Остерегайтесь Video Jacking

https://ib-bank.ru/bisjournal/news/14404

Владимир Безмалый

Малоизвестной особенностью многих современных смартфонов является их способность дублировать видео на экране устройства, так что оно также отображается на гораздо большем дисплее — например, на телевизоре. Однако новое исследование показывает, что эта функция может незаметно открыть пользователям простую и дешёвую новую форму цифрового подслушивания.

Атака, которую её вдохновители назвали «Video Jacking», использует специальную электронику, спрятанную внутри того, что похоже на зарядную станцию USB. Как только вы подключаете уязвимый телефон к соответствующему USB-шнуру для зарядки, шпионская машина разделяет видеодисплей телефона и записывает видео всего, что вы нажимаете, вводите или просматриваете, пока он подключён, включая ПИН-коды, пароли, учётную запись номера, электронные письма, тексты, изображения и видео.

Видеоджекинг позволяет злоумышленнику записывать каждую клавишу и прикосновение пальца, которое пользователь делает на телефоне, чтобы владелец злой зарядной станции мог позже воспроизвести видео и увидеть любые цифры или клавиши, нажатые на смартфоне.

Уязвим ли мой телефон?

Большинство телефонов, уязвимых для этой атаки, — это Android или другие смартфоны с поддержкой HDMI от Asus , Blackberry , HTC , LG , Samsung и ZTE. В случае сомнений поищите в Интернете марку и модель вашего телефона, чтобы узнать, поддерживает ли он HDMI или MHL.

Подключение видео является проблемой для пользователей телефонов с поддержкой HDMI в основном потому, что очень трудно отличить USB-шнур, который просто заряжает телефон, от кабеля, который также использует возможность вывода видео с телефона. Кроме того, на телефоне обычно нет предупреждений, предупреждающих пользователя о том, что видео с устройства передаётся другому источнику.

Все эти телефоны имеют функцию доступа через HDMI, которая включена по умолчанию», — сказал он. «Некоторые телефоны с поддержкой HDMI будут на короткое время мигать чем-то вроде «HDMI Connected» всякий раз, когда они подключены к источнику питания, который также использует функцию HDMI, но большинство из них вообще не будут отображать никаких предупреждений.

При тестировании этой атаки в магазине Apple, видео с домашнего экрана iPhone 6 появилось на дисплее в магазине без каких-либо подсказок. . Чтобы заставить его работать на дисплее,

потребовался специальный цифровой AV-адаптер Lightning от Apple, который можно было легко спрятать внутри опасной зарядной станции и подключить к нему удлинительный адаптер, а затем обычный кабель Lightning.

Мое мнение о видеоджекинге? Это интересная и очень реальная угроза, особенно если у вас есть телефон с поддержкой HDMI и вы привыкли подключать его к любому старому USB-порту. Вероятным, что кому-то из нас придётся беспокоиться об этом в реальной жизни? Ответ может быть во многом связан с тем, чем вы занимаетесь и насколько вы параноик, но мне не кажется очень вероятным, что у большинства простых смертных были бы причины беспокоиться о взломе видео.

С другой стороны, это был бы довольно дешёвый и достаточно эффективный (хотя и случайный) способ собрать секреты от группы ничего не подозревающих людей в определенном месте, например, в отеле, аэропорту, пабе или даже на рабочем месте.

Что могут сделать уязвимые пользователи, чтобы защитить себя от взлома видео?

Надеюсь, ваш телефон поставляется с двухконтактным зарядным шнуром, который подключается прямо к стандартной розетке. Если нет, подумайте об использовании адаптера зарядного устройства для телефона USB, который имеет обычную вилку питания переменного / постоянного тока. Во время путешествий носите с собой дополнительную док-станцию для зарядки мобильного устройства.

Также проверьте настройки своего мобильного телефона и посмотрите, позволяет ли он отключить зеркальное отображение экрана. Обратите внимание, что даже если вы сделаете это, возможность зеркалирования может не отключиться .

Что должны делать производители мобильных устройств, чтобы минимизировать угрозу видеоджекинга?

Проблема здесь в том, что производители устройств продолжают добавлять функции и не дают нам подсказок. Благодаря этой функции он автоматически подключается, несмотря ни на что. По умолчанию выход HDMI должен быть отключён, а если он включен, пользователь должен быть об этом уведомлен.