Об этом сообщили специалисты «Лаборатории Касперского». Они назвали новый вредонос ShrinkLocker. Это «хитрая» программа, написанная на языке VBScript, который используется для автоматизации выполнения задач на старых и новых версиях Windows, поэтому уязвимы перед вымогателем все версии.

Когда вирус попадает на устройство, то сначала изменяет параметры загрузки ОС, после этого шифрует разделы жёсткого диска с помощью технологии BitLocker. Для успешной загрузки по новым параметрам создаётся новый загрузочный раздел.

Чтобы замести следы, вредонос удаляет из системы все логи и файлы с данными своей работы, а на сервер оператора уходит вся информация о системе и ключ шифрования.

Никакие защитные механизмы Windows не срабатывают — просто отключаются. При этом основная цель злоумышленников — фармацевтические и промышленные компании, иногда госорганы. Поэтому работа ShrinkLocker преимущественно нацелена на корпоративные устройства.