Пробел в швейцарской системе кибербезопасности? | Une faille dans le système de cybersécurité suisse?

Автор: Заррина Салимова, Берн , 13.05.2024.

Фото: Philipp Katzenberger, Unsplash

Как выяснили журналисты телеканала RSI, федеральные управления полиции (Fedpol) и вооружений (Armasuisse) используют российское программное обеспечение для подбора и расшифровки паролей на мобильных телефонах и компьютерах.

|

Selon une enquête de RSI, Fedpol et Armasuisse utilisent un logiciel russe pour décrypter des téléphones portables et des ordinateurs.

Une faille dans le système de cybersécurité suisse?

Тот факт, что власти многих стран, в том числе и Швейцарии, прибегают к техническим уловкам, чтобы при необходимости взломать чьи-то электронные устройства, давно известен и удивления не вызывает. На фоне идущей войны в Украине, дебатов о нейтралитете, кибератак на швейцарскую инфраструктуру со стороны России и непрекращающихся новостей о шпионаже удивительно другое: швейцарские федеральные ведомства для достижения этих целей пользуются российскими программами.

Согласно расследованию телеканала Итальянской Швейцарии RSI, российская система для расшифровки телефонов и компьютеров применяется специалистами Fedpol и Armasuisse. Речь идет о программном обеспечении компании Elcomsoft, продукцией которой обычно пользуются судебные эксперты, следственные органы и частные фирмы. Основанное в 1990-х годах предприятие предлагает широкий спектр услуг – от решений для извлечения данных до инструментов для мобильной криминалистики.

На открывающемся из Швейцарии сайте указано, что компания базируется в Праге. С помощью web.archive.org журналисты RSI обнаружили, что еще в ноябре 2021 года на сайте была другая информация: штаб-квартира находилась в Москве. Однако этот адрес и данные о российской юрисдикции были удалены со страницы после начала войны. Значит ли это, что компания «релоцировалась»? Не совсем. В Москве Elcomsoft работает по сей день, о чем свидетельствуют данные российского торгового реестра. Сотрудники, программисты и генеральный директор Elcomsoft, найденные журналистами на платформе LinkedIn, также живут в России.

На сайте Elcomsoft говорится, что ее инструментами пользуются большинство компаний из списка Fortune 500, военные подразделения, иностранные правительства и все крупные бухгалтерские фирмы. А также, как оказалось, швейцарские федеральные ведомства. Представители Armasuisse ответили на вопросы RSI по электронной почте, объяснив, что ведомство действительно приобрело программное обеспечение у Elcomsoft для тестовых целей. Однако федеральное управление вооружений не уточнило, о каких тестах идет речь и как используется продукт. Что касается Fedpol, то федеральное управление полиции сначала отказалось отвечать из соображений безопасности. Однако после ряда запросов RSI и на основании Закона о прозрачности ведомство подтвердило, что в 2024 году оно приобрело лицензии на четыре продукта у Elcomsoft, причем эти продукты используются исключительно офлайн (т. е. без подключения к сети).

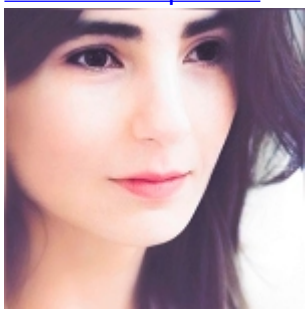
Такая ситуация не вызывает восторга у специалистов. Эксперт по технологиям Себастьен Фанти, до недавнего времени ответственный за защиту данных в кантоне Вале, считает, что использование этого программного обеспечения пробуждает серьезные сомнения в национальной кибербезопасности. «Эта компания подчиняется российскому законодательству. Это означает, что власти и спецслужбы в Москве потенциально имеют доступ к работе с использованием этого программного обеспечения», - отметил он в комментарии RSI. По его словам, ничто не гарантирует отсутствие «черных ходов» – своеобразных «секретных дверей», которые часто устанавливаются по умолчанию, например, в целях технического обслуживания. Его не успокаивает и тот факт, что программа используется Fedpol в автономном режиме, ведь «достаточно, чтобы программное обеспечение в какой-то момент вошло в контакт с любой сетью, чтобы кто-то смог получить доступ и извлечь все данные». По мнению специалиста, выбор должен быть сделан в пользу надежного партнера, который работает в стране с демократическими правилами и

верховенством закона, а «с Россией дело обстоит иначе». Для Себастьяна Фанти подобное программное обеспечение для слежки сравнимо с оружием, и «относиться к нему следует именно так».

Применение этого программного обеспечения поднимает вопросы и в парламенте. Представитель «зеленых» Герхард Андрей, входящий в комиссию по политике безопасности и сам являющийся ИТ-специалистом, видит проблему в том, что Швейцария слишком зависит от иностранных инструментов и компаний, базирующихся «в проблемных для нас странах, таких как Россия или Китай». По мнению парламентария, тот факт, что программа используется в автономном режиме, не является синонимом полной безопасности, ведь существуют обновления.

Тем временем многие швейцарские компании продолжают продавать свою продукцию в России. По информации RTS, доходы швейцарских транснациональных корпораций почти такие же высокие, как и до начала войны. По предварительным данным, в 2023 году Швейцария экспортировала в Россию товаров на сумму более 2,6 млрд франков, в основном фармацевтической продукции (2,1 млрд франков), поскольку лекарства и фармацевтические товары исключены из санкций по гуманитарным соображениям. Данные не включают в себя товары, производимые швейцарскими компаниями в России. Эта деятельность нередко подвергается критике по этическим соображениям, так как она подразумевает уплату налогов, что является косвенной финансовой поддержкой действий Кремля. Тем не менее, не нарушающий санкций бизнес не запрещен и остается легальным: в настоящее время только военные товары, товары двойного назначения и предметы роскоши (с закупочной ценой более 300 франков) запрещены к экспорту в Россию.

кибербезопасность
кибератаки швейцария
война в Украине



Заррина Салимова
Zaryna Salimava
