

Поставщиком приложения является компания Justice AV Solutions, производитель программного обеспечения из Луисвилля. Взломанная версия JAVS Viewer 8.3.7 была доступна для загрузки до 1 апреля. Установщик с обратной подписью «Vanguard Tech Limited» вместо легитимной «Justice AV Solutions Inc.» представлял значительную опасность, отмечают эксперты. После установки он связывался с командно-контрольным сервером, похищая пароли от браузеров и системные данные.

Исследователи рекомендуют немедленно принять меры тем, кто использует версию 8.3.7: сбросить учетные данные и установить последнюю версию. Простого удаления скомпрометированного ПО недостаточно, так как в него могли быть внедрены дополнительные бэкдоры.

Justice AV Solutions подтвердила факт взлома и удалила вредоносный установщик со своего сайта. Они заверили пользователей, что текущие файлы на их сайте являются подлинными и не содержат вредоносных программ.