McAfee TIE and ATP Rule Content Update 1409

Below is the new/modified rule information for McAfee Threat Intelligence Exchange and ATP Rule content

**New Rules**

**Rule 268** – Protect against abuse of common process's spawned from non-standard locations

**Description:** Files may masquerade as legitimate files by hiding in non-standard locations. This rule protects against the suspicious running of common process's if spawned from non-standard locations (Mitre Technique-T1036)

**Default State:** ON

**Changes in this release:** New rule to block suspicious process'es

**Affected Products:**

✔ Endpoint Security ENS 10.6.x, 10.7.x versions

**Updated Rules**

**Rule 260** – Detect AMSI bypass techniques

**Description:** This rule is designed to prevent different techniques used to bypass Antimalware Scan Interface-AMSI (Tactic: Defense Evasion - Technique: T1562)

**Default State:** Evaluate

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

✔ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 500** – Block lateral movement from other windows machines in the network
Description: This rule blocks lateral movement from Windows Clients. It should only be turned on for systems that are in highly restrictive environments as it may generate many false positives (Tactic:Evasion and Escalation - Technique:T1078)

Default State: OFF

Changes in this release: Reduce Falses if enabled in high security environments

Affected Products:

✓ Endpoint Security ENS 10.6.x, 10.7.x versions

Rule 512 – Detect commands that allow for indirect execution outside of cmd and powershell

Description: Detect commands that can execute commands other than cmd or powershell. Indirect command execution can be a way for adversaries to evade some detections (Mitre Technique-T1202)

Default State: OFF

Changes in this release: Reduce Falses if enabled in high security environments

Affected Products:

✓ Endpoint Security ENS 10.6.x, 10.7.x versions

Rules That Changed Exposure or Security Posture:
None

Notes:
For more information refer the KB82925.