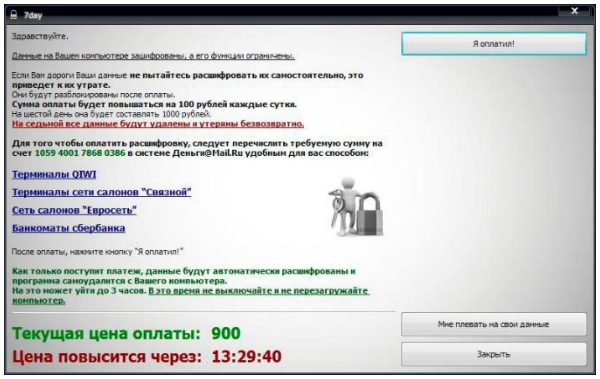

Портал коллективной борьбы с вирусами-шифровальщиками

По данным компании «Лаборатория Касперского» количество атакованных вирусами-шифровальщиками (вредоносным ПО, блокирующим работу компьютера или шифрующим данные на заражённом компьютере пользователя, за устранение чего злоумышленники требуют выкуп) пользователей выросло за год в 5,5 раз – со 131 тыс. в 2014-2015 гг. до 718 тыс. в 2015-2016 гг. Дошло до того, что правоохранительные органы Евросоюза считают вирусы-шифровальщики одной из наиболее актуальных для стран Евросоюза угроз. Ведь подобные атаки зачастую направлены не только на рядовых пользователей, но и на корпорации, и на государственные структуры. При этом расшифровке данные во многих случаях не поддаются, а единственной надеждой вернуть данные является выплата требуемого злоумышленниками выкупа (даже ФБР США «сдалось» и в ходе Cyber Security Summit 2015 дало жертвам простую рекомендацию – платить).

И вот, подвизавшись на борьбу с этим набирающим обороты злом, недавно в интернете появился плод коллективных трудов (Интерпола, полиции Нидерландов, Intel Security (McAfee) и уже упоминавшейся «Лаборатории Касперского») – портал «No More Ransom» (https://www.nomoreransom.org/index.html), основная цель которого – бесплатная помощь жертвам вирусов-шифровальщиков. Примечательно, что, в отличие от ФБР США, общая и главная рекомендация, которая даётся пользователям на портале – как раз не платить вымогателям. Поскольку это «показывает злоумышленникам, что их методы работают», а пользователь не имеет никаких гарантий, что, заплатив деньги, он взамен действительно получит ключ для расшифровки.

Портал бесплатно предоставляет, как минимум, 6 средств для самостоятельной расшифровки данных, зашифрованных, например, криптовымогателями Shade, Chimera и Teslacrypt. Для расшифровки пользователю необходимо загрузить файлы-результаты работы вируса на портал, после чего ему возвращаются дешифрованные файлы.
Также портал позволяет пользователю просканировать свой компьютер на наличие вредоносного ПО. При обнаружении зашифрованных файлов осуществляется поиск ключа для их расшифровки в базе портала, содержащей около 160 000 таких ключей.
Бдительные пользователи могут с помощью портала сообщить «куда следует» о появлении вирусов-шифровальщиков либо о новых случаях заражения (несмотря на то, что одним из «учредителей» портала является российская компания, на портале указаны адреса этих «куда следует» только для жителей стран Евросоюза, США и Нидерландов – российским пользователям писать почему-то некуда).
Кроме того, портал несёт значимую образовательно-просветительскую функцию по информированию пользователей о способах заражения и принципах работы вирусов-шифровальщиков, а также, разумеется, о том, что следует делать, чтобы избежать заражения (почти все эти рекомендации внимательные читатели наших выпусков уже знают):

- Лучшим средством противостоять вирусам-шифровальщикам до сих пор является полное и регулярное резервное копирование всех важных данных;
- Следует использовать надёжное и актуальное антивирусное ПО;
- Необходимо своевременно обновлять используемое на компьютере ПО;
- Никому не следует доверять: даже самые правдоподобно выглядящие сообщения и ссылки могут таить угрозу;
- Рекомендуется включить функцию «Показывать расширения файлов» в «Проводнике» операционной системы Windows;
- При появлении подозрительной активности жёсткого диска или сетевых соединений следует немедленно проверить перечень активных процессов для выявления процесса шифрования данных вирусом-шифровальщиком и отключить компьютер от интернета (отключить как проводное, так и беспроводное соединения).