

# Malicious PowerShell Detections

## PLATFORM FEATURE UPDATE

**PowerShell** is a trusted management tool for system administrators that is also frequently used as an attack vector. The Malicious PowerShell Detection model utilizes a large dataset of legitimate PowerShell executions to detect string patterns associated with normal operations. PowerShell executions that break these patterns are flagged as anomalous and the behavior is summarized to help security analysts determine its significance.

Some important things to note are:

- Anomalous PowerShell executions are grouped together in one detection if they have similar signatures.
- Any execution containing 'PowerShell' in the command-line is a candidate for this detection.
- This model executes daily and produces detections for the previous day.

The screenshot displays the Adlum interface for a specific detection. At the top, navigation links include Settings, Learning Center, Reports, Tools, Modules, Tenants, and Support. The current tenant is 'Demonstration Tenant'. The main heading is 'Process Execution Detection - 15819' with a detection time of '2021-08-09 07:40:35 UTC'. Action buttons for '+ Add Note', 'Add to Investigation', and 'Clear' are visible.

**Detection Details:**  
 A machine learning algorithm has identified an anomalous set of process executions.  
 Details: powershell.exe -download

5	<b>Total Events</b> 5 Events Surrounding this Detection
📅	<b>First Occurrence</b> 2021-08-09 07:40:35 UTC
📅	<b>Last Occurrence</b> 2021-08-09 07:41:15 UTC

**Event Timeline:**

- August 09 2021 @ 07:40:35 Process: ping.exe
- August 09 2021 @ 07:40:45 Process: powershell.exe
- August 09 2021 @ 07:40:55 Process: powershell.exe
- August 09 2021 @ 07:41:05 Process: powershell.exe
- August 09 2021 @ 07:41:15 Process: wscript.exe

**Surrounding Events:**  
 Show 10 entries