LoLbas

Binary	ATT&CK; Techniques	Common Abuse (defense lens)	Hunt Clues (tokens)	Sigma Ideas
certutil.exe	T1105 Ingress Tool Transfer; T1027 Obfuscated/Compressed Files; T1564.004 Hide Artifacts: NTFS ADS	Use to fetch/encode files and stash data (e.g., base64, ADS) under trusted Microsoft signer.	certutil -urlcache; certutil -decode; -encode; http:// or https:// in CommandLine; writes to :Zone.Identifier	selection Image: *\certutil.exe AND CommandLine contains any(http, -urlcache, -decode, -encode); flag network connections by certutil; rare parent processes
mshta.exe	T1218.005 Signed Binary Proxy Execution: Mshta; T1059.007 Command and Scripting Interpreter: JavaScript; T1204.002 User Execution	Execute HTA/JScript (often remote) for in-memory code under a signed binary.	mshta http; mshta https; mshta file://; .hta or javascript: in CommandLine	Image: *\mshta.exe AND (CommandLine contains http OR CommandLine endswith .hta); unusual parent (Office, browser), network start by mshta
rundll32.exe	T1218.011 Signed Binary Proxy Execution: Rundll32; T1106 Native API; T1055 Process Injection (variants)	Call exported DLL functions or scriptlet COM objects to proxy execution.	rundll32 , rundll32.exe ,EntryPoint; suspicious DLL from temp/user profile; .zip/.dat masquerading	Image: *\rundll32.exe AND CommandLine contains .dll; look for non-system DLL paths; rare parent-child pairs; no file version info
regsvr32.exe	T1218.010 Signed Binary Proxy Execution: Regsvr32; T1117 Regsvr32 Scriptlet Execution	Execute COM objects/Scriptlets (.sct) potentially from remote locations; bypass some controls.	regsvr32 /s /n /u /i:; scrobj.dll; .sct; http/https in CommandLine	Image: *\regsvr32.exe AND CommandLine contains scrobj.dll OR .sct; network start; parent from Office/Explorer
bitsadmin.exe	T1197 BITS Jobs; T1105 Ingress Tool Transfer; T1053 Scheduled Task (via BITS trigger)	Create BITS jobs to fetch/persist payloads that survive reboots and blend with system traffic.	bitsadmin /create; /addfile; /setnotifycmdline; /resume; URLs in CommandLine	Image: *\bitsadmin.exe AND CommandLine contains any(/create, /addfile, /setnotifycmdline); new BITS jobs by non-admin users
wmic.exe	T1047 Windows Management Instrumentation; T1021.002 SMB/Remote Services; T1105 Data Transfer	Remote process execution and reconnaissance via WMI; lateral movement on legacy hosts.	wmic /node:; process call create; /user:; /password:; SELECT * FROM; remote IPs	Image: *\wmic.exe AND CommandLine contains process call create OR /node:; remote logons followed by wmic from same host

Binary	ATT&CK; Techniques	Common Abuse (defense lens)	Hunt Clues (tokens)	Sigma Ideas
msbuild.exe	T1127 Trusted Developer Utilities Proxy Execution: MSBuild; T1059.005 Visual Basic (inline C# execution patterns)	Compile/run inline code from project files for memory-only execution under signed dev tool.	msbuild .proj .xml; invocation from user profile/temp; suspicious inline tasks	Image: *\msbuild.exe AND (CommandLine contains .xml OR .proj); parent not Visual Studio; network start by msbuild
installutil.exe	T1218.004 Signed Binary Proxy Execution: InstallUtil; T1127 Trusted Dev Utilities	Load managed assemblies with installer hooks to run attacker code.	installutil /?; installutil .dll; odd DLL names/paths in user space	Image: *\installutil.exe AND CommandLine contains .dll; file path outside Windows\Microsoft.NET; rare parent processes
schtasks.exe	T1053.005 Scheduled Task; T1037 Boot or Logon Autostart; T1021 Remote Services (via /S)	Create/modify scheduled tasks for persistence and remote execution.	schtasks /create; /change; /S ; /RU; /TR with unusual paths	Image: *\schtasks.exe AND CommandLine contains /create OR /change; new tasks owned by low-priv users; remote /S usage
fodhelper.exe	T1548.002 Bypass UAC; T1218 Signed Proxy Execution (context)	Auto-elevated binary used for registry-based UAC bypass chains.	fodhelper.exe with suspicious registry writes (shell open commands) shortly before	Image: *\fodhelper.exe; registry modifications to HKCU\Software\Classes\ms-settings\ (shell/open) preceding exec
computerdefaults.exe	T1548.002 Bypass UAC; T1218 Signed Proxy Execution (context)	Older UAC bypass technique leveraging defaults handler hijack.	computerdefaults.exe launched from user context; default handlers registry anomalies	Image: *\computerdefaults.exe; correlate with handler registry changes within short time window
msiexec.exe	T1218.007 Msiexec; T1105 Ingress Tool Transfer; T1059 Script Execution (custom actions)	Installers fetching/launching payloads or executing custom actions via MSI.	msiexec /i http; /qn; /quiet; ALLUSERS=; TRANSFORMS=; unusual MSI sources	Image: *\msiexec.exe AND CommandLine contains /i AND http; unsigned MSI; odd parent processes; network start by msiexec