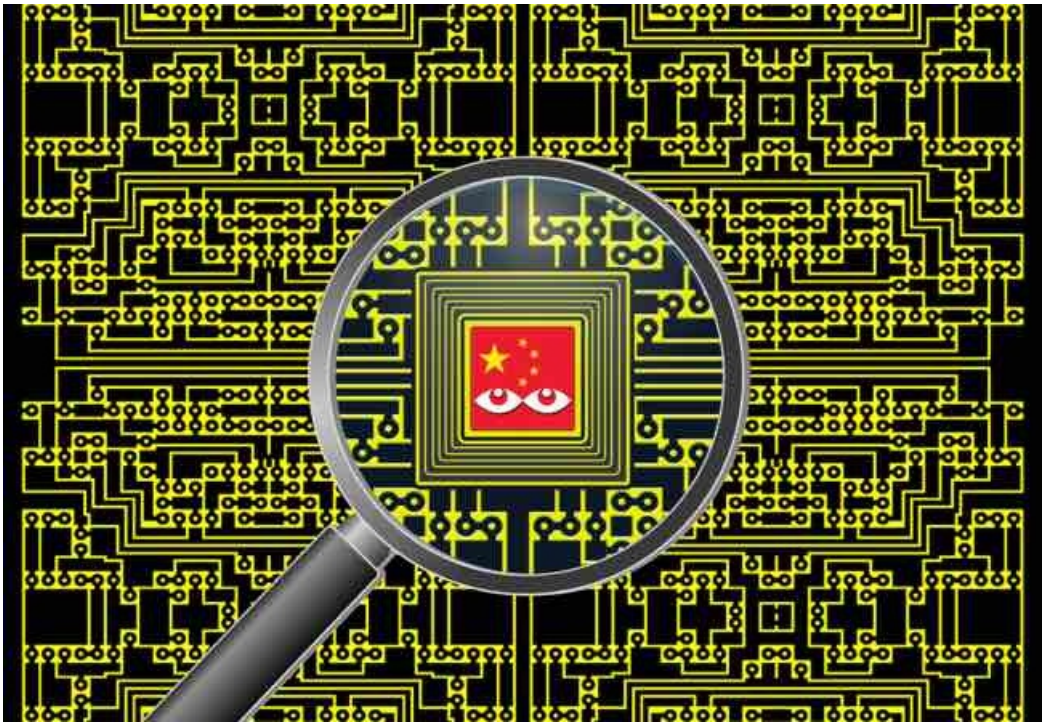
“Шпионские чипы” Supermicro, продолжение

Агентство Bloomberg решило вспомнить свою скандальную историю о "закладках" в серверах Supermicro, которая наделала много шума осенью 2018 года. Напомним, почти 2,5 года назад агентство опубликовало серию статей о посторонних чипах в материнских платах серверов Supermicro, с помощью которых Китай якобы шпионит за американскими компаниями.



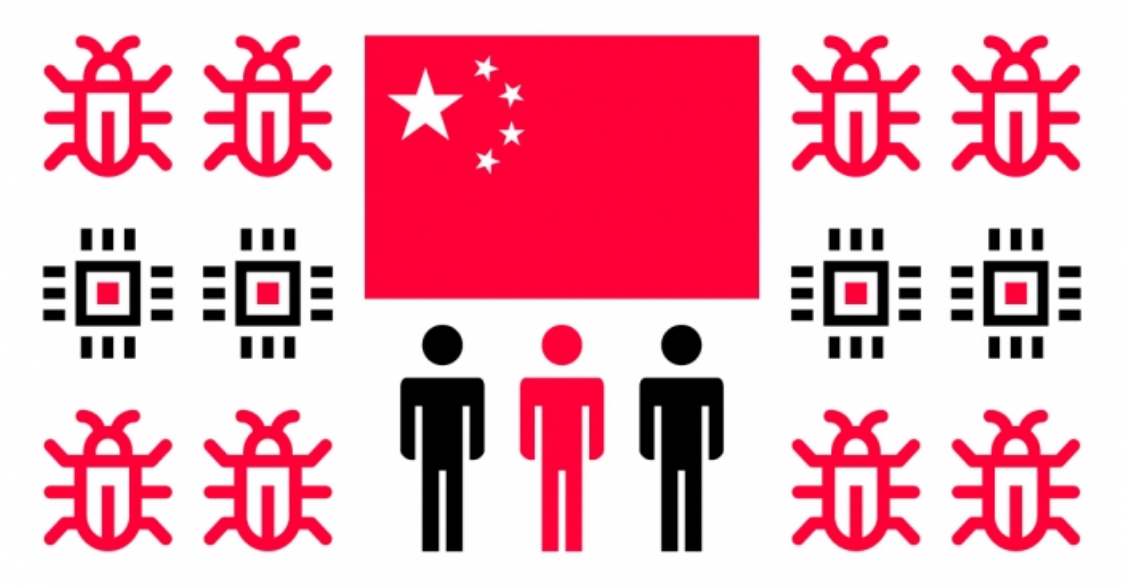
В феврале 2021 года вышло продолжение ″шпионской саги″. Теперь журналисты Джордан Робертсон (Jordan Robertson) и Майкл Райли (Michael Riley) утверждают, что оперативники китайских спецслужб больше десяти лет встраивали шпионские чипы в оборудование компании Super Micro Computer, более известной под названием Supermicro, причем происходило это с ведома разведки США. Американские власти якобы намеренно замалчивали информацию, чтобы получше изучить тактику противника и создать защиту от такого рода атак.

> ″История основана на интервью более чем с 50 сотрудниками правоохранительных органов, вооруженных сил, Конгресса, спецслужб и частных компаний. Большинство собеседников поделились информацией на условиях конфиденциальности. Некоторые из предоставленных сведений нашли подтверждение в корпоративных документах, изученных Bloomberg News″, - пишут авторы.

В центре новой истории три эпизода. В первом, который датируется 2010 годом, речь о том, что Министерство обороны США выявило шпионскую активность на тысячах своих серверов. Благодаря коду, вшитому в чипы, управляющие стартовой загрузкой компьютеров, в Китай передавались данные о сетях военного ведомства.

Второй эпизод, произошедший в 2014 году, связан с Intel. Американская корпорация обнаружила, что группировка высококлассных хакеров из Китая сумела проникнуть в ее сеть через сервер, загрузивший вредоносное ПО с сайта обновлений поставщика.

Годом позднее, в 2015-м, ФБР предупредило компании о том, что агенты китайских спецслужб тайно внедряют в серверах одного из производителей чипы со встроенным бэкдор-кодом.



В Bloomberg акцентируют, что во всех трех эпизодах фигурируют китайская сторона и компания Supermicro. Третья общая черта - это то, что американские спецслужбы раскрыли попытки шпионажа, но сохранили информацию в тайне, чтобы больше узнать о возможностях КНР.

Ссылаясь на свидетельства 14 бывших сотрудников правоохранительных органов и разведки, Bloomberg утверждает, что американские спецслужбы наблюдают за практикой КНР по использованию серверов Supermicro в своих интересах большую часть последнего десятилетия. В 2012 году ФБР начало контрразведывательную операцию, в рамкой которой велось наблюдение за группой сотрудников Supermicro.

Продолжается ли операция по сей день, журналисты не выяснили. Один из собеседников агентства сообщил, что в 2018 году ФБР привлекало частный бизнес к анализу оборудования Supermicro со шпионскими чипами.

Описанный Bloomberg сценарий нельзя назвать совсем уж неправдоподобным, считает Алан Паллер (Alan Paller), директор некоммерческой организации SANS Technology Institute, которая занимается подготовкой специалистов по кибербезопасности.

> ″В иерархии методов кибератак, которые предпочитают спецслужбы, атаками высочайшего уровня считаются те, которые продолжаются даже при выключении компьютеров и перезагрузке программного обеспечения. Внедрение шпионского чипа - самое простой способ [достигнуть этого]. Простые решения обычно работают″, - заявил специалист, комментируя публикацию Bloomberg изданию The Register.

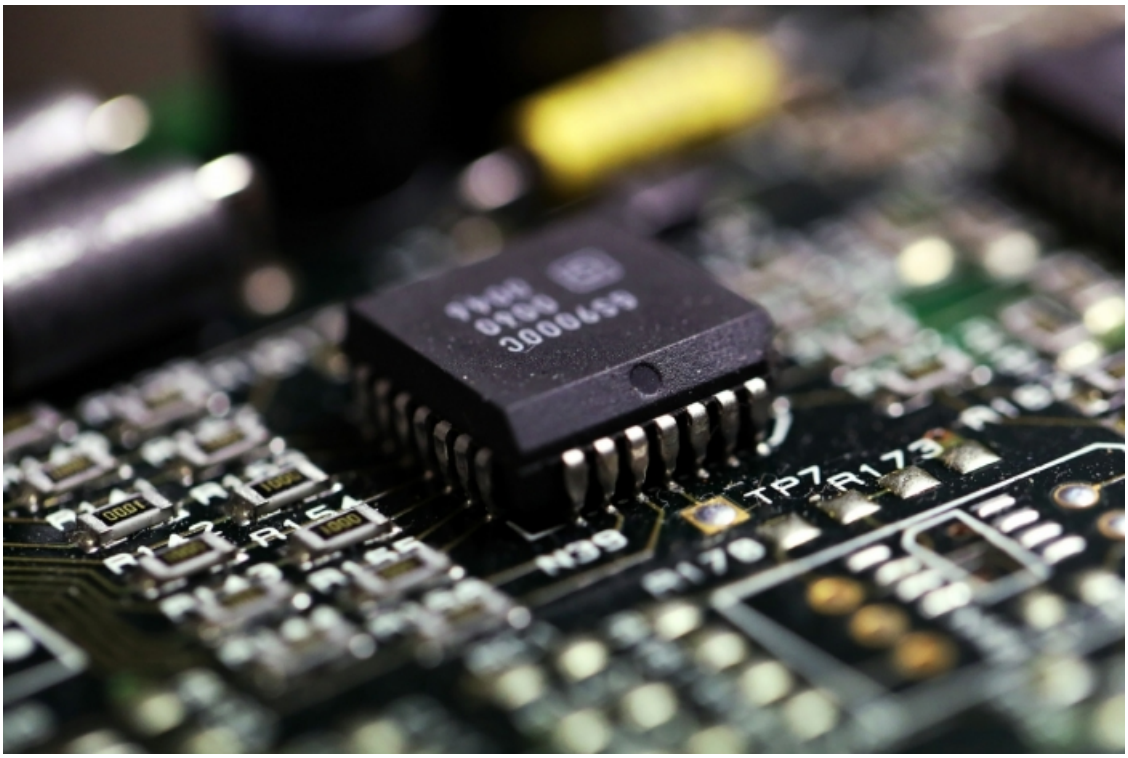


В Supermicro ожидаемо опровергли статью и заверили в безопасности своих серверных продуктов.

> ″Изложенная Bloomberg история - это мешанина разрозненных и недостоверных предположений о событиях многолетней давности. Сделанные в статье выводы притянуты за уши и в очередной раз не выдерживают никакой критики. На самом деле, в ответ на запрос Bloomberg в прошлом месяце Агентство Национальной безопасности, как и в 2018 году, снова отказалось подтвердить, что описанные в материале эпизоды и последующие события когда-либо имели место. Несмотря на утверждения Bloomberg о проводившемся расследовании спецслужб,... к Supermicro по этому поводу никто ни разу не обращался - ни со стороны властей США, ни со стороны партнеров или клиентов″, - говорится в заявлении на сайте Supermicro.

Обозреватели отмечают, что до сегодняшнего дня общественности не предъявлено никаких материальных доказательств существования шпионских чипов. Никто не взял материнскую плату и не показал на ней - вот он, тот самый чип. Многие авторитетные эксперты в области кибербезопасности, в том числе специалист Google Security Тевис Орманди (Tavis Ormandy), скептически высказывались по поводу истории Bloomberg.

Кроме того, в 2018 году с опровержениями выступили несколько государственных должностных лиц и представителей частного бизнеса, в том числе Дэн Коутс (Dan Coats), занимавший тогда должность директора Национальной разведки, и директора ФБР Кристофер Рэй (Christopher Wray). Корпорации Amazon и Apple, упомянутые в нашумевшем материале, требовали, чтобы агентство отозвало статью, а гендиректор Apple Тим Кук (Tim Cook) даже назвал ее "100-процентной ложью".



Впрочем, в продолжении ″шпионской саги″ Bloomberg все же есть персонаж, который не стал скрывать своего имени. Это Мукул Кумар (Mukul Kumar), в прошлом - главный специалист по кибербезопасности разработчика FPGA-чипов Altera, который в 2015 году был куплен Intel. Мужчина утверждает, что узнал о шпионских чипах в 2015 году на неком несекретном мероприятии, где он присутствовал по роду своих обязанностей в Altera.

Поскольку речь в статье Bloomberg идет о чипах, журналисты The Register попросили оценить правдоподобность истории бывшего руководителя крупной полупроводниковой компании, который предпочел остаться анонимом. Тот не только подтвердил возможность существования шпионских чипов, но и заявил, что держал доказательства этого в своих руках. По словам бывшего топ-менеджера, в такого рода шпионских операциях особенно преуспели Китай, Израиль и Великобритания. Франция, Германия и Россия тоже практиковали аппаратные ″закладки″, но они менее опытны в подобных диверсиях, заявил специалист.

> ″Если вы встроите [в плату] то, чего там быть не должно, то постороннее можно обнаружить с помощью рентгеновского контроля. Но если немного изменить форму и размер существующих полупроводниковых компонентов, то найти подвох уже сложнее. Нетрудно добавить небольшую схему, которая не будет слишком заметной″, - добавил собеседник издания.

Журналисты поинтересовались у Supermicro, не собирается ли компания судиться с Bloomberg из-за его очередного опуса, но пресс-секретарь ответила уклончиво, заявив, что производитель еще

изучает материал и рассматривает возможные варианты действий.