Автор: Administrator
06.07.2020 11:42

{jcomments on}

Злоумышленники распространяют новое вымогательское ПО Avaddon с помощью макросов Excel 4.0.

Как сообщают специалисты Microsoft Security Intelligence, шифровальщик Avaddon появился в начале июня и распространялся в масштабной спам-кампании, не нацеленной на какую-либо определенную категорию жертв. Сейчас операторы вымогательского ПО ищут партнеров для его распространения.

Avaddon использует надежное шифрование, и восстановить зашифрованные им файлы самостоятельно жертвы не могут. Как минимум один вариант вымогателя требует выкуп в размере $900.

По словам специалистовMicrosoft Security Intelligence, последняя спам-кампания нацелена исключительно на пользователей в Италии. Вымогательское ПО попадает на их системы через спам-письма с документом с вредоносными макросами Excel 4.0.

Одно из таких писем, обнаруженное исследователем безопасности JamesWT_MHT, было адресовано представителям малого бизнеса якобы Инспекцией по защите труда Италии. В его теме было указано, будто адресата ожидают штрафы и судебные иски за нарушения ограничительных норм для работников во время карантина. Письмо содержало ZIP-архив с названием «Официальное уведомление».

Автор: Administrator
06.07.2020 11:42

В свою очередь, документ содержал макросы Excel 4.0 (XML), до сих пор совместимые с современным ПО, где вместо них уже используется код VBA. После запуска макросы загружали Avaddon непосредственно на систему без использования загрузчика-посредника.

Источник: www.securitylab.ru