LOLBAS

Archived: 2026-04-06 00:47:26 UTC

AddinUtil.exe

Execute (.NetObjects)

Binaries

T1218: System Binary Proxy Execution

AppInstaller.exe

Download (INetCache)

Binaries

T1105: Ingress Tool Transfer

Aspnet_Compiler.exe

AWL bypass

Binaries

T1127: Trusted Developer Utilities Proxy Execution

At.exe

Execute (CMD)

Binaries

T1053.002: At

Atbroker.exe

Execute (EXE)

Binaries

T1218: System Binary Proxy Execution

Bash.exe

Execute (CMD)

AWL bypass (CMD)

Binaries

T1202: Indirect Command Execution

T1218: System Binary Proxy Execution

Bitsadmin.exe

Alternate data streams

Download

Copy

Execute

Binaries

T1564.004: NTFS File Attributes

T1105: Ingress Tool Transfer

T1218: System Binary Proxy Execution

CertOC.exe

Execute (DLL)

Download

Binaries

T1218: System Binary Proxy Execution

T1105: Ingress Tool Transfer

CertReq.exe

Download

Upload

Binaries

T1105: Ingress Tool Transfer

Certutil.exe

Download (GUI)

Alternate data streams

Encode

Decode

Binaries

T1105: Ingress Tool Transfer

T1564.004: NTFS File Attributes

T1027.013: Encrypted/Encoded File

T1140: Deobfuscate/Decode Files or Information

Change.exe

Execute (EXE, Rename)

Binaries

T1218: System Binary Proxy Execution

Cipher.exe

Tamper

Binaries

T1485: Data Destruction

T1562: Impair Defenses

Cmd.exe

Alternate data streams

Download

Upload

Binaries

T1564.004: NTFS File Attributes

T1059.003: Windows Command Shell

T1105: Ingress Tool Transfer

T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol

Cmdkey.exe

Credentials

Binaries

T1078: Valid Accounts

cmdl32.exe

Download

Binaries

T1105: Ingress Tool Transfer

Cmstp.exe

Execute (INF, DLL, Registry Change)

AWL bypass (INF, Remote)

Binaries

T1218.003: CMSTP

Colorcpl.exe

Copy

Binaries

T1036.005: Match Legitimate Resource Name or Location

ComputerDefaults.exe

UAC bypass

Binaries

T1548.002: Bypass User Account Control

ConfigSecurityPolicy.exe

Upload

Download (INetCache)

Binaries

T1567: Exfiltration Over Web Service

T1105: Ingress Tool Transfer

Conhost.exe

Execute (CMD)

Binaries

T1202: Indirect Command Execution

Control.exe

Alternate data streams (DLL)

Execute (DLL)

Binaries

T1218.002: Control Panel

Csc.exe

Compile

Binaries

T1127: Trusted Developer Utilities Proxy Execution

Cscript.exe

Alternate data streams (WSH)

Binaries

T1564.004: NTFS File Attributes

CustomShellHost.exe

Execute (EXE)

Binaries

T1218: System Binary Proxy Execution

DataSvcUtil.exe

Upload

Binaries

T1567: Exfiltration Over Web Service

Desktopimgdownldr.exe

Download

Binaries

T1105: Ingress Tool Transfer

DeviceCredentialDeployment.exe

Conceal

Binaries

T1564: Hide Artifacts

Dfsvc.exe

AWL bypass (ClickOnce, Remote)

Binaries

T1127.002: ClickOnce

Diantz.exe

Alternate data streams (Compression)

Download (Compression)

Execute (Compression)

Binaries

T1564.004: NTFS File Attributes

T1105: Ingress Tool Transfer

T1036: Masquerading

Diskshadow.exe

Dump (CMD)

Execute (CMD)

Binaries

T1003.003: NTDS

T1202: Indirect Command Execution

Dnscmd.exe

Execute (DLL, Remote)

Binaries

T1543.003: Windows Service

Esentutl.exe

Copy

Alternate data streams

Download

Binaries

T1105: Ingress Tool Transfer

T1564.004: NTFS File Attributes

T1003.003: NTDS

Eudcedit.exe

UAC bypass (CMD, GUI)

Binaries

T1548.002: Bypass User Account Control

Eventvwr.exe

UAC bypass (GUI, EXE, .NetObjects)

Binaries

T1548.002: Bypass User Account Control

Expand.exe

Download

Copy

Alternate data streams

Binaries

T1105: Ingress Tool Transfer

T1564.004: NTFS File Attributes

Explorer.exe

Execute (EXE)

Binaries

T1202: Indirect Command Execution

Extexport.exe

Execute (DLL)

Binaries

T1218: System Binary Proxy Execution

Extrac32.exe

Alternate data streams (Compression)

Download

Copy

Binaries

T1564.004: NTFS File Attributes

T1105: Ingress Tool Transfer

Findstr.exe

Alternate data streams

Credentials

Download

Binaries

T1564.004: NTFS File Attributes

T1552.001: Credentials In Files

T1105: Ingress Tool Transfer

Finger.exe

Download

Binaries

T1105: Ingress Tool Transfer

fltMC.exe

Tamper

Binaries

T1562.001: Disable or Modify Tools

Forfiles.exe

Execute (EXE)

Alternate data streams (EXE)

Binaries

T1202: Indirect Command Execution

T1564.004: NTFS File Attributes

Fsutil.exe

Tamper

Execute (EXE)

Binaries

T1485: Data Destruction

T1218: System Binary Proxy Execution

Ftp.exe

Execute (CMD)

Download

Binaries

T1202: Indirect Command Execution

T1105: Ingress Tool Transfer

Gpscript.exe

Execute (CMD)

Binaries

T1218: System Binary Proxy Execution

Hh.exe

Download (EXE, GUI)

Execute (EXE, GUI, CMD, CHM, Remote)

Binaries

T1105: Ingress Tool Transfer

T1218.001: Compiled HTML File

IMEWDBLD.exe

Download (INetCache)

Binaries

T1105: Ingress Tool Transfer

Ie4uinit.exe

Execute (INF)

Binaries

T1218: System Binary Proxy Execution

iediagcmd.exe

Execute (EXE)

Binaries

T1218: System Binary Proxy Execution

Ieexec.exe

Download (Remote, EXE (.NET))

Execute (Remote, EXE (.NET))

Binaries

T1105: Ingress Tool Transfer

T1218: System Binary Proxy Execution

Ilasm.exe

Compile

Binaries

T1127: Trusted Developer Utilities Proxy Execution

Infdefaultinstall.exe

Execute (INF)

Binaries

T1218: System Binary Proxy Execution

Installutil.exe

AWL bypass (DLL (.NET), EXE (.NET))

Execute (DLL (.NET), EXE (.NET))

Download (INetCache)

Binaries

T1218.004: InstallUtil

T1105: Ingress Tool Transfer

iscsicpl.exe

UAC bypass (DLL, CMD, GUI)

Binaries

T1548.002: Bypass User Account Control

Jsc.exe

Compile (JScript)

Binaries

T1127: Trusted Developer Utilities Proxy Execution

Ldifde.exe

Download

Binaries

T1105: Ingress Tool Transfer

Makecab.exe

Alternate data streams (Compression)

Download (Compression)

Execute (Compression)

Binaries

T1564.004: NTFS File Attributes

T1105: Ingress Tool Transfer

T1036: Masquerading

Mavinject.exe

Execute (DLL)

Alternate data streams (DLL)

Binaries

T1218.013: Mavinject

T1564.004: NTFS File Attributes

Microsoft.Workflow.Compiler.exe

Execute (VB.Net, Csharp, XOML)

AWL bypass (XOML)

Binaries

T1127: Trusted Developer Utilities Proxy Execution

Mmc.exe

Execute (COM)

UAC bypass (DLL)

Download (GUI)

Binaries

T1218.014: MMC

MpCmdRun.exe

Download

Alternate data streams

Binaries

T1105: Ingress Tool Transfer

T1564.004: NTFS File Attributes

Msbuild.exe

AWL bypass (CSharp)

Execute (CSharp, DLL, XSL, CMD)

Binaries

T1127.001: MSBuild

T1036: Masquerading

Msconfig.exe

Execute (CMD)

Binaries

T1218: System Binary Proxy Execution

Msdt.exe

Execute (GUI, MSI)

AWL bypass (GUI, MSI, CMD)

Binaries

T1218: System Binary Proxy Execution

T1202: Indirect Command Execution

Msedge.exe

Download

Execute (CMD)

Binaries

T1105: Ingress Tool Transfer

T1218.015: Electron Applications

Mshta.exe

Execute (HTA, Remote, VBScript, JScript)

Alternate data streams (HTA)

Download (INetCache)

Binaries

T1218.005: Mshta

T1105: Ingress Tool Transfer

Msiexec.exe

Execute (MSI, Remote, DLL, MST)

Binaries

T1218.007: Msiexec

Netsh.exe

Execute (DLL)

Binaries

T1546.007: Netsh Helper DLL

Ngen.exe

Download (INetCache)

Binaries

T1105: Ingress Tool Transfer

Odbcconf.exe

Execute (DLL)

Binaries

T1218.008: Odbcconf

OfflineScannerShell.exe

Execute (DLL)

Binaries

T1218: System Binary Proxy Execution

OneDriveStandaloneUpdater.exe

Download

Binaries

T1105: Ingress Tool Transfer

Pcalua.exe

Execute (EXE, DLL, Remote)

Binaries

T1202: Indirect Command Execution

Pcwrun.exe

Execute (EXE)

Binaries

T1218: System Binary Proxy Execution

T1202: Indirect Command Execution

Pktmon.exe

Reconnaissance

Binaries

T1040: Network Sniffing

Pnputil.exe

Execute (INF)

Binaries

T1547: Boot or Logon Autostart Execution

Presentationhost.exe

Execute (XBAP)

Download (INetCache)

Binaries

T1218: System Binary Proxy Execution

T1105: Ingress Tool Transfer

Print.exe

Alternate data streams

Copy

Binaries

T1564.004: NTFS File Attributes

T1105: Ingress Tool Transfer

PrintBrm.exe

Download (Compression)

Alternate data streams (Compression)

Binaries

T1105: Ingress Tool Transfer

T1564.004: NTFS File Attributes

Provlaunch.exe

Execute (CMD)

Binaries

T1218: System Binary Proxy Execution

Psr.exe

Reconnaissance

Binaries

T1113: Screen Capture

Query.exe

Execute (EXE, Rename)

Binaries

T1218: System Binary Proxy Execution

Rasautou.exe

Execute (DLL)

Binaries

T1218: System Binary Proxy Execution

rdrleakdiag.exe

Dump

Binaries

T1003: OS Credential Dumping

T1003.001: LSASS Memory

Reg.exe

Alternate data streams

Credentials

Binaries

T1564.004: NTFS File Attributes

T1003.002: Security Account Manager

Regasm.exe

AWL bypass (DLL (.NET))

Execute (DLL (.NET))

Binaries

T1218.009: Regsvcs/Regasm

Regedit.exe

Alternate data streams

Binaries

T1564.004: NTFS File Attributes

Regini.exe

Alternate data streams

Binaries

T1564.004: NTFS File Attributes

Register-cimprovider.exe

Execute (DLL)

Binaries

T1218: System Binary Proxy Execution

Regsvcs.exe

Execute (DLL (.NET))

AWL bypass (DLL (.NET))

Binaries

T1218.009: Regsvcs/Regasm

Regsvr32.exe

AWL bypass (SCT, Remote)

Execute (SCT, Remote, DLL)

Binaries

T1218.010: Regsvr32

Replace.exe

Copy

Download

Binaries

T1105: Ingress Tool Transfer

Reset.exe

Execute (EXE, Rename)

Binaries

T1218: System Binary Proxy Execution

Rpcping.exe

Credentials

Binaries

T1003: OS Credential Dumping

T1187: Forced Authentication

Rundll32.exe

Execute (DLL, Remote, JScript, COM)

Alternate data streams (DLL)

Binaries

T1218.011: Rundll32

T1564.004: NTFS File Attributes

Runexehelper.exe

Execute (EXE)

Binaries

T1218: System Binary Proxy Execution

Runonce.exe

Execute (CMD)

Binaries

T1218: System Binary Proxy Execution

Runscripthelper.exe

Execute (PowerShell)

Binaries

T1218: System Binary Proxy Execution

Sc.exe

Alternate data streams (EXE)

Binaries

T1564.004: NTFS File Attributes

Schtasks.exe

Execute (CMD)

Binaries

T1053.005: Scheduled Task

Scriptrunner.exe

Execute (EXE, Remote, CMD)

Binaries

T1202: Indirect Command Execution

T1218: System Binary Proxy Execution

Setres.exe

Execute (EXE)

Binaries

T1218: System Binary Proxy Execution

SettingSyncHost.exe

Execute (EXE, CMD)

Binaries

T1218: System Binary Proxy Execution

Sftp.exe

Execute (CMD)

Binaries

T1202: Indirect Command Execution

Sigverif.exe

Execute (EXE, GUI)

Binaries

T1218: System Binary Proxy Execution

ssh.exe

Execute (CMD)

Binaries

T1202: Indirect Command Execution

Stordiag.exe

Execute (EXE)

Binaries

T1218: System Binary Proxy Execution

SyncAppvPublishingServer.exe

Execute (PowerShell)

Binaries

T1218: System Binary Proxy Execution

Tar.exe

Alternate data streams (Compression)

Copy (Compression)

Binaries

T1564.004: NTFS File Attributes

T1105: Ingress Tool Transfer

Ttdinject.exe

Execute (EXE)

Binaries

T1127: Trusted Developer Utilities Proxy Execution

Tttracer.exe

Execute (EXE)

Dump

Binaries

T1127: Trusted Developer Utilities Proxy Execution

T1003: OS Credential Dumping

Unregmp2.exe

Execute (EXE)

Binaries

T1202: Indirect Command Execution

vbc.exe

Compile

Binaries

T1127: Trusted Developer Utilities Proxy Execution

Verclsid.exe

Execute (COM)

Binaries

T1218.012: Verclsid

Wab.exe

Execute (DLL)

Binaries

T1218: System Binary Proxy Execution

wbadmin.exe

Dump

Binaries

T1003.003: NTDS

wbemtest.exe

Execute (GUI, CMD)

Binaries

T1047: Windows Management Instrumentation

winget.exe

Execute (Remote, EXE)

Download

AWL bypass

Binaries

T1105: Ingress Tool Transfer

Wlrmdr.exe

Execute (EXE)

Binaries

T1202: Indirect Command Execution

Wmic.exe

Alternate data streams (EXE)

Execute (CMD, Remote, XSL)

Copy

Binaries

T1564.004: NTFS File Attributes

T1218: System Binary Proxy Execution

T1105: Ingress Tool Transfer

WorkFolders.exe

Execute (EXE, Rename, Registry change)

Binaries

T1218: System Binary Proxy Execution

Wscript.exe

Alternate data streams (WSH)

Binaries

T1564.004: NTFS File Attributes

Wsreset.exe

UAC bypass

Binaries

T1548.002: Bypass User Account Control

wuauclt.exe

Execute (DLL)

Binaries

T1218: System Binary Proxy Execution

Xwizard.exe

Execute (COM)

Download (INetCache)

Binaries

T1218: System Binary Proxy Execution

T1105: Ingress Tool Transfer

msedge_proxy.exe

Download

Execute (CMD)

Binaries

T1105: Ingress Tool Transfer

T1218.015: Electron Applications

msedgewebview2.exe

Execute (EXE, CMD)

Binaries

T1218.015: Electron Applications

odbcad32.exe

UAC bypass (CMD, GUI)

Binaries

T1548.002: Bypass User Account Control

write.exe

Execute (EXE, Registry Change)

Binaries

T1218: System Binary Proxy Execution

wt.exe

Execute (CMD)

Binaries

T1202: Indirect Command Execution

Advpack.dll

AWL bypass (INF)

Execute (DLL, EXE, CMD)

Libraries

T1218.011: Rundll32

Desk.cpl

Execute (EXE, Remote)

Libraries

T1218.011: Rundll32

Dfshim.dll

AWL bypass (ClickOnce, Remote)

Libraries

T1127.002: ClickOnce

Ieadvpack.dll

AWL bypass (INF)

Execute (DLL, EXE, CMD)

Libraries

T1218.011: Rundll32

Ieframe.dll

Execute (URL)

Libraries

T1218.011: Rundll32

Mshtml.dll

Execute (HTA)

Libraries

T1218.011: Rundll32

Pcwutl.dll

Execute (EXE)

Libraries

T1218.011: Rundll32

PhotoViewer.dll

Download (INetCache)

Libraries

T1105: Ingress Tool Transfer

Scrobj.dll

Download (INetCache)

Libraries

T1105: Ingress Tool Transfer

Setupapi.dll

AWL bypass (INF)

Execute (INF)

Libraries

T1218.011: Rundll32

Shdocvw.dll

Execute (URL)

Libraries

T1218.011: Rundll32

Shell32.dll

Execute (DLL, EXE, CMD)

Libraries

T1218.011: Rundll32

Shimgvw.dll

Download (INetCache)

Libraries

T1105: Ingress Tool Transfer

Syssetup.dll

AWL bypass (INF)

Execute (INF)

Libraries

T1218.011: Rundll32

Url.dll

Execute (HTA, URL, EXE)

Libraries

T1218.011: Rundll32

Zipfldr.dll

Execute (EXE)

Libraries

T1218.011: Rundll32

Comsvcs.dll

Dump

Libraries

T1003.001: LSASS Memory

AccCheckConsole.exe

Execute (DLL (.NET))

AWL bypass (DLL (.NET))

OtherMSBinaries

T1218: System Binary Proxy Execution

adplus.exe

Dump

Execute (CMD, EXE)

OtherMSBinaries

T1003.001: LSASS Memory

T1127: Trusted Developer Utilities Proxy Execution

AgentExecutor.exe

Execute (PowerShell, EXE)

OtherMSBinaries

T1218: System Binary Proxy Execution

AppLauncher.exe

Execute (EXE)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

AppCert.exe

Execute (EXE, MSI)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

T1218.007: Msiexec

Appvlp.exe

Execute (CMD, EXE)

OtherMSBinaries

T1218: System Binary Proxy Execution

Bcp.exe

Download

OtherMSBinaries

T1105: Ingress Tool Transfer

Bginfo.exe

Execute (WSH, Remote)

AWL bypass (WSH, Remote)

OtherMSBinaries

T1218: System Binary Proxy Execution

Cdb.exe

Execute (Shellcode, CMD)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

coregen.exe

Execute (DLL)

AWL bypass (DLL)

OtherMSBinaries

T1055: Process Injection

T1218: System Binary Proxy Execution

Createdump.exe

Dump

OtherMSBinaries

T1003: OS Credential Dumping

csi.exe

Execute (CSharp)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

DefaultPack.EXE

Execute (CMD)

OtherMSBinaries

T1218: System Binary Proxy Execution

Devinit.exe

Execute (MSI, Remote)

OtherMSBinaries

T1218.007: Msiexec

Devtoolslauncher.exe

Execute (CMD)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

dnx.exe

Execute (CSharp)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Dotnet.exe

AWL bypass (DLL (.NET), CSharp)

Execute (DLL (.NET), FSharp)

OtherMSBinaries

T1218: System Binary Proxy Execution

T1059: Command and Scripting Interpreter

dsdbutil.exe

Dump

OtherMSBinaries

T1003.003: NTDS

dtutil.exe

Copy

OtherMSBinaries

T1105: Ingress Tool Transfer

Dump64.exe

Dump

OtherMSBinaries

T1003.001: LSASS Memory

DumpMinitool.exe

Dump

OtherMSBinaries

T1003.001: LSASS Memory

Dxcap.exe

Execute (EXE, Rename)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

ECMangen.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

Excel.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

Fsi.exe

AWL bypass (FSharp)

OtherMSBinaries

T1059: Command and Scripting Interpreter

FsiAnyCpu.exe

AWL bypass (FSharp)

OtherMSBinaries

T1059: Command and Scripting Interpreter

IntelliTrace.exe

Execute (EXE)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Logger.exe

Execute (CMD)

OtherMSBinaries

T1202: Indirect Command Execution

Mftrace.exe

Execute (EXE)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Microsoft.NodejsTools.PressAnyKey.exe

Execute (EXE)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Mpiexec.exe

Execute (CMD)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

MSAccess.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

Msdeploy.exe

Execute (CMD)

AWL bypass (CMD)

Copy

OtherMSBinaries

T1218: System Binary Proxy Execution

T1105: Ingress Tool Transfer

MsoHtmEd.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

Mspub.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

msxsl.exe

Execute (XSL, Remote)

AWL bypass (XSL, Remote)

Download

Alternate data streams

OtherMSBinaries

T1220: XSL Script Processing

T1105: Ingress Tool Transfer

T1564: Hide Artifacts

Nmcap.exe

Reconnaissance

OtherMSBinaries

T1040: Network Sniffing

ntdsutil.exe

Dump

OtherMSBinaries

T1003.003: NTDS

Ntsd.exe

Execute (CMD)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

OpenConsole.exe

Execute (EXE)

OtherMSBinaries

T1202: Indirect Command Execution

Pixtool.exe

Execute (EXE)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Powerpnt.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

Procdump.exe

Execute (DLL)

OtherMSBinaries

T1202: Indirect Command Execution

ProtocolHandler.exe

Download

OtherMSBinaries

T1105: Ingress Tool Transfer

rcsi.exe

Execute (CSharp)

AWL bypass (CSharp)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Remote.exe

AWL bypass (EXE)

Execute (EXE, Remote)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Sqldumper.exe

Dump

OtherMSBinaries

T1003: OS Credential Dumping

T1003.001: LSASS Memory

Sqlps.exe

Execute (PowerShell)

OtherMSBinaries

T1218: System Binary Proxy Execution

SQLToolsPS.exe

Execute (PowerShell)

OtherMSBinaries

T1218: System Binary Proxy Execution

Squirrel.exe

Download

AWL bypass (Nuget, Remote)

Execute (Nuget, Remote)

OtherMSBinaries

T1218: System Binary Proxy Execution

te.exe

Execute (WSH, DLL, Custom Format)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Teams.exe

Execute (Node.JS, CMD)

OtherMSBinaries

T1218.015: Electron Applications

TestWindowRemoteAgent.exe

Upload

OtherMSBinaries

T1048: Exfiltration Over Alternative Protocol

Tracker.exe

Execute (DLL)

AWL bypass (DLL)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Update.exe

Download

AWL bypass (Nuget, Remote, CMD)

Execute (Nuget, Remote, CMD, EXE)

OtherMSBinaries

T1218: System Binary Proxy Execution

T1547: Boot or Logon Autostart Execution

T1070: Indicator Removal

VSDiagnostics.exe

Execute (EXE, CMD)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

VSIISExeLauncher.exe

Execute (EXE)

OtherMSBinaries

T1218: System Binary Proxy Execution

Visio.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

VisualUiaVerifyNative.exe

AWL bypass (.NetObjects)

OtherMSBinaries

T1218: System Binary Proxy Execution

VSLaunchBrowser.exe

Download (INetCache)

Execute (EXE, Remote)

OtherMSBinaries

T1105: Ingress Tool Transfer

T1127: Trusted Developer Utilities Proxy Execution

Vshadow.exe

Execute (EXE)

OtherMSBinaries

T1202: Indirect Command Execution

vsjitdebugger.exe

Execute (EXE)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

WFMFormat.exe

Execute (EXE, .NET Framework 3.5)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

Wfc.exe

AWL bypass (XOML)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

WinDbg.exe

Execute (CMD)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

WinProj.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

Winword.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

Wsl.exe

Execute (EXE, CMD)

Download

OtherMSBinaries

T1202: Indirect Command Execution

T1105: Ingress Tool Transfer

T1218: System Binary Proxy Execution

XBootMgr.exe

Execute (EXE)

OtherMSBinaries

T1202: Indirect Command Execution

XBootMgrSleep.exe

Execute (EXE)

OtherMSBinaries

T1202: Indirect Command Execution

devtunnel.exe

Download

OtherMSBinaries

T1105: Ingress Tool Transfer

vsls-agent.exe

Execute (DLL)

OtherMSBinaries

T1218: System Binary Proxy Execution

vstest.console.exe

AWL bypass (DLL)

OtherMSBinaries

T1127: Trusted Developer Utilities Proxy Execution

winfile.exe

Execute (EXE)

OtherMSBinaries

T1202: Indirect Command Execution

xsd.exe

Download (INetCache)

OtherMSBinaries

T1105: Ingress Tool Transfer

CL_LoadAssembly.ps1

Execute (DLL (.NET))

Scripts

T1216: System Script Proxy Execution

CL_Mutexverifiers.ps1

Execute (PowerShell)

Scripts

T1216: System Script Proxy Execution

CL_Invocation.ps1

Execute (CMD)

Scripts

T1216: System Script Proxy Execution

Launch-VsDevShell.ps1

Execute (EXE)

Scripts

T1216: System Script Proxy Execution

Manage-bde.wsf

Execute (EXE)

Scripts

T1216: System Script Proxy Execution

Pubprn.vbs

Execute (SCT)

Scripts

T1216.001: PubPrn

Syncappvpublishingserver.vbs

Execute (PowerShell)

Scripts

T1216.002: SyncAppvPublishingServer

UtilityFunctions.ps1

Execute (DLL (.NET))

Scripts

T1216: System Script Proxy Execution

winrm.vbs

Execute (CMD, Remote)

AWL bypass (XSL)

Scripts

T1216: System Script Proxy Execution

T1220: XSL Script Processing

Pester.bat

Execute (EXE)

Scripts

T1216: System Script Proxy Execution
