Эксперты по кибербезопасности предупредили о новой вредоносной кампании, нацеленной на пользователей macOS. Атака использует приём под названием ClickFix — обманную проверку CAPTCHA, чтобы заставить человека запустить вредоносный код.

Злоумышленники создают поддельные сайты, похожие на официальный сайт провайдера Spectrum. При входе на такую страницу пользователя просят пройти CAPTCHA. Когда тот нажимает на «Я не робот», появляется сообщение об ошибке и предложение «альтернативной проверки». Нажав на кнопку, человек получает инструкции по запуску команды в терминале. На macOS это команда запускает скрипт, который крадёт пароли и устанавливает вирус — Atomic macOS Stealer (AMOS).

Исследователи считают, что за атакой стоят говорящие на русском хакеры, так как в коде встречаются комментарии на русском. Проблемы с логикой на сайтах (например, Windows-инструкции для пользователей Linux и macOS) говорят о том, что всё делалось в спешке.

ClickFix уже используется в других атаках — от фальшивых email от Booking.com до поддельных кнопок «Принять cookies». Пользователей просят быть осторожными и не запускать подозрительные команды из Сети.