Threat Intelligence Exchange Rule Content Update 329

Release Notes: 2015-05-28

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

New Rules

No new rules.

Updated Rules

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

- Bug corrected that improperly calculated prevalence on first contact with file.

Rules That Changed Exposure or Security Posture:

None.

Notes:

A defect was identified and addressed that could have possibly allow rules to finalize without setting reputation.