Заражённые приложения успешно выполняют свою функцию, снабжая палестинских хакеров ценными данными.

Группа хакеров Arid Viper, известная также как APT-C-23 и Desert Falcon, развивает новую кампанию мобильного шпионажа, распространяя вредоносное ПО AridSpy через заражённые Android – операционная система для мобильных устройств, разработанная компанией Google. Она основана на ядре Linux и предоставляет широкий спектр функций и сервисов для смартфонов, планшетов, умных часов, телевизоров и других устройств.

 Android позволяет пользователям скачивать и устанавливать приложения из магазина Google Play, обеспечивая множество возможностей для индивидуализации и работы с различными приложениями.

 Android является наиболее популярной в мире ОС для мобильных устройств и продолжает активно развиваться и обновляться." data-html="true" data-original-title="Android" >Android-приложения.

По данным исследователей ESET – это международная компания, специализирующаяся на разработке антивирусных программ и решений для компьютерной безопасности. Компания была основана в Словакии в 1992 году. Её продукты включают антивирусное программное обеспечение, антиспам и защиту от вредоносных программ для компьютеров и мобильных устройств.

 ESET известна своими продуктами, такими как NOD32 и Smart Security, которые предлагают надежную защиту от вирусов и прочих угроз в сети Интернет. Компания имеет множество клиентов по всему миру и придерживается высоких стандартов безопасности в своих продуктах." data-html="true" data-original-title="ESET" >ESET, вредоносное ПО распространяется через специализированные сайты, имитирующие различные приложения, в которые был добавлен вредоносный код AridSpy.

Вредоносная кампания длится с 2022 года и включает пять активных операций, три из которых продолжаются до сих пор. Сама по себе группировка Arid Viper, предположительно связанная с ХАМАС, известна использованием мобильного вредоносного ПО с 2017 года, нацеливаясь на военных, журналистов и диссидентов на Ближнем Востоке.

Анализ последней версии AridSpy исследователями ESET показывает, что вредонос со временем превратился в многоступенчатый троян, способный загружать дополнительные вредоносные компоненты с командного сервера. Основные цели атаки — пользователи в Палестине и Египте, которые загружают заражённые приложения с поддельных сайтов.

Некоторые из таких приложений представляются защищёнными мессенджерами, такими как LapizaChat, NortirChat и ReblyChat, которые основаны на легитимных приложениях StealthChat, Session и Voxer Walkie Talkie Messenger. Также есть приложение, имитирующее программу Палестинского гражданского регистра.

Сайт «palcivilreg[.]com», зарегистрированный 30 мая 2023 года, рекламируется через специальную страницу на Facebook со 179 подписчиками. Вредоносное приложение на этом сайте создано на основе легитимного приложения из Google Play, но использует собственный клиент для связи с легитимным сервером.

Также обнаружено, что AridSpy распространяется через приложение для поиска работы с сайта «almoshell[.]website», зарегистрированного в августе 2023 года. Это приложение не имеет аналога среди легитимных программ.

После установки вредоносное ПО проверяет наличие антивирусных программ и, в случае их отсутствия, загружает первый этап вредоносного кода. Этот этап мимикрирует под обновление Google Play Services и работает независимо от первоначального зараженного приложения.

Основная задача первого этапа — загрузить следующий компонент, который обладает шпионскими функциями и использует домен Firebase для связи с командным сервером. Вредоносное ПО может выполнять различные команды для сбора данных с устройства и деактивировать себя при необходимости.

Если пользователь блокирует или разблокирует телефон, AridSpy делает снимок с фронтальной камеры и отправляет его на сервер, при условии, что с последнего снимка прошло более 40 минут, а уровень заряда батареи выше 15%.

Пользователям следует проявлять бдительность при установке приложений из непроверенных источников, не переходить по сомнительным ссылкам и своевременно обновлять программное обеспечение. Только комплексный подход к кибербезопасности позволит снизить риски заражения вредоносными программами и предотвратить кражу конфиденциальной информации злоумышленниками.