Осуждён хакер, “сломавший” Deutsche Telekom и интернет в Либерии

Британский хакер, совершивший такую мощную атаку, что вывел из строя интернет в целой стране, получил в наказание 32 месяца тюрьмы.

Сам хакер, по имени Дэниел Кей признался, что в 2016 году атаковал африканскую телефонную компанию, но атака оказалась такой мощной, что целая страна, Либерия, оказалась без интернета, сообщает BBC.

Сегодня Дэниэл Кей обвиняется в сотнях кибер-атак по всему миру. В британском агентстве по борьбе с преступностью считают, что Кей – один из самых крупных киберпреступников, когда-либо пойманных в Великобритании.

Кей, хакер-самоучка, продавал свои услуги в даркнете. Его предложения адресовались бизнесменам, которые хотели бы навредить своим конкурентам.

По данным следствия, в 2015 году Кея наняли представители компании Cellcom, чтобы тот атаковал конкурента – крупнейшего оператора связи Либерии, Lonestar.

Предполагается, что за нанесение максимального ущерба репутации Lonestar, Кею было обещано до 10 000 долларов США в месяц.

Для того, чтобы выполнить заказ, Кей построил ботнет для организации DDoS-атаки.

Вирус, известный как "Mirai # 14", заразил ПО огромного количества китайских веб-камер Dahua, которые используются для обеспечения безопасности в домах и на предприятиях по всему миру. Кей обнаружил, что уровень киберзащиты у дешевых камер и другого подобного оборудования невелик, и использовал уязвимость для захвата оборудования. В результате, в его распоряжении оказалась целая "армия кибер-зомби", готовая по приказу хозяина "пойти в атаку".

Повод для атаки – заказ из даркнета – появился в ноябре 2016 года. Кей привёл в действие ботнет, созданный на основе оборудования, размещённого на Кипре. Находясь в удалённом доступе, взломщик через мобильный телефон приказал ботнету из сотен тысяч веб-камер нагружать запросами системы Lonestar. И что характерно, вполне успешно. А чтобы усилить эффективность атаки, Кей подключил к нападению дополнительные мощности, на сей раз из Германии, где он инфицировал порядка 900 тысяч пользовательских DSL-роутеров на сетях национального оператора Deutsche Telekom.

Исследователи обнаружили, что на пике атаки вирусом Mirai # 14 было скомпрометировано около миллиона устройств по всему миру.

Абоненты в Либерии обнаружили, что их мобильные устройства отключены от сети.

Компания обратилась к специалистам по кибербезопасности, которые попытались отразить атаку, но сделать это без ущерба для пользователей и компании было уже невозможно.

В то время стабильность работы интернета в Либерии зависела от единственного подводного кабеля, проходящего по дну Атлантического океана, и небольшого числа провайдеров. Атака Кея оказалась

настолько мощной, что создала проблемы всем операторам связи в стране, но качество услуг Lonestar во время атаки оказалось настолько низким, что множество абонентов не раздумывая ушли к конкуренту.

По словам исследователей, в период с 3 по 4 ноября 2016 года интернет в Либерии неоднократно выходил из строя. Считается, что это был первый случай, когда один злоумышленник нарушил работу интернета всей страны.

Конечно, найти Кея было очень непросто. Он был задержан в феврале 2017 года, когда приехал в Великобританию на каникулы. В момент задержания, при нём было 10 тысяч долларов, которые, по данным Национального агентства по борьбе с преступностью, были частью вознаграждения за нападение на Lonestar.

Германия потребовала экстрадиции Кея, как причастного ко вмешательству в работу сетей Deutsche Telekom, и в том же году он был осужден в суде Кёльна. За сбой, от которого пострадали более 124 000 клиентов Deutsche Telekom, Кей получил 18 месяцев условно.

На суде хакер пояснил, что не хотел создавать проблемы немецкому оператору и его клиентам, а просто пытался незаметно перехватить контроль над устройствами и использовать их для осуществления DDoS-атак. По его словам, причиной случайного сбоя в работе маршрутизаторов стал модифицированный им образец Mirai.

После оглашения приговора в Германии, Кея экстрадировали в Великобританию, где он вновь предстал перед судом по гораздо более серьёзным обвинениям, связанным с атакой на интернет в Либерии (британский закон разрешает привлекать киберпреступников к ответственности за преступление в любой точке мира).

К этому времени кибер-специалисты Национального агентства по борьбе с преступностью установили, что ботнет Mirai # 14 был применён в ходе атак на три британских банка – Lloyds, Barclays и Halifax в январе 2017 года.

Тогда анонимный злоумышленник потребовал выкуп, чтобы прекратить DDoS-атаку.

В отличие от Lonestar и Либерии, более современные и мощные средства защиты отразили натиск во всех трех банках.

Первоначально Кая обвинили и в организации этих атак, но он заявил, что дал ботнет в аренду кому-то в даркнете. На днях обвинения в нападении на банки были официально сняты, но Майк Хьюлетт, глава Национального отдела киберпреступлений в NCA, подчеркнул, что следователи всего мира сейчас пытаются установить количество и масштаб кибератак, которые Кей совершил по всему миру.

> "Я считаю Дэниела Кея одним из самых значительных киберпреступников, арестованных в Великобритании, – сказал Хьюлетт. Тем более, что его атаки принесли огромный ущерб, и нельзя сказать, что они обошлись полностью без жертв".

В суде адвокат Кея заявил, что ответчик не согласен с потерями, которые, судя по заявлению истца, понёс Lonestar. Что же касается Либерии, то, по мнению адвоката хакера, проблемы с доступом в интернет в этой стране возникли независимо от атаки Кея:

> Речь идёт всего лишь о том, что относительно медленный интернет-сервис стал еще медленнее. Невозможно доказать, что такое замедление стало прямой угрозой для Либерии, – заявил адвокат.

Он также сообщил суду, что Кей получил предложения от крупных технологических компаний, которые хотели использовать его умения, несмотря на преступное прошлое, поскольку готовы использовать уникальные навыки и знания Дэниэла Кея для создания мощной системы киберзащиты.

Напомним, что атака на крупнейшего в Германии оператора связи вызвала массу домыслов и кривотолков. Службы безопасности подозревали, что хакеры хотели прежде всего подчеркнуть уязвимость крупнейших компаний ФРГ и экономики страны в целом. Предполагали, что первая атака – всего лишь прелюдия к более мощному нападению, которое могло случиться во время саммита G-20 в Гамбурге, в 2017 году. Главными подозреваемыми, до задержания Кея, были назначены гипотетические русские правительственные хакеры из группы "Медведи", которые, якобы, с помощью атак мстят западу за санкции, писала в те дни газета Der Tagesspiegel.

В те дни никто и предположить не мог, что атаку организовал британец, а его целью был оператор связи в далёкой африканской Либерии.