Хакерская группировка APT29 запустила новую фишинговую кампанию, нацеленную на европейских дипломатов. По данным Check Point Research, с января 2025 года злоумышленники используют поддельные приглашения на дегустацию вин, чтобы распространять два вредоносных ПО: GRAPELOADER и обновлённый WINELOADER. Кампания ориентирована на министерства иностранных дел и посольства в Европе, с отдельными случаями атак на дипломатов на Ближнем Востоке.

GRAPELOADER — это новый загрузчик, который заменяет прежний ROOTSAW. Он отвечает за сбор данных об устройстве жертвы, обеспечение постоянного присутствия в системе и доставку следующего этапа атаки, включая WINELOADER — модульный бэкдор для шпионажа. Фишинговые письма содержат ссылку на архив wine.zip. В нём находятся легитимный исполняемый файл PowerPoint, модифицированная библиотека DLL и вредоносный ppcore.dll, который активирует GRAPELOADER. Для повышения скрытности хакеры применяют технику DLL side-loading, позволяющую запускать вредоносный код через легитимные программы.

Для защиты рекомендуется проверять отправителей писем и обновлять системы безопасности.