Легендарный Android-троян возвращается спустя почти год затишья.

Банковский троян Medusa 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, также известный как TangleBot, вновь появился в поле зрения исследователей после почти года бездействия. Новые кампании с его использованием были зафиксированы в таких странах, как Франция, Италия, США, Канада, Испания, Великобритания и Турция.

Активность Medusa была замечена с мая текущего года. Новые версии трояна стали компактнее, требуют меньше разрешений и обладают новыми функциями для инициирования транзакций прямо с зараженного устройства.

Впервые троян Medusa был обнаружен в 2020 году как Malware-as-a-Service (MaaS) — вредоносное ПО как услуга — аренда программного и аппаратного обеспечения для проведения кибератак. Владельцы MaaS-серверов предоставляют платный доступ к ботнету, распространяющему вредоносное ПО. Клиенты могут контролировать атаку через личный кабинет, а также обращаться за помощью в техническую поддержку." data-html="true" data-original-title="MaaS" >MaaS-операция (malware-as-a-service). Он предоставляет атакующим возможности для записи нажатий клавиш, управления экраном и манипуляций с SMS. Несмотря на сходство в названии, этот троян не связан с одноименными группировками, занимающимися вымогательством и DDoS-атаками.

Исследователи из компании Cleafy — это компания, которая занимается кибербезопасностью. Она предлагает решения для защиты информации и активов от киберугроз и взлома. Основными продуктами Cleafy являются услуги по информационной безопасности и аналитика угроз." data-html="true" data-original-title="Cleafy" >Cleafy, специализирующейся на выявлении онлайн-мошенничества, сообщили о новых вариантах Medusa. Они стали легче, требуют меньше разрешений и включают такие функции, как наложение на весь экран и захват скриншотов.

Cleafy обнаружила 24 вредоносных кампании, использующих троян, и приписала их пяти различным ботнетам (UNKN, AFETZEDE, ANAKONDA, PEMBE и TONY). UNKN,

например, управляется отдельной группой злоумышленников, которые нацелены на страны Европы, в частности Францию, Италию, Испанию и Великобританию. В последнее время в атаках использовались поддельные приложения, такие как фейковый браузер Chrome, приложение для 5G-соединения и поддельное приложение для стриминга под названием 4K Sports.

Cleafy отмечает, что все кампании и ботнеты управляются центральной инфраструктурой Medusa, которая динамически получает URL («Uniform Resource Locator» или «Единый Указатель Ресурсов») — единый для всех сайтов определитель места положения ресурса в сети Интернет. URL делится на составные части: домен, путь к странице и имя файла.

 Изначально URL был изобретен для обозначения местоположения различных файлов в Интернете, и только со временем стал использоваться для того, чтобы обозначать адреса всех ресурсов, независимо от их типа." data-html="true" data-original-title="URL" >URL-адреса 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-серверов из публичных профилей в социальных сетях.

Авторы Medusa сократили количество запрашиваемых разрешений, чтобы вызывать у жертв меньше подозрений, но по-прежнему требуют доступа к службам специальных возможностей Android. Кроме того, троян всё так же имеет доступ к списку контактов жертвы и функции отправки SMS, что является ключевым методом распространения угрозы.

Согласно анализу Cleafy, из новой версии трояна были удалены 17 команд и добавлены 5 новых, среди которых:

Особенно важной является команда «setoverlay», позволяющая злоумышленникам выполнять обманные действия, такие как создание видимости заблокированного устройства для маскировки вредоносной активности, что идеально работает в паре с OLED-экранами, которые не излучают свет, отображая чёрные пиксели.

Новая возможность захвата скриншотов предоставляет злоумышленникам дополнительные пути для кражи конфиденциальной информации с заражённых устройств. Операция Medusa продолжает расширять масштабы и становиться более скрытной, что может привести к большему количеству жертв.

Несмотря на то, что Cleafy пока не наблюдала поддельные приложения на Google Play, с увеличением числа киберпреступников, использующих MaaS, стратегии распространения будут становиться всё более разнообразными и изощрёнными.

Для защиты от Medusa и схожих угроз следует проявлять бдительность при установке приложений и тщательно проверять запрашиваемые разрешения. Избегайте перехода по подозрительным ссылкам в сообщениях и будьте особенно осторожны с приложениями, требующими доступ к специальным возможностям Android. Соблюдение этих правил цифровой гигиены существенно снизит риск стать жертвой банковских троянов и прочего вредоносного ПО.