Ноутбуки и смартфоны говорят о ваших действиях, излучая шумы и сигналы

Ноутбуки и смартфоны, даже не подключенные к Wi-Fi, расскажут о ваших действиях злоумышленникам без вашего ведома. Причина — слабые сигналы и шумы, которые излучают привычные нам гаджеты.

Сидя в кафе с ноутбуком или начав в метро или в любой непонятной ситуации копаться в смартфоне, вы не можете быть уверенными, что ваши действия незаметны для хакеров. Злоумышленники могут узнать, какие буквы вы печатаете и какие действия выполняете, просто анализируя маломощные электрические сигналы, которые излучает в пространство ваш гаджет.

И главное – вашему устройству вовсе не обязательно для этого быть подключенным к интернету по Wi-Fi.

К такому выводу пришли инженеры из Технологического института Джорджии, которые занялись исследованием слабых сигналов, которые излучают привычные нам гаджеты. Исследуя при помощи специальных датчиков электромагнитные импульсы, ученые пытаются выяснить, какие именно электронные элементы создают эти утечки по так называемым сторонним каналам и, зная это, разработать системы защиты.

«Люди сосредоточены на безопасности в интернете и беспроводной связи, однако нас волнует то, что мы можем извлечь из вашего

компьютера, даже если он специально что-то не посылает, — пояснила Аленка Зайич, старший преподаватель института. — Даже если вы отключены от интернета, вы продолжаете распространять информацию, которую кто-то может использовать для атаки на ваш компьютер или смартфон».

Результаты исследования, которое финансировалось Национальным научным фондом (США), были представлены на 47-м международном симпозиуме в Кембридже. Сигналы по сторонним каналам могут быть измерены в нескольких метрах от излучающего устройства при помощи целого набора различных шпионских «штучек». Электромагнитные импульсы можно уловить при помощи антенны, спрятанной, например, в портфель.

Звуковые колебания, которые издаются конденсаторами внутри каждого устройства, могут быть пойманы при помощи микрофонов под столом.

Узнать, что делает компьютер, можно даже по микроскачкам напряжения, которые можно зафиксировать при помощи «фейковых» зарядных устройств, вставленных в ту же розетку, что и адаптер ноутбука. Некоторые сигналы можно уловить при помощи обычного AM/FM-приемника, другие — при помощи изощренных анализаторов электромагнитного спектра.

Выяснилось, что такие электронные компоненты компьютеров, как регуляторы напряжения, создают электромагнитное излучение, которое несет информацию о работе других его компонентов. В

качестве демонстрации Зайич продемонстрировала эксперимент. Сидя в одной части комнаты, она набирает случайный пароль на компьютере, не подключенном к интернету.

Ее коллега, сидящий у другого края стены, читает этот пароль на другом ноутбуке, перехватывая сигналы, посылаемые при нажатии на клавиши.

До настоящего времени в открытых источниках не было информации об использовании хакерами сторонних каналов, однако, по мнению исследователей, это всего лишь вопрос времени. О риске подобных утечек говорят давно, однако команде Зайич впервые удалось экспериментально доказать существующие угрозы.

«Конечно, есть вероятность, что кто-то использует это прямо сейчас, они же не говорят об этом», — считает Зайич. Чтобы лучше оценить угрозы, ученые пытаются точнее определить местоположение источников утечек. «Мы пытаемся понять, почему возникают эти сторонние каналы и что можно сделать, чтобы справиться с ними. Мы изучаем компьютеры и смартфоны, чтобы определить места, в которых происходят утечки. Эта информация позволит перестроить их архитектуру так, чтобы изменить их поведение», — говорит исследовательница.

Каждая операция, которую выполняет компьютер, вызывает разные сигналы. Процессор потребляет ток в зависимости от характера выполняемой операции, создавая колебания физических полей в пространстве, которые могут быть измерены.

К громким операциям относится, например, сохранение информации.

Ученые также сосредоточились на изучении утечек со смартфонов, у которых энергопотребление в спящем и работающем режимах сильно отличается, что делает их наиболее уязвимыми. «Если у вашего ноутбука положили странный прибор, остерегайтесь», — предупредила автор исследования.

Тэги: которые , нам , без , ваших , вашего , сигналы , ноутбуки , злоумышленникам , действиях , wi-fi , расскажут , подключенные , излучают , привычные , шумы