Threat Intelligence Exchange Rule Content Update 795

Release Notes: 2019-01-17

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

New Rules

None

Updated Rules

Rule 2 – Use Enterprise file reputation to identify trusted or malicious files

Description: Determines if a file is trusted or malicious based on the file's Enterprise reputation

Default State: On

Changes in this release: Improve performance of the rule

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 15.x, 16.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 300 – Prevent office applications from launching child processes that can execute script commands

Description: Attempts to prevent office applications from being abused to deliver malicious payloads

Default State: On

Changes in this release: Improve detection effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

Rule 243 – Identify and block suspicious process executions

Description: This rule identifies and blocks suspicious execution of a process in an application by giving dirty reputation

Default State: Evaluate

Changes in this release: Improve product performance

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 15.x, 16.x versions

Rules That Changed Exposure or Security Posture:

Rule 255 – Detect potentially obfuscated command line parameters

Description: This rule is designed to analyze command line parameters passed to programs to alert on potentially obfuscated strings that could indicate malicious behavior

Changed State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions
- ✓ WSS 16.x versions

Rule 256 – Detect use of long -encodedcommand powershell

Description: Attempts to look for suspicious usage of the -encodedcommand option in powershell. Usage can indicate potentially malicious invocations of powershell

Changed State: Evaluate

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions
- ✓ Endpoint Security ENS 10.5.x versions

- ✓ WSS 16.x versions

Notes:

For more information refer the KB82925.