Threat Intelligence Exchange Rule Content Update 711

Release Notes: 2017-12-14

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

New Rules

Rule 243 – Identify and block suspicious process executions

Description: This rule identifies suspicious execution of an application through execution parameters

Default State: Evaluate

Changes in this release: Added New rule to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.5.3 version

Updated Rules

Rule 239 – Identify suspicious command parameter execution

Description: This rule identifies suspicious execution of an application through execution parameters

Default State: Evaluate

Changes in this release: Added New rule to improve detection effectiveness

Affected Products:

- ✓ Endpoint Security 10.5.3 version

Rules That Changed Exposure or Security Posture:

Rule 136 – Identify unsigned NativeImage Files that Might Be Trusted

Description: This rule detects pre compiled binary files that Might Be Trusted that have been installed into the NativeImages folder and do not contain suspicious attributes

Default State: On

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x, 16.x versions

Notes:

None.