Новые мошеннические схемы

1. Вредоносные флешки (USB-накопители)

Механизм атаки:
Злоумышленники намеренно разбрасывают флешки и другие накопители с вредоносным программным обеспечением около офисов, в лифтах и на парковках бизнес-центров. При подключении такой флешки к компьютеру файл, замаскированный под документ или фото, при открытии запускает вредоносный код. Устройство может определяться не как накопитель, а как другое подключенное устройство, автоматически выполняя команды от имени пользователя. Также возможен вывод компьютера из строя подачей высокого напряжения через порт.

Статистика: в экспериментах по информационной безопасности более половины людей подключают найденные флешки к своим устройствам.

Риски:
- кража сохранённых паролей, токенов, файлов, переписки и конфиденциальной информации;
- уничтожение или шифрование важных данных;
- получение злоумышленниками точки входа во внутреннюю сеть компании для доступа к другим компьютерам, системам и сервисам.

Как защититься:
1. никогда не подключайте найденные флешки к своему компьютеру, независимо от их внешнего вида и места находки;
2. не пытайтесь самостоятельно проверить устройство, в том числе физически;
3. если флешка найдена в офисе — немедленно передайте её специалистам по ИТ или информационной безопасности;
4. помните: если что-то выглядит как «бесплатный подарок», скорее всего, это не подарок и не случайность.

2. QR-код как инструмент атаки

Механизм атаки:
Злоумышленники распространяют поддельные QR-коды от имени Роскомнадзора или от Почты России для оплаты посылок. Они могут наклеиваться стикерами на терминалах, размещаться во вложениях электронных писем или передаваться в виде изображений через мессенджеры. Сканирование QR-кода ведет на фишинговый сайт или инициирует загрузку APK-файла в обход магазина приложений.

Статистика: около 15% QR-кодов могут вести на опасные ресурсы.

Риски:
- кража учётных данных;
- перехват управления приложениями (в том числе популярными мессенджерами и банковскими приложениями);
- загрузка вирусов в обход магазина приложений.

Как защититься:
1. всегда проверяйте источник QR-кода перед сканированием;
2. не вводите логины, пароли и платёжные данные после перехода по QR-коду;
3. запретите установку приложений из неизвестных источников на смартфон, устанавливайте приложения только из официальных магазинов (Google Play, RuStore и др.).

3. Новый Android-троян Massiv

Механизм атаки:
Выявлен банковский троян Massiv, распространяемый под видом легитимных IPTV-приложений. Целевая аудитория — пользователи, которые добровольно отключают защиту для просмотра «бесплатного» или «эксклюзивного» ТВ-контента. Актуально в период отпусков и дач, когда пользователи хотят провести досуг за просмотром любимых сериалов и передач на Android-устройствах.

Риски:
- кража данных банковских карт и учётных записей через поддельные окна;
- перехват СМС-сообщений и push-уведомлений;
- удалённое управление устройством жертвы в реальном времени (просмотр экрана, клики).

Признаки опасности: IPTV-приложение запрашивает разрешения на доступ к уведомлениям, экрану или специальные возможности (Accessibility).

Как защититься:
1. запретите установку приложений из неизвестных источников на смартфон, устанавливайте приложения только из официальных магазинов (Google Play, RuStore и др.);
2. не переходите по ссылкам на «эксклюзивные» IPTV-сервисы из мессенджеров и с сомнительных сайтов;
3. регулярно обновляйте ОС и приложения.

4. Дипфейк + поддельные видеоконференции

Механизм атаки:
Создаются фальшивые онлайн-встречи с «фейковыми» лицами, созданными искусственным интеллектом и полностью имитирующими знакомых людей или публичных лиц. Жертва подключается к видеовстрече, где идут зацикленные видеозаписи и аватары. Через 8–10 секунд появляется сообщение «SDK устарел» с требованием «обновить» компонент системы. После нажатия на кнопку «Обновить» выполняется вредоносный код в зависимости от операционной системы жертвы.

Риски:
- кража видео с камеры жертвы в реальном времени;
- выполнение произвольного кода на устройстве;
- кража сессий мессенджеров, данных браузеров (логины, cookies, история), скриншотов экрана;
- полный удалённый доступ к компьютеру жертвы.

Как защититься:
1. не переходите по подозрительным ссылкам на совещания, даже если они получены от «знакомых» лиц (возможен взлом аккаунтов ваших друзей);
2. при появлении неожиданного сообщения «SDK устарел» немедленно закройте страницу и проверьте устройство на наличие вирусов.

Ваша бдительность и соблюдение правил цифровой гигиены — главный барьер на пути злоумышленников.