Вредоносы были обнаружены на компьютерах пользователей после того, как хакеры взломали системы провайдера и применили технику «отравления DNS», перенаправляя трафик на зараженные сайты.

Исследователи компании Volexity заметили аномалии в работе одного из провайдеров, что позволило им выявить источник распространения вредоносного ПО.

Хакеры манипулировали DNS-записями, направляя запросы пользователей на поддельные страницы, где вместо легального софта загружались вирусы.

Для устранения последствий, провайдер был вынужден перезагрузить оборудование, чтобы прекратить перенаправление трафика.

Сообщается, что вредоносные программы, такие как MACMA и MGBot, могли удаленно делать скриншоты, перехватывать нажатия клавиш и скачивать файлы и пароли с компьютеров пользователей.