Хакеры использую поддельную проверку на роботов для заражения компьютеров вирусами

В начале июня эксперты BI.ZONE Threat Intelligence выявили атаки на около 30 российских компаний с использованием техники ClickFix. Ранее она применялась исключительно против зарубежных организаций. Злоумышленники отправляли поддельные письма от имени силовых ведомств с вложением в формате PDF, содержание которого было заблюрено. Для доступа к файлу предлагалось подтвердить, что пользователь не робот, но, клик по CAPTCHA незаметно копировал в буфер обмена вредоносный скрипт PowerShell.

Далее пользователя убеждали выполнить команды для якобы корректного открытия документа. Комбинация действий Win + R, Ctrl + V и Enter фактически запускала код, который загружал вредоносное ПО с сервера атакующих. Это ПО включало загрузчик Octowave Loader, способный прятать вредоносные программы внутри файлов PNG с использованием стеганографии. Одной из таких программ оказался ранее неизвестный троян удалённого доступа (RAT), вероятно, созданный самими злоумышленниками для шпионажа.

Атаки начинались с поддельных писем и нацеливались на обход систем безопасности. RAT позволял атакующим собирать данные о системе и запускать команды на устройствах жертв. Эксперты отмечают, что для защиты важно использовать фильтры для почты и решения EDR, которые помогают обнаруживать и пресекать атаки на ранних стадиях. Подобные меры могут значительно снизить риск успешной компрометации.