

В число хакеров, предположительно похитивших до 100 миллионов долларов по всему миру за последние десять лет, действительно входят выходцы из России и Восточной Европы, считают опрошенные РИА Новости эксперты, ссылаясь на ряд имеющихся в их распоряжении улик. Власти США объявили во вторник о раскрытии одной из крупнейших хакерских схем, которая функционировала около десяти лет. Остановить ее удалось лишь по решению американского суда, который разрешил правительству отключить серверы, используемые хакерами для управления сетью зараженных компьютеров.

Представитель некоммерческой организации SAN Institute Алан Пэлер (Alan Paller), помогающей бороться с киберпреступлениями, выразил уверенность в том, что за преступлениями стояла группа хакеров, следы которой ведут в Россию.

По данным Министерства юстиции США, хакеры с помощью вируса Coreflood создали ботнет - сеть из около 2 миллионов компьютеров, управляемых злоумышленниками. Используя вредоносное программное обеспечение, им удавалось воровать по всему миру личные данные пользователей интернета и сведения об их кредитных картах.

"По нашим данным, за этим ботнетом действительно стоит преступная группа из России. В ходе расследования были выявлены финансовые "следы", ведущие к российским системам моментальных платежей, которыми пользовались злоумышленники", - сообщил РИА Новости Илья Сачков, генеральный директор компании Group-IB, занимающейся расследованием компьютерных преступлений.

Информацию о причастности к ботнету выходцев из России подтвердил и Александр Матросов, директор Центра вирусных исследований и аналитики ESET - компании, специализирующейся на разработке антивирусного программного обеспечения. "Есть ряд косвенных улик, указывающих на то, что киберпреступники, стоящие за этим ботнетом, родом из России и Восточной Европы", - заявил РИА Новости Матросов.

"Первые версии вредоносной программы, использовавшейся в этом ботнете, были обнаружены в 2002 году. Тогда она обладала функционалом для работы с чатами и поддержки диалогов на русском и английском языках", - сообщил ведущий вирусный аналитик антивирусной компании "Лаборатория Касперского" Сергей Голованов.

Американские власти отметили, что основная часть зараженных компьютеров расположена на территории США, однако сами хакеры, по мнению Пэлера, скорее всего, находились за пределами США.

"Наиболее активный период развития этого ботнета зафиксирован в 2008 году, когда он насчитывал несколько сотен тысяч активных зараженных компьютеров, действующих одновременно. Причем наибольшая доля составляющих ботнет компьютеров приходилась в тот момент на США", - пояснил Матросов.

"Полиция смогла получить данные об оплате хостинга и получила информацию о том, что она производилась с территории России", - отмечает Сачков.

Среди жертв хакеров оказались риэлтерская компания из штата Мичиган, которая потеряла более 115,7 тысячи долларов, адвокатская контора из Южной Каролины, лишившаяся более 78,4 тысячи долларов, и подрядчик военного ведомства США в штате Теннеси, не досчитавшийся более 241,8 тысячи долларов.

По действующему международному законодательству, дело рассматривается судом той страны, где есть пострадавшие. В настоящее время на рассмотрении суда Коннектикута находится иск против 13 иностранцев, имена которых не называются. Прокуратура обвиняет их в банковских махинациях с использованием электронных средств.

Сачков считает, что названная американскими экспертами сумма денег, которых хакерам удалось украсть за десять лет работы ботнета, сильно занижена. "С учетом того, что только за прошлый год русскоговорящие хакеры "заработали" 2,5 миллиарда долларов, уверен, что за десять лет организаторы этой хакерской схемы могли

заработать не меньше", - пояснил гендиректор Group IB.

Голованов объясняет безнаказанность хакеров на протяжении десяти лет их осторожностью. "Этот ботнет не был замечен ни в организации DDoS-атак, ни в рассылке спама", - сообщил специалист.

Источник ibank.ua