Threat Intelligence Exchange Rule Content Update 339

Release Notes: 2015-08-03

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

New Rules

Rule 153 - Identify files that ATD does not report as suspicious.

Description:

This rule identifies files that have been assessed by Advanced Threat Defense and are not reported as suspicious.

Default State: Evaluate

Updated Rules

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

- Bug corrected that under certain conditions could cause a file outside of the secured locations to be improperly detected as malicious.

Rules That Changed Exposure or Security Posture:

None.

Notes:

This release provides translated rule names, descriptions, and long descriptions.