Текст · 19 июля 2021, 12:16
Александр Бородихин,

Троянский «Пегас». Израильские хакеры вскрывают телефоны журналистов и активистов по заказу правительств

Журналисты ведущих мировых изданий и специалисты по кибербезопасности проверяли список из 50 тысяч телефонных номеров, который оказался в распоряжении парижской некоммерческой организации *Forbidden Stories* и правозащитников из *Amnesty International.*

Смартфоны граждан различных государств могли быть взломаны при помощи программного комплекса *Pegasus* разработки *NSO Group;* программа дает практически полный доступ к памяти и функциям устройства, то есть позволяет удаленно читать переписки, передавать данные о местоположении, включать камеру или микрофон.

Основной вывод: по меньшей мере 37 раз власти различных стран заказывали взлом смартфонов журналистов, правозащитников, бизнесменов и близких к ним людей.

Pegasus позволяет взламывать айфоны со всеми последними обновлениями без какого-либо участия жертвы: не нужно ни открывать ссылки, ни вводить где бы то ни было пароли. Скорее всего, *NSO Group* использует различные уязвимости мобильных приложений, но *Amnesty International* удалось

подтвердить использование бага в мессенджере *iMessage.*

Что такое NSO Group?

Израиль — мировой лидер по числу стартапов, и крупнейшим направлением инвестиций там стали IT-разработки, в том числе так или иначе связанные с военным сектором.

«Множество отставных специалистов компьютерных и телекоммуникационных подразделений израильской армии успешно реализовывают смелые идеи, применяя военные технологии для развития стартапов», — поясняет депутат Кнессета Идал Ролл.

NSO Group основали по той же схеме: в 2009 году на фоне развития рынка смартфонов бывшие военные из подразделения 8200, занимающегося радиоэлектронной разведкой, решили разработать программный комплекс для удаленного взлома. Предполагается, что программный комплекс *Pegasus* «дает полномочным органам власти технологии, помогающие бороться с терроризмом и преступностью».

Впервые о *Pegasus* заговорили в 2016 году, когда журналист и правозащитник Ахмед Мансур получил по смс ссылку на «новые секреты» о пытках в ОАЭ. Мансур заподозрил неладное и связался с IT-экспертами из канадской *Citizen Lab*, которые проверили ссылку и обнаружили за ней код, позволяющий удаленно взломать *iPhone* адресата при помощи нескольких 0-*day* уязвимостей[1] и предоставить полный доступ к функциям и памяти устройства.

К 2018 году исследователи зафиксировали взломы, для которых использовали *Pegasus*, в 45 странах — от Мексики, где ловили наркобарона Коротышку-[2] и заодно прослушивали журналистов, до Индии, где премьер Нарендра Моди укреплял «вертикаль власти». С российскими властями, по крайней мере по данным *Citizen Lab*, израильтяне не сотрудничали.

На следующий год *NSO Group* ждал новый громкий скандал: разработчики мессенджера *WhatsApp* заметили уязвимость, которая позволяла установить *Pegasus* — в *NSO* использовали баг в коде мессенджера, чтобы позвонить жертве и установить шпионскую программу, даже если та не ответит на звонок. Владеющая мессенджером корпорация *Facebook* обратилась в суд; в *NSO* парировали, что *Facebook* сам вел переговоры о покупке доступа к *Pegasus*.

Формально экспорт технологий двойного назначения контролируется израильским Минобороны, однако ведомство не слишком внимательно следит за успешными стартапами, поэтому они оказываются в центре скандалов из-за работы с правительствами, не заинтересованными в соблюдении свободы слова или прав человека.

Акция протеста против убийства Джамаля Хашогджи в Стамбуле. Фото: Emrah Gurel / AP

Что произошло?

Список из 50 тысяч номеров, оказавшийся в распоряжении правозащитников, не содержит имен, но журналистам удалось идентифицировать более тысячи их владельцев из более чем 50 государств: это члены королевских семей арабских стран, десятки бизнесменов и топ-менеджеров, 85 правозащитников, 189 журналистов мировых СМИ и более 600 политиков и чиновников.

Чтобы подтвердить факт взлома, исследователи *Amnesty International* осмотрели 67 смартфонов, чьи владельцы упоминались в списке из 50 тысяч номеров и явно не были причастны к террористической деятельности. Из них 23 были успешно инфицированы *Pegasus*, еще на 14 обнаружены следы попыток проникновения. Остальные 30, по всей видимости, были куплены владельцами уже после заказа на взлом; 15 из этих телефонов были устройствами на ОС *Android*, которая

не записывает телеметрию, на которую опирались исследователи для фиксации факта успешного заражения.

NSO Group отчитывается, что поставляет свою технологию 60 силовым структурам из 40 государств, но не называет их. Изучая группы телефонных номеров в слитой базе жертв *Pegasus,* исследователи пришли к выводу, что взломы заказывали власти Азербайджана, Бахрейна, Венгрии, Индии, Казахстана, Мексики, Марокко, Руанды, Саудовской Аравии и ОАЭ.

Лидером по числу заказанных номеров оказалась Мексика — 15 тысяч. В списке есть политики, представители профсоюзов, журналисты и оппозиционеры. Существенная доля номеров из базы пришлась на Ближний Восток; в Индии в списке оказались телефоны сотен журналистов, активистов и оппозиционных политиков.

В 2018 году после гибели активиста Джамаля Хашогджи — его заманили в консульство Саудовской Аравии в Стамбуле, убили и расчленили — в *NSO Group* заявили, что саудовские спецслужбы не использовали их программу. Расследование показало, что это не так: *Pegasus* использовали для взлома телефонов двух близких к нему женщин — жены и невесты.

Венгерские власти заинтересовались номерами по меньшей мере десяти адвокатов, оппозиционера и пятерых журналистов. Телефон известного репортера Сабольча Паньи при обследовании оказался неоднократно инфицированным, причем даты заражения совпадали с датами запросов,

которые Пани направлял правительственным чиновникам по чувствительным темам.

Сама *NSO Group* через юристов сообщила, что 50 тысяч жертв — «преувеличенное число», выводы о масштабных взломах некорректны, а база номеров могла быть собрана при помощи не связанных со взломами функций *Pegasus*.

«А вы задали те же вопросы властям США, Великобритании, Германии или Франции? Если да, то как долго пришлось ждать ответа — и как они ответили? Помогала ли вам составлять вопросы какая-нибудь разведка?» — таким списком встречных вопросов ответила пресс-служба венгерского правительства на попытку журналистов *Guardian* получить комментарий к статье.

«Более самоизобличающего ответа на запрос о комментарии я в жизни не видел», — возмущается Эдвард Сноуден, но пишет это из России, где государственный вотэбаутизм[3] отработан до совершенства годами советской и постсоветской практики.

Редактор: Дмитрий Трещанин

---

1. Уязвимостями «нулевого дня» называют проблемы в коде, о которых разработчик пока ничего не знает, поэтому не может внести исправления.

2. Хоакин Гусман, он же el Chapo — Коротышка, арестован в Мексике в январе 2016 года и позже выдан США, где его приговорили к пожизненному заключению.

3. От английского термина whataboutism, попытка уйти от неудобного вопроса встречным «А что там в [другой стране]?»; такая подмена используется для снижения остроты вопроса через «неуникальность» проблемы.