Феміда на швидкості 150 км/год: чому в Україні статус нардепа став «ліцензією на вбивство»

Магічне зникнення підстав для санкцій проти резидента ФСБ Юрія Іванющенка

РПЦ як секта депортацій: свідчення Владислава Гаврилова про викрадення

Троянский Pegasus. Хакеры из Израиля вскрывают телефоны журналистов по заказу правительств

КІБЕРЗЛОЧИННІСТЬ | СР, 2021-07-21 08:26

Версия для печати

Если зайти на официальный сайт израильской NSO Group, можно узнать, что компания занимается «киберразведкой в интересах глобальной безопасности и стабильности». Если же открыть сегодня крупнейшие мировые СМИ, можно выяснить, что за этой формулировкой скрывается куда более банальная торговля программами для взлома смартфонов неугодных журналистов и активистов.

В издании «**Медиазона**» кратко пересказывают результаты масштабного расследования взломов NSO Group, в котором приняли участие полтора десятка крупнейших мировых изданий.

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.

> На эту тему: **Эксперты заявили, что компьютеры Демократической партии США взломали хакеры из России**

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.

> На эту тему: **«Дія Сіті» — цифровой колхоз**

Что такое NSO Group?

Израиль — мировой лидер по числу стартапов, и крупнейшим направлением

НОВИНИ

13:01 **2500 гектарів лісу палає на Чернігівщині через російські обстріли**

12:19 **Підозрювана у хабарництві: ВРП звільнила львівську суддю Ірину Малех**

11:50 **УПЦ МП має повернути державі споруди Богоявленського монастиря у Кременці - суд**

10:53 **Біля Ормузької протоки застрягли 1600 суден**

09:59 **Сергій Гнезділов: Згаяний шанс на встановлення справедливих термінів служби**

08:00 **Доба на Сумщині: п’ятеро вбитих та 11 поранених**

20:00 **Прогноз погоди в Україні на 7 – 10 травня 2026 року**

19:04 **Бутусов: Про іноземців у ЗСУ, СЗЧ і плани ворога (ВІДЕО)**

18:05 **Чернігів, Полтава та Харків серед аутсайдерів у рейтингу прозорості фінансів — дослідження TI Ukraine**

17:08 **Виконавча служба: з гривні боргу вдається стягнути лише 1,5 копійки**

ПІДПИСКА НА КАНАЛ

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 и предоставить полный доступ к функциям и памяти устройства.

> На эту тему: **Георгий Рошка — российский террорист. Почту президента Франции взломали сотрудники ГРУ**

К 2018 году исследователи **зафиксировали** взломы, для которых использовали Pegasus, в 45 странах — от Мексики, где ловили наркобарона Коротышку 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.

> На эту тему: **Первая Мировая кибервойна. Почему "государство в смартфоне" не только полезно, но и опасно**

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.

> На эту тему: **Русские взломали и фальсифицировали заседание исполкома ВАДА - СМИ**

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 отработан до совершенства годами советской и постсоветской практики.

* * * * *

Шпионская программа Pegasus может взломать любой смартфон

В издании Настоящее время поговорили с ее создателями и жертвой взлома.

Крупнейший поставщик облачных хранилищ Amazon Web Services (AWS) перестал обслуживать компанию NSO Group после того, как стало известно, что ее программы использовались для кибератак на оппозиционных активистов и журналистов по всему миру. "Когда мы узнали об этой деятельности, мы оперативно закрыли соответствующую инфраструктуру и учетные записи", – **сообщил** представитель AWS изданию Motherboard.

18 июля несколько журналистских организаций во главе с французской Forbidden Stories **рассказали** о шпионской программе Pegasus: она взламывает телефоны на расстоянии, скачивает с них переписку, фото и видео, а также активирует камеру и микрофон без ведома владельцев. В NSO Group утверждают, что продают программу правоохранительным органам для борьбы с преступностью и терроризмом. Но как выяснили журналисты, объектами слежки Pegasus стали 180 их коллег из 20 стран, а в широком списке потенциальных целей – более 50 тысяч человек. Источник этой утечки не раскрывается.

В 2016-2018 годах жертвы получали СМС-сообщения со ссылками, похожими, например, на уведомления о доставке. Успех операции зависел от того, перейдет ли пользователь по ссылке. Но в последние годы NSO Group научилась присылать невидимые СМС, не требующие перехода: для взлома злоумышленнику достаточно знать номер телефона жертвы.

Использование Pegasus против журналистов и правозащитников могли санкционировать правительства 11 стран. Так, в Азербайджане мишенями кибератак стали сотрудники местной службы Радио Свобода и бывшая глава бакинского бюро корпорации Хадиджа Исмаилова (ее рассказ приведен ниже). Кроме того, шпионской программой могли воспользоваться власти Казахстана, Венгрии, Индии, Бахрейна, Саудовской Аравии, Объединенных Арабских Эмиратов, Мексики, Марокко, Того и Руанды.

России среди этих стран нет, но **опубликованный** лабораторией безопасности Amnesty International список доменов, связанных с NSO Group, содержит несколько "русскоязычных" адресов, например, oplata-shtraf.info, photo-afisha.net, mystulchik.com, prikol-girls.com и sputnik-news.info. Последний похож на адрес российского государственного информационного агентства "Спутник". Сейчас эти адреса отключены и не представляют опасности. Один сайт из сети NSO Group располагался на сервере индивидуального предпринимателя из Днепра, еще один – на сервере крупного киевского телеком-оператора (конкретные "украинские" адреса исследователи не называют). Всего в Amnesty International обнаружили 1407 доменов, использовавшихся для установки вируса, их адреса менялись в зависимости от жертвы.

В NSO Group не раскрывают, есть ли у них клиенты в России или Украине. "По контрактным обязательствам и из соображений национальной безопасности NSO Group не может подтвердить или опровергнуть принадлежность наших государственных клиентов, а также клиентов, которых мы отключили от системы", – сообщил представитель компании Настоящему Времени (для общения с прессой там наняли вашингтонскую консалтинговую фирму Mercury Public Affairs).

Мишени: журналисты, активисты и потенциально – кто угодно

Объектами слежки Pegasus становились журналисты, которые работают в опасных условиях. Так, номер телефона мексиканского разоблачителя коррупции Сесилио Пинеда Бирто попал в систему в 2017 году – за несколько недель до того, как его застрелили на автомойке на юге Мексики. Само устройство Бирто исчезло сразу после убийства, подтвердить, что его местонахождение вычислили именно с помощью Pegasus, не удалось.

Pegasus также использовали для слежки за двумя женщинами, которые были близки к колумнисту The Washington Post Джамалю Хашогджи, – его пытали и убили в 2018 году в консульстве Саудовской Аравии в Стамбуле.

Одной из самых частых мишеней кибератак стала азербайджанская журналистка Хадиджа Исмаилова. Она пользовалась "старым, глючным" iPhone 6, рассказывает журналистка Настоящему Времени. "Память была, видимо, маленькая, и фотографий было в архиве много – я не знаю, но все время приходилось его выключать и включать", – отмечает Исмаилова. При каждой перезагрузке уязвимость, позволявшая Pegasus следить за пользователем, слетает, утверждают в Amnesty International. В итоге злоумышленникам пришлось атаковать телефон Исмаиловой сотни раз в 2019-2021 годах.

Одно из расследований Исмаиловой (на фото) было посвящено передаче золотоносных месторождений семье президента Азербайджана

В канадской исследовательской организации Citizen Lab, которая ранее исследовала кибератаки NSO Group, считают, что возраст телефона (iPhone 6 был выпущен в 2014 году) не влияет на вероятность, с которой данные окажутся в руках у злоумышленников. "У новых телефонов обычно больше функций безопасности, поэтому их сложнее взломать, – говорит Настоящему Времени старший научный сотрудник Citizen Lab Билл Марчак. – Однако шпионская программа Pegasus от NSO Group может проникнуть в новейшие iPhone. Стоит телефону проанализировать невидимое сообщение в iMessage, запускается вредоносное вложение, которое приводит к установке Pegasus и слежке за телефоном".

После установки Pegasus никак не проявляет себя, продолжает Исмаилова: "Прослушка телефонных разговоров – это все рутина, с которой нам приходится сталкиваться, но с этой задачей можно справиться и без установки этой программы. Мы-то думали, что, используя мессенджер Signal (известный своими продвинутыми криптографическими протоколами – НВ), мы можем защитить себя. Мы думали, что использовать iPhone безопасно, потому что iOS круче, чем Android. Но для этой программы это не имеет никакого значения".

Исмаилова улетела из Азербайджана за несколько недель для публикации расследования об NSO Group. В 2015 году в Азербайджане ее приговорили к семи с половиной годам лишения свободы по обвинению в растрате и налоговых преступлениях. Адвокаты Исмаиловой настаивали, что дело политическое: журналистка расследовала коррупцию в высших эшелонах власти, в том числе в правящей семье Алиевых.

Личные данные журналистов нужны властям, чтобы шантажировать их, а также провоцировать ненависть, считает Исмаилова. "В 2012 году физически поставили камеру у меня в спальне, в ванной комнате и в гостиной. И потом эти съемки были использованы для шантажа, и когда я отказалась и опубликовала угрозы, все это было выложено в интернет", – рассказывает журналистка.

Интимные переписки критиков азербайджанских властей периодически показывает местный канал Real TV. Его руководитель Миршахин Агаев также оказался в списке мишеней NSO Group, утверждает Исмаилова. На момент публикации на телеканале не ответили на запрос Настоящего Времени.

Помимо Исмаиловой, мишенями кибератак стали еще четверо действующих и бывших журналистов азербайджанской службы Радио Свобода. Президент компании Джейми Флай осудил это, заявив: "Радио Свобода решительно осуждает это трусливое вторжение в частную жизнь работающих журналистов. Мы давно отмечаем оскорбительные действия правительства Азербайджана в отношении нашей азербайджанской службы. Мы призываем правительство Азербайджана прекратить блокировать наш веб-сайт, прекратить слежку за нашими сотрудниками и прекратить преследование бывшего руководителя нашего бюро Хадиджу Исмаилову".

Кто ответит за взломы

Главы государств и правительств, а также несколько членов королевских семей арабских стран также попали в список возможных целей Pegasus, отмечают расследователи. "В случае Азербайджана есть чиновники высшего и среднего рангов, и депутаты, и сотрудники проправительственных НКО", – добавляет Хадиджа Исмаилова.

Деятельность NSO Group осудили IT-гиганты. "Подобные кибератаки очень изощренны, их разработка стоит миллионы долларов, они недолговечны и используются для нацеливания на конкретных лиц, – заявил руководитель отдела разработки и архитектуры безопасности Apple Иван Крстич. – Хотя это означает, что они не представляют угрозы для подавляющего большинства наших пользователей, мы продолжаем неустанно работать, чтобы защитить всех наших клиентов".

"Опасное шпионское ПО NSO Group используется для совершения ужасных нарушений прав человека по всему миру, и его необходимо остановить", – **написал** в твиттере глава мессенджера WhatsApp Уилл Кэткарт. Могут ли правительства и бизнес объединиться, чтобы остановить хакерские атаки на журналистов и активистов?

"В законодательстве большинства стран есть правовые нормы, запрещающие использование таких программ, – объясняет Настоящему Времени эксперт

российского правозащитного проекта "Роскомсвобода" Владимир Ожерельев. – Но формально в отношении самой разработки программы данные статьи могут применяться только в случае, если программа заведомо создавалась с противоправной целью, что не позволит привлечь разработчиков Pegasus к ответственности. Тем не менее понести ответственность могут лица, заведомо неправомерно использующие программу, в том числе с использованием служебного положения". Эксперт не исключает, что в отдельных случаях жертвы кибератак могут добиться компенсации в национальных и международных судах.

"Слухи и инсинуации": NSO Group отрицает все обвинения

Компания NSO Group Technologies Ltd. основана в 2010 году выходцами из "подразделения 8200" израильской армии. Оно занимается радиоэлектронной разведкой. "8200 может брать 1% из 1% [лучших специалистов] в стране", – **рассказывала** журналу Forbes бывшая сотрудница этого подразделения.

Разработчиков Pegasus не впервые обвиняют в сотрудничестве с авторитарными режимами. Так, в Citizen Lab Настоящему Времени рассказали, что им известно по меньшей мере 130 случаев, когда программа использовалась с нарушением закона, 50 из которых – это кибератаки против журналистов.

Офис NSO Group в Герцлии

Но и раньше, и сейчас в NSO Group отвергают любые обвинения. "История с самого начала была недостоверной, – написал представитель компании Настоящему Времени. – Когда на прошлой неделе редакторы связались с NSO Group после нескольких месяцев изучения слухов и инсинуаций, их утверждения были еще более сенсационными, если не сказать выдуманными. Первоначально они утверждали, что 50 тысяч номеров были найдены на сервере NSO. Поняв, что это невозможно, поскольку Pegasus никогда не лицензировался на такое количество номеров и поскольку на серверах NSO Group нет таких данных, редакторы быстро превратили свою историю в огромное "а что, если", только чтобы не испортить хороший заголовок".

Основываясь на попавшем к ним списке, расследователи обещают публиковать новые сведения о мишенях NSO Group.

—

Использованы материалы изданий Медиазона и Настоящее время

На эту тему:

- **Хакеры взломали проекты крупного подрядчика ФСБ, среди них - деанонимизация пользователей Tor**
- **Reuters: западные спецслужбы взломали «Яндекс»**
- **Sandworm. Как хакеры ГРУ отключали энергетику в Украине и взламывали избирком США**
- **Урок не выучен? Как Украина (не)защищает свое киберпространство**
- **"Все, что они могут сделать нам, мы можем сделать им». Украинские хакеры выходят из тени**

Читайте «Аргумент» в **Facebook** и **Twitter**

Если вы заметили ошибку, выделите ее мышкой и нажмите ***Ctrl+Enter.***

Коментарі

ВІДЕО

Воїни «Альфи» СБУ — ТОП-1 серед підрозділів Сил оборони за результатами бойової роботи у квітні

Про що не можна було жартувати в СРСР

HEAVY SHOT, VAMPIRE, NEMESIS: як «Баба Яга» б’є ок*пантів

Контакт: ***uargumentum@gmail.com***