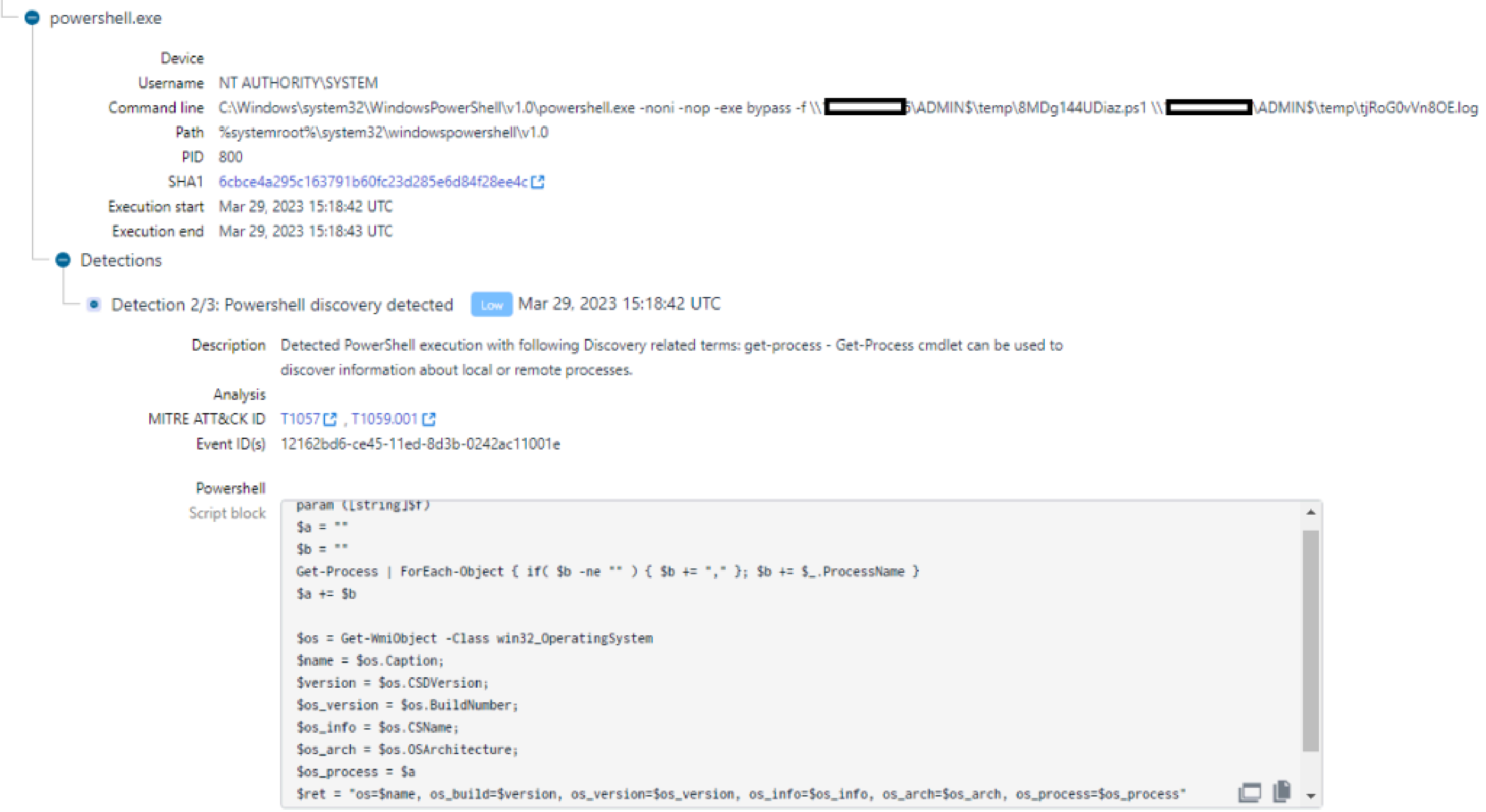

powershell.exe

Device
Username NT AUTHORITY\SYSTEM
Command line C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -noni -nop -exe bypass -f \\[redacted]\ADMIN$\temp\8MDg144UDiaz.ps1 \\[redacted]\ADMIN$\temp\tjRoG0vVn8OE.log
Path %systemroot%\system32\windowspowershell\v1.0
PID 800
SHA1 6cbce4a295c163791b60fc23d285e6d84f28ee4c
Execution start Mar 29, 2023 15:18:42 UTC
Execution end Mar 29, 2023 15:18:43 UTC

Detections

Detection 2/3: Powershell discovery detected Low Mar 29, 2023 15:18:42 UTC

Description Detected PowerShell execution with following Discovery related terms: get-process - Get-Process cmdlet can be used to discover information about local or remote processes.
Analysis
MITRE ATT&CK ID T1057 , T1059.001
Event ID(s) 12162bd6-ce45-11ed-8d3b-0242ac11001e

Powershell Script block

```
param ([string]$f)
$a = ""
$b = ""
Get-Process | ForEach-Object { if( $b -ne "" ) { $b += "," }; $b += $_.ProcessName }
$a += $b

$os = Get-WmiObject -Class win32_OperatingSystem
$name = $os.Caption;
$version = $os.CSDVersion;
$os_version = $os.BuildNumber;
$os_info = $os.CSName;
$os_arch = $os.OSArchitecture;
$os_process = $a
$ret = "os=$name, os_build=$version, os_version=$os_version, os_info=$os_info, os_arch=$os_arch, os_process=$os_process"
```