Киберпреступники запустили новую кампанию, нацеленную на геймеров, с использованием вредоносной программы AgeoStealer, сообщает GBHackers. Эта программа, способная красть пароли, данные браузеров и криптовалютные кошельки, распространяется через фальшивые предложения протестировать инди-игры. Хакеры, выдавая себя за разработчиков, заманивают жертв на игровых платформах, таких как Discord, обещая доступ к “бета-версиям” игр.

AgeoStealer доставляется в виде запароленного архива (RAR или ZIP), содержащего установщик, замаскированный под легитимное ПО Unity. После запуска он выполняет сложный JavaScript-код, который обходит антивирусы и крадет данные в реальном времени. Вредоносная программа также использует PowerShell-скрипты для отключения инструментов анализа, таких как Wireshark, что затрудняет ее обнаружение. По данным Flashpoint, в 2024 году инфостилеры, подобные AgeoStealer, украли 2,1 миллиарда учетных данных по всему миру.

Атака эксплуатирует доверие геймеров, особенно молодых пользователей, которые могут не заподозрить подвоха в “игровых” предложениях. Эксперты рекомендуют проверять источники загрузок, избегать запароленных архивов и использовать поведенческий анализ для обнаружения угроз.