**Пегасус софтуер**

Пегасус е шпионски софтуер, разработен от израелската кибер-оръжейна компания NSO Group, който е предназначен да бъде тайно и отдалечено инсталиран на мобилни телефони с операционни системи iOS и Android.[1] Въпреки че NSO Group пазарува Пегасус като продукт за борба с престъпността и тероризма, правителства по целия свят рутинно използват шпионския софтуер за наблюдение на журналисти, адвокати, политически дисиденти и активисти за правата на човека.

**Първи случай на експлоатация с Pegasus software**

За експлоатацията на Pegasus за iOS се открива през август 2016 г. Арабският защитник на правата на човека Ахмед Мансур получава текстово съобщение, обещаващо да сподели тайни за мъченията на затворници в Обединените арабски емирства, ако последва линк прикачен към съобщението. Мансур изпраща линка до Citizen Lab лабораторията на Университета в Торонто, който разследва съвместно с Lookout, като установяват, че ако Мансур бе последвал линка, той би позволил на шпионският софтуер да се инсталира на телефона му.

**Технически спецификации**

Шпионският софтуер Pegasus може да зарази устройства с iOS и определени версии на Android чрез различни уязвимости, включително експлоатации без необходимост от кликване. Той може да бъде инсталиран чрез линкове, приложението Photos, Apple Music и iMessage. След като е инсталиран, Pegasus може да извлича данни като контакти, обаждания, съобщения, снимки и история на браузъра. Също така може да достъпва информация от комуникационни приложения като iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram и Skype.

**Как да открием Pegasus на устройството ни**

Поради скришния характер на своето инсталиране, Pegasus преди единствено можеше да бъде открит чрез дигитална форензика. На 16 януари 2024 г. Kaspersky Labs обяви нов метод за откриване на шпионския софтуер за iOS устройства, който включва проверка на файла shutdown.log, който регистрира информация по време на рестартирането, като може да се засече следи от Pegasus софтуера. Kaspersky Labs са разработили инструмент, който извлича и анализира файла shutdown.log, за да улесни процеса на откриване на софтуера. Обаче, този метод е ефективен само ако устройството се рестартира в същия ден, в който е заразено с Pegasus.

**Случаят Сноудън**

Едуард Джозеф Сноудън е американски агент с връзки с ЦРУ и Агенцията за национална сигурност на САЩ и бивш системен администратор, който емигрира в Русия. Той разкрива секретни схеми за глобално наблюдение и разузнаване, много от които са ръководени от споменатите организации и съюза "Пет очи", в сътрудничество с телекомуникационни компании и някои европейски правителства.

На 21 юни 2013 г. Министерството на юстицията на САЩ обяви обвинения срещу Сноудън за два случая на нарушаване на Закона за шпионаж от 1917 г. и кражба на държавно имущество, след което Министерството на външните работи отмени паспорта му. Два дни по-късно той пристига в московското летище Шереметьево, където руските власти забелязват анулирания паспорт и го ограничават в летищния терминал за повече от един месец. По-късно Русия му предоставя право на убежище с първоначална виза за пребиваване за една година, която последващо е многократно удължавана. През октомври 2020 г. му е предоставено постоянно пребиваване в Русия. През септември 2022 г. Сноудън получава руско гражданство от президента Владимир Путин.