Автор: Administrator
23.10.2014 12:58

{jcomments on}

Вредонос распространяется в фишинговых письмах, отправленных якобы от имени Высшего Арбитражного Суда РФ

Российские кибермошенники стали использовать новое семейство вымогательского ПО Cryakl, которое шифрует пользовательские файлы и требует совершения денежного перевода для их дешифровки. Отличительной особенностью нового вредоноса является то, что требование об оплате за расшифровку пользовательских файлов поступает от имени Фантомаса. Об этом сообщается в отчете «Лаборатории Касперского».

Вредонос распространяется в фишинговых письмах, отправленных якобы от имени Высшего Арбитражного Суда РФ. Пользователя уведомляют о том, что в его отношении начато административное делопроизводство и предлагают загрузить файл, содержащий документы с дополнительной информацией. Но вместо этого жертва загружает на свой компьютер троян.

Наибольшая активность вредоноса зафиксирована в России, Германии, Казахстане, Украине и Беларуси. На территории одной лишь РФ было обнаружено как минимум 2,5 тысячи атак.

Одна из самых актуальных версий вымогательского ПО была обнаружена специалистами «ЛК» в октябре этого года. Как и все трояны этого семейства, Trojan-Ransom.Win32.Cryakl.bo рассылается через фишинговые письма якобы от Высшего Арбитражного Суда РФ. Перейдя по ссылке, указанной в письме, пользователь загружает на компьютер ZIP-архив, содержащий один-единственный файл attachment.scr. Он представлял собой дроппер, загружающий троян для похищения паролей и программу-шифратор. После запуска вредоносное ПО копирует себя в папку C:Program Files(x86)temp под именем winrar.exe и запускает новую копию. Затем троян прописывается в автозагрузку. Таким образом, пользователь не может прервать шифрование, выключив свой компьютер.

Автор: Administrator
23.10.2014 12:58

Вымогательское ПО шифрует офисные документы, архивы, образы дисков и файлы программ резервного копирования. Перед началом процесса троян посылает POST-запрос на сервер злоумышленников, оповещая их о начале работы.

По завершению процесса шифрования Trojan-Ransom.Win32.Cryakl.bo изменяет изображение на рабочем столе пользователя. Жертва видит обращение от имени знаменитого героя кинофильмов Фантомаса, который в обмен на определенную сумму может расшифровать файлы пользователя. На совершение денежного перевода жертве выделяется 48 часов, при этом точная сумма денег не указывается – в каждом случае хакер может назначить любую сумму выкупа.

С отчетом «Лаборатории Касперского» можно ознакомиться здесь .

Источник: www.securitylab.ru