Злоумышленники окончательно превратили Discord в шпионское логово.

Исследователи из компании Volexity — это компания, специализирующаяся на кибербезопасности и предоставлении услуг в области обнаружения и реагирования на инциденты информационной безопасности. Основанная в США, Volexity известна своими исследованиями и аналитическими отчётами по вопросам угроз в киберпространстве. Компания активно работает над выявлением и исследованием сложных кибератак, а также предоставляет консультационные услуги по укреплению защиты организаций от подобных угроз. Volexity часто сотрудничает с другими организациями и экспертами в области безопасности, чтобы обмениваться информацией и лучше противостоять современным киберугрозам." data-html="true" data-original-title="Volexity" >Volexity недавно связали хакерскую группировку из Пакистана с кампанией кибершпионажа, нацеленной на индийские государственные учреждения.

Деятельность этой группы отслеживается под кодовым именем UTA0137. Хакеры используют в своих атаках вредоносное ПО под названием DISGOMOJI, написанное на языке Golang и предназначенное для заражения систем на базе Linux – это свободная и открытая операционная система, разработанная Линусом Торвальдсом в 1991 году. С тех пор Linux стал одной из наиболее популярных альтернатив коммерческим операционным системам.

 Основное преимущество Linux заключается в его открытом исходном коде, что позволяет пользователям свободно изменять и распространять систему в соответствии с лицензией GNU GPL.

 Linux предоставляет стабильную, надежную и гибкую платформу для работы с компьютером или сервером. Большинство дистрибутивов Linux (например, Ubuntu, Fedora, Debian) поставляются с разнообразными программами и инструментами для работы, включая офисные приложения, интернет-браузеры, мультимедийные инструменты и многое другое.

 Linux также широко используется в серверной сфере и встроенных системах, таких как маршрутизаторы и мобильные устройства." data-html="true" data-original-title="Linux" >Linux.

«Это модифицированная версия публичного проекта Discord-C2, которая использует мессенджер Discord для управления, применяя эмодзи для передачи вредоносных команд», — сообщают эксперты Volexity.

DISGOMOJI — это универсальный инструмент для шпионажа типа «всё в одном», который в мае этого года обнаружила компания BlackBerry в ходе анализа инфраструктуры, связанной с Transparent Tribe, хакерской группой с пакистанскими корнями.

Атаки начинаются с фишинговых писем, содержащих исполняемый файл Golang ELF, упакованный в ZIP-архив. Этот файл загружает безвредный документ, одновременно скрытно скачивая полезную нагрузку DISGOMOJI с удалённого сервера.

DISGOMOJI, являясь кастомной версией Discord-C2, предназначен для сбора информации о хосте и выполнения команд, полученных с сервера Discord, контролируемого злоумышленниками. Он использует уникальную систему команд, отправляемых с помощью эмодзи:

«Вредоносное ПО создаёт для себя отдельный канал на сервере Discord, что означает, что каждый канал представляет собой отдельную жертву», — добавили в Volexity.

Компания обнаружила различные вариации DISGOMOJI с возможностью обеспечивать устойчивость, предотвращать запуск дублирующих процессов DISGOMOJI, динамически получать учётные данные для подключения к серверу Discord и избегать анализа, отображая ложные информационные и ошибочные сообщения.

UTA0137 также использует легитимные и открытые инструменты, такие как Nmap, Chisel и Ligolo для сканирования сети и туннелирования, а также эксплуатирует уязвимость DirtyPipe (CVE-2022-0847) для повышения привилегий на хостах Linux.

Ещё одна тактика после эксплуатации касается использования утилиты Zenity для отображения вредоносного диалогового окна, маскирующегося под обновление Firefox, чтобы обманным путём заполучить пароли пользователей.

«Злоумышленникам удалось заразить ряд жертв с помощью своего вредоносного ПО на Golang, DISGOMOJI», — сообщили в Volexity. «UTA0137 со временем улучшила DISGOMOJI».

Таким образом, применяя, казалось бы, безобидные смайлики в качестве команд, злоумышленники смогли замаскировать свои злонамеренные действия под невинный обмен сообщениями. Эта уникальная тактика демонстрирует растущую изобретательность киберпреступников в поисках новых способов обхода систем безопасности.

Организациям необходимо повышать свою бдительность в отношении нетрадиционных векторов атак, ведь хакеры становятся всё более креативными в использовании самых неожиданных инструментов и методов для достижения своих преступных целей.