Release Announcement: ESET Enterprise Inspector 1.5.1485

2020-11-06 - Steef | ESET Nederland - Reacties (0) - Releases

It is with great pleasure that I would like to announce the release of ESET Enterprise Inspector v1.5 which introduces improvements in multiple areas but this release is especially focused on strengthening its detection capabilities. This is a smaller service release, however we recommend this version to be used by all Enterprise Inspector customers.

I would like to point out things like the ability to work with rules via API which makes it even more suitable to be used in conjunction with SIEM tools and the ability to automate Network Isolation of Windows endpoints thanks to opening this action to the internal rule engine. The detection capability improvements are also a strong benefit of this version and we believe that existing users will also notice the performance improvements we have introduced in many areas. Please find the full changelog below.

Changelog

- **General Improvements**
  - Added: Ability to work with rules via Public REST API (list, create, edit and delete)
  - Added: Ability to trigger Network Isolation via Rules (only for Windows endpoints)
  - Added: Support for full Unicode characters
  - Added: Ability to add multiple comments to Detection, Executables, Computers, and Processes
  - Added: Various performance improvements (e.g. faster search, purge, rules engine and others)
  - Fixed: Multiple issues related to internal server errors and exclusions
- **New Detection Capabilities**
  - Added: Improved detection capability for advanced code injection methods
  - Added: Ability to invalidate trust attributes of compromised processes
  - Added: Information related to execution of files via shortcuts (LNK files)
  - Added: Visibility into file reading operations for specific scenarios (e.g. reading of passwords)
  - Added: Visibility into WMI Query behavior
  - Added: Information about named pipes (to detect e.g. Cobalt Strike)
  - Added: Visibility into MS Office VBA macros (if enabled in MS Office)
  - Added: Ability to detect suspicious protocols (e.g. TOR, VNC, and BitTorrent)

Known Issues

- When upgrading to v1.5 from previous versions installer doesn't remove obsolete rules. You can delete obsolete rule 'Network communication through port typical for TOR [B0503]' manually.

Release notes

- Please use the .msi installer to upgrade the EEI server

Installation packages

- EEI build 1.5.1485 available on our official download page

Language

- English