7 месяцев расследования, $1.3 млн. конфиската. Хакеры получат по заслугам.

Сингапурская полиция объявила об экстрадиции двух мужчин из Малайзии по обвинению в участии в мобильной вредоносной кампании, нацеленной на граждан страны с июня 2023 года.

Мужчины в возрасте 26 и 47 лет, имя которых не разглашается, участвовали в мошеннической деятельности, заставляя пользователей загружать вредоносные приложения на устройства Android – операционная система для мобильных устройств, разработанная компанией Google. Она основана на ядре Linux и предоставляет широкий спектр функций и сервисов для смартфонов, планшетов, умных часов, телевизоров и других устройств.

 Android позволяет пользователям скачивать и устанавливать приложения из магазина Google Play, обеспечивая множество возможностей для индивидуализации и работы с различными приложениями.

 Android является наиболее популярной в мире ОС для мобильных устройств и продолжает активно развиваться и обновляться." data-html="true" data-original-title="Android" >Android через фишинговые кампании с целью кражи личных данных и банковских учётных данных. Полученная информация использовалась для проведения мошеннических транзакций на банковских счетах жертв, что приводило к финансовым потерям последних.

После семимесячного расследования, начавшегося в ноябре 2023 года в сотрудничестве с полицией Гонконга, Королевской полицией Малайзии, а также ИБ-компанией Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, исследования высокотехнологичных преступлений и защиты интеллектуальной собственности в сети." data-html="true" data-original-title="Group-IB" >Group-IB — сингапурская полиция нашла доказательства, связывающие двух мужчин с преступной группировкой, ответственной за проведение вредоносных атак.

По данным полиции, мужчины управляли серверами, предназначенными для установки на смартфоны жертв специального вредоносного приложения, позволяющего контролировать заражённые устройства и «изменять их содержимое», что облегчало последующую кражу денежных средств с банковских счетов пострадавших.

«Активы, включая криптовалюту и недвижимость общей стоимостью примерно $1.33 миллиона, были конфискованы у арестованных лиц», — сообщила полиция Сингапура.

Специалисты Group-IB заявили, что вредоносные приложения, использованные в данной кампании, часто маскировались под предложения специальных цен на товары и продукты и содержали функции для сбора широкого спектра информации.

«После установки и предоставления необходимых разрешений, Существует две расшифровки аббревиатуры RAT:

 • Remote Administration Tool — инструмент удалённого администрирования;
 • Remote Access Trojan — троян удалённого доступа.

 В обоих случаях подразумевается инструмент, который позволяет производить удалённое подключение к целевой системе и последующее выполнение определённых действий. В зависимости от того, кто использует RAT, законный системный администратор или киберпреступник, меняется как расшифровка аббревиатуры, так и спектр выполняемых действий.

 Забавно, что само слово «RAT» можно дословно перевести с английского как «крыса»." data-html="true" data-original-title="RAT" >RAT позволял злоумышленникам удалённо управлять устройством Android, захватывая чувствительные личные данные и пароли с помощью функций кейлоггера и захвата экрана», — заявили в компании.

Троян давал злоумышленникам возможность отслеживать SMS-сообщения, содержащие одноразовые пароли, отправляемые финансовыми организациями для двухфакторной аутентификации. Кроме того, он способствовал отслеживанию геолокации устройства и его пользователя в реальном времени.

«Работая незаметно в фоновом режиме, вредонос сохранял активность даже после перезагрузки устройства», — добавили специалисты.

Один из подозреваемых может получить до семи лет тюремного заключения, штраф в размере до $50 000 или сразу оба наказания. Другой — штраф до $500 000, до 10 лет тюрьмы или сразу оба наказания.

Арест в Сингапуре прошёл в рамках международной операции DISTANTHILL. Среди других достижений правоохранителей стоит выделить задержание четырёх человек, подозреваемых в аналогичных действиях в Тайване. Всего в рамках операции было задержано 16 киберпреступников. По примерным оценкам, жертвами их мошенничества стали более 4000 человек.

Примечательно, что эти события происходят на фоне обвинений министерства юстиции США против двух мужчин — Томаса Пейви и Рахейма Гамильтона, которые управляли даркнет-рынком Empire Market. Этот рынок позволял тысячам продавцов и покупателей анонимно торговать нелегальными товарами и услугами. Общая выручка

от всех нелегальных сделок составила внушительные $430 миллионов, а преступников вполне могут посадить на пожизненный срок.