Хакеры массово маскируют вредоносное ПО под Instagram и WhatsApp.

Согласно недавнему отчёту компании Check Point Software Technologies Ltd. – это компания, специализирующаяся на разработке и поставке продуктов и решений в области кибербезопасности для защиты компьютерных сетей, серверов и мобильных устройств от различных видов киберугроз. Она является одним из лидеров в отрасли кибербезопасности.
 Компания предлагает решения для защиты от различных угроз, таких как вредоносные программы, хакерские атаки, кибершпионаж, атаки на приложения и многое другое." data-html="true" data-original-title="Check Point" >Check Point, киберпреступные группы, включая те, что преследуют своей целью кибершпионаж, в последнее время активно применяют открытый инструмент удалённого администрирования 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 под названием Rafel Существует две расшифровки аббревиатуры RAT:

 • Remote Administration Tool — инструмент удалённого администрирования;
 • Remote Access Trojan — троян удалённого доступа.

 В обоих случаях подразумевается инструмент, который позволяет производить удалённое подключение к целевой системе и последующее выполнение определённых действий. В зависимости от того, кто использует RAT, законный системный администратор или киберпреступник, меняется как расшифровка аббревиатуры, так и спектр выполняемых действий.

 Забавно, что само слово «RAT» можно дословно перевести с английского как «крыса»." data-html="true" data-original-title="RAT" >RAT, маскируя его под Instagram*, WhatsApp и различные приложения для электронной коммерции и антивирусы.

Исследователи сообщили, что этот инструмент предоставляет злоумышленникам мощный набор возможностей для удалённого управления и контроля, что позволяет совершать различные злонамеренные действия, от кражи данных до манипуляции устройствами.

Rafel RAT обладает широким набором функций, таких как возможность стирать SD-карты, удалять журналы вызовов, перехватывать уведомления и даже действовать как программа-вымогатель.

Ранее специалисты Check Point уже фиксировали использование Rafel RAT группой DoNot Team в кибератаках, которые использовали уязвимость в Foxit Reader для обмана пользователей. Эта кампания, прошедшая в апреле 2024 года, использовала PDF-файлы с военной тематикой для доставки вредоносного ПО.

Check Point идентифицировала около 120 различных злонамеренных кампаний, некоторые из которых были направлены на высокопрофильные объекты в таких странах, как Австралия, Китай, Чехия, Франция, Германия, Индия, Индонезия, Италия, Новая Зеландия, Пакистан, Румыния, Россия и США.

Большинство жертв Rafel RAT использовали телефоны Samsung, за ними следовали пользователи Xiaomi, Vivo и Huawei. Более 87,5% инфицированных устройств работали на устаревших версиях Android, которые больше не получают обновления безопасности.

Типичные цепочки атак включали социальную инженерию, чтобы манипулировать жертвами и заставить их предоставить приложениям с вредоносным ПО доступ к конфиденциальным данным, таким как контактная информация, SMS-сообщения, местоположение и журналы вызовов.

Rafel RAT в основном использует HTTP(S) для Инфраструктура управления и контроля, также известная как C2, или C&C (сокр. от англ. «command-and-control»), представляет собой набор инструментов и методов, которые злоумышленники используют для обмена данными со скомпрометированными устройствами после первоначального вторжения (постэксплуатации). Конкретные механизмы атак сильно отличаются друг от друга, но обычно C2 включает один или несколько скрытых каналов связи между устройствами в атакуемой организации и контролируемой злоумышленником платформой. Эти каналы связи используются для передачи инструкций взломанным устройствам, загрузки дополнительных вредоносных данных и передачи украденных данных злоумышленнику." data-html="true" data-original-title="C2" >C2-коммуникаций, но также может использовать API Discord для связи с серверами злоумышленников. Кроме того, инструмент имеет PHP-панель управления, которую зарегистрированные пользователи могут использовать для управления скомпрометированными устройствами.

Эффективность этого инструмента подтверждается его применением в операции по вымогательству, проведённой атакующим, предположительно из Ирана, который отправил записку с требованием выкупа на арабском языке через SMS, призывая жертву из Пакистана связаться с ним в Telegram.

Эксперты Check Point отметили, что Rafel RAT является ярким примером эволюции Android-вредоносов, характеризующегося открытым исходным кодом, обширным набором функций и широким применением в различных незаконных действиях. Присутствие Rafel RAT в киберпространстве подчёркивает необходимость постоянной бдительности и проактивных мер безопасности для защиты устройств Android от злонамеренного использования.

* Компания Meta и её продукты признаны экстремистскими, их деятельность запрещена на территории РФ.