Эта техника не нова и носит название BYOVD — «принеси свой собственный уязвимый драйвер». Такой метод широко используется различными киберпреступниками, включая вымогателей и «государственных» хакеров.

В связи с этим в мае 2024 года исследователи безопасности компании Sophos обнаружили данные о ПО EDRKillShifter в ходе расследования дела о вымогательстве. Были обнаружены два образца EDRKillShifter, использующих уязвимые драйверы с GitHub: RentDrv2 и ThreatFireMonitor. В процессе расследуемого инцидента в мае операторы зловреда пытались использовать EDRKillShifter для отключения программ защиты Sophos, но не смогли.

Также злоумышленникам не удалось запустить исполняемый файл вымогательского софта на контролируемом компьютере.

Эксперты отметили, что выполнение вредоносного загрузчика состоит из трёх этапов. Сначала киберпреступник запускает двоичный файл EDRKillShifter со строкой пароля для расшифровки и выполнения встроенного ресурса с именем BIN в памяти. Затем этот код распаковывается и выполняет конечную полезную нагрузку, загружающую и эксплуатирующую уязвимый легитимный драйвер для повышения привилегий и отключения активных процессов и служб защиты EDR.

«После того как вредоносная программа создаёт новую службу для драйвера, запускает её и загружает драйвер, затем вступает в бесконечный цикл, который непрерывно перечисляет запущенные процессы, завершая их, если их имя появляется в жёстко заданном списке целей», — объяснил принцип работы хакерского ПО исследователь угроз Sophos Андреас Клопш.