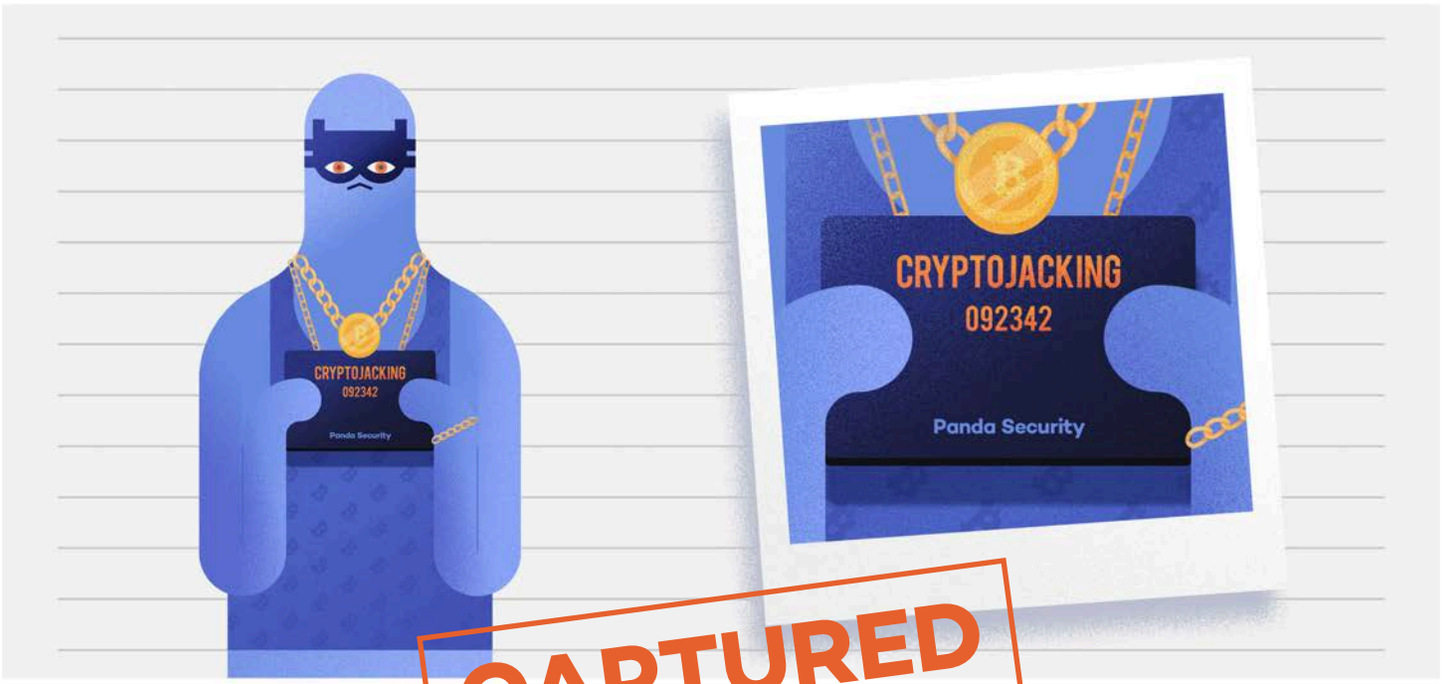


## Название

Криптоджекинг

## Дата рождения

2011

## Происхождение

Подсказки указывают на Россию

## Описание

Криптоджекинг использует чужие устройства без разрешения для незаконной добычи криптовалюты.

Преступники используют вредоносные программы для захвата компьютеров, планшетов или смартфонов, и используют их мощности для тайной добычи (майнинга) криптовалют, потребляя электроэнергию жертв.

Большинство атак криптоджекинга используют код CoinHive для майнинга криптовалют.

## Арест

**Данная угроза уже арестована и нейтрализована Panda Security.**

Но если Вы не используете антивирус Panda или Ваш уровень защиты требует улучшения, Вам необходимо обратить внимание на решения безопасности Panda для дома или офиса.

**Решения безопасности Panda**

## Криминальное прошлое

**Smominru**

В начале 2018 года была обнаружен Smominru - зловред для майнинга Monero. Заразил более полумиллиона компьютеров с мая 2017 года, в основном, в России, Индии и Тайване. По оценкам, кибер-преступники сумели заработать до 3,6 млн. долларов США.

**Adylkuzz и Wannamine**

Одна из самых проблематичных уязвимостей в 2018 году, - это EternalBlue, которая также использовалась для WannaCry. С ее помощью на компьютеры проникал и Adylkuzz. Этот зловред использовался для майнинга Monero, заразив сотни тысяч компьютеров во всем мире. Считается, что он поразил даже больше ПК, чем известный WannaCry.

**Атака на DoubleClick**

К концу января 2018 г. YouTube узнал, что был заражен, когда было обнаружено, что внутри его рекламных объявлений был скрыт вредоносный код, подвергающий риску многих пользователей. В этом случае жертвой атаки стала рекламная платформа DoubleClick, где был спрятан код CoinHive для криптоджекинга через рекламу на YouTube.

**WinstarNssmMiner**

В мае 2018 года другая очень опасная угроза под названием WinstarNssmMiner заразила полмиллиона ПК за три дня. Эта вредоносная программа использовала фишинговые письма и зараженные сайты. Попав в систему, использовала все ресурсы ПК для майнинга.

**HiddenMiner**

Обнаруженный в марте 2018 года, HiddenMiner сумел пробиться в мобильные устройства через приложения, загруженные со сторонних сайтов (не через официальные магазины приложений).

Он был еще опасен потому, что в старых версиях Android от него невозможно было избавиться. Оказавшись внутри, он использовал все ресурсы устройства, которое перегревалось и ломалось.