Как Necro обманул систему безопасности и причем тут реклама.

В конце августа специалисты Лаборатории Касперского зафиксировали активность вредоносного ПО под названием Necro, который проник в популярные приложения на платформе Google Play — это официальный магазин контента для устройств с операционной системой Android. Он позволяет пользователям загружать и устанавливать приложения, игры, музыку, фильмы, книги и другой контент на свои Android-устройства.
 Google Play предлагает огромный выбор контента для загрузки, включая бесплатные и платные приложения. Пользователи могут просматривать описание и отзывы других пользователей перед тем, как сделать покупку. Для загрузки контента требуется учетная запись Google, а для покупок может потребоваться кредитная карта." data-html="true" data-original-title="Google Play" >Google Play и неофициальных источниках. Necro — это загрузчик для 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, способный скачивать и запускать на устройстве жертвы различные вредоносные модули. Заражения были выявлены в Бразилии, России, Вьетнаме, Эквадоре и Мексике.

Троян обладает обширными функциями. Necro способен загружать на устройство модули, которые показывают рекламу в скрытых окнах и автоматически прокликивают её, скачивают исполняемые файлы и устанавливают сторонние приложения. Necro может открывать произвольные ссылки в WebView — это компонент в разработке мобильных приложений, который позволяет отображать веб-содержимое (HTML, CSS, JavaScript) непосредственно внутри приложения. Это позволяет интегрировать веб-страницы, веб-приложения или онлайн-ресурсы внутрь мобильного приложения, делая их доступными для пользователей без необходимости переключения в браузер. WebView используется в различных мобильных операционных системах, таких как Android и iOS, для создания гибких и интерактивных приложений, в которых можно отображать веб-контент и взаимодействовать с ним." data-html="true" data-original-title="WebView" >WebView и запускать JavaScript-код, а также, вероятно, оформлять платные подписки. Кроме того, злоумышленники могут пересылать интернет-трафик через заражённые устройства, используя их как прокси для обхода ограничений и

создания ботнетов.

Одним из первых приложений, заражённых Necro, стал модифицированный Spotify Plus, который распространялся на неофициальных площадках. В описании утверждалось, что приложение безопасно и предоставляет расширенные функции по сравнению с официальной версией. Кроме того, специалисты обнаружили заражённые версии WhatsApp и популярных игр, таких как Minecraft, Stumble Guys и Car Parking Multiplayer. Necro попал в эти приложения через вредоносный рекламный модуль.

Опасность Necro не ограничилась только сторонними площадками. Вредоносное ПО также было найдено в приложениях Wuta Camera и Max Browser, доступных на Google Play. По данным платформы, общее количество загрузок этих приложений превысило 11 миллионов. Necro проник в программы через непроверенный рекламный модуль.

После уведомления Google, из Wuta Camera был удалён вредоносный код, а Max Browser было полностью удалено из магазина. Однако риск заражения сохраняется для пользователей, скачивающих приложения из неофициальных источников.

Особо интересно, что версия Necro использовала стеганографию — метод скрытия данных в изображениях — для маскировки вредоносной активности. Такой приём редко встречается в мобильных угрозах.

Для защиты устройств пользователям рекомендуется скачивать приложения только из официальных источников, регулярно обновлять операционную систему и использовать проверенные антивирусные решения.