Бэкдоры АНБ: дело ясное, что дело темное

В Агентстве Национальной безопасности США наотрез отказываются раскрывать информацию относительно новых деталей спорной практики ведомства по внедрению в технологических продуктах так называемых ″бэкдоров″ - скрытых лазеек, которые открывают спецслужбам доступ к оборудованию и позволяют сканировать передаваемый трафик без каких-либо судебных постановлений. По данным Рейтер, вывести АНБ ″на чистую воду″ стремится сенатор-демократ Рон Уайден (Ron Wyden), который резко критикует неоднозначные методы спецслужб, настаивая, что они вредят развитию промышленности и национальной безопасности США.



О том, что АНБ склоняет технологические компании к сотрудничеству и добивается внедрения бэкдоров, мир доподлинно узнал из документов, раскрытых бывшим подрядчиком АНБ Эдвардом Сноуденом. Выдержки из них в 2013 году опубликовали Рейтер и другие СМИ. Те, кто считает подобные действия спецслужб оправданными, утверждают, что они облегчили сбор важных разведданных в зарубежных странах, в том числе - перехват сообщений террористов.

После скандальной утечки, организованной Сноуденом, в АНБ разработали новые правила спорной практики, чтобы снизить риски разоблачения и компрометации. Об этом Рейтер рассказали трое экс-сотрудников разведслужб, имена которых, само собой, не называются. Собеседники утверждают, что согласно новым требованиям АНБ, перед тем, как внедрять бэкдор, в агентстве должны оценить возможные последствия и предусмотреть какой-то способ предупреждения на случай, если секретная ″закладка″ раскрыта и используется противоположной стороной.

В АНБ отказались говорить, как именно была скорректирована политика агентства по внедрению лазеек для доступа спецслужб к оборудованию. Представители ведомства лишь заявили, что в АНБ стараются восстановить доверие частного бизнеса с помощью таких мер, как оповещение о выявляемых в ПО уязвимостях.

В беседе с журналистами помощники сенатора Уайдена, ведущего представителя Демпартии в комитете по разведке Сената США (Senate Intelligence Committee), выразили обеспокоенность из-за того, что АНБ упорно молчит о внесенных в правила поправках и не раскрывает даже их общей сути.

> ″Скрытые лазейки в шифровании - это угроза национальной безопасности и безопасности наших семей. Это лишь вопрос времени, когда зарубежные хакеры или преступники воспользуются ими для подрыва американской национальной безопасности. Правительство не должно никаким образом участвовать во внедрении секретных бэкдоров в технологии шифрования, используемые американцами″, - сказал сенатор в интервью Рейтер.



Сенатор Рон Уайден

Критики методов АНБ предупреждают, что спецслужбы создают мишени для потенциальных атак со стороны противников, подрывают доверие к американских технологиям и дискредитируют доводы об опасности китайского оборудования из-за угрозы шпионажа, с помощью которых Вашингтон убеждает союзников отказаться от технологий КНР. Чем лучше тогда США, если американская аппаратура может использоваться для этих же целей?

Компании Juniper Networks, которая в 2015 году сообщила о компрометации своего оборудования, известен как минимум один пример, когда зарубежный противник сумел воспользоваться бэкдором, созданным американскими спецслужбами. В распоряжении у Рейтер оказался ранее не освещавшийся в прессе отчет Juniper перед членами Конгресса. В нем компания признается, что власти некоего иностранного государства воспользовались разработанным в АНБ механизмом.

В 2018 году АНБ сообщило сотрудникам сенатора Уайдена, что в ведомстве был подготовлен отчет об извлеченных уроках после инцидента с Juniper, но теперь в АНБ заявляют, что не могут отыскать этот документ, рассказал в беседе с Рейтер пресс-секретарь Уайдена Кейт Чу.

Судя по публикациям о разоблачениях Сноудена, для внедрения бэкдоров в АНБ в одних случаях заключали коммерческие сделки с компаниями, принуждая к сотрудничеству со спецслужбами, а в других - использовали маневры со стандартами безопасности и вводили такие процедуры, в результате которых фирмы сами того не зная устанавливали ПО с ″закладками″, позволяющими АНБ проникнуть в систему.



Технологические компании, позднее уличенные в подобных сделках, лишились доверия и клиентов. Некоторые фирмы потеряли бизнес за рубежом, поскольку клиенты стали опасаться длинных рук американских спецслужб.

Громкие скандалы побудили задуматься о пересмотре политики. По словам бывшего координатора Белого дома по вопросам кибербезопасности Майкла Дэниела, который консультировал тогдашнего президента США Барака Обаму после ″слива″ информации Сноуденом, из произошедшего были извлечены уроки.

Назначенная президентом США специальная комиссия заявила, что правительство никогда не должно ослаблять киберзащиту технологических продуктов или компрометировать стандарты безопасности. Однако публичного одобрения рекомендаций со стороны Белого дома не последовало. По словам Дэниела и других источников Рейтер, вместо этого в правительстве США усилили надзор за порядком рассмотрения вопроса о том, следует ли использовать выявленные недочеты в ПО для наступательных кибероперациий или необходимо исправить их для повышения киберзащиты.

Секретные правительственные контракты на внедрение бэкдоров и вовсе остались за рамками официального рассмотрения. Один из юристов из среды разведсообщества рассказал Рейтер, что у АНБ были контракты с компаниями по всему миру, но информация о них строго охраняется.

То, какие риски создают практикуемые спецслужбами США методы, ярко иллюстрирует нашумевшая история с компонентом системы шифрования Dual Elliptic Curve. Разработанный АНБ генератор случайных чисел Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) считался криптографически стойким, и агентство, работая с Министерством торговли США, продвигало его в качестве международного стандарта. Однако позднее специалисты по криптографии показали, что АНБ с помощью Dual EC могло получать доступ к зашифрованным данным.



В декабре 2013 году из документов, переданных Сноуденом, выяснилось, компания RSA Security получила от АНБ 10 миллионов долларов за использование алгоритма Dual EC в криптобиблиотеке BSAFE в качестве основного генератора псевдослучайных чисел. В попытке оправдаться в RSA публично заверяли, что намеренно никогда не стали бы внедрять бэкдор. Однако репутация компании была испорчена, и в 2016 году RSA Security продали.

Неприятности из-за Dual EC приключились и в Juniper Networks. В 2015 году американский производитель сетевого оборудования сообщил о выявленном вредоносном коде в программном обеспечении некоторых из своих брандмауэров. Позже эксперты по информационной безопасности (ИБ) выяснили, что хакеры внесли изменения в версию Dual EC от Juniper и превратили брандмауэры в собственный шпионский инструмент.

В Juniper неохотно распространяются о случившемся. В 2016 году компания призналась ИБ-эксперту Энди Айзексону, что Dual EC была установлена по требованию заказчика. Айзексон и его коллеги из ИБ-сообщества полагают, что этим заказчиком было правительственное агентство США, поскольку только США настаивали на установке Dual EC.

В Juniper не комментируют эту информацию, как и то, с кем связаны хакеры, которые воспользовались ″закладками″ в брандмауэре. Собеседники Рейтер, осведомленные об этом деле, утверждают, что следствие пришло к выводу о причастности КНР. Источники отказались говорить о доказательствах, на основании которых было сделано заключение. В тоже время китайская сторона отрицает свою причастность к хакерским атакам, а в МИД КНР указывают на то, что АНБ стоит за созданием технологии бэкдоров.



В АНБ и Juniper отказались от комментариев к статье Рейтер. Уайден же полон решимости разобраться с произошедшим в Juniper и выяснить, как изменилась ситуация с тех пор, как стали накаляться страсти вокруг шифрования, отмечают журналисты.

Со слов бывшего высокопоставленного сотрудника АНБ, многие технологические компании по-прежнему опасаются тайно работать на правительство, но спецслужбы продолжают склонять фирмы к сотрудничеству, поскольку возможность скрытного доступа слишком ценна, чтобы от нее отказываться.

После таких откровений, вопрос о наличии и возможности использования спецслужбами бэкдоров в оборудовании крупных китайских брендов, например Huawei, даже и ставить-то неудобно. Незримая война разведок идёт постоянно, а это значит, что крупные коммерческие интересы или вопросы, затрагивающие военно-политическую сторону жизни любой страны, могут оказаться под постоянным тайным контролем заинтересованного "соседа".