Эксперты из «Лаборатории Касперского» обнаружили скрытый майнер криптовалют, маскирующийся под приложение YouTube для Windows. Это поддельное приложение появилось на популярной платформе GitHub несколько месяцев назад и с тех пор активно распространяется среди пользователей, особенно IT-специалистов и разработчиков. Эксперты выяснили, что приложение, внешне работающее как обычный YouTube-клиент, в реальности запускает на устройстве пользователя скрытый майнер, silent-XMRig.

Как поясняют специалисты, угроза от этого майнера особенно актуальна, поскольку только с весны 2024 года было выявлено несколько тысяч его уникальных экземпляров, которые использовались в атаках на российских пользователей. Программа действительно позволяет просматривать видео на YouTube, но в то же время незаметно добывает криптовалюту, перегружая устройство. В «Лаборатории Касперского» предупреждают, что последствия могут быть куда серьёзнее: устройства начинают тормозить, перегреваться, а в редких случаях могут даже выйти из строя. Кроме того, майнер потребляет много электроэнергии, и за это приходится платить пострадавшему пользователю.

Существует и другой риск — если такая программа уже запущена на ПК или смартфоне, это значит, что устройство недостаточно защищено. Руководитель Kaspersky GReAT в России Дмитрий Галов отметил, что сам майнер может быть лишь частью более сложного вредоносного ПО, которое выполняет на устройстве другие опасные действия. Он также подчеркнул, что пользователи, доверяя программам на GitHub, могут не подозревать о том, что даже на такой авторитетной платформе можно столкнуться с вредоносным ПО.