search order hijacking via the IKEEXT service, running with LocalSystem privileges, to load the TAXHAUL DLL for persistence.[12][13]

G0073 APT19

APT19 launched an HTTP malware variant and a Port 22 malware variant using a legitimate executable that loaded the malicious DLL.[14]

G0022 APT3

APT3 has been known to side load DLLs with a valid version of Chrome with one of their tools.[15][16]

G0050 APT32

APT32 ran legitimately-signed executables from Symantec and McAfee which load a malicious DLL. The group also side-loads its backdoor by dropping a library and a legitimate, signed executable (AcroTranscoder).[17][18][19]

G0096 APT41

APT41 has used search order hijacking to execute malicious payloads, such as Winnti for Windows.[20] APT41 has also used legitimate executables to perform DLL side-loading of their malware.[21]

C0040 APT41 DUST

APT41 DUST involved the use of DLL search order hijacking to execute DUSTTRAP.[22] APT41 DUST used also DLL side-loading to execute DUSTTRAP via an AhnLab uninstaller.[22]

G0143 Aquatic Panda

Aquatic Panda has used DLL search-order hijacking to load `exe`, `dll`, and `dat` files into memory.[23] Aquatic Panda loaded a malicious DLL into the legitimate Windows Security Health Service executable (`SecurityHealthService.exe`) to execute malicious code on victim systems.[24]

S0373 Astaroth

Astaroth can launch itself via DLL Search Order Hijacking.[25]

G0135 BackdoorDiplomacy

BackdoorDiplomacy has executed DLL search order hijacking.[26]

S0128 BADNEWS

BADNEWS typically loads its DLL file into a legitimate signed Java or VMware executable.[27][28]

S0127 BBSRAT

DLL side-loading has been used to execute BBSRAT through a legitimate Citrix executable, ssonsvr.exe. The Citrix executable was dropped along with BBSRAT by the dropper.[29]

G0098 BlackTech

BlackTech has used DLL side loading by giving DLLs hardcoded names and placing them in searched directories.[30]

S1226 BOOKWORM

BOOKWORM has used DLL side-loading to execute the malicious payload. [31][32] BOOKWORM has also side-loaded DLL components into a legitimate process, including Microsoft Malware Protection `MsMpEng.exe` and Kaspersky Anti-Virus `ushata.exe`.[33]

S0415 BOOSTWRITE

BOOSTWRITE has exploited the loading of the legitimate Dwrite.dll file by actually loading the gdi library, which then loads the gdiplus library and ultimately loads the local Dwrite dll.[34]

G0060 BRONZE BUTLER

BRONZE BUTLER has used legitimate applications to side-load malicious DLLs.[35]

S1063 Brute Ratel C4

Brute Ratel C4 has used search order hijacking to load a malicious payload DLL as a dependency to a benign application packaged in the same ISO.[36] Brute Ratel C4 has loaded a malicious DLL by spoofing the name of the legitimate Version.DLL and placing it in the same folder as the digitally-signed Microsoft binary OneDriveUpdater.exe.[36]

S1237 CANONSTAGER

CANONSTAGER has abused legitimate executables to side-load malicious DLLs.[37]

S0631 Chaes

Chaes has used search order hijacking to load a malicious DLL.[38]

G0114 Chimera

Chimera has used side loading to place malicious DLLs in memory.[39]

S1041 Chinoxy

Chinoxy can use a digitally signed binary ("Logitech Bluetooth Wizard Host Process") to load its dll into memory.[40]

G1021 Cinnamon Tempest

Cinnamon Tempest has used search order hijacking to launch Cobalt Strike Beacons.[41][42] Cinnamon Tempest has also abused legitimate executables to side-load weaponized DLLs.[43]

S1236 CLAIMLOADER

CLAIMLOADER has used a legitimately signed executable to execute a malicious payload within a DLL file.[44]

S0660 Clambling

Clambling can store a file named `mpsvc.dll`, which opens a malicious `mpsvc.mui` file, in the same folder as the legitimate Microsoft executable `MsMpEng.exe` to gain execution.[45][46]

S1235 CorKLOG

CorKLOG has leveraged legitimate binaries to conduct DLL side-loading.[47]

S0538 Crutch

Crutch can persist via DLL search order hijacking on Google Chrome, Mozilla Firefox, or Microsoft OneDrive.[48]

G1034 Daggerfly

Daggerfly has used legitimate software to side-load PlugX loaders onto victim systems.[49] Daggerfly is also linked to multiple other instances of side-loading for initial loading activity.[50]

S1111 DarkGate

DarkGate includes one infection vector that leverages a malicious "KeyScramblerE.DLL" library that will load during the execution of the legitimate KeyScrambler application.[51]

S0354 Denis

Denis exploits a security vulnerability to load a fake DLL and execute its code.[17]

S0134 Downdelph

Downdelph uses search order hijacking of the Windows executable sysprep.exe to escalate privileges.[52]

S0384 Dridex

Dridex can abuse legitimate Windows executables to side-load malicious DLL files.[53]

G1006 Earth Lusca

Earth Lusca has placed a malicious payload in `%WINDIR%\SYSTEM32\oci.dll` so it would be sideloaded by the MSDTC service.[54]

S0624 Ecipekac

Ecipekac can abuse the legitimate application policytool.exe to load a malicious DLL.[55]

S0554 Egregor

Egregor has used DLL side-loading to execute its payload.[56]

S0363 Empire

Empire contains modules that can discover and exploit various DLL hijacking opportunities.[57]

G0120 Evilnum

Evilnum has used the malware variant, TerraTV, to load a malicious DLL placed in the TeamViewer directory, instead of the original Windows DLL located in a system folder.[58]

G1016 FIN13

FIN13 has used IISCrack.dll as a side-loading technique to load a malicious version of httpodbc.dll on old IIS Servers (CVE-2001-0507).[59]

S0182 FinFisher

FinFisher uses DLL side-loading to load malicious programs.[60][61] A FinFisher variant also uses DLL search order hijacking.[60][62]

S0661 FoggyWeb

FoggyWeb's loader has used DLL Search Order Hijacking to load malicious code instead of the legitimate `version.dll` during the `Microsoft.IdentityServer.ServiceHost.exe` execution process.[63]

G0093 GALLIUM

GALLIUM used DLL side-loading to covertly load PoisonIvy into memory on the victim machine.[64]

S0032 gh0st RAT

A gh0st RAT variant has used DLL side-loading.[65]

S0477 Goopy

Goopy has the ability to side-load malicious DLLs with legitimate applications from Kaspersky, Microsoft, and Google.[18]

G0126 Higaisa

Higaisa's JavaScript file used a legitimate Microsoft Office 2007 package to side-load the `OINFO12.OCX` dynamic link library.[66]

S0009 Hikit

Hikit has used DLL to load `oci.dll` as a persistence mechanism.[67]

S1230 HIUPAN

HIUPAN has abused legitimate executables to side-load malicious DLLs to include the legitimate exe UsbConfig.exe.[68][69]

S0070 HTTPBrowser

HTTPBrowser abuses the Windows DLL load order by using a legitimate Symantec anti-virus binary, VPDN_LU.exe, to load a malicious DLL that mimics a legitimate Symantec DLL, navlu.dll.[70] HTTPBrowser has also used DLL side-loading.[71]

S1097 HUI Loader

HUI Loader can be deployed to targeted systems via legitimate programs that are vulnerable to DLL search order hijacking.[42]

S0398 HyperBro

HyperBro has used a legitimate application to sideload a DLL to decrypt, decompress, and run a payload.[72][73]

S0260 InvisiMole

InvisiMole can be launched by using DLL search order hijacking in which the wrapper DLL is placed in the same folder as explorer.exe and loaded during startup into the Windows Explorer process instead of the legitimate library.[74]

S0528 Javali

Javali can use DLL side-loading to load malicious DLLs into legitimate executables.[25]

S0585 Kerrdown

Kerrdown can use DLL side-loading to load malicious DLLs.[75]

G0032 Lazarus Group

Lazarus Group has replaced `win_fw.dll`, an internal component that is executed during IDA Pro installation, with a malicious DLL to download and execute a payload.[76] Lazarus Group utilized DLL side-loading to execute malicious payloads through abuse of the legitimate processes `wsmprovhost.exe` and `dfrgui.exe`.[77]

S1101 LoFiSe

LoFiSe has been executed as a file named DsNcDiag.dll through side-loading.[78]

S0582 LookBack

LookBack side loads its communications module as a DLL into the `libcurl.dll` loader.[79]

G1014 LuminousMoth

LuminousMoth has used legitimate executables such as `winword.exe` and `igfxem.exe` to side-load their malware.[80][81]

S1213 Lumma Stealer

Lumma Stealer has leveraged legitimate applications to then side-load malicious DLLs during execution.[82]

S0530 Melcoz

Melcoz can use DLL hijacking to bypass security controls.[25]

G0045 menuPass

menuPass has used DLL side-loading to launch versions of Mimikatz and PwDump6 as well as UPPERCUT.[83][84][85] menuPass has also used DLL search order hijacking.[86]

S1059 metaMain

metaMain can support an HKCMD sideloading start method.[87]

S0455 Metamorfo

Metamorfo has side-loaded its malicious DLL file.[88][89][90]

S0280 MirageFox

MirageFox is likely loaded via DLL hijacking into a legitimate McAfee binary.[91]

G0069 MuddyWater

MuddyWater maintains persistence on victim networks through side-loading dlls to trick legitimate programs into running malware.[92]

G0129 Mustang Panda

Mustang Panda has used a legitimately signed executable to execute a malicious payload within a DLL file.[93][94][95][31][96][97][98][99][100][101][33][102][47][103] Mustang Panda has abused legitimate executables to side-load malicious DLLs.[104][105][44][68][37]

G0019 Naikon

Naikon has used DLL side-loading to load malicious DLL's into legitimate executables.[106]

S0630 Nebulae

Nebulae can use DLL side-loading to gain execution.[107]

S1100 Ninja

Ninja loaders can be side-loaded with legitimate and signed executables including the VLC.exe media player.[78]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the legitimate Windows services `IKEEXT` and `PrintNotify` to side-load malicious DLLs.[108]

S1233 PAKLOG

PAKLOG has leveraged legitimate binaries to conduct DLL side-loading.[47]

S0664 Pandora

Pandora can use DLL side-loading to execute malicious payloads.[73]

G0040 Patchwork

A Patchwork .dll that contains BADNEWS is loaded and executed using DLL side-loading.[109]

S1102 Pcexter

Pcexter has been distributed and executed as a DLL file named Vspmsg.dll via DLL side-loading.[78]

S0013 PlugX

PlugX has the ability to use DLL search order hijacking for installation on targeted systems.[110][102] PlugX has also used DLL side-loading to evade anti-virus.[16][71][111][83][112][45][113] PlugX has also used a legitimately signed executable to side-load a malicious payload within a DLL file.[93][95][96][102][114]

S0194 PowerSploit

PowerSploit contains a collection of Privesc-PowerUp modules that can discover and exploit DLL hijacking opportunities in services and processes.[115][116]

S1046 PowGoop

PowGoop can side-load `Goopdate.dll` into `GoogleUpdate.exe`.[92][117]

S0113 Prikormka

Prikormka uses DLL search order hijacking for persistence by saving itself as ntshrui.dll to the Windows directory so it will load before the legitimate ntshrui.dll saved in the System32 subdirectory.[118]

S1228 PUBLOAD

PUBLOAD has abused legitimate executables to side-load malicious DLLs.[95][104][105][68][100][32][119]

S0650 QakBot

QakBot has the ability to use DLL side-loading for execution.[120]

S0629 RainyDay

RainyDay can use side-loading to run malicious executables.[107]

S0458 Ramsay

Ramsay can hijack outdated Windows application dependencies with malicious versions of its own DLL payload.[121]

S1130 Raspberry Robin

Raspberry Robin can use legitimate, signed EXE files paired with malicious DLL files to load and run malicious payloads while bypassing defenses.[122]

S0662 RCSession

RCSession can be installed via DLL side-loading.[123][45][113]

C0047 RedDelta Modified PlugX Infection Chain Operations

Mustang Panda used DLL search order hijacking on vulnerable applications to install PlugX payloads during RedDelta Modified PlugX Infection Chain Operations.[124]

S0153 RedLeaves

RedLeaves is launched through use of DLL search order hijacking to load a malicious dll.[125]

G0048 RTM

RTM has used search order hijacking to force TeamViewer to load a malicious DLL.[126]

S0074 Sakula

Sakula uses DLL side-loading, typically using a digitally signed sample of Kaspersky Anti-Virus (AV) 6.0 for Windows Workstations or McAfee's Outlook Scan About Box to load malicious DLL files.[127]

G1008 SideCopy

SideCopy has used a malicious loader DLL file to execute the `credwiz.exe` process and side-load the malicious payload `Duser.dll`.[128]

G0121 Sidewinder

Sidewinder has used DLL side-loading to drop and execute malicious payloads including the hijacking of the legitimate Windows application file rekeywiz.exe.[129]

S1232 SplatDropper

SplatDropper has leveraged legitimate binaries to conduct DLL side-loading.[47]

S1227 StarProxy

StarProxy has been side-loaded by the legitimate, signed executable, IsoBurner.exe. [103]

G1046 Storm-1811

Storm-1811 has deployed a malicious DLL (7z.DLL) that is sideloaded by a modified, legitimate installer (7zG.exe) when that installer is executed with an additional command line parameter of `b` at runtime to load a Cobalt Strike beacon payload.[130]

S1183 StrelaStealer

StrelaStealer has sideloaded a DLL payload using a renamed, legitimate `msinfo32.exe` executable.[131]

S0663 SysUpdate

SysUpdate can load DLLs through vulnerable legitimate executables.[73]

S0098 T9000

During the T9000 installation process, it drops a copy of the legitimate Microsoft binary igfxtray.exe. The executable contains a side-loading weakness which is used to load a portion of the malware.[132]

G0027 Threat Group-3390

Threat Group-3390 has performed DLL search order hijacking to execute their payload.[133] Threat Group-3390 has also used DLL side-loading, including by using legitimate Kaspersky antivirus variants as well as `rc.exe`, a

legitimate Microsoft Resource Compiler.[71][134][135][72][136]

S1239 TONESHELL

TONESHELL has abused legitimate executables to side-load malicious DLLs.[104][137][98][99][100][138] TONESHELL has also been loaded via DLL side-loading, using legitimate, signed executables to include: FastVD.exe, Bandizip.exe and gpgconf.exe.[103]

G0131 Tonto Team

Tonto Team abuses a legitimate and signed Microsoft executable to launch a malicious DLL.[139]

G0081 Tropic Trooper

Tropic Trooper has been known to side-load DLLs using a valid version of a Windows Address Book and Windows Defender executable with one of their tools.[140][141]

G1047 Velvet Ant

Velvet Ant has used malicious DLLs executed via legitimate EXE files through DLL search order hijacking to launch follow-on payloads such as PlugX.[142]

S0612 WastedLocker

WastedLocker has performed DLL hijacking before execution.[143]

S0579 Waterbear

Waterbear has used DLL side loading to import and load a malicious DLL loader.[30]

S0109 WEBC2

Variants of WEBC2 achieve persistence by using DLL search order hijacking, usually by copying the DLL file to `%SYSTEMROOT%` (`C:\WINDOWS\ntshrui.dll`).[144]

G0107 Whitefly

Whitefly has used search order hijacking to run the loader Vcrodat.[145]

S0176 Wingbird

Wingbird side loads a malicious file, sspisrv.dll, in part of a spoofed lssas.exe service.[146][147]

S0230 ZeroT

ZeroT has used DLL side-loading to load malicious payloads.[148][149]

Source: https://attack.mitre.org/techniques/T1574/001