Исследователи раскрыли многолетнюю операцию, организованную киберсилами Пакистана.

Связанные с Пакистаном хакеры участвуют в длительной вредоносной кампании под названием «Operation Celestial Force» («Операция Небесная Сила»), которая длится как минимум с 2018 года. По данным исследователей из Cisco Talos, в этой кампании используется вредоносное ПО GravityRAT для Android и загрузчик HeavyLift для Windows. Управление осуществляется с помощью отдельного инструмента GravityAdmin.

Киберэксперты отнесли эту вредоносную активность к группе Cosmic Leopard (также известной как SpaceCobra), которая демонстрирует тактическое сходство с Transparent Tribe.

«"Operation Celestial Force" активна с 2018 года и продолжает развиваться, используя всё более сложные и разнообразные вредоносные программы, что свидетельствует о высоком уровне успешности в атаке на пользователей на индийском субконтиненте», — отметили исследователи Асир Мальхотра и Витор Вентура в своём техническом отчёте.

GravityRAT впервые был обнаружен в 2018 году как вредоносное ПО для Windows, которое атаковало индийские организации через фишинговые письма. С тех пор вредоносное ПО было адаптировано для работы на Android и macOS, что сделало его многофункциональным инструментом.

В прошлом году Meta* и ESET сообщили о продолжении использования версии GravityRAT для Android, нацеленной на военных в Индии, а также сотрудников BBC Пакистана, маскируя его под облачное хранилище, развлекательные и чат-приложения.

Для координации атак хакеры используют программу GravityAdmin. Они активно применяют фишинг и социальную инженерию, чтобы завоевать доверие потенциальных жертв, после чего отправляет им ссылку на вредоносный сайт с программой, устанавливающей GravityRAT или HeavyLift в зависимости от операционной системы.

GravityRAT находится в арсенале киберпреступников с 2016 года, а GravityAdmin — с августа 2021 года. Последний вредонос используется для управления заражёнными системами через 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-серверы хакеров.

GravityAdmin включает несколько встроенных пользовательских интерфейсов для различных кампаний, таких как «FOXTROT», «CLOUDINFINITY» и «CHATICO» для Android-устройств, а также «CRAFTWITHME», «SEXYBER» и «CVSCOUT» для атак с использованием HeavyLift.

HeavyLift — это новый софт, появившийся у хакеров совсем недавно. Он представляет из себя загрузчик на базе Electron, распространяемый через вредоносные установщики для Windows, и имеет некоторые сходства с версиями GravityRAT на базе Electron, описанными «Лабораторией Касперского» в 2020 году.

После запуска вредоносное ПО собирает и отправляет системные метаданные на C2-сервер и периодически запрашивает новые задачи для выполнения. Оно также может выполнять аналогичные функции на macOS.

«Эта многолетняя операция постоянно нацелена на индийские организации и лица, связанные с обороной, правительством и технологиями», — подчеркнули исследователи.

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