Банковский троян незаметно заражает устройства с помощью популярных приложений.

Специалисты Zscaler – это основанная в 2008 году американская компания, предоставляющая решения в области кибербезопасности.
 Основным продуктом компании является Zscaler Internet Access (ZIA), предоставляющий безопасный доступ в Интернет для организаций и их сотрудников. ZIA обеспечивает защиту от вредоносных программ, фишинга, атак DDoS и других угроз, используя облачные технологии.
 Zscaler также предоставляет решения для защиты облачных приложений, анализа трафика, контроля доступа и управления политиками безопасности." data-html="true" data-original-title="Zscaler" >Zscaler обнаружили более 90 вредоносных приложений в 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, предназначенных для распространения вредоносного и рекламного ПО, включая банковский троян Anatsa. Приложения были скачаны более 5,5 миллионов раз.

Описание Anatsa (Teabot)

Anatsa — это банковский троян, нацеленный на более 650 приложений финучреждений в Европе, США, Великобритании и Азии. Троян похищает учетные данные онлайн-банков для выполнения мошеннических транзакций. С конца 2023 года Anatsa заразила устройства как минимум 150 000 раз через Google Play, используя различные приложения из категории повышения производительности.

Распространение Anatsa через Google Play

Согласно данным Zscaler, Anatsa вернулась в Google Play и распространяется через два приложения-приманки: «PDF Reader & File Manager» и «QR Reader & File Manager». На момент анализа приложения были установлены 70 000 раз, что указывает на высокий риск их ускользания от процесса проверки Google.

Приложения-дропперы Anatsa

Механизм доставки вредоносного ПО

Anatsa использует многоэтапный механизм доставки полезной нагрузки, включающий четыре этапа:

Этапы загрузки вредоносного ПО

Антианализ и защита

DEX-файл выполняет проверки системы антианализа, чтобы гарантировать, что вредоносное ПО не будет запущено в песочницах или эмулирующих средах. После запуска Anatsa загружает конфигурацию бота и результаты сканирования приложения, а затем загружает инъекции, соответствующие местоположению и профилю жертвы.

Другие вредоносные приложения

За последние несколько месяцев Zscaler обнаружила более 90 вредоносных приложений в Google Play, которые в общей сложности были установлены 5,5 миллиона раз. Большинство из них маскировались под приложения для персонализации, утилиты для фотографий, приложения для повышения производительности, а также приложения для здоровья и фитнеса.

Исследователи не раскрыли названия всех приложений и не уточнили, сообщили ли они в Google о кампании. На данный момент 2 приложения были удалены из Google Play.

По данным Zscaler, на рынке доминируют несколько семейств вредоносных программ: Joker, Facestealer, Anatsa, Coper и различные рекламные приложения. Несмотря на то, что Anatsa и Coper составляют всего 3% от общего числа вредоносных загрузок, они гораздо опаснее, так как способны совершать злонамеренные действия и красть конфиденциальную информацию.

Вредоносные программы (слева) и типы приложений-дропперов (справа)

Рекомендации пользователям

При установке новых приложений в Google Play обязательно проверяйте запрашиваемые разрешения и отклоняйте те, которые связаны с действиями высокого риска, такими как доступ к службе специальных возможностей, SMS и списку контактов.