Threat Intelligence Exchange Rule Content Update 452

Release Notes: 2016-05-19

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

New Rules

Rule 246 - Identify new suspicious files seen on a small number of systems (v3)

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

Updated Rules

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:

None.

Notes: