Threat Intelligence Exchange Rule Content Update 696

Release Notes: 2017-09-22

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

New Rules

None.

Updated Rules

Rule 136 – Identify unsigned NativeImage Files that Might Be Trusted

Description: This rule detects pre compiled binary files that Might Be Trusted that have been installed into the NativeImages folder and do not contain suspicious attributes

Default State: Evaluate

Changes in this release: Add logic to improve performance

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan
- ✓ Cloud-AV
- ✓ WSS 15.x, 16.x versions

Rules That Changed Exposure or Security Posture:

Rule 233 – Identify suspicious files from the Internet

Description: Identifies files that come from an untrusted URL. They are malicious and have suspicious characteristics such as being packed, or having a low age or prevalence

Default State: Off

Changes in this release: Changes in logic to improve detection effectiveness in progress

Affected Products:

- ✓ Endpoint Security 10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Notes:

None.