Threat Intelligence Exchange Rule Content Update 667

Release Notes: 2017-06-22

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

New Rules

Rule 252 – Identify files that CTD reports as suspicious

Description: Identifies files that Cloud Threat Detection reports as High or Very High and issues a Most Likely Malicious reputation

Default State: Evaluate

Changes in this release: New Rule to identify files that Cloud Threat Detection reports wilth High or Very High trust score and issues a Most Likely Malicious reputation. This rule will not issue a reputation for files that CTD determines with Medium trust score

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

Updated Rules

None.

Rules That Changed Exposure or Security Posture:

Rule 217 – Identify a suspicious password stealer

Description: Identifies files that have been incorrectly installed into the user's roaming profile and has suspicious characteristics

Default State: On

Changes in this release: Changed from required TIE Connectivity to GTI connectivity exposure level

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

Notes:

None.