Как MS Office доставляет коктейль из вирусов на компьютер.

Киберпреступники распространяют набор вредоносного ПО через взломанные версии Microsoft Office — это пакет офисных программ, разработанный корпорацией Microsoft. Включает в себя разнообразные приложения, такие как текстовый редактор Word, инструмент для работы с электронными таблицами Excel, приложение для создание презентаций PowerPoint, средство управления базами данных Access и прочие инструменты. Microsoft Office широко используется в офисной среде, образовании, а также для домашнего использования по всему миру." data-html="true" data-original-title="Microsoft Office" >Microsoft Office, которые продвигаются на торрент-сайтах. Вредоносные программы включают трояны, майнеры криптовалют, загрузчики вредоносных программ, прокси-инструменты и программы, нарушающие работу антивирусов.

Команда AhnLab Security Emergency response Center (ASEC) – это центр круглосуточной поддержки и реагирования на инциденты безопасности. Он занимается мониторингом, анализом и устранением угроз безопасности, включая вирусы, хакерские атаки и фишинг." data-html="true" data-original-title="ASEC" >ASEC выявила кампанию и предупредила о рисках загрузки пиратского ПО. Исследователи обнаружили, что злоумышленники используют несколько приманок, включая Microsoft Office, Windows и популярный в Корее текстовый редактор Hangul Word Processor.

Взломанный установщик Microsoft Office имеет продуманный интерфейс, позволяющий пользователям выбирать версию, язык и разрядность (32 или 64 бит).

Интерфейс установщика

Однако в фоновом режиме установщик запускает обфусцированное вредоносное ПО на основе .NET, которое связывается с каналом Telegram или Mastodon, чтобы получить действительный URL для загрузки дополнительных компонентов. URL указывают на Google Drive или GitHub — легитимные сервисы, которые редко вызывают предупреждения антивирусов.

Полезные нагрузки base64, размещенные на Google Drive и GitHub, содержат команды PowerShell, которые вводят в систему различные штаммы вредоносного ПО, распакованные с помощью 7Zip. Один из компонентов, названный «Updater», регистрирует задачи в планировщике задач Windows, чтобы гарантировать их сохранение между перезагрузками системы.

В конечном итоге в систему доставляются следующие программы:

Цепочка заражения

Пользователи должны быть осторожны при установке файлов, загруженных из сомнительных источников, и избегать использования пиратского программного обеспечения. Подобные кампании также часто используются для распространения программ-вымогателей, таких как Surveillance Technology Oversight Project (STOP) — это организация, которая занимается оценкой и регулированием использования технологий наблюдения и контроля гражданской жизни. Она была основана в 2019 году и базируется в Нью-Йорке. STOP стремится противостоять угрозам нарушения прав граждан и распространению систем массового наблюдения. Она проводит исследования и анализирует использование таких технологий, как системы видеонаблюдения, распознавание лиц, анализ поведения и другие. STOP также работает на законодательном уровне для ужесточения нормативных актов, которые регулируют использование технологий наблюдения и защиту конфиденциальности." data-html="true" data-original-title="STOP" >STOP, которая является одной из самых активных операций по вымогательству, нацеленной на потребителей.