

Bloomberg: Huawei под запретом в США, но камеры с ее чипами повсюду

Власти США развернули войну против Huawei, крупнейшей технологической компании КНР, обвиняя ее в краже коммерческих секретов, нарушении американских санкций против Ирана и продаже оборудования со скрытыми уязвимостями, которыми китайское правительство может воспользоваться в шпионских целях.

В центре внимания Вашингтона – телекоммуникационное оборудование Huawei, за последние годы широко распространившееся по всему миру. Однако повод для беспокойства представляет и другая продукция китайского вендора, а именно – чипы HiSilicon, полупроводникового подразделения Huawei, сообщает Bloomberg.



По данным агентства, микросхемы HiSilicon используются примерно в 60 процентах камер видеонаблюдения, имеющих сегодня на рынке.

"Это значит, что китайские чипы отвечают за обработку видеоданных с камер, установленных в самых разных местах – от пиццерий до офисов и банков по всей территории США", – говорится в [статье Bloomberg](#) под названием "Huawei под запретом в США, но камеры с ее чипами повсюду".

В Bloomberg узнали, что американские законодатели всерьез обеспокоены присутствием китайских чипов в миллионах камер по всей Америке. Высказываются опасения, что Китай, преуспевший в тотальной слежке за собственными гражданами, может обернуть эти возможности против Соединенных Штатов.



"С помощью камер наблюдения Китай создает у себя в стране огромное оруэлловское государство. Перспектива того, что они могут тайно что-то сделать и за пределами своих границ, вызывает тревогу", – заявил в интервью агентству республиканец Майк Галлахер (Mike Gallagher), входящий в Комитет Палаты представителей США по вооруженным силам (U.S. House Committee on Armed Services).

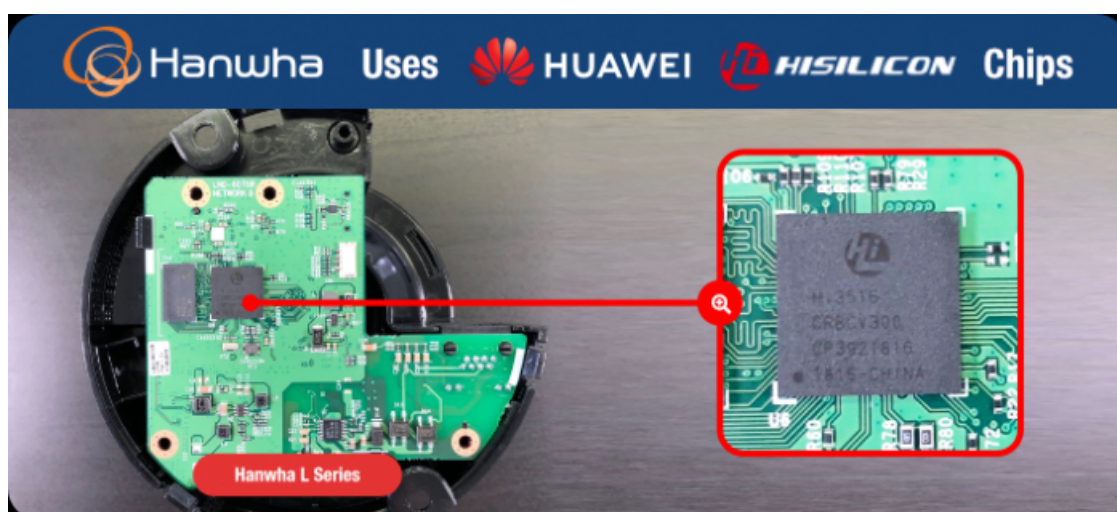
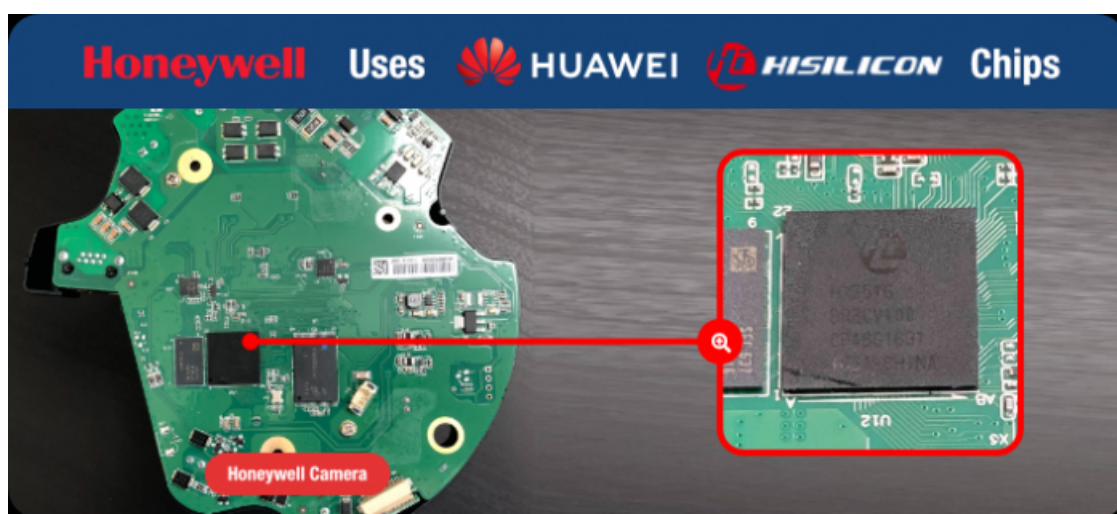
Сама Huawei неоднократно отрицала свою связь с правительством КНР и то, что ее оборудование может служить для шпионажа. Нет никаких свидетельств того, что камеры с чипами HiSilicon использовались таким образом, отмечает Bloomberg. Тем не менее, журналисты напомнили о мощной DDoS-атаке на DNS-провайдера Dyn, которую хакеры устроили в октябре 2016 года с помощью ботнета Mirai и миллионов втянутых в него IP-камер производства китайской компании Hangzhou Xiongmai Technology.

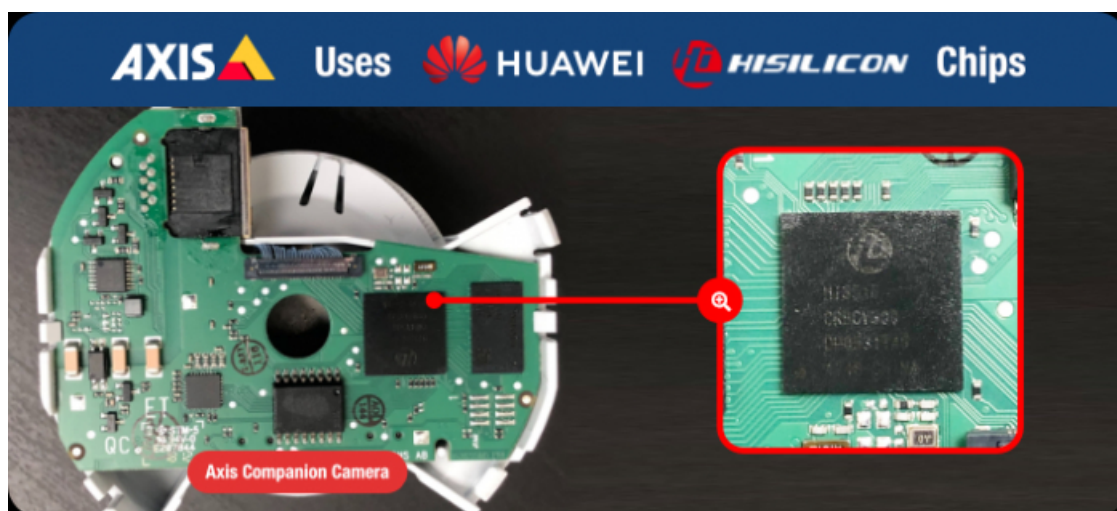
"Впрочем, уязвимостей, подобных тем, что допустили в Xiongmai, в продукции HiSilicon до сих пор не обнаружено", - пишут авторы статьи Марк Берген (Mark Bergen) и Блейк Шмидт (Blake Schmidt) со ссылкой на отраслевых инсайдеров.

Ранее на присутствие микросхем HiSilicon в десятках миллионов IoT-устройств, выпускаемых западными брендами, обратил внимание отраслевой портал IPVM, основанный Джоном Хоновичем (John Honovich), одним из авторитетных специалистов в области IP-видеонаблюдения в США.

"Из-за крайне низкой стоимости чипы HiSilicon более всего распространены в недорогих IoT-устройствах...Для профессиональных IP-камер с ценой менее 200 долларов наличие компонентов HiSilicon - это норма", - [сообщает](#) издание.

По данным портала, компоненты HiSilicon используются такими компаниями, как Hanwha, Honeywell, Panasonic и Axis. Bloomberg отмечает, что камеры с чипами HiSilicon в большом ассортименте представлены в интернет-магазине Amazon.com.





В интервью IPVM аналитик Австралийского института стратегической политики (Australian Strategic Policy Institute) Том Урен (Tom Uren) заявил, что широкое присутствие чипов HiSilicon в IoT-устройствах может представлять риск для кибербезопасности.

"Чипы китайского производства, безусловно, могут использоваться для создания уязвимостей в устройствах, которыми они укомплектованы", - считает специалист. Впрочем, он добавил, что китайским разведслужбам вряд ли имеет смысл прибегать к масштабной компрометации IP-камер на аппаратном уровне, поскольку IoT-устройства без труда взламываются с помощью программных эксплойтов. Скорее, спецслужбы КНР просто пользуются недостаточным уровнем защиты в IoT-сфере, нежели специально что-то разрабатывают и встраивают для шпионажа, полагает Том Урен.

В США уже принимаются меры по ограничению присутствия HiSilicon на американском рынке. В августе 2018 года президент Дональд Трамп подписал Закон о национальной обороне США (National Defense Authorization Act - NDAA), который запретил Пентагону и другим правительственным организациям, а также работающим с ними подрядчикам, пользоваться оборудованием и услугами китайских вендоров, представляющих угрозу национальной безопасности страны. К таковым Вашингтон, прежде всего, причисляют Huawei и ZTE, но конгрессмен Майк Галлахер заявил Bloomberg, что закон однозначно распространяется и на продукцию HiSilicon, поскольку эта компания - стопроцентная дочерняя структура Huawei. В документе также упомянуты китайские производители камер видеонаблюдения Zhejiang Dahua Technology Co. и Hangzhou Hikvision Digital Technology Co., с которыми госструктуры США тоже не могут работать.

Стоит добавить, что тема шпионских чипов поднимается в СМИ уже не в первый раз. В октябре 2018 года журнал Bloomberg BusinessWeek [написал](#), что спецслужбы КНР через китайских подрядчиков могли внедрять в материнские платы Supermicro сторонние микросхемы для слежки за американскими вендорами.

The Big Hack



How China used
a tiny chip to
infiltrate America's
top companies

Supermicro, акции которой рухнули более чем на 40 процентов после скандальной публикации, категорически отвергла обвинения в свой адрес, назвав их немыслимыми и несоответствующими действительности. Amazon и Apple, также фигурирующие в нашумевшей статье, потребовали отозвать ее, а гендиректор Apple Тим Кук (Tim Cook) даже назвал материал "стопроцентной ложью".

Представители министерства национальной безопасности США, АНБ и британского центра национальной кибербезопасности высказывали сомнения по поводу информации Bloomberg, либо заявляли, что у них нет причин не верить опровержениям компаний.

Тем не менее, даже после того, как Supermicro [сообщила](#) о результатах независимой экспертизы, которая не выявила шпионских "закладок" в материнских платах вендора, никаких опровержений со стороны Bloomberg не последовало.

С остальными материалами по теме вы можете ознакомиться здесь:

- [Кто следующий за ZTE?](#)
- [Facebook прекратит передачу данных пользователей компании Huawei](#)
- [Huawei: "Невиноватая я!"](#)
- [Австралия будет строить 5G без Huawei](#)
- [Huawei и ZTE не пригласили участвовать в 5G-проектах Индии](#)
- [Ericsson зарится на клиентов Huawei в США](#)
- [США призвали союзников отказаться от Huawei](#)
- [Кто выиграет от проблем у Huawei?](#)
- [ВТ избавляется от оборудования Huawei в своих опорных сетях](#)
- [Финдиректора Huawei арестовали в Канаде по запросу США](#)
- [Все больше стран отворачиваются от Huawei](#)
- [Huawei - заложница борьбы США и Китая за лидерство в 5G?](#)
- [Чем грозит Huawei шпионский скандал в Польше](#)
- [Huawei - это вам не ZTE!](#)

- [США обвиняют Huawei в попытке кражи технологий T-Mobile](#)