Trellix Threat Intelligence Exchange and ATP Rule Content Update 1807

Below is the new/modified rule information for McAfee Threat Intelligence Exchange

New Rules

None

Updated Rules

Rule 238: ProcessCommandLocationInEval

Description: Identify abuse of common process's spawned from non-standard locations in Observe mode.

Default State: JcmExposureLevel_NoConnectivity_Evaluate

Changes in this release: Changes made to rule logic to improve effectiveness

Affected Products:

- Endpoint Security ENS 10.6.x, 10.7.x version

Rule 258: MasqueradedFileInEval

Description: Detect most likely masqueraded files which can result in suspicious process launches

Default State: JcmExposureLevel_NoConnectivity_Evaluate

Changes in this release: Changes made to rule logic to improve effectiveness

Affected Products:

- Endpoint Security ENS 10.6.x, 10.7.x version

Rules That Changed Exposure or Security Posture:

None