Threat Intelligence Exchange Rule Content Update 878
Release Notes: 2018-3-7

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

New Rules

None

Updated Rules

Rule 324 – Prevent mshta from launching suspicious process

Description: Attempts to prevent Prevent mshta from launching suspicious process

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 309 – Block processes attempting to launch from office applications. Rule enabled only in high security policies

Description: Attempts to prevent office applications from being abused to deliver malicious payloads when it is enabled to systems with a high security policies

Default State: Evaluate / On (only in HighSecurity)

Changes in this release: Improve in 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

Rule 221 – Identify new suspicious files seen on a small number of systems

Description: This rule detects files that originated from an externally-facing application (a network-aware application that downloads files). The files have been in the environment for less than 10 days and are seen on less than 1% of machines. The files are not signed with a prevalent or trusted certificate, and they have some suspicious characteristics, such as being packed, having no resources, and missing version information. They also have import functions that indicate they are suspicious, such as using native APIs, creating remote threads, checking for debuggers, or installing layered service providers

Default State: Evaluate

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 219 – Identify a suspicious file that hides in a secure location

Description: This rule identifies files that are in secured locations, such as folders reserved for system drivers. The files do not use the native subsystem, and have suspicious characteristics such as missing or incorrect version information, or a file type that does not match the extension

Default State: GTI Connectivity

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 217 – Identify a suspicious password stealer

Description: This rule identifies a file that has been incorrectly installed into the user's roaming profile and has suspicious characteristics. The file imports APIs that are used for monitoring keystrokes, capturing screenshots, or checking for active debuggers

Default State: GTI Connectivity

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 207 – Identify suspicious files executing from the Recycle bin

Description: This rule identifies suspicious files that reside in and are executed from the Recycle bin

Default State: GTI Connectivity

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 205 – Identify suspicious files that have odd creation dates and are likely not packed

Description: Identifies suspicious files that are likely not packed, have odd creation dates, and are in locations such as the Temp or Downloads folders

Default State: Evaluate

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 152 – Identify safe files extracted by Windows Installer

Description: This rule identifies safe files extracted by Windows Installer based on actor process, certificate and cloud reputation. If anything is suspicious about the installer dropped file, the rule will not yield a clean reputation

Default State: Evaluate

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 139 – Identify unsigned DOTNet assemblies that Might Be Trusted

Description: This rule detects files that Might Be Trusted that have been installed into the global assembly cache folders and do not contain suspicious attributes. These files are often on few systems in the network and may include pre-compiled DOTNet native image files and similar assemblies

Default State: GTI Connectivity

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 138 – Identify trusted unsigned Microsoft DOTNet assemblies

Description: This rule detects Microsoft-provided files that have CLR code (DOTNet), have been installed into the global assembly cache folders, and do not contain suspicious attributes. The files may or may not be found on multiple machines within the enterprise, which could include just-in-time compiled assemblies

Default State: GTI Connectivity

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 137 – Identify unsigned DOTNet assemblies that Might Be Trusted

Description: This rule detects files that Might Be Trusted that have been installed into the global assembly cache folders and do not contain suspicious attributes. These files are often on few systems in the network and may include pre-compiled DOTNet native image files and similar assemblies

Default State: GTI Connectivity

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 136 – Identify unsigned NativeImage Files that Might Be Trusted

Description: This rule detects pre compiled binary files that Might Be Trusted that have been installed into the NativeImages folder and do not contain suspicious attributes

Default State: GTI Connectivity

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

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

Description: This rule identifies trusted Digital Rights Management libraries that are signed and whose certificate is trusted. These files are in the Windows DRM and DRM cache folders

Default State: Mandatory

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 130 – Identify trusted signed drivers

Description: This rule identifies device drivers that are signed and installed on the local system. They use the native subsystem and are located in the %windir%\\system32\\drivers or driverstore folders

Default State: Mandatory

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 128 – Identify trusted help resource libraries

Description: This rule identifies signed resource libraries that are used by trusted software. The libraries are generally used as part of the application Help documentation. They are signed and do not have a malicious certificate reputation. They have characteristics indicating it is a resource library such as no imports or exports and a small number of Portable Executable (PE) Sections. They are also located in application installation folders

Default State: Mandatory

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 127 – Identify trusted Help resource libraries

Description: This rule identifies resource libraries that are used by trusted software. The files are signed and do not have a malicious certificate reputation. They have characteristics indicating it is a resource library, such as no imports or exports and a small number of Portable Executable (PE) Sections

Default State: Mandatory

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 126 – Identify trusted signed applications

Description: This rule identifies files that are signed and have a valid non self-signed certificate. File location is considered along with environmental attributes such as Start menu entry

Default State: Evaluate

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 125 – Identify files marked as Trusted Windows AppStore Applications

Description: This rule identifies files that are marked as trusted Windows AppStore Applications based on the file attributes, file location and process attributes

Default State: Evaluate

Changes in this release: Support for Windows CaseSensitivity feature

Affected Products:

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

Rule 58 – Identify trust for files executed on network shares

Description: This will identify trust for files executed on network shares using scanner results and file attributes to indicate trust

Default State: Evaluate

Changes in this release: Support for Windows CaseSensitivity feature

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:

None

Notes:

For more information refer the KB82925.