FORVM GEOPOLITICA
Independent Commentary on a Fractured World

Шифрование и кибербезопасность

Россия, Китай и Северная Корея не попали в ловушку, расставленную США - в отличие от 120 других стран! И будьте внимательны: Шифрование небезопасно, а кибербезопасность - это миф!

Феликс Абт

сбт 28 окт 2023

Краткое вступление от Питера Хензелера

Мы рады представить вам еще одну очень интересную статью Феликса Абта. Феликс Абт - автор блога easternangle.com.

Введение

В швейцарской компании Crypto AG, которая, по мнению журнала The Economist "после Второй мировой войны заняла доминирующее положение на мировом рынке шифровальных устройств" и в течение десятилетий была ведущим производителем шифровального оборудования для голосовой связи и цифровых сетей передачи данных, Ганс Бюлер был главным менеджером по продажам, на долю которого приходилось около 40% всего объема продаж компании.

Опасный поворот в карьере суперуспешного бизнесмена: кто и что за ним стоит?

Он поставлял шифровальное оборудование многим странам, по большей части ближневосточным, в том числе и Ирану. Во время своего 25-го визита в Тегеран 18 марта 1992 г. его задержали и заключили в тюрьму. Девять месяцев он провел в одиночной камере тегеранской тюрьмы "Эвин", где его допрашивали по пять часов в день.

Иран обвинил Бюлера в передаче ключей шифрования западным разведкам. Бюлер был освобожден в январе 1993 года, поскольку компания Crypto AG внесла залог в размере 1 млн. долл. Ирану, хотя он ничего не знал о каких-либо проблемах с оборудованием. Вскоре после освобождения Бюлера компания уволила его и стала сама его преследовать, чтобы вернуть деньги в размере 1 млн. долл., внесенные в качестве залога.

CIA controlled global encryption company for decades, says report

Swiss government orders inquiry after revelations Crypto AG was owned and operated by US and German intelligence

'It was the intelligence coup of the century,' the CIA report concluded. Photograph: Saul Loeb/AFP/Getty Images

"Это был настоящий переворот века в разведке", - пишет британская газета Guardian. Скриншот заголовка из газеты The Guardian, 11 февраля 2020 г.

"Несколько лет спустя я познакомился с Гансом Бюлером, высоким, стройным человеком, который уверенно и спокойно говорил: "До ареста в Тегеране я верил в порядочность своей компании. Но иранцы знали то, чего не знал я. Очевидно, они узнали, что секретные данные, которые, как они считали, находятся в безопасности на криптоустройствах, отправляются во враждебные им страны. И, вероятно, уже тогда они знали, что западные правительственные агентства завладели компанией, чтобы использовать ее в качестве инструмента шпионажа против них".

Ханс Бюлер отвечает на вопросы журналистов после освобождения из Ирана. Изображение: *Handelszeitung*, Цюрих

Тотальный обман: бизнес-модель компании, контролируемой ЦРУ

Компания Бюлера делает себе имя и обеспечивает безопасность своих клиентов, прикрываясь нейтралитетом своей страны, и 120 государств, включая Ватикан, приобрели у нее самые передовые и якобы самые надежные технологии шифрования. Поскольку многие страны по понятным причинам с опаской относились к криптографическому оборудованию, продаваемому в странах НАТО, они прибегали к услугам нейтральной третьей стороны - Швейцарии. Некоторые страны, такие как Китай, Россия и Северная Корея, продолжали опасаться приобретения "троянского коня" на Западе и предпочли создать собственную технологию шифрования. Их подозрения были обоснованы тем, что эти гаджеты действительно использовались для подслушивания доверчивых пользователей. Так, например, газета Washington Post и немецкая государственная телекомпания ZDF сообщили, что "американская разведка на протяжении десятилетий активно отслеживала дипломатическую и военную переписку многих латиноамериканских стран с помощью шифровальных машин, поставляемых швейцарской компанией, которая тайно принадлежала ЦРУ и немецкой разведке".

Ганс рассказал мне, что сам верил в то, что это были честные сделки, и он заверял своих клиентов, что их сообщения будут в полной безопасности, при передаче из столиц в посольства, военным атташе, в торговые представительства и точки шпионажа по всему миру и обратно. Он сам и его клиенты были шокированы, узнав, что это не так!

Из минувшей эпохи, когда СМИ еще умели проводить расследования и критически освещали события

После освобождения Ганса Бюлера из тюрьмы журналисты продолжили расследование его дела и беседовали с ним. Сообщения стали появляться в немецких журналах типа Der Spiegel, на Международном радио Германии, на Швейцарском телевидении и во всех основных швейцарских газетах. Журналисты пытались выяснить информацию о том, не вмешивались ли западные спецслужбы в работу оборудования Crypto AG, и если да, то каким образом. Они беседовали с другими сотрудниками Crypto AG и продолжали все больше и больше погружаться в детали. Чтобы положить конец этой истории и заставить Ханса Бюлера и других сотрудников замолчать, компания Crypto AG подала ответный иск. Однако помешать средствам массовой информации узнать о происходящем в то время было невозможно. Они продолжали выяснять обстоятельства дела: Выяснилось, что в Crypto AG часто наведывались агенты АНБ - американского агентства по слежке. Например, криптограф АНБ Нора Л. Маккеби в августе 1975 года посетила секретный семинар в Crypto AG, чтобы представить новый прототип шифровального устройства. Она была указана как независимый "консультант", чтобы скрыть свою истинную роль участника от имени АНБ.

Кроме того, убедительным доказательством тайного соглашения между Crypto AG и АНБ с 1951 года стали засекреченные ранее документы, которые были частично раскрыты АНБ в 2014 году. Нет сомнений в том, что ЦРУ и БНД, немецкая разведслужба, давно сотрудничающая с правительством США, договорились о покупке Crypto в 1970 году. Однако, опасаясь разоблачения, БНД продала США свою долю в компании в начале 1990-х годов. По данным The Washington Post, ЦРУ использовало этот бизнес вплоть до 2018 года, после чего его активы были проданы двум частным фирмам.

А теперь сравните это с тем, как те же самые СМИ недавно отнеслись к самому серьезному теракту в Европе со времен Второй мировой войны - взрыву на газопроводе Nordstream, и даже не провели расследования: Наверняка сегодня они проявили бы ту же самую халатность и равнодушие в отношении Бюлера, если бы он был жив и вернулся из иранской тюрьмы сейчас.

Самая масштабная в мире программа промышленного шпионажа

В течение десятилетий США регулярно перехватывали и расшифровывали сверхсекретные шифрованные сообщения 120 стран. С помощью ключа шифровальщики БНД и АНБ могли расшифровать любое сообщение, отправленное одним из 120 клиентов Crypto AG. Аналитики АНБ могли проанализировать поток сообщений с той же легкостью как прочитать утреннюю газету. Кроме того, чтобы ничего не ускользнуло от их глаз и ушей, ЦРУ провело тщательную проверку Omnisec, главного конкурента Crypto AG, еще одного швейцарского предприятия.

Попавшие в Иран файлы "Штази" (службы государственной безопасности) из бывшей Восточной Германии, скорее всего, предоставили иранцам информацию о взломе американских шифровальных систем.

Информация, украденная у ничего не подозревающих друзей и врагов, систематически используется против них

Согласно опубликованным материалам, во время Фолклендской войны США использовали в своих интересах зависимость Аргентины от шифровальной технологии Crypto AG, передавая союзной Великобритании перехваченные разговоры о военных планах Аргентины. Нарушение аргентинских дипломатических правил публично признал бывший министр иностранных дел Великобритании Тед Роулендс.

Кроме того, США могли отслеживать все переговоры президента Египта Садата с Каиром во время его встречи с премьер-министром Израиля Бегином и президентом США Картером в Кэмп-Дэвиде в 1978 году по поводу заключения мирного договора между Египтом и Израилем.

США также неоднократно требовали закупки определенного оборудования в качестве условия получения льгот. Пакистан получал от США военные кредиты в обмен на покупку у компании Crypto AG своих технологий шифрования.

В течение 50 лет США и их союзники пользовались перехваченными сообщениями, касающимися торговли, дипломатии, экономики и стратегии. Они получили возможность влиять на международные договоры и переговоры, узнавая "итоговые" переговорные позиции иностранных правительств - как "друзей", так и "врагов". Например, им становится известно точное состояние здоровья короля Саудовской Аравии, тайные финансовые операции президента Аргентины,

переговорная позиция торговой делегации ЮАР во Всемирной торговой организации, отношение президента Южной Кореи к присутствию американских войск в своей стране или позиция Папы Римского по вопросу борьбы с абортами. Такая информация, ежедневно предоставляемая президенту и госсекретарю в ходе брифингов, очень удобна и позволяет США играть в дипломатический покер с высокими ставками, держа зеркало за спиной у всех остальных.

Крупнейшее в мире государство слежки отвлекает внимание от себя, указывая пальцем на Китай

Парадоксально, но правительство США и его партнеры в основных СМИ часто делают вид, что возмущены слежкой в Китае, хотя США построили самое всеобъемлющее и глобальное государство слежки, не имеющее себе равных в Китае, который якобы все еще использует воздушные шары-шпионы. Один из китайских инсайдеров даже задает вполне закономерный вопрос: "В Западных страшилках раздувают из мухи слона о якобы существующей в Китае системе социального кредита или social credit score, но существует ли она вообще?" Правительство США шпионит за людьми по всему миру, включая глав государств, которых оно называет "союзниками" и "друзьями", а также за своими собственными гражданами. Даже если ваш мобильный телефон выключен, они знают, когда вы ночью пукаете в постели, независимо от того, в какой постели и где.

Лгать, обманывать, воровать: методы работы самого могущественного правительства в мире

В 2018 году, когда Ханс Бюлер скончался, ЦРУ потеряло интерес к Crypto AG после того, как выяснилось, что это был тайный проект ЦРУ. Однако, безусловно, ЦРУ по-прежнему заинтересовано в целенаправленной деградации технологий шифрования, чтобы использовать их для шпионажа за своими пользователями. И оно, несомненно, будет придерживаться принципов, которые повторил бывший глава ЦРУ Майк Помпео: "Мы лгали, мы обманывали, мы крали!". Для этого оно, скорее всего, получит доступ к ряду других предприятий.

Насколько легко проникнуть в ваши устройства?

Конечное шифрование, используемое в таких приложениях, как Zoom, Signal, Telegram и WhatsApp, невозможно обойти, если нет доступа к содержимому передачи или ключей или шифров. Это можно сделать только путем взлома. Однако конечные устройства (смартфон, ПК или другое устройство) являются самым

слабым звеном в цепи, поскольку они почти не защищены и их можно взломать бесконечным числом способов. Об этом следует помнить пользователям программного обеспечения, претендующего на обеспечение безопасности сквозной передачи данных. И даже если шифрование не позволяет прочитать содержимое сообщений, метаданные не скрываются и не шифруются, а значит, можно определить, кому вы отправили сообщения, и, возможно, догадаться об их содержании. Даже если вы идеально защитите все свои устройства и будете уверены, что никто не имеет доступа к сообщениям, нельзя быть уверенным, что устройство вашего собеседника не взломано. С него также может быть отправлено вредоносное ПО. Сквозное шифрование здесь не поможет.

Что касается наиболее крупного и самого серьезного объекта правительственной слежки, то АНБ использовало свои суперкомпьютеры для взлома гораздо более сложных алгоритмов шифрования и дешифровки систем на захваченном оборудовании и/или в сообщениях иностранных спецслужб. При таких возможностях, вероятно, нет ничего, что АНБ не смогло бы взломать, и оно это сделает, если захочет. В том числе, оно может легко расшифровать сообщения iPhone, не получая ключи от Apple.

ТЕГИ СТАТЬИ:

Анализ Бюлер, Ганс Китай Северная Корея Россия Швейцария США Crypto AG Помпео, Майкл Der Spiegel Центральное разведывательное управление (ЦРУ) НАТО The Washington Post Агентство национальной безопасности (АНБ)