Threat Intelligence Exchange Rule Content Update 424

Release Notes: 2016-03-14

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

New Rules

Rule 240 - Identify suspicious files with characteristics that have been predominantly seen in ransomware

Description:

Identify suspicious files with characteristics that have been predominantly seen in ransomware, are in uncommonly used locations and less than 7 days old

Default State: Evaluate

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

Updated Rules

Rule 10 - Identify that a file is the main component of a trusted installer using the file's reputation

Description:

This rule determines if file is a trusted installer based on the file's GTI or Enterprise reputation. It also looks at the file and company name to determine if it is an updater or installer component that can be trusted.

Default State: Mandatory

Changes in this release:

- **Updated Trusted Installer algorithm to reduce potential false negatives.**

Rule 139 - Identify trusted DOTNet assemblies

Description:

This rule detects files that have CLR code (DOTNet) and have been installed into the global assembly cache folders. The files are present on multiple machines within the enterprise, indicating they are not just-in-time compiled assemblies.

Default State: Mandatory

Changes in this release

- **Changed how age and prevalence are handled in DOTNet validation algorithm.**

Rules That Changed Exposure or Security Posture:

Rule 219 - Identify a suspicious file that hides in a secure location

Description:

This rule identifies files that are in secured locations, such as folders reserved for system drivers. The files do not use the native subsystem, and have suspicious characteristics such as missing or incorrect version information, or a file type that does not match the extension.

Default State: On

Changes in this release

- **Adjusted the criteria to determine under what conditions the rule will evaluate the file.**