Process Injection, Technique T1055 - Enterprise

Archived: 2026-04-05 17:54:13 UTC

C0028 2015 Ukraine Electric Power Attack

During the 2015 Ukraine Electric Power Attack, Sandworm Team loaded BlackEnergy into svchost.exe, which then launched iexplore.exe for their C2. [1]

C0057 3CX Supply Chain Attack

During the 3CX Supply Chain Attack, AppleJeus's VEILEDSIGNAL uses process injection to inject the C2 communication module code in the first found process instance of Chrome, Firefox, or Edge web browsers. It also monitors the established named pipe and re-injects the C2 communication module if necessary.[2]

S0469 ABK

ABK has the ability to inject shellcode into svchost.exe.[3]

S0331 Agent Tesla

Agent Tesla can inject into known, vulnerable binaries on targeted hosts.[4]

S1074 ANDROMEDA

ANDROMEDA can inject into the `wuauclt.exe` process to perform C2 actions.[5]

G0050 APT32

APT32 malware has injected a Cobalt Strike beacon into Rundll32.exe.[6]

G0067 APT37

APT37 injects its malware variant, ROKRAT, into the cmd.exe process.[7]

G0082 APT38

APT38 has injected malicious payloads into the `explorer.exe` process.[8]

G0096 APT41

APT41 malware TIDYELF loaded the main WINTERLOVE component by injecting it into the iexplore.exe process.[9]

G1023 APT5

APT5 has used the CLEANPULSE utility to insert command line strings into a targeted process to alter its functionality.[10]

C0046 ArcaneDoor

ArcaneDoor included injecting code into the AAA and Crash Dump processes on infected Cisco ASA devices.[11]

S0438 Attor

Attor's dispatcher can inject itself into running processes to gain higher privileges and to evade detection.[12]

S0347 AuditCred

AuditCred can inject code from files to other running processes.[13]

S0473 Avenger

Avenger has the ability to inject shellcode into svchost.exe.[3]

S0093 Backdoor.Oldrea

Backdoor.Oldrea injects itself into explorer.exe.[14][15]

S1081 BADHATCH

BADHATCH can inject itself into an existing explorer.exe process by using `RtlCreateUserThread`.[16][17]

S0534 Bazar

Bazar can inject code through calling `VirtualAllocExNuma`.[18]

S0470 BBK

BBK has the ability to inject shellcode into svchost.exe.[3]

G1043 BlackByte

BlackByte has injected Cobalt Strike into `wuauclt.exe` during intrusions.[19] BlackByte has injected ransomware into `svchost.exe` before encryption.[20]

S1181 BlackByte 2.0 Ransomware

BlackByte 2.0 Ransomware injects into a newly-created `svchost.exe` process prior to device encryption.[21]

S1039 Bumblebee

Bumblebee can inject code into multiple processes on infected endpoints.[22]

S0348 Cardinal RAT

Cardinal RAT injects into a newly spawned process created from a native Windows executable.[23]

S0660 Clambling

Clambling can inject into the `svchost.exe` process for execution.[24]

S1105 COATHANGER

COATHANGER includes a binary labeled `authd` that can inject a library into a running process and then hook an existing function within that process with a new function from that library.[25]

G0080 Cobalt Group

Cobalt Group has injected code into trusted processes.[26]

S0154 Cobalt Strike

Cobalt Strike can inject a variety of payloads into processes dynamically chosen by the adversary.[27][28][29]

S0614 CostaBricks

CostaBricks can inject a payload into the memory of a compromised host.[30]

C0029 Cutting Edge

During Cutting Edge, threat actors used malicious SparkGateway plugins to inject shared objects into web process memory on compromised Ivanti Secure Connect VPNs to enable deployment of backdoors.[31]

S0695 Donut

Donut includes a subproject `DonutTest` to inject shellcode into a target process.[32]

S1159 DUSTTRAP

DUSTTRAP compromises the `.text` section of a legitimate system DLL in `%windir%` to hold the contents of retrieved plug-ins.[33]

S0024 Dyre

Dyre has the ability to directly inject its code into the web browser process.[34]

S0554 Egregor

Egregor can inject its payload into iexplore.exe process.[35]

S0363 Empire

Empire contains multiple modules for injecting into processes, such as `Invoke-PSInject`.[36]

G0047 Gamaredon Group

Gamaredon Group has injected Remcos into explorer.exe.[37]

S0168 Gazer

Gazer injects its communication module into an Internet accessible process through which it performs C2.[38][39]

S0032 gh0st RAT

gh0st RAT can inject malicious code into process created by the "Command_Create&Inject" function.[40]

S0561 GuLoader

GuLoader has the ability to inject shellcode into a donor processes that is started in a suspended state. GuLoader has previously used RegAsm as a donor process.[41]

S0376 HOPLIGHT

HOPLIGHT has injected into running processes.[42]

S0040 HTRAN

HTRAN can inject into into running processes.[43]

S0398 HyperBro

HyperBro can run shellcode it injects into a newly created process.[44]

S0260 InvisiMole

InvisiMole can inject itself into another process to avoid detection including use of a technique called ListPlanting that customizes the sorting algorithm in a ListView structure.[45]

S0581 IronNetInjector

IronNetInjector can use an IronPython scripts to load a .NET injector to inject a payload into its own or a remote process.[46]

S0044 JHUHUGIT

JHUHUGIT performs code injection injecting its own functions to browser processes.[47][48]

S0201 JPIN

JPIN can inject content into lsass.exe to load a module.[49]

G0094 Kimsuky

Kimsuky has used Win7Elevate to inject malicious code into explorer.exe.[50]

S0681 Lizar

Lizar can migrate the loader into another process.[51]

S1059 metaMain

metaMain can inject the loader file, Speech02.db, into a process.[52]

S0084 Mis-Type

Mis-Type has been injected directly into a running process, including `explorer.exe`.[53]

S1122 Mispadu

Mispadu's binary is injected into memory via `WriteProcessMemory`.[54][55]

S0247 NavRAT

NavRAT copies itself into a running Internet Explorer process to evade detection.[56]

S0198 NETWIRE

NETWIRE can inject code into system processes including notepad.exe, svchost.exe, and vbc.exe.[57]

S1100 Ninja

Ninja has the ability to inject an agent module into a new process and arbitrary shellcode into running processes.[58][59]

C0013 Operation Sharpshooter

During Operation Sharpshooter, threat actors leveraged embedded shellcode to inject a downloader into the memory of Word.[60]

C0014 Operation Wocao

During Operation Wocao, threat actors injected code into a selected process, which in turn launches a command as a child process of the original.[61]

S0664 Pandora

Pandora can start and inject code into a new `svchost` process.[62]

S1050 PcShare

The PcShare payload has been injected into the `logagent.exe` and `rdpclip.exe` processes.[63]

G0068 PLATINUM

PLATINUM has used various methods of process injection including hot patching.[49]

S0378 PoshC2

PoshC2 contains multiple modules for injecting into processes, such as `Invoke-PSInject`.[64]

S0650 QakBot

QakBot can inject itself into processes including explore.exe, Iexplore.exe, Mobsync.exe., and wermgr.exe.[65][66][67][68][69]

C0056 RedPenguin

During RedPenguin, UNC3886 exploited CVE-2025-21590 to enable malicious code injection into the memory of legitimate processes.[70][71]

S0332 Remcos

Remcos has a command to hide itself through injecting into another process.[72]

S0496 REvil

REvil can inject itself into running processes on a compromised host.[73]

S0240 ROKRAT

ROKRAT can use `VirtualAlloc`, `WriteProcessMemory`, and then `CreateRemoteThread` to execute shellcode within the address space of `Notepad.exe`.[74]

S0446 Ryuk

Ryuk has injected itself into remote processes to encrypt files using a combination of `VirtualAlloc`, `WriteProcessMemory`, and `CreateRemoteThread`.[75]

S0596 ShadowPad

ShadowPad has injected an install module into a newly created process.[76]

G0091 Silence

Silence has injected a DLL library containing a Trojan into the fwmain32.exe process.[77]

S0692 SILENTTRINITY

SILENTTRINITY can inject shellcode directly into Excel.exe or a specific process.[78]

S0633 Sliver

Sliver includes multiple methods to perform process injection to migrate the framework into other, potentially privileged processes on the victim machine.[79][80][81][82]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA can inject into running processes on a compromised host.[83]

S0226 Smoke Loader

Smoke Loader injects into the Internet Explorer process.[84]

S0380 StoneDrill

StoneDrill has relied on injecting its payload directly into the process memory of the victim's preferred browser.[85]

G1018 TA2541

TA2541 has injected malicious code into legitimate .NET related processes including regsvcs.exe, msbuild.exe, and installutil.exe.[86][87]

S0266 TrickBot

TrickBot has used `Nt*` Native API functions to inject code into legitimate processes such as `wermgr.exe`.[88]

S0436 TSCookie

TSCookie has the ability to inject code into the svchost.exe, iexplorer.exe, explorer.exe, and default browser processes.[89]

G0010 Turla

Turla has also used PowerSploit's `Invoke-ReflectivePEInjection.ps1` to reflectively load a PowerShell payload into a random process on the victim system.[90]

G1047 Velvet Ant

Velvet Ant initial execution included launching multiple `svchost` processes and injecting code into them.[91]

S0670 WarzoneRAT

WarzoneRAT has the ability to inject malicious DLLs into a specific process for privilege escalation.[92]

S0579 Waterbear

Waterbear can inject decrypted shellcode into the LanmanServer service.[93]

S0206 Wiarp

Wiarp creates a backdoor through which remote attackers can inject files into running processes.[94]

S0176 Wingbird

Wingbird performs multiple process injections to hijack system processes and execute malicious code.[95]

G0102 Wizard Spider

Wizard Spider has used process injection to execute payloads to escalate privileges.[96]

S1065 Woody RAT

Woody RAT can inject code into a targeted process by writing to the remote memory of an infected system and then create a remote thread.[97]
