Threat Intelligence Exchange Rule Content Update 310

Release Notes: 2015-03-05

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

New Rules

Rule 152 - Identify safe files extracted by Windows Installer

Description:

This rule identified safe files extracted by Windows Installer based on the actor process, certificate and cloud reputation. If anything suspicious about the installer dropped file, the rule will not yield a clean reputation

Default state: Evaluate

Updated Rules

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

- Rule fine-tuned to reduce false positives.