Microsoft предупредила о новом типе атак на цепочку поставок

Специалисты компании Microsoft предупредили предприятия о новом типе атаки под названием «несоответствие используемых зависимостей» (dependency confusion) или «атака с подменой» (substitution attack), суть которого заключается во вмешательстве в процесс разработки приложения в корпоративной среде.

В настоящее время разработчики как в небольших, так и в крупных компаниях при создании корпоративных приложений используют пакетные менеджеры для загрузки и импорта библиотек, которые затем ассемблируются вместе с помощью инструментов для разработки. Эти корпоративные приложения предлагаются клиентам компании или могут использоваться сотрудниками для внутренних нужд.

Иногда в зависимости от предназначения в приложениях также может содержаться проприетарный или чувствительный код. Для таких программ как правило используются приватные библиотеки, хранящиеся в закрытых (внутренних) репозиториях внутри сетей самой компании. В процессе их создания разработчики совмещают приватные библиотеки с публичными, загруженными из открытых порталов с пакетами, таких как PyPI, NuGe и пр. По словам специалистов Microsoft, подобной смешанной средой разработки в больших корпорациях могут воспользоваться киберпреступники, осуществив атаку «несоответствие используемых зависимостей».

Как пояснили эксперты, узнав имена приватных библиотек, использующихся в процессе разработки корпоративных приложений, злоумышленники могут зарегистрировать их в открытых репозиториях пакетов и загрузить публичные библиотеки с вредоносным кодом.

Подробнее: https://www.securitylab.ru/news/516423.php