Активное участие ФБР помогло правосудию настигнуть юного киберпреступника.

Полиция Испании задержала ключевого члена известной киберпреступной группы Scattered Spider. Задержанный — 22-летний гражданин Великобритании, был арестован на этой неделе в испанском городе Пальма-де-Мальорка, когда пытался сесть на рейс в Италию. Операция стала результатом совместных усилий ФБР США и испанской полиции.

Мужчина обвиняется во взломе корпоративных аккаунтов, что позволило злоумышленникам незаконно получить миллионы долларов. Сообщается, что подозреваемый в какой-то момент контролировал биткоины на сумму 27 миллионов долларов.

Задержанный связан сразу с несколькими крупными атаками с использованием программ-вымогателей, осуществлёнными Scattered Spider. Группа исследователей vx-underground подтвердила, что задержанный является SIM-свопером, действовавшим под псевдонимом «Tyler».

SIM Swapping (SIM-свопинг, Port Out) – вид мошенничества, в ходе которого номер телефона жертвы переназначается на SIM-карту в телефоне мошенника, чтобы мошенник получал звонки и СМС, которые отправляются на номер жертвы. Злоумышленник таким образом может обойти двухфакторную аутентификацию и получить доступ к учётным записям жертвы, в том числе в банковских и криптовалютных сервисах.
" data-html="true" data-original-title="SIM Swapping" >SIM Swapping — это атака, при которой преступники обращаются к оператору связи с целью переноса номера жертвы на свой SIM, чтобы перехватывать сообщения и получать доступ к онлайн-аккаунтам. По информации журналиста Брайана Кребса, задержанный — 22-летний шотландец Тайлер Бьюкенен, известный под ником «tylerb» в Telegram-каналах, посвящённых SIM-свопингу.

Тайлер стал вторым арестованным членом группы Scattered Spider после Ноя Майкла Урбана, которого в феврале этого года обвинили в мошенничестве с использованием проводной связи и краже личных данных, приведших к краже $800 000 у пяти жертв.

Scattered Spider, известная также под именами 0ktapus, Octo Tempest и UNC3944, — это группа, занимающаяся финансово мотивированными атаками с использованием социальной инженерии для получения доступа к организациям. Члены группы, возможно, входят в состав крупной киберпреступной сети The Com.

Изначально фокусируясь на краже учётных данных и SIM-свопинге, группа перешла к вымогательству данных и атакующим атакам без шифрования, направленным на кражу данных из приложений, работающих по подписке (SaaS).

По данным компании Mandiant, участники Scattered Spider активно использовали тактики запугивания для получения учётных данных жертв, включая угрозы разглашения личной информации, физической расправы и распространения компрометирующих материалов.

Ранее представители ФБР высказывали предположения, что группировка состоит преимущественно из молодых людей и даже тинейджеров. Вполне возможно, что именно из-за юного возраста и определённой степени максимализма, злоумышленники используют столь жёсткие методы.

Активность Scattered Spider имеет сходства с другой группой, отслеживаемой Palo Alto Networks Unit 42 под именем Muddled Libra, также занимающейся кражей данных из SaaS-приложений. Однако эксперты подчёркивают, что это не одна и та же группа.

Scattered Spider известна использованием фишинговых наборов для кражи учётных данных Okta, что затрудняет определение виновных. Также группа использовала злоупотребление правами доступа Okta, чтобы расширить вторжение на облачные и SaaS-приложения.

Атаки группы характеризуются использованием легитимных утилит для синхронизации облаков, таких как Airbyte и Fivetran, для экспорта данных в контролируемые злоумышленниками хранилища, а также созданием новых виртуальных машин для установления постоянного доступа и обхода защиты.

В рамках своих атак Scattered Spider также использовала решения для обнаружения и реагирования на инциденты на конечных устройствах (EDR) для выполнения команд и тестирования доступа к среде.