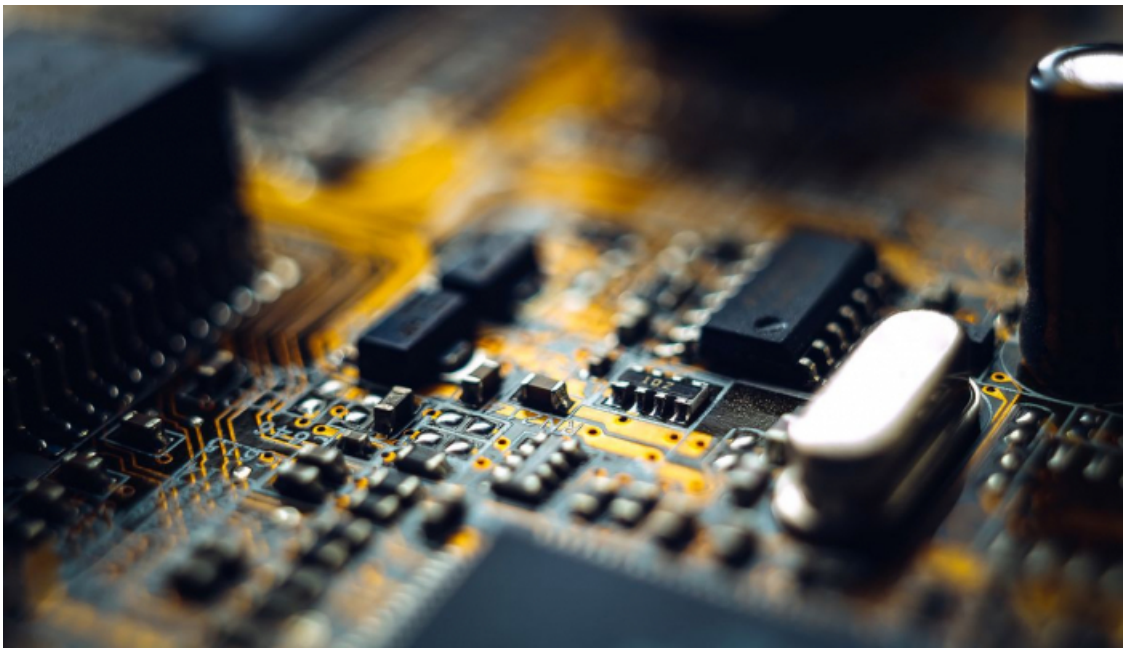
"Шпионская сага" Bloomberg продолжается

Несколько дней спустя после выхода скандального материала о сторонних чипах в серверах Supermicro, с помощью которых Китай якобы шпионит за американскими компаниями, Bloomberg опубликовало новую статью на эту тему.

В продолжении "шпионской саги" рассказывается, что одна из ведущих телекоммуникационных компаний США в августе 2018 года изъяла из своей сети скомпрометированное оборудование Super Micro Computer Inc., после того, как специалисты партнерской ИБ-фирмы нашли в нем "закладку". На этот раз издание ссылается не на закрытые источники, пожелавшие остаться неизвестными, а на конкретного человека - эксперта в области кибербезопасности Йосси Эпплбаума (Yossi Appleboum), который участвовал в расследовании и передал Bloomberg документы и другие свидетельства инцидента.



Эпплбаум, прежде работавший в технологическом подразделении израильской военной разведки, теперь занимает пост исполнительного директора американской компании Sepio Systems, которая специализируется на аппаратной безопасности. В совет директоров фирмы, расположенной в городе Гейтерсберг, штат Мэриленд, также входит Тамир Пардо (Tamir Pardo), в прошлом глава "Моссад", политической разведки Израиля, а среди консультантов компании числится экс-директор по защите информации ЦРУ Роберт Бигман (Robert Bigman).

Sepio Systems наняли для проверки нескольких крупных дата-центров некой телекоммуникационной компании. Название последней не раскрывается, поскольку Эпплбаум связан договором о неразглашении.

Внимание экспертов привлекла необычная сетевая активность сервера Supermicro в ЦОД. Физически осмотрев оборудование, специалисты обнаружили чужеродный элемент, вмонтированный в Ethernet-разъем.

Эпплбаум утверждает, что встречал такого рода "закладки" не только в серверах Supermicro, но и в оборудовании других вендоров, изготовленном китайскими контрактниками.

> "Supermicro - просто жертва, как и остальные", - заявил специалист.

По его словам, в цепочке поставок КНР существует масса возможностей для подобных махинаций с

оборудованием, выявить которые во многих случаях невозможно. Эпплбаум назвал это серьезной проблемой.

Supermicro, биржевые котировки которой обрушились на фоне шпионского скандала, вновь заявила, что ей ничего не известно о компрометирующих находках в ее серверах.

> "Безопасность клиентов и целостность нашей продукции - основа бизнеса и главная ценность компании. Мы заботимся о целостности наших продуктов на протяжении всего производственного процесса, а безопасность цепочки поставок - важная тема для обсуждения в нашей отрасли. Мы по-прежнему ничего не знаем ни о каких несанкционированных компонентах в оборудовании и никто из клиентов не сообщал нам о них. Мы обеспокоены тем, что в Bloomberg нам предоставили лишь ограниченную информацию и никаких документов. Компании дали всего полдня, чтобы отреагировать на новые обвинения", - говорится в пресс-релизе Supermicro. В своем предыдущем заявлении в ответ на первую статью Bloomberg производитель также открестился от того, что в его серверах могут присутствовать шпионские микрочипы.

В агентстве отметили, что сообщили Supermicro о новой публикации утром 8 октября и дали компании 24 часа на ответную реакцию, прежде чем выпускать материал.

Акции Supermicro, подешевевшие больше чем на 40 процентов неделю назад, после новых откровений Bloomberg Businessweek снова упали в цене - на этот раз на 27 процентов.

По словам Эпплбаума, изучив скомпрометированное устройство, он пришел к выводу, что модификации в сервер телекоммуникационной компании внесли на предприятии, где он был произведен. От коллег из западных спецслужб ему удалось узнать, что устройство изготовили на заводе одного из субподрядчиков Supermicro в китайском городе Гуанчжой.

В ходе проверки дата-центра телекоммуникационной компании специалисты Sepio Systems установили, что скомпрометированный сервер Supermicro присутствовал в сети в виде двух устройств, генерирующих разнонаправленный трафик. Однако поскольку активность исходила от доверенного сервера, неавторизованный трафик успешно проходил фильтры системы безопасности.

Специалист отметил, что в модифицированном Ethernet-разъеме присутствовали металлические вставки, в то время как обычно такие коннекторы выполняются из пластика. Металл понадобился для отвода тепла от скрытого внутри чипа, который служил в качестве мини-компьютера. Эпплбаум добавил, что внешне разъем выглядел вполне безобидно и был похож на оригинальную заводскую деталь высокого качества.

Когда специалисты Sepio Systems уведомили клиента о своих находках, сотрудники отдела безопасности телекоммуникационной компании изъяли устройство для дальнейшего анализа, в котором ИБ-фирма Эпплбаума уже не участвовала. Bloomberg не удалось узнать, обращалась ли компания в ФБР по данному поводу.

Ведущие американские операторы сотовой связи AT&T, Verizon Communications и Sprint на запрос агентства ответили, что инцидент не касается их компаний. В Sprint подчеркнули, что в ее сетях вообще не используется оборудование Supermicro. В T-Mobile U.S. не отреагировали на просьбу Bloomberg о комментарии.

Amazon и Apple категорически отрицают информацию Bloomberg, а в Министерстве национальной безопасности США заявили, что у них нет причин сомневаться в опровержениях вендоров.

В профессиональном ИБ-сообществе также ставят под вопрос разоблачения Bloomberg. Накануне Джо Фицпатрик (Joe FitzPatrick), имя которого упомянуто в первой в статье, заявил, что приведенные в материале технические детали беспорядочны и запутаны. Он также признался, что испытывает неловкость из-за публикации, потому что журналисты представили его предположения о возможности аппаратных "закладок" в оборудовании, как доказанный факт.

Обозреватели The Register, изучившие обе статьи и следящие за онлайн-обсуждениями "горячей" темы, допускают, что в Bloomberg могли недостаточно тщательно проверить достоверность сведений перед публикацией. Также британское издание не исключает вероятность того, что журналистов в своих интересах используют спецслужбы. Преследуя собственные цели, разведывательные ведомства могли намеренно "слить" дезинформацию о махинациях с оборудованием в китайской цепи поставок электронных компонентов.