Gipy – не просто приложение для изменения голоса, а мощный инструмент хакеров.

Лаборатория Касперского выявила новую вредоносную кампанию под названием Gipy, которая нацелена на пользователей в Германии, Испании и на Тайване. Мошенники используют фишинговые приманки, предлагая жертвам якобы легитимное приложение для изменения голоса с помощью искусственного интеллекта.

Вредоносное ПО Gipy впервые появилось в начале 2023 года и сразу привлекло внимание специалистов. После установки приложение действительно начинает выполнять обещанные функции по изменению голоса, однако параллельно с этим происходит скрытая загрузка вредоносного ПО. Gipy позволяет злоумышленникам красть данные, добывать криптовалюту и устанавливать дополнительное вредоносное ПО на систему жертвы.

Специалисты выяснили, что при запуске Gipy загружает с GitHub – это платформа для хостинга и совместной разработки программного обеспечения.

 Одним из ключевых аспектов GitHub является его социальная составляющая. Разработчики могут подписываться на интересующие их проекты, следить за обновлениями, вносить свои предложения и комментарии, а также взаимодействовать с другими разработчиками, делая процесс разработки быстрее и эффективнее.

 GitHub является популярным инструментом в сообществе разработчиков и служит платформой для сотен тысяч открытых и закрытых проектов в различных областях программного обеспечения." data-html="true" data-original-title="GitHub" >GitHub запароленный архив с вредоносным ПО. В ходе анализа было изучено более 200 таких архивов. Большинство из них содержат известный Стилер Lumma представляет собой обновленную версию стилера Arkei, который впервые был обнаружен в мае 2018 года. Lumma распространяется через поддельный веб-сайт, предназначенный для конвертации файлов формата .docx в .pdf.

 Lumma способен красть кэшированные файлы, конфигурационные файлы и логи криптовалютных кошельков. Он может функционировать как плагин для браузера и совместим с приложением Binance. Также Lumma предоставляет хакеру списки системных процессов, усовершенствованные техники шифрования, а также использование динамических конфигурационных файлов." data-html="true" data-original-title="Lumma" >Lumma Stealer. Однако были обнаружены Apocalypse ClipBanker, модифицированный криптомайнер Corona, а также несколько RAT-троянов, включая DCRat и RADXRat. Дополнительно были выявлены стилеры RedLine и RisePro, написанные на языке Golang, стелс-программа Loli и бэкдор TrueClient.

Специалисты настоятельно призывают пользователей быть бдительными и

осторожными при скачивании и установке новых приложений, особенно тех, которые обещают необычные возможности с использованием искусственного интеллекта. Злоумышленники активно эксплуатируют растущую популярность ИИ-инструментов для проведения своих атак.