Исследование распространённости Russian Trusted CA и самоподписанных SSL-сертификатов в российском Интернете

Постоянная ссылка на исследование

Введение

В данном отчете рассматриваются вопросы информационной безопасности и использования цифровых сертификатов в российском сегменте Интернета. Анализируется распространённость корневых сертификатов Министерства Цифрового Развития, Связи и Массовых Коммуникаций, а так же распространённость самоподписанных SSL-сертификатов, связанных с Россией. SSL-сертификаты играют важнейшую роль в обеспечении безопасности интернет-коммуникаций. Это исследование проливает свет на их использование в российском киберпространстве.

Примечание: Информация в GitHub репозитории регулярно обновляется с целью предоставления актуальной статистики использования корневых и самоподписанных сертификатов.

Роль Russian Trusted CA

Санкции и центры сертификации

Одной из основных причин использования российского корневого сертификата являются санкции, введенные против российских компаний после 24 февраля 2022 года (такая причина декларируется российским правительством во всяком случае). Санкции заставили многие международные компании отказаться от финансовых операций с российскими партнерами, чтобы избежать расследований, связанных с неисполнением санкций. Даже некоторые удостоверяющие центры, которые выдают SSL-сертификаты для веб-сайтов, воздерживаются от сотрудничества с российскими компаниями из-за них.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

В результате, некоторые сайты прибегают к использованию сертификатов, выданных Министерством связи и массовых коммуникаций Российском Федерации. Однако, важно отметить, что эти сертификаты помечаются как небезопасные во всех современных браузерах, за некоторым исключением. Например, в "Яндекс.Браузере" и некоторых

собственных сборках Chromium Browser, используемых в государственных учреждениях. Кроме того, следует отметить, что анализ исходного кода Яндекс.Браузера показывает, что применение российского корневого сертификата в настоящее время возможно только на сайтах из специального списка [источник]. Попытка применить сертификат к другим доменам приведет к стандартной ошибке и недоступности сайта для пользователя.

Описание набора данных

Это исследование основано на обширной базе, включающей 21 698 сайт. Эта база служит основой для изучения особенностей использования цифровых сертификатов среди различных категорий сайтов.

Пояснение: Что такое SSL-сертификат?

Прежде чем мы продолжим, необходимо пояснить, что такое SSL-сертификат. Сертификат Secure Sockets Layer (SSL) – это цифровой сертификат, удостоверяющий подлинность веб-сайта и шифрующий данные, отправляемые на сервер. Проще говоря, он обеспечивает конфиденциальность и безопасность информации, передаваемой между браузером пользователя и веб-сайтом.

Сайты, связанные с правительством

Мы выявили 715 сайтов, связанных с государственным сектором, для которых требуется установка корневого сертификата, а так же 249 сайтов, использующих самоподписанные SSL-сертификаты, связанные с Россией. Эти данные свидетельствуют о значительном присутствии таких сертификатов в государственном секторе.

Социально значимые сайты

Мы также рассмотрели социально значимые сайты. В этой категории 7 ресурсов требуют наличие корневого сертификата, при этом, ни один из них не использует самоподписанный SSL-сертификат, выпущенный в России.

Примечание:

- К *сайтам, связанным с правительством*, относятся официальные сайты министерств, регионов и т.д. То есть сайты, имеющие прямое или косвенное отношение к правительству. Список таких сайтов можно найти тут.
- *Социально значимые сайты* это сайты, к которым операторы связи по закону обязаны предоставлять свободный доступ [источник]. Такие сайты считаются критически важными для доступа всех граждан, и включают в себя российские социальные сети, банки, государственные порталы и т.д.

Важно отметить, что в эти категории, а особенно в *Социально значимые сайты*, входят крайне популярные платформы, такие как Сбербанк (самый популярный банк в России) и ГосУслуги – портал, обеспечивающий доступ к государственным сервисам и услугам. Следовательно, требование использования российского корневого сертификата для этих сайтов может заставить большое количество людей установить такой сертификат на своё основное устройство.

Топ-100 сайтов в России

В ходе исследования были рассмотрены 100 самых популярных сайтов в России. Среди них только один сайт требует наличие российский корневого сертификата, и ни один из ресурсов не использует самоподписанный SSL-сертификат. Но этот единственный сайт – Сбербанк. И это очень популярный банк. Но в целом, полученные данные показывают, что самые популярные сайты в России склонны использовать сертификаты, выпущенные международно признанными центрами сертификации.

Риски и проблемы безопасности

Использование российских сертификатов сопряжено с определенными рисками. Остается неясным, соответствуют ли эти сертификаты строгим стандартам, предъявляемым к доверенным центрам сертификации. Такая неопределенность вызывает опасения относительно надежности и безопасности сертификатов, выдаваемых российскими удостоверяющем центром.

Важно отметить, что криптография в России уже подвергалась критике, например отсутствие случайности в таблице перестановок [источник] и теоретическая возможность наличия "бэкдора" в S-Box [источник] в алгоритмах "Стриборг" и "Кузнечик".

Существует явное несоответствие в восприятии безопасности российскими браузерами и теми, которые используются за рубежом. Если российские браузеры могут принимать такие сертификаты, то большинство международных браузеров относятся к ним скептически. Такое расхождение в стандартах доверия может привести к непредвиденным последствиям для пользователей и организаций, полагающихся на такие сертификаты.

Возможные злоупотребления

Существуют также опасения, что российские центры сертификации могут выпускать дополнительные закрытые ключи для государственных структур, таких как Федеральная служба безопасности (ФСБ) и других спецслужб. См. инцидент MITM в Казахстане. Подобная практика может поставить под угрозу безопасность и конфиденциальность сетевых коммуникаций.

Последствия

Результаты нашего исследования свидетельствуют о сложном ландшафте цифровой безопасности в российском Интернете. Распространение российского корневого сертификата и самоподписанных SSL-сертификатов, связанных с Россией, создаёт значительные проблемы и риски, как для отдельных пользователей, так и для организаций.

Заключение

В заключение следует отметить, что проведённое исследование позволило получить ценные сведения об использовании корневых и самоподписанных сертификатов в российском Интернете. Несмотря на то, что эти сертификаты широко распространены в некоторых секторах, их использование сопряжено с проблемами безопасности и надежности. Для пользователей и организаций очень важно делать осознанный выбор при использовании Интернета, чтобы обеспечить свою цифровую безопасность и конфиденциальность. И последствия выходят за рамки технических; они затрагивают саму ткань гражданского общества и общества в целом, где неприкосновенность частной жизни и безопасность являются фундаментальными правами, которые должны быть защищены. Использование таких сертификатов может иметь непредвиденные последствия, учитывая неопределённость в отношении их соответствия международным стандартам и некоторые опасения по поводу возможного доступа государства к приватным ключам шифрования.