Threat Intelligence Exchange Rule Content Update 493

Release Notes: 2016-07-21

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

New Rules

None.

Updated Rules

Rule 12 – Identify that a file is the main component of a trusted installer based on a specific file identified by hash

Description:

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

Default State: On

Changes in this release:

- **Updated algorithm to increase performance**

Rule 138 - Identify trusted unsigned Microsoft DOTNet assemblies

Description:

Ths rule detects Microsoft-provided files that have a CLR code (DOTNet), have been installed into the global assembly cache folders, and do not contain suspicious attributes. The files may or may not be found on multiple machines within the enterprise, which could include just-in-time compiled assemblies.

Default State: On

Changes in this release:

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

Rules That Changed Exposure or Security Posture:

Rule 20 - Identify trusted files with McAfee Privileges

Description:

This rule identifies trusted files using certificates or hashes that are distributed in the AV DAT files and may also have elevated privileges with McAfee processes and drivers.

Default State: On

Changes in this release:

- **Increased priority of rule to run earlier in the evaluation process.**

Notes:

None.