McAfee TIE and ATP Rule Content Update 1420

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

New Rules

Rule 342 – Identify and block patterns being used in Ransomware attacks

Description: Looks for any potentially malicious invoking of patterns which are common in Ransomware attacks and blocks the execution

Default State: ON

Changes in this release: New rule to block suspicious patterns

Affected Products:

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

Rule 514 – Identify and detect DLL loads that have potentially been hijacked

Description: Detect attempts to hijack execution flow by preventing suspicious DLLs from being loaded

Default State: OFF

Changes in this release: New rule to detect attempts of Control flow hijacking legitimate binaries. (Tactic: Persistence, Privilege Escalation, Defense Evasion - Technique: T1574).

Affected Products:

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

Rule 515 – Protect against office apps launching unknown processes from non-standard locations

Description: Office Apps are commonly used to deliver malwares, this rule looks for launching of suspicious processes from office apps. This rule can generate false positives so it should be enabled in highly restrictive environments

Default State: OFF

Changes in this release: New rule to block suspicious execution from office apps

Affected Products:

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

Updated Rules

Rule 5 – Use GTI URL reputation to identify trusted or malicious process

Description: . This rule is designed to detect based on URL reputation available in GTI

Default State: On

Changes in this release: Improve detection effectiveness

Affected Products:

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

Rule 307 – Prevent wmiprvse.exe and netsh.exe from launching script interpreters or other dual use tools

Description: . Prevent wmiprvse.exe and netsh.exe from launching script interpreters or other dual use tools

Default State: Evaluate

Changes in this release: Improve detection effectiveness

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.