McAfee TIE and ATP Rule Content Update 1496

Below is the new/modified rule information for McAfee TIE and ATP Rule Content Update

New Rules

Rule 517 : Prevent actor process with unknown reputations from launching processes in common system folders

Description: This rule targets processes with an unknown process reputation (or lower) launching binaries from common system folders. It also looks for blank command lines as is common in some cobalt strike spawnto uses

Default State: Off

Changes in this release: New rule to detect common Cobalt strike spawnto's . The rule is aggressive in nature and could lead to false positives. It could be turned ON in high security environments through the EPO UI

Affected Products:

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

Updated Rules

None

Rules That Changed Exposure or Security Posture:

None

Notes:

For more information refer the KB82925.