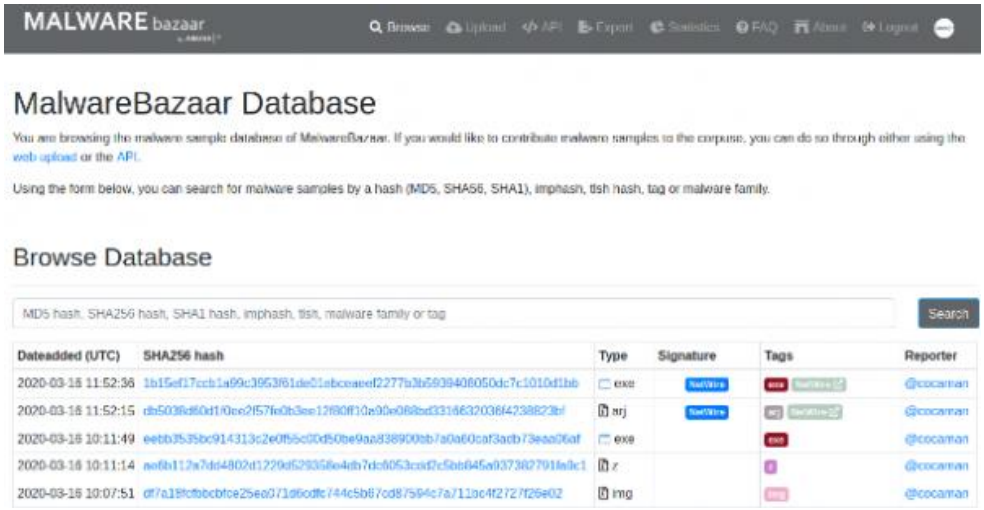
В Сети появился новый бесплатный репозиторий вредоносного ПО



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 вредоносов, 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