**Windows Sysmon Detection Queries**

**Network Connections**

|  |  |
| --- | --- |
| $SplitEvents | Where-Object { $\_.Id -eq 3 } | Where-Object { $\_.DestinationIp -notlike $SUBNET } | Look for connections made outside of the local subnet |
| $SplitEvents | where id -eq 3 | Where-Object { $\_.Image -match $Images } | Check for rundll32, powershell, cmd, or notepad |

**Process Creates**

|  |  |
| --- | --- |
| $SplitEvents | Where-Object {$\_.Id -eq 1 } | Where-Object {$\_.ParentCommandLine -match "noprofile"} | process creates with suspicious flags; encoded command, window hidden, no profile, IEX |
| $SplitEvents | where id -eq 1 | where image -match “ADMIN\$” | process create originating from admin share |
| $SplitEvents | Where-Object { $\_.Id -eq 1 } | Where-Object { $\_.User -eq "NT AUTHORITY\SYSTEM" } | Processes spawned by SYSTEM |
| $SplitEvents | Where-Object { $\_.Id -eq 1 } | Where-Object { $\_.Image -eq $Bad\_Files } | Check file executed against array of known bad; wmi, cscript, wscript, regsrv, rundll32, mshta, bitsadmin |
| $SplitEvents | Where-Object { $\_.Id -eq 1 } | Where-Object { $\_.Image -match "wmiprvse" } | Processes spawned from WMI |
| $SplitEvents | where id -eq 1 | where {$\_.CommandLine.length -gt 500 -and $\_.CommandLine -match "^powershell"} | powershell commands greater than a certain length (200-500ish?) |

**Process Injection**

|  |  |
| --- | --- |
| $SplitEvents | Where-Object { $\_.Id -eq 8 } | Possible process injection events; can narrow down to lsass specifically for mimikatz; check winlogon.exe for keylogger |

**Named Pipe Pivoting**

|  |  |
| --- | --- |
| $SplitEvents | Where-Object { $\_.Id -eq 17/18 } | SMB beacon |

**Unmanaged PowerShell**

|  |  |
| --- | --- |
| $SplitEvents | Where-Object { $\_.Id -eq 7 } | powerpick and psinject; processes that load the system.management dlls |

**File Creates**

|  |  |
| --- | --- |
| $SplitEvents | Where-Object { $\_.Id -eq 11 } | Where-Object { $\_.TargetFilename -match ".dll"} | File creates with .dll extension |