LOLBAS

☆ Star 7,060

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib. More information on programmatically accesssing this project can be found on the API page.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.
If you are looking for drivers, please visit loldrivers.io.

Search among 207 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
AddinUtil.exe	Execute	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	Binaries	**T1053.002**: At
Atbroker.exe	Execute	Binaries	**T1218**: System Binary Proxy Execution
Bash.exe	Execute AWL bypass	Binaries	**T1202**: Indirect Command 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 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
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)	Binaries	**T1218.003**: CMSTP

	AWL bypass (INF)		
Colorcpl.exe	Copy	Binaries	**T1036.005**: Match Legitimate 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	Binaries	**T1202**: Indirect Command Execution
Control.exe	Alternate data streams (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	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	Binaries	**T1127**: Trusted Developer Utilities Proxy Execution
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 Execute	Binaries	**T1003.003**: NTDS **T1202**: Indirect Command Execution
Dnscmd.exe	Execute (DLL)	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
Eventvwr.exe	UAC bypass (GUI)	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	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 Alternate data streams	Binaries	**T1202**: Indirect Command Execution **T1564.004**: NTFS File Attributes
Fsutil.exe	Tamper Execute	Binaries	**T1485**: Data Destruction **T1218**: System Binary Proxy Execution
Ftp.exe	Execute Download	Binaries	**T1202**: Indirect Command Execution **T1105**: Ingress Tool Transfer
Gpscript.exe	Execute	Binaries	**T1218**: System Binary Proxy Execution
Hh.exe	Download Execute	Binaries	**T1105**: Ingress Tool Transfer **T1218.001**: Compiled HTML File
IMEWDBLD.exe	Download (INetCache)	Binaries	**T1105**: Ingress Tool Transfer
Ie4uinit.exe	Execute	Binaries	**T1218**: System Binary Proxy Execution
iediagcmd.exe	Execute	Binaries	**T1218**: System Binary Proxy Execution
Ieexec.exe	Download Execute	Binaries	**T1105**: Ingress Tool Transfer **T1218**: System Binary Proxy Execution
Ilasm.exe	Compile	Binaries	**T1127**: Trusted Developer Utilities Proxy Execution
Infdefaultinstall.exe	Execute	Binaries	**T1218**: System Binary Proxy Execution
Installutil.exe	AWL bypass (DLL, Custom Format) Execute (DLL, Custom Format) Download (INetCache)	Binaries	**T1218.004**: InstallUtil **T1105**: Ingress Tool Transfer
Jsc.exe	Compile (WSH)	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 AWL bypass	Binaries	**T1127**: Trusted Developer Utilities Proxy Execution
Mmc.exe	Execute UAC bypass	Binaries	**T1218.014**: MMC
MpCmdRun.exe	Download Alternate data streams	Binaries	**T1105**: Ingress Tool Transfer **T1564.004**: NTFS File Attributes
Msbuild.exe	AWL bypass Execute (DLL, WSH)	Binaries	**T1127.001**: MSBuild **T1036**: Masquerading
Msconfig.exe	Execute	Binaries	**T1218**: System Binary Proxy Execution

Msdt.exe	Execute (GUI) AWL bypass (GUI)	Binaries	T1218: System Binary Proxy Execution T1202: Indirect Command Execution
Msedge.exe	Download Execute	Binaries	T1105: Ingress Tool Transfer T1218.015: Electron Applications
Mshta.exe	Execute (WSH) Alternate data streams (WSH) Download (INetCache)	Binaries	T1218.005: Mshta T1105: Ingress Tool Transfer
Msiexec.exe	Execute (DLL)	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 (DLL)	Binaries	T1202: Indirect Command Execution
Pcwrun.exe	Execute	Binaries	T1218: System Binary Proxy Execution T1202: Indirect Command Execution
Pktmon.exe	Reconnaissance	Binaries	T1040: Network Sniffing
Pnputil.exe	Execute	Binaries	T1547: Boot or Logon Autostart Execution
Presentationhost.exe	Execute 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	Binaries	T1218: System Binary Proxy Execution
Psr.exe	Reconnaissance	Binaries	T1113: Screen Capture
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, Custom Format) Execute (DLL, Custom Format)	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, Custom Format) AWL bypass (DLL, Custom Format)	Binaries	T1218.009: Regsvcs/Regasm
Regsvr32.exe	AWL bypass Execute	Binaries	T1218.010: Regsvr32
Replace.exe	Copy Download	Binaries	T1105: Ingress Tool Transfer
Rpcping.exe	Credentials	Binaries	T1003: OS Credential Dumping T1187: Forced Authentication
Rundll32.exe	Execute (DLL) Alternate data streams (DLL)	Binaries	T1218.011: Rundll32 T1564.004: NTFS File Attributes
Runexehelper.exe	Execute	Binaries	T1218: System Binary Proxy Execution
Runonce.exe	Execute	Binaries	T1218: System Binary Proxy Execution
Runscripthelper.exe	Execute	Binaries	T1218: System Binary Proxy Execution
Sc.exe	Alternate data streams	Binaries	T1564.004: NTFS File Attributes
Schtasks.exe	Execute	Binaries	T1053.005: Scheduled Task
Scriptrunner.exe	Execute	Binaries	T1202: Indirect Command Execution T1218: System Binary Proxy Execution
Setres.exe	Execute	Binaries	T1218: System Binary Proxy Execution
SettingSyncHost.exe	Execute	Binaries	T1218: System Binary Proxy Execution
ssh.exe	Execute	Binaries	T1202: Indirect Command Execution
Stordiag.exe	Execute	Binaries	T1218: System Binary Proxy Execution
SyncAppvPublishingServer.exe	Execute	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	Binaries	T1127: Trusted Developer Utilities Proxy Execution
Tttracer.exe	Execute Dump	Binaries	T1127: Trusted Developer Utilities Proxy Execution T1003: OS Credential Dumping
Unregmp2.exe	Execute	Binaries	T1202: Indirect Command Execution
vbc.exe	Compile (WSH)	Binaries	T1127: Trusted Developer Utilities Proxy Execution
Verclsid.exe	Execute	Binaries	T1218.012: Verclsid
Wab.exe	Execute	Binaries	T1218: System Binary Proxy Execution
wbadmin.exe	Dump	Binaries	T1003.003: NTDS

winget.exe	Execute Download	Binaries	T1105: Ingress Tool Transfer
Wlrmdr.exe	Execute	Binaries	T1202: Indirect Command Execution
Wmic.exe	Alternate data streams Execute (WSH) Copy	Binaries	T1564.004: NTFS File Attributes T1218: System Binary Proxy Execution T1105: Ingress Tool Transfer
WorkFolders.exe	Execute	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 Download (INetCache)	Binaries	T1218: System Binary Proxy Execution T1105: Ingress Tool Transfer
msedge_proxy.exe	Download Execute	Binaries	T1105: Ingress Tool Transfer T1218.015: Electron Applications
msedgewebview2.exe	Execute	Binaries	T1218.015: Electron Applications
wt.exe	Execute	Binaries	T1202: Indirect Command Execution
Advpack.dll	AWL bypass (INF) Execute (DLL)	Libraries	T1218.011: Rundll32
Desk.cpl	Execute	Libraries	T1218.011: Rundll32
Dfshim.dll	AWL bypass	Libraries	T1127: Trusted Developer Utilities Proxy Execution
Ieadvpack.dll	AWL bypass Execute (DLL)	Libraries	T1218.011: Rundll32
Ieframe.dll	Execute	Libraries	T1218.011: Rundll32
Mshtml.dll	Execute	Libraries	T1218.011: Rundll32
Pcwutl.dll	Execute	Libraries	T1218.011: Rundll32
Scrobj.dll	Download (INetCache)	Libraries	T1105: Ingress Tool Transfer
Setupapi.dll	AWL bypass (INF) Execute (INF)	Libraries	T1218.011: Rundll32
Shdocvw.dll	Execute	Libraries	T1218.011: Rundll32
Shell32.dll	Execute (DLL)	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	Libraries	T1218.011: Rundll32
Zipfldr.dll	Execute	Libraries	T1218.011: Rundll32
Comsvcs.dll	Dump	Libraries	T1003.001: LSASS Memory
AccCheckConsole.exe	Execute (DLL) AWL bypass (DLL)	OtherMSBinaries	T1218: System Binary Proxy Execution
adplus.exe	Dump Execute	OtherMSBinaries	T1003.001: LSASS Memory

			T1127: Trusted Developer Utilities Proxy Execution
AgentExecutor.exe	Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution
AppCert.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution **T1218.007**: Msiexec
Appvlp.exe	Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution
Bginfo.exe	Execute (WSH) AWL bypass (WSH)	OtherMSBinaries	**T1218**: System Binary Proxy Execution
Cdb.exe	Execute	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	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
DefaultPack.EXE	Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution
Devinit.exe	Execute	OtherMSBinaries	**T1218.007**: Msiexec
Devtoolslauncher.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
dnx.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
Dotnet.exe	AWL bypass Execute	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	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
Excel.exe	Download (INetCache)	OtherMSBinaries	**T1105**: Ingress Tool Transfer
Fsi.exe	AWL bypass	OtherMSBinaries	**T1059**: Command and Scripting Interpreter
FsiAnyCpu.exe	AWL bypass	OtherMSBinaries	**T1059**: Command and Scripting Interpreter
Mftrace.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
Microsoft.NodejsTools.PressAnyKey.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
MSAccess.exe	Download (INetCache)	OtherMSBinaries	**T1105**: Ingress Tool Transfer
Msdeploy.exe	Execute AWL bypass 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 AWL bypass Download Alternate data streams	OtherMSBinaries	**T1220**: XSL Script Processing **T1105**: Ingress Tool Transfer **T1564**: Hide Artifacts
ntdsutil.exe	Dump	OtherMSBinaries	**T1003.003**: NTDS
OpenConsole.exe	Execute	OtherMSBinaries	**T1202**: Indirect Command 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 AWL bypass	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
Remote.exe	AWL bypass Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
Sqldumper.exe	Dump	OtherMSBinaries	**T1003**: OS Credential Dumping **T1003.001**: LSASS Memory
Sqlps.exe	Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution
SQLToolsPS.exe	Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution
Squirrel.exe	Download AWL bypass Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution
te.exe	Execute (DLL, Custom Format)	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
Teams.exe	Execute	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 Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution **T1547**: Boot or Logon Autostart Execution **T1070**: Indicator Removal
VSDiagnostics.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
VSIISExeLauncher.exe	Execute	OtherMSBinaries	**T1218**: System Binary Proxy Execution
Visio.exe	Download (INetCache)	OtherMSBinaries	**T1105**: Ingress Tool Transfer
VisualUiaVerifyNative.exe	AWL bypass	OtherMSBinaries	**T1218**: System Binary Proxy Execution
VSLaunchBrowser.exe	Download (INetCache) Execute	OtherMSBinaries	**T1105**: Ingress Tool Transfer **T1127**: Trusted Developer Utilities Proxy Execution
Vshadow.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
vsjitdebugger.exe	Execute	OtherMSBinaries	**T1127**: Trusted Developer Utilities Proxy Execution
Wfc.exe	AWL bypass	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 Download	OtherMSBinaries	**T1202**: Indirect Command Execution **T1105**: Ingress Tool Transfer
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	OtherMSBinaries	**T1202**: Indirect Command Execution
xsd.exe	Download (INetCache)	OtherMSBinaries	**T1105**: Ingress Tool Transfer
CL_LoadAssembly.ps1	Execute (DLL)	Scripts	**T1216**: System Script Proxy Execution
CL_Mutexverifiers.ps1	Execute	Scripts	**T1216**: System Script Proxy Execution
CL_Invocation.ps1	Execute	Scripts	**T1216**: System Script Proxy Execution
Launch-VsDevShell.ps1	Execute	Scripts	**T1216**: System Script Proxy Execution
Manage-bde.wsf	Execute	Scripts	**T1216**: System Script Proxy Execution
Pubprn.vbs	Execute	Scripts	**T1216.001**: PubPrn
Syncappvpublishingserver.vbs	Execute	Scripts	**T1216.002**: SyncAppvPublishingServer
UtilityFunctions.ps1	Execute (DLL)	Scripts	**T1216**: System Script Proxy Execution
winrm.vbs	Execute AWL bypass	Scripts	**T1216**: System Script Proxy Execution **T1220**: XSL Script Processing
Pester.bat	Execute	Scripts	**T1216**: System Script Proxy Execution