Threat Intelligence Exchange Rule Content Update 513

Release Notes: 2016-08-17

Below is the new/modified rule information for McAfee Threat Intelligence Exchange 1.0

New Rules

None.

Updated Rules

Rule 126 – Identify trusted signed applications

Description:

This rule identifies files that are signed and have a valid non self-signed certificate. File location is considered along with environmental attributes such as Start menu entry.

Default State: On

Changes in this release:

- **Updated algorithm to reduce potential false postives.**

Rule 241 – Identify new suspicious files seen on a small number of systems (v2)

Description:

Detects files that originated from an externally-facing application (a network-aware application that downloads files). These are newly discovered files in the environment and have characteristics and import functions that indicate they are suspicious.

Default State: Evaluate

Changes in this release:

- **Updated algorithm to reduce potential false postives.**

Rules That Changed Exposure or Security Posture:

Rule 153 Identify files that ATD does not report as suspicious.

Description:

This rule identifies files that have been assessed by Advanced Threat Defense and are not reported as suspicious.

Default State: Evaluate

Changes in this release:

- **Fixed a defect that prevented this rule from acting on a reputation notification from an ATD appliance.**

Notes:

None.