F.A.C.C.T., компания, занимающаяся борьбой с киберпреступлениями, сообщает о новой преступной группе вымогателей MorLock, которая стала активной в России с начала 2024 года и особенно активизировалась в апреле–мае. Они проникают в сети российских компаний, используя популярные корпоративные антивирусы, аналогично группе Muliaka.

MorLock начали атаковать российские компании с начала 2024 года, затронув уже не менее 9 средних и крупных компаний. Они используют программы-вымогатели LockBit 3 (Black) и Babuk для шифрования данных и требуют огромные выкупы за их восстановление. Однако суммы могут быть снижены почти вдвое в процессе переговоров.

MorLock не копируют или не хищат данные, поэтому их атаки длительностью всего несколько дней с момента доступа до начала шифрования данных. Они используют уязвимости в публичных приложениях, таких как Zimbra, и доступы, купленные на закрытых торговых площадках. В последних атаках злоумышленники использовали скомпрометированные учётные данные партнёров пострадавших компаний.

В случае, если у компании был установлен популярный российский корпоративный антивирус, атакующие отключали его защиту через административную панель и использовали для распространения программ-вымогателей в сети компании.