Antivirus Settings

The settings below control the behavior of the ClamAV antivirus engine. ClamAV is the default engine that comes pre-configured with Hermes SEG. Additional antivirus scanners can be installed such as Sophos but the settings below ONLY apply to ClamAV.

Scan Email Files

This setting enables the scanning of email files. If this setting gets disabled, it will effectively completely disable the ClamAV antivirus engine. Recommended to be set to **Enabled**.

Scan Archives

This setting enable scanning of archive files such as ZIP, RAR, GZ etc. This setting will also enable the scanning of Microsoft Word .DOCX files, which are considered archives by the system. Recommended to be set to **Enabled**.

Mark Encrypted Archives as Viruses

This setting tells ClamAV to treat any encrypted archives such as encrypted ZIP, RAR and .DOCX files as viruses. ClamAV is not able to open and scan encrypted archives so it's impossible to tell if there are malware present in the archive. Recommended to be set to **Disabled**.

Scan Portable Executables

This settings enables the scanning of Portal Executable files. Portable Executable is a file format is a file format used in all version of Windows OS. This option allows ClamAV to perform a deeper analysis of executable files and it's also required for decompression of popular executable packers such as UPX. Recommended to be set to **Enabled**.

Scan OLE2 files

This setting enables the scanning of OLE2 files such as Mcrosoft Office Documents and .MSI files. Recommended to be set to **Enabled**.

Block OLE2 Macros

This setting will bypass ALL Antivirus signatures and block ALL OLE2 files with VBA Macros in them whether malicious or not. In effect, it will treat any macros embedded in OLE2 files as a virus. This setting has no effect Scan OLE2 files setting above is set to disabled. Recommended to be set to **Disabled**.

Scan PDF files

This setting enables the scanning of .PDF files. Recommended to be set to **Enabled**.

Scan and normalize HTML

This setting enables HTML detection and normalisation. Recommended to be set to **Enabled**.

Algorithmic Detection

This setting enables the detection of complex malware and exploits in graphic files and others by allowing ClamAV to use special algorithms in order to provide accurate detection. Recommended to be set to **Enabled**.

Scan Executable and Linking Format Files (ELF)

This setting enables the scanning of ELF files. ELF files are is a standard format for Unix executables. Recommended to be set to **Enabled**.

Signature Based Detection of Phishing Attempts

This setting enables the detection of phishing attempts by using signatures. Recommended to be set to **Enabled**.

Scan Email URLs for Phishing Attempts

This settings enables the detection of phishing attempts in URLs using heuristics. This setting will classify unwanted phishing emails as **Phishing.Heuristics.Email.***. Recommended to be set to **Enabled**.

Block SSL Mismatches in Email URLs

This setting will always block SSL mismatches in URLs, even if the the URL isn't in the threat database. This setting has can lead to false positives. Recommended to be set to **Disabled**.

Block Cloaked Email URLs

This setting will always block cloaked URLs even if the URL isn't in the threat database. This setting can lead to false positives. Recommended to be set to **Disabled**.

Detect Possibly Unwanted Applications

This setting enables the detection of Possibly Unwanted Applications (PUA) such as runtime packers, password tools, network tools, P2P clients, IRC clients, remote access trojans, process killers, keyloggers and various spying tools, Javascript scripts, ActiveX scripts etc. Recommended to be set to **Enabled**.

Heuristic Scan Precedence

When this setting is enabled, if a heuristic malware matches, the scanning will stop immediately thus saving CPU. When this setting is disabled, heuristic matches will be reported at the end of the scan. For example, if disabled and an archive contains both a heuristically detected malware and a signature based malware, the signature based malware will be reported. If signature based malware is found, the scan stops immediately regardless of whether this option is enabled or not. Recommended to be set to **Disabled**.

Revision #1
Created 2 January 2021 14:20:27 by Dino Edwards
Updated 20 May 2023 22:22:35 by Dino Edwards