# ДЛЯ ОБХОДА АНТИВИРУСОВ КИБЕРПРЕСТУПНИКИ ПРЯЧУТ ВРЕДОНОСНОЕ ПО В АУДИОФАЙЛЫ

Специалисты BlackBerry Cylance обнаружили новую вредоносную кампанию по распространению бэкдоров и ПО для майнинга криптовалюты. Главная особенность данной операции заключается в том, что для сокрытия и загрузки вредоносного ПО на атакуемые компьютеры злоумышленники используют аудиофайлы в формате WAV.

Как в июне нынешнего года сообщали исследователи компании Symantec, киберпреступная группировка Turla прятала общественно доступный бэкдор Metasploit Meterpreter в WAV-файле и с его помощью заражала атакуемые системы. Однако недавно специалисты BlackBerry Cylance обнаружили, что данная техника также стала использоваться для распространения криптовалютного майнера XMRig и кода Metasploit для установки обратной оболочки.

Кто стоит за новой кампанией, исследователи пока не могут понять. Хотя метод распространения вредоносного ПО с помощью WAV-файлов ранее уже использовала группировка Turla, новая операция может быть делом рук кого-то другого.

Подробнее: https://www.securitylab.ru/news/501808.php