Yara

The page displays a list of YARA signatures. YARA signatures can be used to detect known malware, malicious behavioral patterns, and their classification.

There is a mandatory list of signatures from the vendor, highlighted in gray.

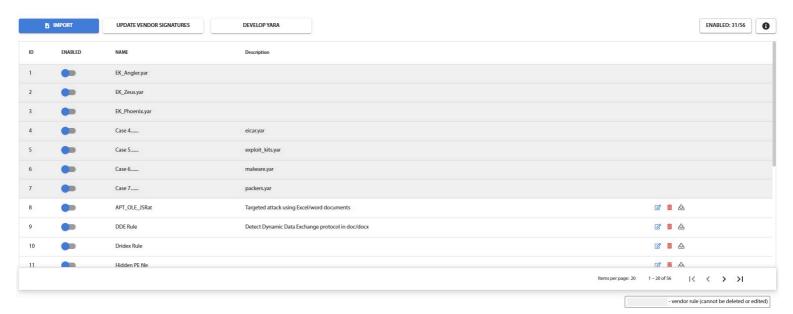


Fig. 4.6.1 - YARA signatures table

By clicking on the button



you can open a window with detailed information about the modules and more.

Information	
Service version:	1.0.3
Vendor rules create time:	12/04/21 11:43:41
Vendor rules update time:	12/04/21 11:50:19
Vendor rules version:	1
Yara modules:	PE, ELF, Hash, Math, Time, Cuckoo, Magic,
	Dotnet
Yara version:	4.0.2

Fig. 4.6.2 - Window with detailed information about Yara

The button 🕹 allows you to download the Yara signature as a .yara file format.

The import of a rule is carried out using the button



For import, you need to specify the path to the file in the ".yara" format, as well as provide a name and description. Vendor signatures can only be updated through the system functionality using the button

UPDATE VENDOR SIGNATURES . An archive file with signatures is used as input.

Edit this page