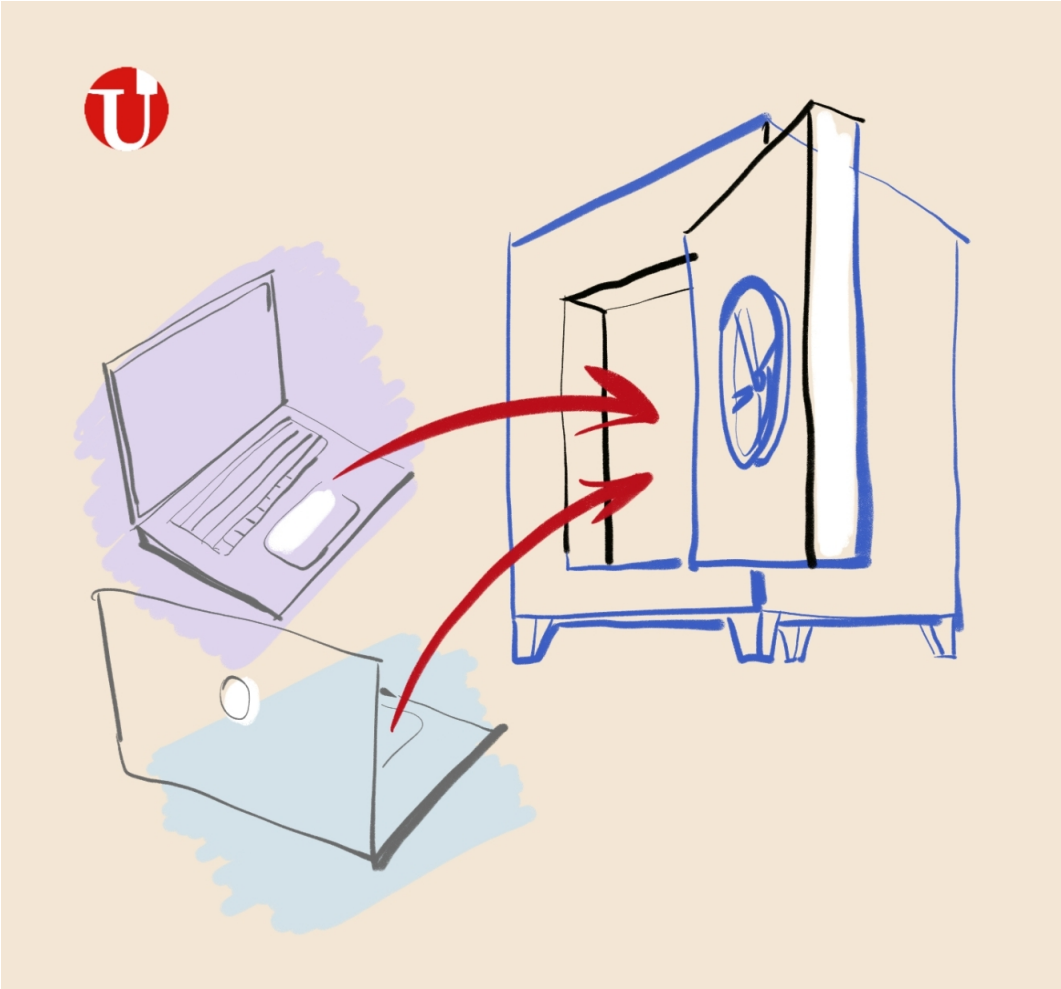
Храните свой MacBook в сейфе

(Keep your MacBook in the Safe)



Не оставляйте свой девайс без присмотра

MacBook можно взломать через кабель USB-C. И получить доступ к паролям, зашифрованным данным, установить вредоносную программу.

Обновлением ОС это исправить невозможно, т. к. это уязвимость аппаратная — на уровне железа.

Рассмотрим откуда эта уязвимость взялась и как от неё защититься...

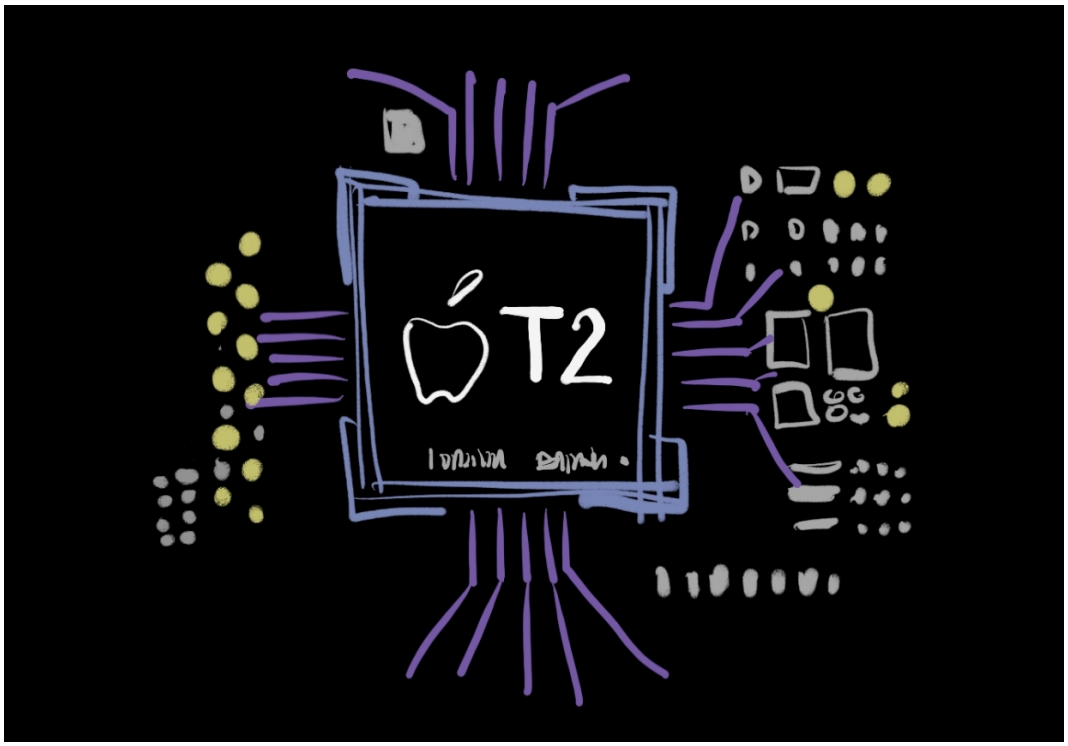
Улучшение принесло уязвимость

Уязвимость кроется в дополнительном процессоре T2, который изначально придумали для улучшения безопасности устройств Apple.

Но разработчики из Apple оставили открытым отладочный интерфейс в процессоре T2 (DFU). Это даёт возможность войти без аутентификации в режим обновления прошивки устройства.

MacBook, Mac Pro, Mac mini, Apple iMac и др. — все они комплектуются этим процессором T2 с 2018 года. По задумке T2 — это чип безопасности (Secure Enclave Processor).

Хранение конфиденциальных данных, паролей, аутентификация TouchID, криптографические операции, безопасная загрузка устройства — все эти операции обрабатывает дополнительный процессор T2, чтобы снять нагрузку с основного процессора.



Злоумышленники и правоохранительные органы всерьёз заинтересовались этой уязвимостью

Действительно, каждый, кто способен изготовить кабель USB-C с внедрённым эксплойтом, сможет запросто взломать любое устройство, оснащённое процессором T2.

> *Напомним, что чипами T2 оснащены практически все устройства Apple, произведённые с 2018 года.*

Сперва сообщения о существующей уязвимости T2 стали изредка появляться на форумах программистов. Изначально к ним не относились всерьёз, воспринимая их, как *«чёрный пиар от завистливых конкурентов»*.

Позже подобные упоминания попали в новостную Twitter-ленту проверенных аккаунтов и специализированные форумы в Reddit. И уже тогда эти сообщения привлекли внимание специалистов по информационной безопасности.

ИБ-специалисты позже подтвердили, что действительно с помощью двух эксплойтов (*chtckm8 & Blackbird*) можно получить полный контроль над устройством с чипом T2. Извлечь конфиденциальные данные, установить вредоносную программу, получить root-доступ, восстановить зашифрованные данные — то есть взять под полный контроль работу всего устройства.

IronPeak — ИБ-компания из Бельгии — также подтвердила эти сообщения. По их данным, во время загрузки необходимо через специально изготовленное USB-C запустить джейлбрейк (*v. 0.11.0 by Checkra1n*). И после

определённой последовательности действий, устройство и вся информация на нём становится доступна злоумышленнику.

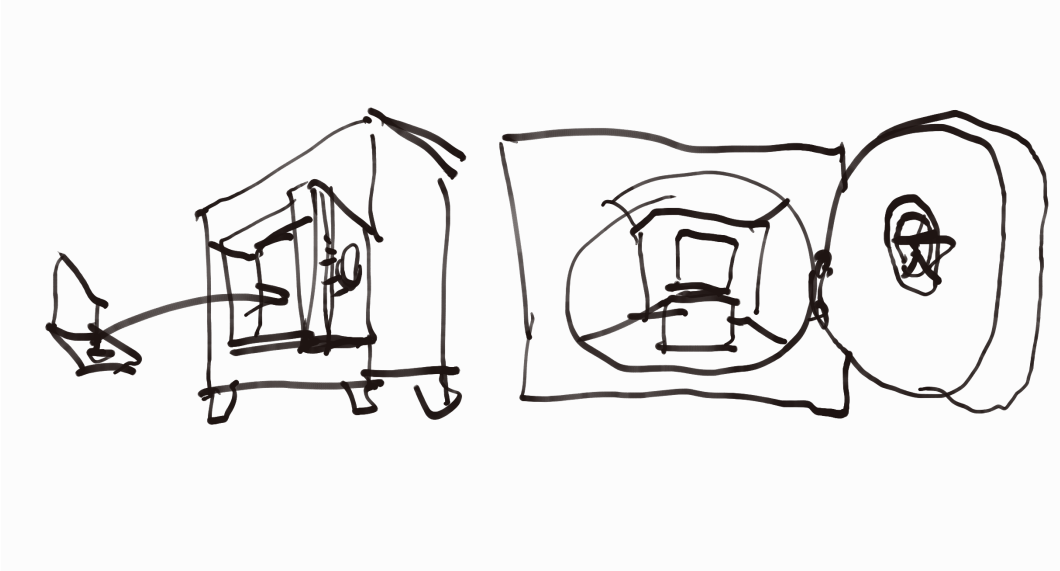
Этот бэкдор несомненно упрощает работу силовых структур, превращая Apple-устройства подозреваемых в *«открытую книгу»*.

Единственное решение — ограничьте доступ к устройству

Теперь, когда Вы уже знаете про эту уязвимость на своём девайсе, единственно возможный вывод — никогда не оставлять Apple-устройства без присмотра.

Никакие заплатки в прошивках и никакие антивирусы здесь не помогут, т. к. уязвимость заложена в аппаратной начинке (hardware). Буквально, в электронной схеме.

Как бы это смешно не прозвучало: надёжный сейф — теперь самый лучший аксессуар для Вашего Apple-устройства.



Дилемма удобства и безопасности

Конечно, мы понимаем, что такое бдительное наблюдение за своим устройством — не самое приятное занятие. Это полностью меняет отношение к его использованию. И даёт повод, чтобы переоценить выгоды, которые дают цифровые устройства.

В Кремниевой долине представители Apple до сих пор пока никак не прокомментировали эту уязвимость чипа T2, обнаруженную ИБ-специалистами.

People like free, and people like convenient

Действительно, людям нравится свобода, но люди также любят и удобство. Это верно подметил Брюс Шнайер в своей книге «Данные и Голиаф», опубликованной в 2015 году (Bruce Schneier, «Data & Goliath»).

Сделка, которую мы заключаем всякий раз, когда доверяем свою информацию цифровым устройствам, почти не осознаётся нами. Пароли, банковские счета, персональные данные — всё это незаметно попадает в наши девайсы. Это стало повсеместной нормой. Это стало удобной привычкой. Привычкой, от которой не так просто впоследствии отказаться.

Этой публикацией мы начинаем цикл статей о безопасности цифровых данных. И в первую очередь, о безопасности проектных данных.

Сейчас повсюду обсуждают защиту персональных данных. Защита проектных данных — это тема, с которой нам всем ещё только предстоит столкнуться.