McAfee TIE and ATP Rule Content Update 1405

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

New Rules

Rule 511 – Detect attempts to dump sensitive information via registry or lsass

Description: This rule detects commands that can be used to dump sensitive OS information related to credentials. Some software may do this legitimately so false positives may be generated using this rule. Hence this rule must be turned ON for highly restricted environments only (Tactic: Credential Access - Technique: T1003).

Default State: OFF

Changes in this release: New rule to block abuse of LSASS utility

Affected Products:

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

Rule 513 – Detect commands used for copying files from a remote system

Description: Block remote copy operations or lateral tool operations from external environment. This rule can generate false positives, hence meant for highly restrictive environments. Some scripts may legitimately use these commands so false positives may be generated when enabling this rule. Hence, to be turned ON for Highly restrictive Environments only. (Tactic: Command and Control - Technique: T1105, T1570).

Default State: OFF

Changes in this release: New rule to detect and block commands for indirect command execution in highly restricted environments

Affected Products:

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

Updated Rules

Rule 333 – Identify suspicious process chains

Description: This rule Identifies interesting process chains and block them if behaviour is not desirable or suspicious

Default State: Evaluate

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 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 341 – Identify and block patterns being used in Ransomware attacks

Description: This rule attempts to detect and prevent abuse of WMI service for execution of code and persistence

Default State: Evaluate

Changes in this release: Improve detection effectiveness

Affected Products:

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

Rule 506 – Detect commands for user discovery

Description: Upon gaining a foothold an attacker may attempt to use common system administration tools to learn more about the system they have gained access to. This rule can generate false positives due to its generic coverage, hence it is meant only for highly restricted environments

Default State: OFF

Changes in this release: Improve detection effectiveness

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 Upon gaining a foothold an attacker may attempt to use common system administration tools to further discover details such as hotfixes installed and OS version to better understand the box they have gained initial access to. This rule can generate false positives due to its generic coverage, hence it is meant only for highly restricted environments

Default State: OFF

Changes in this release: Improve detection effectiveness

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: During the discovery phase of an attack, an adversary may use common tools to enumerate what user and groups have permissions to different assets in the enviornment. These commands can generate false positives due to how generic they are but can serve as a potential indicator of compromise during the discovery phase of an attack

Default State: OFF

Changes in this release: Improve detection effectiveness

Affected Products:

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

Rule 509 – Detect commands used to discover network related configurations

Description: During the discovery phase of an attack, an adversary may use common tools to enumerate network configuration and network connections. These commands can generate false positives due to how generic they are but can serve as a potential indicator of compromise during the discovery phase of an attack
Default State: OFF

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.