Эксперты F6 проанализировали цены на теневые услуги и файлы в интернете

Компания F6 представила исследование дарквеба, в котором проанализировали цены на продажу доступа к корпоративным сетям, базам данных и вредоносным программам. Самыми дешёвыми оказались это аккаунты по цене примерно от 10 долларов, тогда как доступ к партнёрским программам вымогателей может стоить до 100 тысяч долларов, а данные об уязвимостях нулевого дня достигает 250 тысяч. Самыми востребованными у преступников оказались доступы в корпоративные сети, которые в зависимости от компании могут стоить до 10 тысяч долларов.

Исследователи отметили, что на многих криминальных форумах действуют строгие правила: закрытое членство, модерация и система гарантов, помогают снизить риск мошенничества между участниками. Каждый день в дарквебе появляются тысячи объявлений с предложениями продажи баз данных, учётных записей, доступов к внутренним сетям и другим корпоративным системам, банковской информации, вредоносного ПО, эксплойтов и даже инструкций по мошенничеству. Базы с персональными данными стоят от 100 до 1000 долларов, а в исключительных случаях достигают нескольких десятков тысяч, что позволяет злоумышленникам запускать сложные атаки на крупные компании.

Особенно востребованы начальные доступы в корпоративные сети, так называемые Initial Access. Их цена начинается примерно от 100–200 долларов, но может сильно вырасти в зависимости от масштаба и отрасли компании. За последние годы количество таких предложений выросло в десятки раз: в 2019 году продавалось около 130 лотов, а в 2024 году уже более 4000. Среди преступников популярны модели подписки на сервисы с вредоносным ПО, которые позволяют быстро создавать уникальные вирусы и проводить атаки. Эксперты из F6 подчёркивают, что системный мониторинг, дарквеба и кибербразведка помогают не только фиксировать факты утечек, но и вовремя предотвращать атаки, особенно если обнаружить упоминания компании или сотрудников до начала хакерских действий.