Process Injection: Process Hollowing, Sub-technique T1055.012 - Enterprise

Archived: 2026-04-05 14:35:58 UTC

S0331 Agent Tesla

Agent Tesla has used process hollowing to create and manipulate processes through sections of unmapped memory by reallocating that space with its malicious code.[3]

S0373 Astaroth

Astaroth can create a new process in a suspended state from a targeted legitimate process in order to unmap its memory and replace it with malicious code.[4][5]

S0344 Azorult

Azorult can decrypt the payload into memory, create a new suspended process of itself, then inject a decrypted payload to the new process and resume new process execution.[6]

S0128 BADNEWS

BADNEWS has a command to download an .exe and use process hollowing to inject it into a new process.[7][8]

S0234 Bandook

Bandook has been launched by starting iexplore.exe and replacing it with Bandook's payload.[9][10][11]

S0534 Bazar

Bazar can inject into a target process including Svchost, Explorer, and cmd using process hollowing.[12][13]

S0127 BBSRAT

BBSRAT has been seen loaded into msiexec.exe through process hollowing to hide its execution.[14]

G1043 BlackByte

BlackByte used process hollowing for defense evasion purposes.[15]

S0660 Clambling

Clambling can execute binaries through process hollowing.[16]

S0154 Cobalt Strike

Cobalt Strike can use process hollowing for execution.[17][18]

S1111 DarkGate

DarkGate leverages process hollowing techniques to evade detection, such as decrypting the content of an encrypted PE file and injecting it into the process vbc.exe.[19][20]

S0354 Denis

Denis performed process hollowing through the API calls CreateRemoteThread, ResumeThread, and Wow64SetThreadContext.[21]

S0567 Dtrack

Dtrack has used process hollowing shellcode to target a predefined list of processes from `%SYSTEM32%`.[22]

S0038 Duqu

Duqu is capable of loading executable code via process hollowing.[23]

S0367 Emotet

Emotet uses a copy of `certutil.exe` stored in a temporary directory for process hollowing, starting the program in a suspended state before loading malicious code.[24]

S1138 Gootloader

Gootloader can inject its Delphi executable into ImagingDevices.exe using a process hollowing technique.[25][26]

G0078 Gorgon Group

Gorgon Group malware can use process hollowing to inject one of its trojans into another process.[27]

S0483 IcedID

IcedID can inject a Cobalt Strike beacon into cmd.exe via process hallowing.[28]

S0189 ISMInjector

ISMInjector hollows out a newly created process RegASM.exe and injects its payload into the hollowed process.[29]

G0094 Kimsuky

Kimsuky has used a file injector DLL to spawn a benign process on the victim's system and inject the malicious payload into it via process hollowing.[30]

S0447 Lokibot

Lokibot has used process hollowing to inject itself into legitimate Windows process.[31][32]

S1213 Lumma Stealer

Lumma Stealer has used process hollowing leveraging a legitimate program such as "BitLockerToGo.exe" to inject a malicious payload.[33]

G0045 menuPass

menuPass has used process hollowing in iexplore.exe to load the RedLeaves implant.[34]

S0198 NETWIRE

The NETWIRE payload has been injected into benign Microsoft executables via process hollowing.[35][36]

S0229 Orz

Some Orz versions have an embedded DLL known as MockDll that uses process hollowing and Regsvr32 to execute another payload.[37]

G0040 Patchwork

A Patchwork payload uses process hollowing to hide the UAC bypass vulnerability exploitation inside svchost.exe.[38]

S0650 QakBot

QakBot can use process hollowing to execute its main payload.[39]

S1130 Raspberry Robin

Raspberry Robin will execute a legitimate process, then suspend it to inject code for a Tor client into the process, followed by resumption of the process to enable Tor client execution.[40]

S0662 RCSession

RCSession can launch itself from a hollowed svchost.exe process.[41][16][42]

S1018 Saint Bot

The Saint Bot loader has used API calls to spawn `MSBuild.exe` in a suspended state before injecting the decrypted Saint Bot binary into it.[43]

S0226 Smoke Loader

Smoke Loader spawns a new copy of c:\windows\syswow64\explorer.exe and then replaces the executable code in memory with malware.[44][45]

S1086 Snip3

Snip3 can use RunPE to execute malicious payloads within a hollowed Windows process.[46][47]

G1018 TA2541

TA2541 has used process hollowing to execute CyberGate malware.[48]

G0027 Threat Group-3390

A Threat Group-3390 tool can spawn `svchost.exe` and inject the payload into that process.[49][50]

S0266 TrickBot

TrickBot injects into the svchost.exe process.[51][52][53][54]

S0386 Ursnif

Ursnif has used process hollowing to inject into child processes.[55]

S0689 WhisperGate

WhisperGate has the ability to inject its fourth stage into a suspended process created by the legitimate Windows utility `InstallUtil.exe`.[56][57]

S1065 Woody RAT

Woody RAT can create a suspended notepad process and write shellcode to delete a file into the suspended process using `NtWriteVirtualMemory`.[58]

S1207 XLoader

XLoader uses process hollowing by injecting itself into the `explorer.exe` process and other files ithin the Windows `SysWOW64` directory.[59][60][61]
