Threat Intelligence Exchange Rule Content Update 552

Release Notes: 2016-09-27

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

New Rules

None.

Updated Rules

Rule 207 – Identify suspicious files executing from the Recycle bin

Description:

This rule identifies suspicious files that reside in and are executed from the Recycle bin.

Default State: On

Changes in this release:

- **Updated algorithm to improve detection effectiveness.**

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:

- **Updated algorithm to improve detection effectiveness.**

Rules That Changed Exposure or Security Posture:

None

Notes:

None.