# McAfee TIE and ATP Rule Content Update 1314

Below is the new/modified rule information for McAfee Threat Intelligence Exchange and ATP Rule content

## New Rules

**Rule 506 –** Detect commands for user discovery

**Description:** This rule attempts to detect and block common commands used for user discovery. To be turned ON for Highly restrictive Environments only. (Tactic: Execution, Discovery - Techhnique: T1033).

**Default State**: OFF

**Changes in this release:** New rule to detect and block commands for user discovery for highly restricted environments

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 507 –** Detect commands used to discover more information about a system

**Description:** This rule attempts to detect and block common commands used for system discovery. To be turned ON for Highly restrictive Environments only. (Tactic: Execution, Discovery - Techhnique: T1033).

**Default State**: OFF

**Changes in this release:** New rule to detect and block commands for system discovery for highly restricted environments

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 508 –** Detect commands used to discover permission information related to users and groups

**Description:** This rule attempts to detect and block commands used to discover user permissions. To be turned ON for Highly restrictive Environments only (Tactic: Execution, Discovery - Techhnique: T1033).

**Default State**: OFF

**Changes in this release:** New rule to detect and block commands for users and groups permission for highly restrictive environments

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 509 –** Detect commands used to discover network related configurations

**Description:** This rule attempts to detect commands used to discover network related configurations.To be turned ON for Highly restrictive Environments only. (Tactic: Execution, Discovery - Techhnique: T1033).

**Default State**: OFF

**Changes in this release:** New rule to detect and block commands for network discovery in highly restricted environments

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 510 –** Detect data encryption attempts for suspicious activities

**Description:** This rule attempts to detect and block data encryption attempts of suspicious process activities. To be turned ON for Highly restrictive Environments only. (Tactic: Collection Discovery - Techhnique: T1560).

**Default State**: OFF

**Changes in this release:** New rule to detect and block data encryption attempts of suspicious activities

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

## Updated Rules

**Rule 5 –** Use GTI URL reputation to identify trusted or malicious processes

**Description:** This rule determines if a process is trusted or malicious based on the GTI URL reputation

**Default State**: Evaluate

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 239 –** Identify suspicious command parameter execution

**Description:** This rule targets suspicious invocations of command and script interpreters

**Default State**: On

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 243 –** Identify and block suspicious process executions

**Description:** This rule takes a more aggressive approach than the default on rule ID 239 so it is in observe by default in all rule group assignments. It will need to be manually enabled if you wish to use it

**Default State**: Evaluate

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 260 –** Detect AMSI bypass techniques

**Description:** This rule attempts to detect and prevent different techniques used to bypass Antimalware Scan Interface(AMSI)

**Default State**: Evaluate

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 263 –** Detect processes accessing suspicious URLs

**Description:** This rule attempts to detect processes having suspicious URLs in command parameters used to download malicious payload

**Default State**: On

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

**Rule 266 –** Identify target process launching non standard extensions or launched by non-standard actor

**Description:** This rule attempts to detect target process launching non standard file extensions

**Default State**: Evaluate

**Changes in this release:** Improve detection effectiveness

**Affected Products:**

- ✓ Endpoint Security ENS 10.6.x, 10.7.x versions

## Rules That Changed Exposure or Security Posture:

**None**

## Notes:

**For more information refer the KB82925.**