Microsoft раскрыла подробности атак кибергруппы Storm-1977, нацеленных на облачные системы образовательного сектора. Хакеры использовали метод “распыления паролей” — массовую попытку входа с использованием популярных комбинаций паролей, чтобы получить доступ к учетным записям.

Основным инструментом атак стал AzureChecker.exe, программа, которая позволяла злоумышленникам находить уязвимые облачные ресурсы Microsoft Azure. После взлома учетных записей хакеры создавали более 200 виртуальных контейнеров для майнинга криптовалюты. Криптоджекинг — это скрытая установка программ для добычи криптовалюты на чужих устройствах, что замедляет их работу и увеличивает счета за электроэнергию.

Атаки начались в прошлом году и затронули в основном образовательные учреждения США, где облачные технологии широко используются для хранения данных и обучения. Хакеры также захватывали гостевые учетные записи, что позволяло им оставаться незамеченными. Microsoft уже усилила меры безопасности, включая двухфакторную аутентификацию, и призывает учреждения обновлять пароли и отслеживать подозрительную активность.