ЧЕМ ОПАСЕН ТВОЙ СМАРТФОН?

Сейчас сложно представить себе человека, который не пользуется смартфоном. Все под рукой: карта, приложение оплаты, мессенджеры и почта. Но у любой медали две стороны.

Об опасностях, которые скрываются в наших смартфонах, рассказал эксперт департамента противодействия финансовому мошенничеству компании F6 Дмитрий ДУДКОВ.

В последнее время значительно растет интерес злоумышленников к мобильным устройствам на базе Android.

Согласно данным компании F6 об активности кибермошенников в сфере дистанционных банковских услуг (ДБУ) в Беларуси за последние 90 дней, мобильными устройствами на базе Android пользуются 48% клиентов белорусских банков, устройствами iOS – 23%, каналом web – 29%.

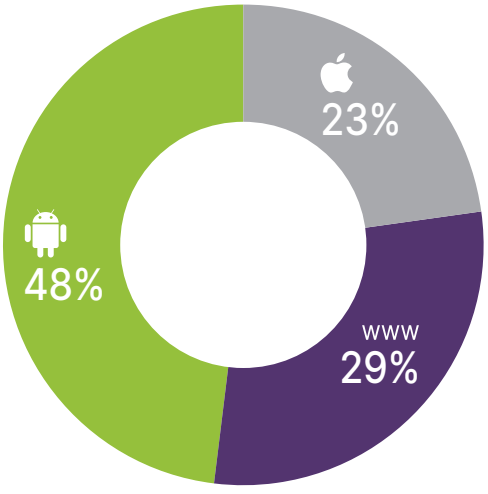
Инструменты распространения вредоносов через мобильные устройства Android:

- фишинговые ссылки из СМС, электронной почты, соцсетей;
- уязвимости в приложениях, которые позволяют получить удаленный доступ к устройствам и извлекать персональные данные;
- поддельные приложения (установка программ из непроверенных источников);
- социальная инженерия (побуждение установить вредоносные программы или открыть опасные файлы);
- пиратское программное обеспечение;
- мошенничество с инвестициями;
- файлы APK в Telegram-сообщениях якобы от знакомых;
- рекламные баннеры.

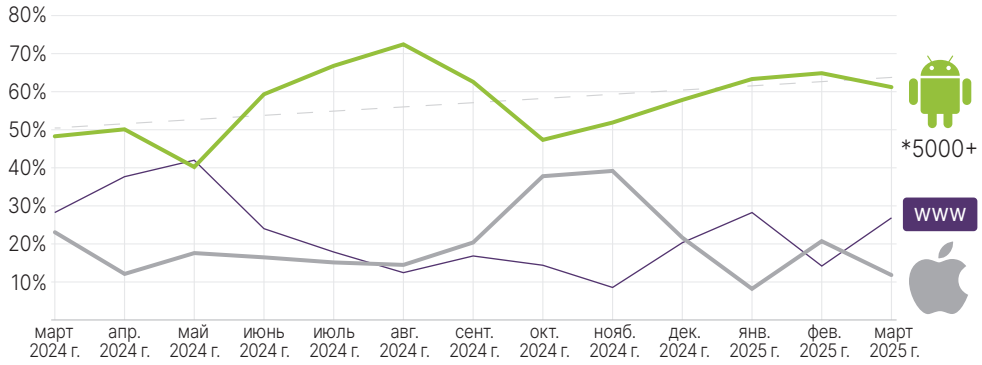
Злоумышленники создают поддельные приложения различных сервисов, в том числе государственных. Наиболее распространенные категории вредоносных программ: приложения оператора сотовой связи – 37,59%, приложения

АКТИВНОСТЬ ПОЛЬЗОВАТЕЛЕЙ В ЗАВИСИМОСТИ ОТ КАНАЛА ДОСТУПА К БАНКОВСКИМ УСЛУГАМ

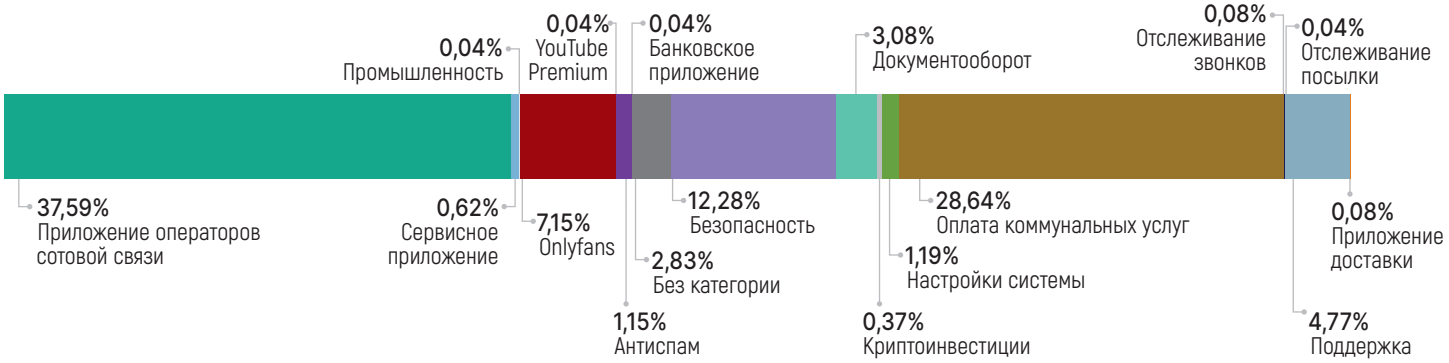
за январь–март 2025 года



АКТИВНОСТЬ КИБЕРПРЕСТУПНИКОВ В СФЕРЕ ДБУ
с марта 2024 года по март 2025 года
В ЗАВИСИМОСТИ ОТ КАНАЛА ДОСТУПА К БАНКОВСКИМ УСЛУГАМ



КАТЕГОРИИ ПРИЛОЖЕНИЙ, КОТОРЫЕ ПОДДЕЛЫВАЮТ КИБЕРМОШЕННИКИ



для оплаты коммунальных услуг – 28,64%, антивирусы – 12,28%.

Последствия атак на устройства Android могут быть весьма неприятными. Злоумышленник перехватывает логины и пароли, отслеживает и записывает звонки, удаленно полностью очищает устройство и так далее.

Слабые места кибермошенники, к сожалению, находят не только в устройствах. Срабатывает человеческий фактор. Киберпреступникам порой удается выманить у доверчивых людей огромные суммы. Один из распространенных способов – рассылка в Telegram сообщений о смерти знакомых. Злоумышленники прикрепляют к «соболезнованиям» фотографии, но на самом деле это не снимки, а вредоносные файлы с расширением .apk. Если их скачать, то мошенники получат полный доступ ко всем данным на устройстве. Затем такие же сообщения они отправляют контактам жертвы.

Также злоумышленники манипулируют детьми. Инструктируют их, чтобы они подсмотрели пароль от онлайн-банка и перевели деньги или приложили палец спящего родителя к экрану устройства для разблокировки.

По словам Дмитрия Дудкова, киберпреступники работают сообществами, а схемы атак усложняются. На закрытых форумах, например, обсуждают способы генерации фейковых приложений, выкладывают инструкции и договариваются о совместных вредоносных кампаниях. Используют программы таких семейств, как Spynote (создание приложений-клонов для полного доступа к смартфону жертвы), NFCGate (захват NFC-трафика, что позволяет снимать деньги жертвы в банкоматах). **ВС**

Алиса РОМАНОВИЧ