Большой хак: Китай шпионил за компаниями из США с помощью микрочипов?

В США разгорается новый шпионский скандал. Издание Bloomberg BusinessWeek утверждает, что власти КНР могли шпионить за американскими компаниями и выведывать их секреты с помощью миниатюрных чипов, вмонтированных в оборудование для ЦОД. По данным агентства, слежка велась за почти тремя десятками вендоров, включая крупный банк, несколько государственных подрядчиков и технологических гигантов Apple и Amazon Web Services (AWS).



Ссылаясь на информированные источники внутри компаний и чиновников, знакомых с секретным расследованием, которое спецслужбы США якобы начали еще в 2015 году и ведут до сих пор, издание сообщает, что атака на аппаратном уровне стала возможна благодаря компании Super Micro Computer (более известна под названием Supermicro). Основанная тайваньским инженером Чарльзом Ляном (Charles Liang), она считается одним из крупнейших в мире производителей серверов и комплектующих для них.

Представители Apple, Amazon, Supermicro категорически отвергли информацию издания и заявили, что она не соответствует действительности. Однако в Bloomberg настаивают на достоверности сведений, отмечая, что 17 человек подтвердили приведенную в статье информацию о шпионских чипах в оборудовании Supermicro и других деталях атаки. Среди этих людей - двое сотрудников Amazon, трое - Apple, шесть действующих и бывших представителей разведслужб США и несколько американских чиновников.

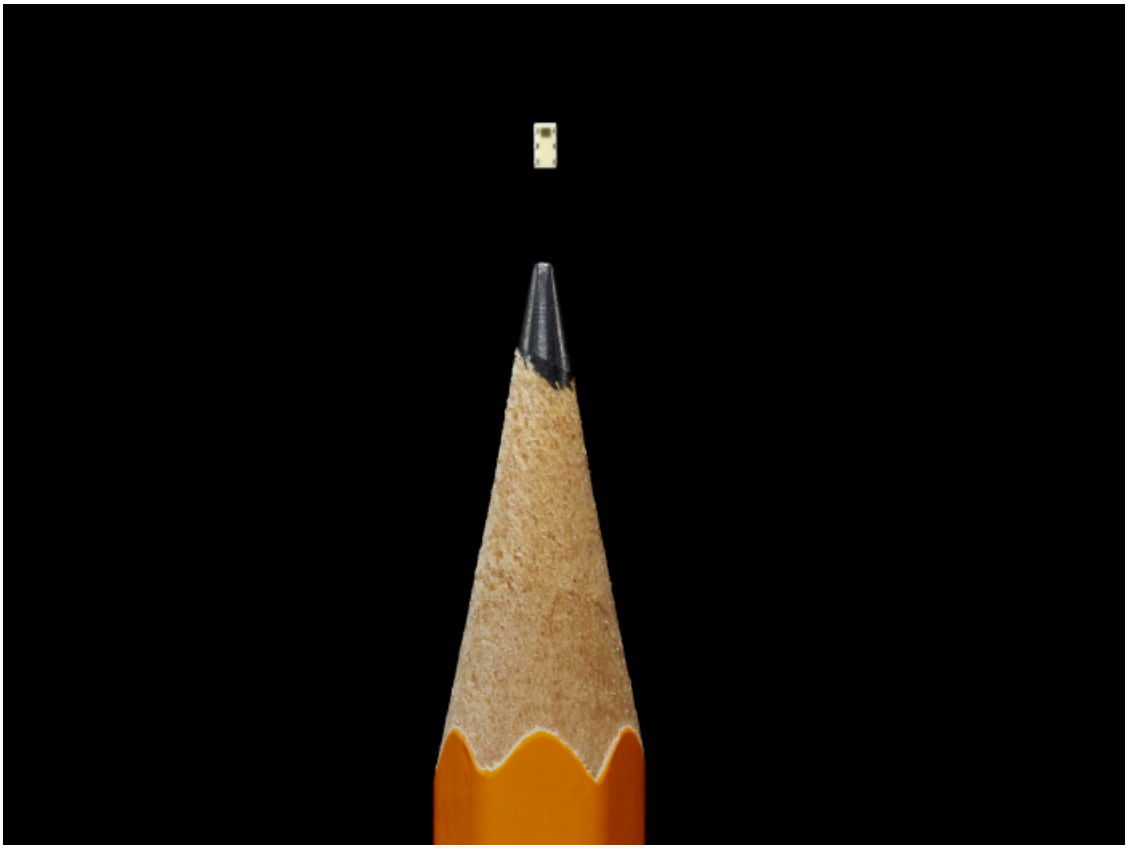
Итак, из публикации следует, что три года назад в материнских платах серверов Elemental Technologies были обнаружены шпионские микрочипы размером не больше рисового зернышка. В то время Amazon присматривалась к покупке этой компании, специализирующейся на разработке решений для доставки онлайн-видео. С помощью поглощения интернет-ритейлер рассчитывал расширить сервис потокового вещания, известный сегодня, как Amazon Prime Video. Также покупка Elemental была интересна по причине наличия у компании государственных контрактов и таких заказчиков, как ЦРУ, для которого Amazon как раз создавала высокозащищенную облачную систему.

Анонсировав сделку в сентябре 2015-го, Amazon за несколько месяцев до этого заказала комплексную оценку объекта приобретения. Как сообщил один из собеседников издания, для проверки Elemental с точки зрения кибербезопасности был привлечен сторонний подрядчик. Он-то первым и заподозрил неладное в дорогостоящих серверах Elemental, устанавливаемых в клиентских сетях для сжатия и обработки видео. Сборкой этих систем по заказу Elemental занималась компания Supermicro.

Поздней весной 2015 года несколько серверов Elemental были отправлены в Канаду на тестирование сторонней ИБ-компании. Специалисты последней нашли в их материнских платах чипы, не предусмотренные в оригинальной конструкции. Amazon немедленно уведомила о своем открытии американские власти, чем вызвала настоящий переполох в спецслужбах, поскольку серверы Elemental использовались в дата-центрах Министерства обороны США, на кораблях ВМФ, а также применялись ЦРУ во время операций с беспилотниками. Плюс, Elemental была лишь одним из сотен клиентов Supermicro.

В ходе расследования под грифом "секретно", которое продолжается и по сей день, выяснилось, что чипы позволяют создавать лазейки в любую сеть, где имеется скомпрометированное оборудование. Также следователи узнали, что шпионские микросхемы в материнских платах устанавливались на предприятиях китайских субподрядчиков, с которыми сотрудничает Supermicro.

В беседе с журналистами Bloomberg двое информированных о деле чиновников сообщили, что чипы были вмонтированы в платы во время производственного процесса при содействии сотрудников одного из подразделений вооруженных сил КНР (Народно-освободительной армии Китая (People’s Liberation Army), официальное название ВС страны).



Спроектированные и произведенные китайскими военными, шпионские микрочипы сравнимы по размеру с кончиком отточенного карандаша. Имея в составе память и сетевой компонент, чипы также обладают достаточной для атаки процессорной мощностью. Разработчики постарались сделать их как можно менее приметными. Серого и грязно-белого оттенка, они выполнены в виде стандартных компонентов материнской платы, утверждают источники, знакомые с отчетом по результатам проверки для Amazon и видевшие фотографии и рентгеновские снимки чипов. Подключенные к контроллеру управления материнской платы, шпионские чипы способны отдать команду на установку интернет-соединения с анонимными серверами, на которых хранится более сложный программных код, а затем обеспечить его исполнение на устройствах.

В публикации описывается, как стала возможна такая атака на аппаратном уровне, намного более серьезная, чем ставшие уже привычными программные взломы.

Площадкой для реализации плана стала компания Supermicro, которая не только входит в тройку ведущих поставщиков серверных материнских плат, но и доминирует на рынке "материнок" для специализированных компьютеров, которые устанавливаются в различном оборудовании - от МРТ-

установок до боевых комплексов.

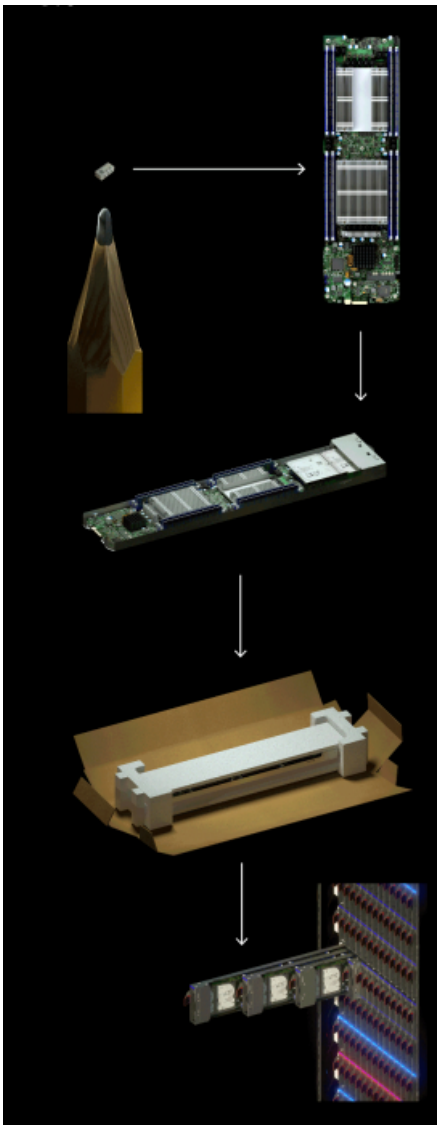
В активе компании более 900 клиентов в 100 странах мира. В интервью Bloomberg бывший сотрудник разведки США, изучавший Supermicro и ее бизнес-модель, охарактеризовал компанию, как аналог Microsoft на рынке компьютерного "железа".

> "Компрометацию материнских плат Supermicro можно сравнить с компрометацией ОС Windows. Это атака на весь мир", - заявил экс-агент спецслужб.

Хотя продукция Supermicro проектируется в США, а сборочные линии компании расположены в Калифорнии, Нидерландах и Тайване, материнские платы Supermicro практически полностью производится подрядчиками в Китае.

По данным портала DigiTimes, по состоянию на 2016 год Supermicro сотрудничала с тремя основными "контрактниками", двое из которых - тайваньские, а один - шанхайский. Однако оказалось, что когда прямые партнеры Supermicro не справлялись с большими объемами заказов, они привлекали дополнительных субподрядчиков.

В ходе расследования спецслужбы сумели отследить происхождение материнских плат со шпионскими чипами - они изготавливались на четырех китайских предприятиях, которые выполняли заказы Supermicro на протяжении как минимум двух лет. Также удалось выяснить, что руководство предприятий согласилось внести изменения в оригинальный дизайн материнских плат и снабдить их дополнительным чипом под давлением неких людей, выдававших себя за представителей Supermicro либо высокопоставленных чиновников со связями в правительстве. Для достижения цели те использовали взятки, а когда деньги не работали - угрозы и шантаж. Разведслужбы пришли к выводу, что план диверсии с материнскими платами Supermicro был разработан в подразделении вооруженных сил КНР, специализирующемся на такого рода атаках.



Таким образом скомпрометированные материнские платы оказывались в серверных системах Supermicro, которые поставлялись в центры обработки данных десятков американских компаний. После того, как серверы устанавливались в ЦОД и начинали работать, микрочипы вносили изменения

в ядро операционной системы, подготавливая почву для дальнейших модификаций. Также чипы могли устанавливать соединение с подконтрольными хакерам компьютерами для получения дальнейших инструкций и внедрения стороннего программного кода.

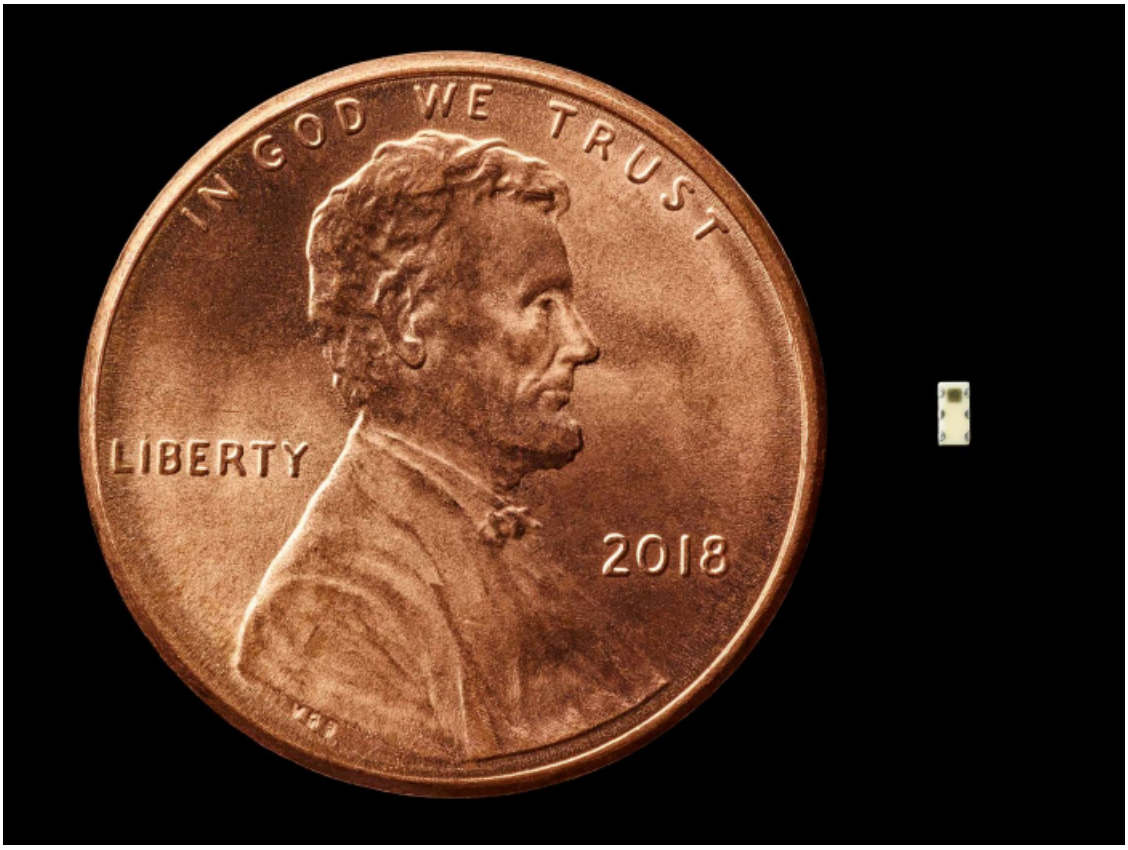
Еще задолго до того, как диверсия с материнскими платами Supermicro вскрылась, американские разведслужбы предупреждали, что их китайские коллеги готовятся внедрить шпионские чипы через канал поставок компьютерных комплектующих. По началу никакой конкретной информации у спецслужб не было, но в первой половине 2014 года разведка доложила правительству США, что ВС КНР планируют использовать для этих целей материнские платы Supermicro.

Публичное предупреждение об угрозе исключалось, поскольку это нанесло бы сокрушительный удар как по Supermicro, которая все же американская компания, так и по ее клиентам. В данных разведки ничего не говорилось о том, против кого нацелена атака и какие задачи преследуют ее организаторы. К тому же, пока от диверсии кто-то действительно не пострадал, спецслужбы были ограничены в ответных мерах. В Белом доме заняли выжидательную позицию, периодически запрашивая информацию о ситуации с этим делом.

Одним из важнейших клиентов Supermicro была корпорация Apple. По данным издания, в рамках плана по строительству новой сети дата-центров по всему миру компания собиралась в течение двух лет закупить у Supermicro более 30 тысяч серверов. Однако в 2016 году Apple внезапно прекратила сотрудничество с партером. Хотя представители компании отрицают всякую связь со шпионским скандалом, о котором говорится в статье Bloomberg, журналисты намекают, что разрыв произошел из-за "жучков" в серверах Supermicro.

Шпионские чипы были найдены в мае 2015 года после того, как в Apple заметили странную сетевую активность и сбои в программной прошивке серверов Supermicro. По словам двух высокопоставленных сотрудников Apple, имена которых по понятным причинам не раскрываются, корпорация проинформировала об инциденте ФБР, после чего строго засекретила все детали случившегося, даже внутри компании.

Один из инсайдеров рассказал, что в течение нескольких недель после обнаружения чипов-шпионов в дата-центрах Apple заменили весь парк серверов Supermicro в количестве около 7 тысяч устройств. Источник из правительственных кругов США утверждает, что Apple не допустила на свои объекты государственных следователей и не предоставила скомпрометированное оборудование, так что масштабы атаки и ее последствий остались для властей неизвестны.



Тем временем, о шпионских "закладках" в серверах сообщила и Amazon. Она передала спецслужбам оборудование, что позволило им детально изучить микрочипы и принципы их работы. По данным источников, информированных о делах Amazon, собственная служба безопасности компании также вела расследование, в ходе которого в пекинском дата-центре AWS были выявлены серверы с модифицированными материнскими платами. В одном из случаев специалисты столкнулись с еще

более изощренным методом маскировки - шпионские чипы сделали тоньше и разместили между слоями стеклотекстолита, на котором крепились все остальные компоненты. По размеру эти микрочипы были даже меньше, чем кончик заточенного карандаша.

По словам одного из собеседников, в Amazon решили не менять оборудование, чтобы организаторы диверсии не заподозрили провала. Вместо этого в компании вели мониторинг за чипами, но не выявили никаких попыток вредоносных действий. Спустя некоторое время, в ноябре 2016-го, стало известно, что Amazon продала всю свою инфраструктуру в Пекине локальному партнеру Beijing Sinnet за 300 миллионов долларов.

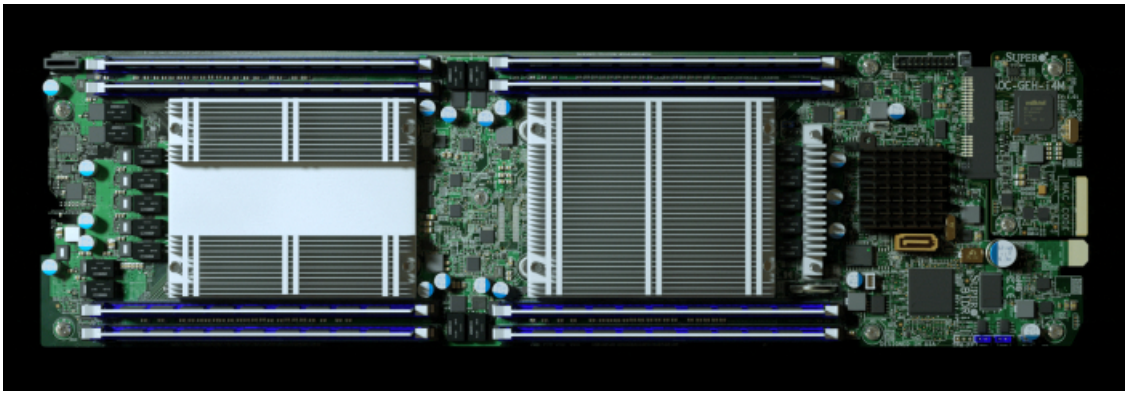
В Amazon и Apple отрицают информацию, представленную в статье Bloomberg.

> "Утверждения о том, что на момент приобретения Elemental компания AWS знала о компрометации в цепи поставок, проблеме со шпионскими чипами и аппаратных модификациях не соответствуют действительности. Также недостоверна информация о том, что AWS знала о присутствии в серверах шпионских чипов, была в курсе изменений в компонентах оборудования в своих китайских ЦОД или содействовала расследованию ФБР, предоставляя данные о скомпрометированной аппаратуре", - сказано в заявлении компании по поводу публикации.
>
> "Никогда, ни в прошлом, ни в настоящее, мы не сталкивались ни с какими проблемами из-за скомпрометированного оборудования или шпионских чипов в материнских платах Supermicro, установленных в серверных системах Elemental или Amazon", - добавили в компании в ответ на запрос CNBC.

Не менее категорично отреагировали и в Apple.

> "Мы совершенно четко заявляем: Apple никогда не находила шпионских чипов, махинаций на аппаратном уровне или преднамеренно созданных уязвимостей ни в каких из серверов. Apple никогда не вступала в контакт с ФБР или другими спецслужбами по поводу подобного инцидента. Мы не в курсе никаких расследований, проводимых ФБР, также, как и наши источники в правоохранительных органах", - говорится в пресс-релизе "яблочной" корпорации.

Также в компании предположили, что журналисты могли перепутать полученные от источников сведения с уже известным киберинцидентом, произошедшим в 2016 году. Тогда компания обнаружила заражённый драйвер на одном из серверов Supermicro, работавших в лаборатории Apple. Эпизод расценили как случайность, исключив целенаправленную атаку на Apple.



Что касается Supermicro, то в пресс-службе отметили, что им не известно ни о каких расследованиях по поводу описанной в статье ситуации, и что представители ни одной из спецслужб не связывались с компанией по данному вопросу.

> "Мы не в курсе того, что кто-либо из наших клиентов отказался от поставок оборудования Supermicro в результате такого рода инцидента", - сказано в заявлении.

На запрос издания в МИДе КНР ответили, что Китай является решительным защитником кибербезопасности, и напомнили, что в 2011 году Пекин вместе с другими странами-участницами ШОС предложил международные гарантии безопасности аппаратного обеспечения.

Представители ФБР, ЦРУ и АНБ отказались от комментариев.

Материал Bloomberg о шпионских чипах в серверах производства Supermicro наделал много шума. По данным The Register, публикация не только спровоцировала обвал акций Supermicro и пошатнула котировки упомянутых в статье Apple и Amazon, но рикошетом задела других азиатских вендоров, имена которых в материале даже не фигурировали. Сильнее всего шпионский скандал аукнулся китайским компаниям Lenovo и ZTE – на следующий день после выхода заметки их акции подешевели

на 15 и 11 процентов. Издание Fortune среди пострадавших также перечислило партнеров Apple, таких как TSMC, Largan Precision, LG Display, TDK и Murata.

Вокруг публикации сразу разгорелись ожесточенные споры насчет того, кому верить – авторам Bloomberg Джордану Робертсону (Jordan Robertson) и Майклу Райли (Michael Riley), либо Amazon и Apple, которые категорически отвергли предположения журналистов.

Между тем, несколько дней спустя после выхода материала ИБ-специалист Джо Фицпатрик (Joe FitzPatrick), имя которого стало едва ли не единственным, открыто названным в статье, поставил под вопрос историю Bloomberg.

Мнение Фицпатрика, основателя компании Hardware Security Resources LLC, обучающей специалистов киберзащите на аппаратном уровне, приводится для иллюстрации того, насколько широкие возможности может дать взлом через комплектующие.

> "Железо открывает любые двери", – цитирует Bloomberg Фицпатрика.

[Большой хак: Китай шпионил за компаниями из США с помощью микрочипов?]

Однако в свежем интервью ведущему профильного блога Risky Biz Патрику Грэю (Patrick Gray) Фицпатрик признался, что теперь он испытывает неловкость из-за статьи Bloomberg. Прочитав материал, специалист узнал в нем многие из своих предположений о возможности вживления в оборудование шпионских жучков, которыми он делился с Джорданом Робертсоном, сообщает AppleInsider.

Фицпатрик впервые побеседовал с Робертсоном в 2017 году перед хакерской конференцией DEF CON, где он выступал с презентацией о шпионских "закладках" в оборудовании. Во время разговора специалист описал принцип работы аппаратных имплантов и рассказал об успешном экспериментальном образце, который он демонстрировал в 2016 году на другом известном хакерском мероприятии – Black Hat.

Занимаясь ИБ-исследованиями, Фицпатрик никак не связан с продажей такого рода устройств. По большей части он занят отработкой теорий, появившихся в ходе его многолетнего опыта преподавания в области киберзащиты оборудования, поясняет издание.

По словам Фицпатрика, он был очен удивлен, когда узнал в статье свой теоретический сценарий, который, как сообщается, на 100 процентов подтверждают некие другие источники. Тем не менее, специалист заявил, что не видит смысла в описанном способе, поскольку есть множество других, гораздо более простых и экономичных возможностей получить доступ к целевой компьютерной сети.

> "Существуют более легкие аппаратные способы, есть возможности на уровне софта и прошивки. Описанный подход нелогичный и плохо масштабируемый. Я бы не стал так действовать. И не только я – никто из тех, кого я знаю", – заявил Фицпатрик.

Также специалист показал ведущему Risky Biz переписку с Робертсоном по электронной почте, которую он вед до публикации материала. В своих сообщениях Фицпатрик высказывал сомнения по поводу целесообразности описанной бэкдор-атаки на аппаратном уровне, учитывая, что той же цели можно добиться с помощью удаленной модификации прошивки BMC-контроллера, которая зачастую бывает устаревшей. Также Фицпатрик задается вопросом – а что если "лишние" чипы, якобы найденные в платах, на самом деле – просто защита от подделки, байпас или какие-то другие компоненты, установленные подрядчиком? По словам эксперта, недостаточно опытный специалист вполне может принять комбинированный элемент за привнесенный извне.

Робертсон в ответном письме признает, что идея действительно кажется "бредовой", но продолжает настаивать на своем, отмечая, что множество источников подтверждают информацию. Однако Фицпатрика доводы журналиста не убедили.

Робертсон не смог раздобыть фотографий пресловутых шпионских чипов. Как он объяснил, внешний вид ему на словах описал закрытый источник. Однако в одном из своих писем журналист спросил у Фицпатрика, как выглядит усилитель сигнала (signal amplifier) или согласователь (coupler), и тот отправил ему ссылку на подобный чип производства Mouser Electronics. Впоследствии фотографии того самого чипа оказалась в статье Bloomberg.

Резюмируя, Фицпатрик заявил, что изложенное Bloomberg – не более, чем подозрения. Ссылаясь на свои знания и опыт, специалист отметил, что приведенные в статье технические детали беспорядочны и запутаны.

> "Не то чтобы они были совершенно неверны, но все это лишь теория. Я не знаю, о чем сообщили другие семнадцать источников, на которые ссылаются авторы, но судя по технической стороне, в остальном может быть такая же путаница", – подытожил эксперт.