Новость · 7 декабря 2021, 18:14

Google заподозрил двух россиян в создании ботнета, который похищал данные пользователей компании

Google подал в суд на двоих россиян, которые, по данным компании, участвовали в создании ботнета[1] *Glupteba*, позволяющего проникать в чужие устройства. Об этом сообщает *Bloomberg*.

В иске компания называет двоих россиян — Дмитрия Старовикова и Александра Филиппова — и еще 15 неизвестных человек. *Google* утверждает, что они создали сеть ботов *Glupteba* для кражи данных пользователей компании.

«*Glupteba* печально известна тем, что крадет учетные данные и данные пользователей, добывает криптовалюту на зараженных хостах», — добавили в *Google*.

По версии компании, Старовиков и Филиппов подключались к ботнету через серверы, которые использовались для настройки их почт.

Как сказано в иске, который цитирует издание, *Glupteba* отличается от других вредоносных ПО своей «технической сложностью» и использует блокчейн.

Согласно данным компании *Chainalysis Inc.*, которая анализировала цепочки ботов, когда один из управляющих серверов *Glupteba* отключается, то он

сканирует блокчейн, чтобы найти новый адрес домена.

«Эта тактика делает чрезвычайно трудным нарушение работы ботнета с помощью традиционных методов кибербезопасности. Это первый известный случай сети ботов, использующей такой подход», — отметили в *Chainalysis*.

Bloomberg не удалось получить комментариев от Минюста США, который работал вместе с компанией над расследованием.

---

1. Сеть, состоящая из нескольких серверов с запущенными ботами. Чаще всего бот в ботнете устанавливается на устройство жертвы скрытно