Легитимная функция безопасности Windows стала инструментом хакеров.

Эксперты «Лаборатории Касперского» выявили атаки на корпоративные устройства с помощью новой программы-вымогателя ShrinkLocker, использующей BitLocker — это технология шифрования дисков, разработанная Microsoft и входящая в состав большинства версий операционных систем Windows. BitLocker предоставляет средства для защиты данных на дисках, шифруя весь диск, что делает его недоступным без корректного ключа шифрования или пароля. Это обеспечивает дополнительный уровень защиты от несанкционированного доступа, особенно в случае утери или кражи компьютера." data-html="true" data-original-title="BitLocker" >BitLocker. BitLocker — это функция безопасности в Windows, позволяющая защитить данные с помощью шифрования. Целями атак стали промышленные и фармацевтические компании, а также государственные учреждения.

Злоумышленники создали вредоносный скрипт на VBScript. Этот скрипт проверяет, какая версия Windows установлена на устройстве, и в соответствии с ней активирует функционал BitLocker. ShrinkLocker может заражать как новые, так и старые версии ОС, вплоть до Windows Server 2008.

Скрипт изменяет параметры загрузки операционной системы, а затем пытается зашифровать разделы жесткого диска с помощью BitLocker. Создаётся новый загрузочный раздел, чтобы позднее иметь возможность загружать зашифрованный компьютер. Злоумышленники также удаляют инструменты безопасности, используемые для защиты ключа шифрования BitLocker, чтобы пользователь потом не смог их восстановить.

Далее вредоносный скрипт отправляет на сервер злоумышленников информацию о системе и ключ шифрования, сгенерированный на заражённом компьютере. Затем он «заметает следы»: удаляет логи и различные файлы, которые могут помочь в исследовании атаки.

На заключительном этапе ShrinkLocker принудительно блокирует доступ в систему. Жертва видит на экране сообщение: «На вашем компьютере нет вариантов восстановления BitLocker».

Эксперты Касперского рекомендуют компаниям использовать надежные пароли, безопасно хранить ключи BitLocker, делать резервные копии данных и применять решения для раннего обнаружения угроз и расследования инцидентов.