Threat Intelligence Exchange Rule Content Update 392

Release Notes: 2015-11-26

Below is the new/modified rule information for McAfee Threat Intelligence Exchange 1.0

New Rules

Rule 61 - Identify internet facing applications

Description:

This rule identifies internet facing applications such as a web browser or email client by using identifiable attributes such as file name and certificate

Default State: Mandatory

Rule 62 - Identify an application which reads content files

Description:

This rule identifies the main executable file of popular applications which reads content such as PDF documents, Microsoft Office documents, videos, etc. This rule does not assign a reputation but generates metadata about a process for use in subsequent rules.

Default State: Mandatory

Rule 235 - Identify suspicious files from the Internet that might be malicious based on GTI reputation

Description:

This rule identifies files that came from an untrusted URL. They are malicious and have suspicious characteristics such as being packed, are less than 15 days old, and appear on less than 10 systems or 1% of the enterprise.

Default State: Mandatory

Rule 238 - Identify a file written or executed by an internet facing application suspiciously

Description:

This rule identifies files that were created, or executed, in a way not typically performed by a user. Furthermore, the files themselves resemble malware rather than legitamte documents and programs.

Default State: Mandatory

Rule 239 - Identify suspicious command parameter execution

Description:

This rule identifies suspicious execution of an application through execution parameters.

Default State: Mandatory

Updated Rules

Rule 1 - Use certificate reputation to identify trusted or malicious files

Description:

This rule determines if a file is trusted or malicious based on the GTI or Enterprise certificate reputation of the signing certificate. The certificate reputation must be at least Known Malicious, Known Trusted, Most Likely Malicious, or Most Likely Trusted.

Default State: Mandatory

Changes in this release

- **Removed the File Reputation override of Certificate Reputation.**

Rules That Changed Exposure or Security Posture:

Rule 57 - Use GTI file reputation to identify files that Might be Trusted or Might be Malicious

Description:

This rule identifies files which are less conclusive in their GTI reputation such as Might be Trusted and Might be Malicious.

Default State: Evaluate

Changes in this release

- **This rule no longer requires TIE Connectivity, but will run with GTI-only Connectivity.**

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

- **This rule no longer requires TIE Connectivity, but will run with GTI-only Connectivity.**

Rule 237 - Find suspicious files signed with a revoked certificate

Description:

This rule detects files with an embedded certificate that has been revoked. The files have been in the environment for less than 5 days and are seen on less than 1% of machines.

Default State: Evaluate

Changes in this release

- **This rule has been downgraded to Evaluate state due to changes in how Certificate Revocation is determined.**

Rule 211 - Identify suspicious files created by an untrusted process

Description:

This rule identifies a file that is suspicious because the process that created it has a reputation of Might be Malicious to Known Malicious at the time of creation. The file also has not been modified since its creation.

Default State: Evaluate

Changes in this release

- **This rule no longer requires TIE Connectivity, but will run with GTI-only Connectivity.**

Rule 213 - Identify a file as suspicious based on how it is packed

Description:

This rule identifies a file as suspicious when it is determined to be packed or encrypted, and there are features in the file that are not commonly found in legitimate software.

Default State: Evaluate

Changes in this release

- **This rule no longer requires TIE Connectivity, but will run with GTI-only Connectivity.**

Rule 218 - Identify a suspicious file that hides its age

Description:

This rule identifies files that modify the presented age of the file. The files contain suspicious characteristics such as being packed, missing version information, tagged as a system file, or importing suspicious APIs. They are not present in a path typically used for installed programs.

Default State: Evaluate

Changes in this release

- **This rule no longer requires TIE Connectivity, but will run with GTI-only Connectivity.**

Rule 220 - Identify new suspicious files

Description:

This rule identifies files that have a creation date in the last 30 days and contain suspicious characteristics. These include modified section names or modified code at the entry point of the binary.

Default State: Evaluate

Changes in this release

- **This rule no longer requires TIE Connectivity, but will run with GTI-only Connectivity.**

Notes: