НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Об активности программы-шифровальщика HardBit

ALRT-20230907.1 | 7 сентября 2023 г.

TLP: WHITE

Описание	По данным НКЦКИ, в настоящее время в российском сегменте сети Интернет активно распространяется программа-шифровальщик HardBit. Семейство программ-шифровальщиков HardBit активно применяется злоумышленниками для кражи данных различных компаний, их шифрования и последующего вымогательства денежных средств для их расшифровки. Специалисты центра расследования киберинцидентов Solar JSOC CERT выпустили подробный отчёт с анализом версий шифровальщика HardBit. Известно о применении как минимум трёх версий вредоносной программы, которые отличаются друг от друга минимальным набором параметров. Версии указываются в расширениях зашифрованных файлов: .hardbit, .hardbit2 и .hardbit3. Расшифровать файлы, зашифрованные вредоносной программой HardBit версии 1.0, без приватного ключа невозможно. Для расшифровки файлов, модифицированных шифровальщиком HardBit версий 2.0 и 3.0, эксперты Solar JSOC CERT разработали программу-декриптор. Скачать декриптор можно по ссылке: https://github.com/solar-jsoc/HardBitDecryptor/releases/tag/Latest. Инструкция по его применению приведена в отчёте. В связи с высоким уровнем угрозы заражения информационных ресурсов многих компаний шифровальщиком HardBit рекомендуем ознакомиться с отчётом, опубликованным на официальном сайте компании «Ростелеком-Солар» и доступным по ссылке: https://rt-solar.ru/analytics/reports/3676/