

# Yara

Страница, на которой отображается список yara-сигнатур. YARA сигнатуры могут быть использованы для обнаружения известных вредоносных программ, вредоносных поведенческих шаблонов и их классификации.

Существует обязательный список сигнатур от вендора, подсвеченных серым цветом.

ID	ВКЛЮЧИТЬ	НАЗВАНИЕ	ОПИСАНИЕ	
1	<input checked="" type="checkbox"/>	EK_Angler.yar		
2	<input checked="" type="checkbox"/>	EK_Zeus.yar		
3	<input checked="" type="checkbox"/>	EK_Phoenix.yar		
4	<input checked="" type="checkbox"/>	Case 4.....	eicaryar	
5	<input checked="" type="checkbox"/>	Case 5.....	exploit_kits.yar	
6	<input checked="" type="checkbox"/>	Case 6.....	malware.yar	
7	<input checked="" type="checkbox"/>	Case 7.....	packers.yar	
8	<input checked="" type="checkbox"/>	APT_OLE_JS Rat	Targeted attack using Excel/word documents	
9	<input checked="" type="checkbox"/>	DDE Rule	Detect Dynamic Data Exchange protocol in doc/docx	
10	<input checked="" type="checkbox"/>	Dridex Rule		
11	<input checked="" type="checkbox"/>	Hidden PE file		

Рис. 4.6.1 - таблица yara-сигнатур

Нажав на кнопку , можно открыть окно с подробной информацией о модулях и другое.

### Информация

<b>Версия модулей:</b>	1.0.3
<b>Дата создания правил вендора:</b>	12/04/21 11:43:41
<b>Дата обновления правил вендора:</b>	12/04/21 11:50:19
<b>Версия правил вендора:</b>	1
<b>Модули Yara:</b>	PE, ELF, Hash, Math, Time, Cuckoo, Magic, Dotnet
<b>Версия Yara:</b>	4.0.2

Рис. 4.6.2 - окно с подробной информацией о Yara

Кнопка позволяет скачать Yara-сигнатуру файлом формата .yara.

Импорт правила осуществляется кнопкой

ИМПОРТ

Для импорта нужно указать путь к файлу формата ".yara", название и описание. Сигнатуры вендора доступны к обновлению только через системный функционал с помощью кнопки

**ОБНОВИТЬ СИГНАТУРЫ ВЕНДОРА**

. На вход подается архивный файл с сигнатурами.

 [Отредактировать эту страницу](#)