MacOS, когда-то считавшаяся более безопасной операционной системой, всё чаще становится мишенью для современных кибератак – особенно в сфере криптовалют и блокчейна. Теперь и северокорейские хакеры, связанные с Lazarus Group, используют вирусы под Mac, чтобы взламывать системы и красть ценные цифровые активы.

В этих атаках используются поддельные предложения о работе и фишинговые письма, чтобы обманом заставить сотрудников установить вредоносное ПО. Попав внутрь, вредоносная программа позволяет хакерам контролировать устройство, красть данные и шпионить за действиями. Чтобы избежать обнаружения, вредоносная программа использует скрытый код и шифрование, поэтому стандартным средствам безопасности сложно ее поймать.

Чтобы оставаться защищенными, компаниям следует:

- Использовать надежные средства защиты, совместимые с MacOS.
- Обучите сотрудников распознавать фишинговые аферы
- Используйте многофакторную аутентификацию (MFA)
- Шифруйте конфиденциальные данные и коммуникации
- Мониторинг систем на предмет необычного поведения

Хотя основными мишенями являются криптовалютные и финтех-компании, риску могут подвергнуться все предприятия, использующие MacOS, особенно те, которые работают с финансовыми данными или цифровыми активами. Атаковать могут и обычных людей.