Threat Intelligence Exchange Rule Content Update 743

Release Notes: 2018-04-26

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

New Rules

Rule 301 – Identify most probable suspicious payloads for office applications

Description: Identify most probable suspicious payloads for office applications

Default State: Evaluate

Changes in this release: New Rule added to improve detection effectiveness for office based malware attacks

Affected Products:

- ✓ Endpoint Security 10.5.3 HF3, 10.5.4 RTS version

Updated Rules

Rule 4 – Use GTI file reputation to identify trusted or malicious files

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

Default State: Mandatory

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

Rule 140 – Identify trusted prevalent files

Description: Detects files that have been present in the enterprise for a long time and are prevalent across multiple machines

Default State: Mandatory

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 129 – Identify trusted signed utility applications

Description: Identifies utility applications that are signed and the certificate is not distrusted. These files do not launch on startup and have characteristics that suggest they are utility programs

Default State: Mandatory

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

Rule 130 – Identify trusted signed drivers

Description: Identifies device drivers that are signed and installed on the local system

Default State: Mandatory

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

Rule 131 – Identify trusted signed Digital Rights Management (DRM) libraries

Description: Identifies signed trusted Digital Rights Management libraries used by Windows

Default State: Mandatory

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

Rule 132 – Identify trusted signed files

Description: Identifies files that are signed and trusted, and whose certificate reputation is trusted

Default State: Mandatory

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

Rule 152 – Identify safe files extracted by Windows Installer

Description: Identifies safe files extracted by Windows Installer installer based on the actor process, certificate and cloud reputation

Default State: Evaluate

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

Rule 222 – Identify a suspicious keylogger hiding as an installed program

Description: Detects files that import keylogging APIs and hide in locations used by an installed program. They have suspicious characteristics such as a small number of imports and being new to the system, while not looking like a legitimate application.

Default State: On

Changes in this release: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

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: Reduction of un-necessary cloud lookup and improve performance

Affected Products:

- ✓ Endpoint Security 10.1,10.2 and 10.5.x versions
- ✓ Threat Intelligence Exchange for Virus Scan

Rule 95 – Identify files that are signed by certificate of known clean reputation and mark them Most Likely Trusted when offline

Description: Identifies files that are signed by certificate of known clean reputation and mark them Most Likely Trusted when offline

Default State: On

Changes in this release: Improve performance

Affected Products:

- ✓ Endpoint Security 10.5.3 version
- ✓ 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

Rules That Changed Exposure or Security Posture:

None.

Notes:

None.