

К шифровальщикам подберут ключи

// 26.07.2016

<https://uzkimyosanoat.uz/ru/press/news-economy/k-shifrovalshchikam-podberut-klyuchi>

Intel Security и "Лаборатория Касперского" совместно с Европол и полицией Нидерландов запустили проект по борьбе с программами-шифровальщиками, которые требуют деньги за восстановление доступа к информации на зараженных компьютерах. Пользователям бесплатно предложено более 160 тыс. ключей для дешифровки вирусов семейства Shade, поразивших компьютеры в России, на Украине, в Германии, Австрии и Казахстане.

Участники проекта вчера запустили сайт www.nomoreransom.org, где размещена информация о программах-вымогателях. Они шифруют файлы и требуют выкуп за дешифровку, угрожая сделать их нечитаемыми. "Лаборатория Касперского" и Intel Security выложили в бесплатный доступ на сайте инструменты для дешифровки наиболее распространенных шифровальщиков, в том числе более 160 тыс. ключей для вирусов семейства Shade. Они были перехвачены ранее на командно-контрольном сервере, распространявшем Shade, активность которого зафиксирована в России, на Украине, в Германии, Австрии, Казахстане, Франции, Чехии, Италии и США. На сайте также есть ссылки, чтобы сообщить о заражении устройства в полицию Нидерландов, Европол и в ФБР.

Вирусы-вымогатели — одна из главных угроз с точки зрения правоохранительных органов Европы: более двух третей стран-членов ЕС ведут расследования по атакам вредоносного ПО такого типа, говорится в сообщении Европола. Целью хакеров являются устройства частных пользователей, но влиянию подвержены корпоративные и даже государственные сети, отмечает Европол. "Основная проблема с шифровальщиками и вымогателями заключается в том, что зачастую жертвы соглашаются заплатить злоумышленникам, так как не видят другого способа вернуть доступ к своим ценным данным", — сообщил старший антивирусный аналитик "Лаборатории Касперского" Федор Сеницын. Это "подстегивает киберпреступную экономику", добавил он. Проект призван показать, что люди сами могут повлиять на ситуацию, не платя выкуп, идя на поводу у злоумышленников, считает технический директор Intel Security в Европе, Африке и на Ближнем Востоке Радж Самани.

По данным "Лаборатории Касперского", с апреля 2015 года по март 2016 года шифровальщики атаковали 718,5 тыс. компьютеров, что в 5,5 раза больше, чем в 2014-2015 годах. Участники инициативы будут рады новым партнерам, правоохранительным органам РФ и компаниям, работающим в сфере информационной безопасности, сообщили в "Лаборатории Касперского". В управлении "К" МВД РФ на запрос "Ъ" не ответили.

Распространение программ-вымогателей приобрело характер эпидемии, считает Михаил Кондрашин, технический директор Trend Micro Россия: "Только за первые пять месяцев текущего года нашими системами в мире было заблокировано 66 млн угроз, связанных с программами-вымогателями (в том числе 1,6 млн — в России)". По его словам, современные программы-вымогатели используют надежную криптографию, и если программе удалось запуститься на компьютере жертвы, то, скорее всего, восстановить информацию без ключа шифрования не получится, но даже ключи способны помочь только небольшому числу "жертв". "Методов "лечения" заражения немного. В некоторых случаях возможна расшифровка файлов — таковых немного, к сожалению", — соглашается глава представительства ESET в России и СНГ Денис Матеев. По его словам, в некоторых случаях ESET рекомендует пользователям обратиться в полицию, потому что некоторые действия вирусописателей попадают под определения, описанные в статьях 159.6, 163, 165, 272, 273 УК РФ. Однако успешных расследований единицы: 90% пострадавших в полицию не обращаются, также процессу расследования мешают особенности законодательства. Кроме того,

искать киберпреступника будут, только если он предположительно находится в России, отметили в ESET.

Источник: www.kommersant.ru