Threat Intelligence Exchange Rule Content Update 778

Release Notes: 2018-10-19

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

New Rules

None

Updated Rules

Rule 239 – Identify suspicious command parameter execution

Description: Identifies the suspicious execution of an application through command line parameters

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 most probable suspicious command parameter execution

Description: Identifies the most probable suspicious execution of an application through command line parameters

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

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

Rule 301 – Aggressively blocks processes with unknown reputations from being spawned by office applications

Description: Any process with an unknown reputation will be blocked when launched by office applications

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 304 – Identify suspicious payloads targeting Browser related applications

Description: Identify suspicious payloads targeting Browser related applications like Firefox, Chrome, Edge and others

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 307 – Identify suspicious payloads targeting Network related services or applications

Description: Identify suspicious payloads targeting Network related services or applications and will not allow launch of tools which indicate suspicious behaviour

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 315 – Aggressively blocks processes with unknown reputations from being spawned by text editors

Description: Any process with an unknown reputation will be blocked when launched by text editors

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 316 – Prevent PDF readers from launching processes that can execute scripts in all rule group assignments

Description: Prevent PDF readers from launching processes that can execute scripts

Default State: On

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rule 318 – Aggressively prevent PDF readers from launching processes with an unknown reputation

Description: Any process with an unknown reputation will be blocked when launched by PDF readers

Default State: Evaluate

Changes in this release: Improve Detection Effectiveness

Affected Products:

- ✓ Endpoint Security ENS 10.6.x versions

Rules That Changed Exposure or Security Posture:

None

Notes:

For more information refer the KB82925