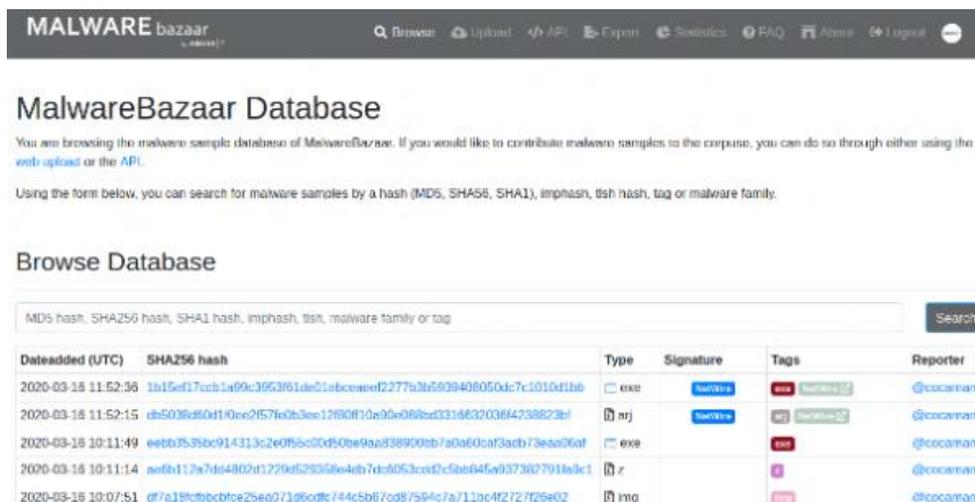


В Сети появился новый бесплатный репозиторий вредоносного ПО



MALWARE bazaar

MalwareBazaar Database

You are browsing the malware sample database of MalwareBazaar. If you would like to contribute malware samples to the corpus, you can do so through either using the [web upload](#) or the [API](#).

Using the form below, you can search for malware samples by a hash (MD5, SHA56, SHA1), imphash, tsh hash, tag or malware family.

Browse Database

MD5 hash, SHA256 hash, SHA1 hash, imphash, tsh, malware family or tag

Dateadded (UTC)	SHA256 hash	Type	Signature	Tags	Reporter
2020-03-18 11:52:36	1b15ef17ccb1499c3953f61de01abceaeef2277b3b5939406050dc7c1010d1bb	exe	Malware	new	@cocartan
2020-03-18 11:52:15	rb5036af60d10ee2f57fe0b3ee17690f10e90e068ed3146320364738823b	nrj	Malware	new	@cocartan
2020-03-18 10:11:49	eetb35f5bc914313c2e0fbc00d50be9aa838900eb7a0a60caf3acb73eaa26af	exe	Malware	new	@cocartan
2020-03-18 10:11:14	nefb112a7db44802d1229af529356e4db7dc0053ced7c5db645a037362791fedc1	z			@cocartan
2020-03-18 10:07:51	df7a13fcbcbcbfce25ee071360dfc744c5b67cd87594c7a7112c4f2727f26e02	img			@cocartan

Проект abuse.ch [запустил](#) новый сервис, позволяющий исследователям безопасности обмениваться образцами вредоносного ПО и дополнительными сведениями о них. Сервис MalwareBazaar разрешает публиковать только проверенные образцы известных вредоносных программ, рекламное и потенциально нежелательное ПО к публикации не допускаются.

Ограничений по количеству загружаемых образцов нет. Исследователи могут добавлять в репозиторий столько образцов, сколько пожелают, находить нужные им образцы по семействам вредоносного ПО, фаззи-хэшу и тегам, а также запрашивать информацию о них по электронной почте. Сервис предоставляет API для автоматизации, поддерживает экспорт хэшей и ежедневно предоставляет набор образцов вредоносного ПО для скачивания.

По словам создателей MalwareBazaar, в настоящее время исследователи используют разведку из открытых источников (OSINT), однако она не всегда позволяет загружать образцы вредоносных программ, на которые есть ссылки, для проведения собственного анализа. Для того чтобы заполучить заветный образец для анализа, исследователям приходится регистрировать несчетное количество различных антивирусных online-сканеров, песочниц или баз данных. Более того, многие платформы ограничивают количество загрузок в сутки, а некоторые и вовсе являются исключительно платными.

Источник: <https://www.securitylab.ru/news/506144.php>