Опасная подмена: как новый троян захватывает банковские приложения

Мобильные банковские приложения стали привычным инструментом для управления финансами. Однако вместе с их популярностью растёт интерес киберпреступников, которые ищут новые способы получить доступ к счетам и личным данным пользователей.

Исследователи ThreatFabric обнаружили троян Hirudo, способный подменять настоящие банковские приложения вредоносными копиями. Об угрозе сообщило издание SecurityLab 16 октября 2026 года. Особенность этой схемы заключается в том, что поддельная программа может сохранять привычный интерфейс, поэтому пользователь не сразу замечает подмену.

Заражение начинается с установки приложения, которое выглядит безобидным: например, имитирует интернет-магазин или сервис коротких видео. Затем пользователю предлагают загрузить обновление, под видом которого на устройство попадает вредоносный компонент.

По данным исследователей, Hirudo способен удалить оригинальное банковское приложение и заменить его изменённой копией. Если человек вводит в ней логин, пароль или другие данные, эта информация может оказаться у злоумышленников.

Возможности трояна включают перехват SMS и уведомлений, фиксацию содержимого экрана и удалённое управление устройством. Это создаёт риск компрометации учётных данных и финансовой информации.

В ходе исследования специалисты обнаружили конфигурацию с 42 финансовыми приложениями и подготовленные вредоносные копии восьми банковских приложений. При этом речь шла о банках Индонезии. Данных, подтверждающих аналогичные атаки на российские банки, в этой публикации не приводится.

Как защитить свои данные

Опасность подобных программ заключается в том, что внешний вид приложения не всегда позволяет определить его подлинность. Поэтому пользователям важно обращать внимание на источник установки и любые необычные действия программы.

Чтобы снизить риск заражения, специалисты рекомендуют:

- устанавливать приложения только из официальных магазинов и проверять разработчика;
- не загружать обновления по подозрительным ссылкам и из неизвестных источников;
- внимательно оценивать запрашиваемые разрешения, особенно доступ к SMS, уведомлениям и управлению устройством;
- своевременно обновлять операционную систему и защитные средства;
- проверять уведомления о банковских операциях и незнакомых входах в аккаунт.

Если приложение неожиданно предлагает удалить банковский сервис, установить дополнительный файл или предоставить необычные разрешения, лучше прекратить установку и проверить информацию через официальный источник.

При подозрении на заражение не следует вводить банковские данные на подозрительном устройстве. Безопаснее связаться с банком по официальному номеру с другого доверенного устройства и уточнить дальнейшие действия.

История с Hirudo показывает, что киберугрозы могут маскироваться под привычные цифровые сервисы. Даже знакомый интерфейс не гарантирует безопасность: большое значение имеют источник установки, запрашиваемые разрешения и поведение приложения.

Ниязбекова Шакизада
кандидат экономических наук, доцент,
доцент Кафедры банковского дела и монетарного регулирования Финансового факультета,
Финансовый университет при Правительстве Российской Федерации

Гришаева Юлия Михайловна
доктор педагогических наук, профессор,
профессор Кафедры «Безопасность жизнедеятельности»,
Финансовый университет при Правительстве Российской Федерации

Бурделова Татьяна Николаевна
кандидат экономических наук, доцент,
доцент Кафедры общественных финансов Финансового факультета,
Финансовый университет при Правительстве Российской Федерации