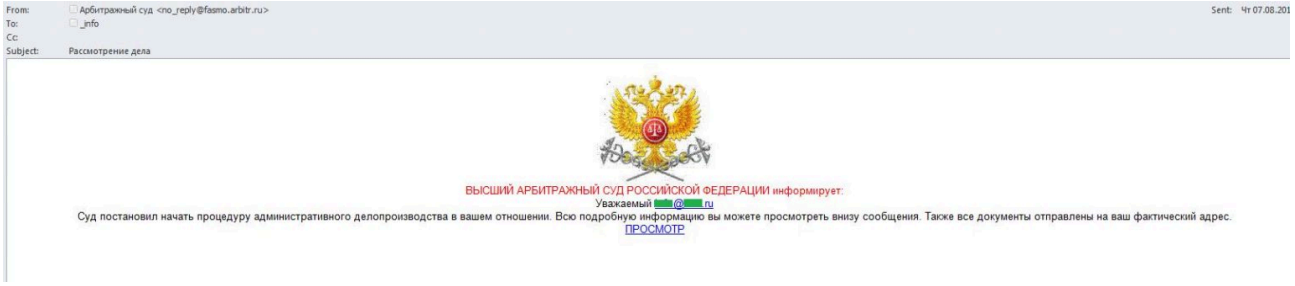
Шифровальщик Cryakl или Фантомас разбушевался

By Artem Semenchenko

Published: 2014-10-22 · Archived: 2026-04-06 01:35:09 UTC

В прошлом месяце мы зафиксировали всплеск атак на пользователей с использованием шифровальщиков семейства Trojan-Ransom.Win32.Cryakl, распространяемых по электронной почте. Потому мы решили рассказать, что же представляют из себя эти зловреды.

Рассылки писем, имитирующих официальные уведомления от имени Высшего Арбитражного Суда РФ, мы впервые обнаружили еще в сентябре прошлого года. И с тех пор неоднократно сталкивались с попытками злоумышленников заразить пользователей одной из вредоносных программ, используя подобные письма – аналогичные рассылки были зафиксированы в январе, августе и октябре этого года. Атаки происходили по устоявшейся схеме: получателю письма сообщают о начале в отношении него административного делопроизводства и предлагают скачать файл с документами для получения дополнительной информации.



Вместо ожидаемых документов потенциальная жертва загружает вредоносную программу, и этой осенью популярностью у злоумышленников пользовались шифровальщики семейства Trojan-Ransom.Win32.Cryakl. Первый представитель этого семейства был добавлен в базы данных «Лаборатории Касперского» еще 29 апреля. С тех пор семейство успело эволюционировать в своём развитии – пополнить список расширений шифруемых файлов, изменить выбор частей файла для шифрования и способ связи с серверами злоумышленников.

Общие черты семейства

Типичный представитель семейства Cryakl написан на языке Delphi и использует самописный алгоритм для шифрования данных. В процессе заражения троянец создает мастер-ключ, который отправляет по почте своим хозяевам. Впоследствии на основе этого мастер-ключа генерируется уникальный ключ для каждого шифруемого файла. При этом файл шифруется не целиком, а лишь первые 29 байт плюс три блока, расположенные в случайных местах файла. Кроме того, в конец файла помещается служебная структура, содержащая:

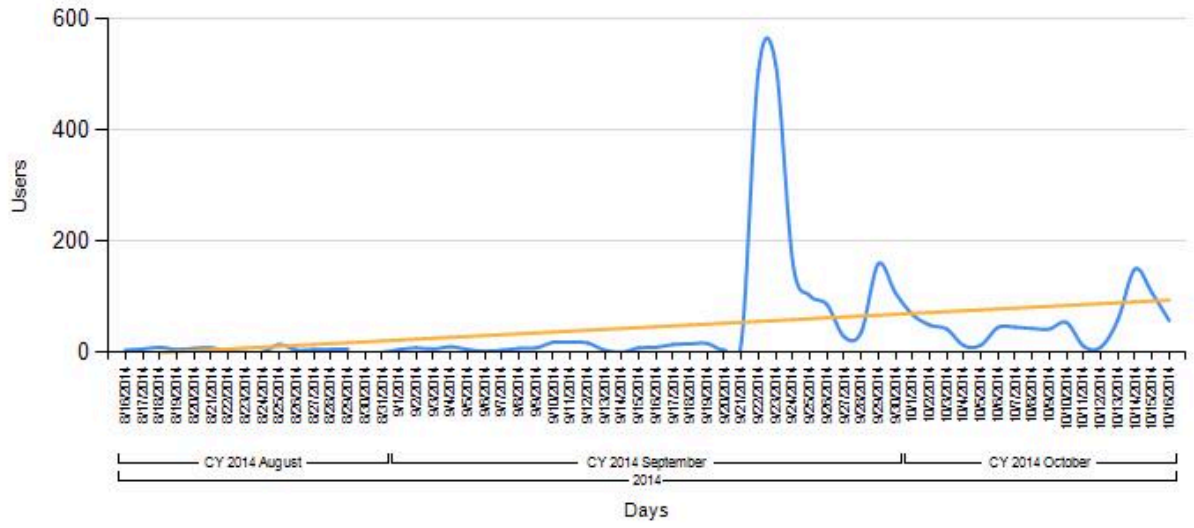
- информацию о размере и расположении зашифрованных блоков,
- MD5-хэши от оригинального файла и его заголовка,
- константы для генерации файлового ключа из мастер-ключа и хэш для проверки его правильности,

- ID жертвы,
- оригинальное имя зашифрованного файла,
- метку заражения {CRYPTENDBLACKDC}.

Распространение

Подавляющее большинство попыток заражения Cryakl зафиксировано в России (почти 2,5 тысячи атак), следом идут Германия, Казахстан и Украина. Беларусь замыкает первую пятерку пострадавших стран.

Пик попыток заражения пришелся на последнюю неделю сентября, когда мы фиксировали почти 600 атак в день. Возросшая активность троянца также наблюдалась в конце сентября и на второй неделе октября.

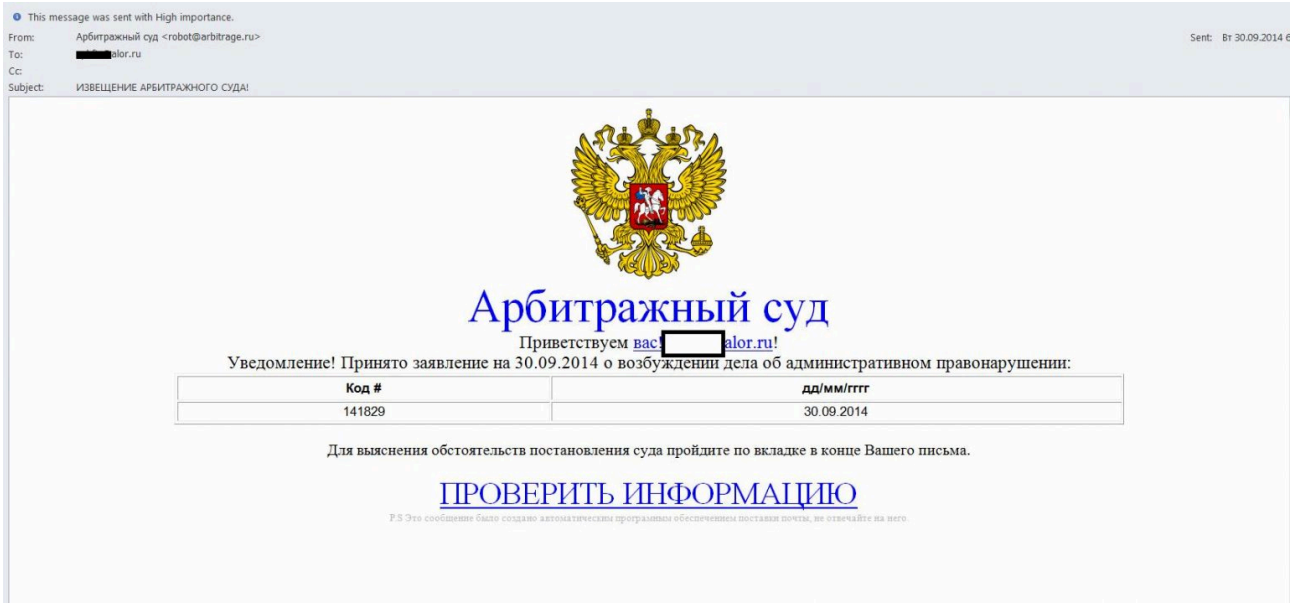


Особо отличились злоумышленники 22 сентября, когда за час разослали модификацию Trojan-Ransom.Win32.Cryakl.ax почти 500 пользователям!

Одна из наиболее свежих модификаций шифровальщика — Trojan-Ransom.Win32.Cryakl.bo – была обнаружена нами в октябре. Рассмотрим на ее примере, что из себя представляет актуальная версия зловреда, как она действует и чем отличается от ранних представителей семейства.

Проникновение в систему

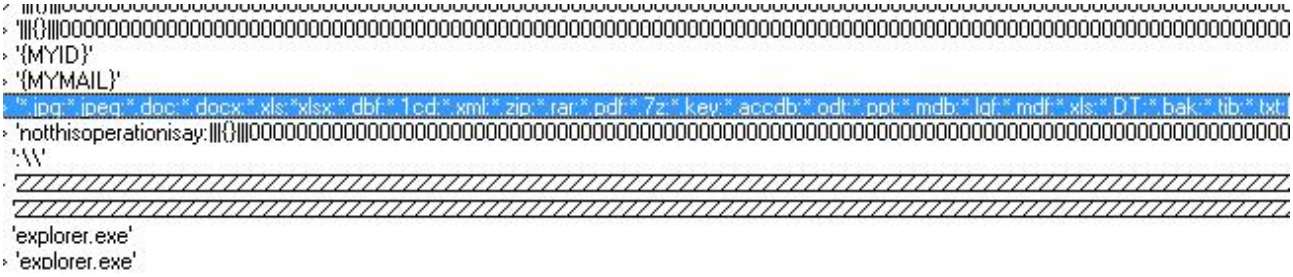
Trojan-Ransom.Win32.Cryakl.bo был найден в одной из спам-рассылок, выполненной в уже знакомом стиле. Если получатель письма кликал по предложенной ссылке «Проверить информацию», то через редирект попадал на вредоносный сайт, откуда на его компьютер загружался архив Attachment.zip, содержащий файл Attachment.scr.



Загруженный файл представлял собой дроппер, который устанавливал на компьютер жертвы сразу два зловреда – предназначенный для кражи паролей троянец Trojan-PSW.Win32.Ruftar (под именем winzip.exe) и интересующий нас шифровальщик Trojan-Ransom.Win32.Cryakl (под именем winrar.exe).

Технические подробности

Trojan-Ransom.Win32.Cryakl.bo представляет собой файл формата PE, упакованный коммерческим протектором Armadillo 9.64 в надежде затруднить анализ. После снятия протектора можно полюбоваться на «внутренности» зловреда.



Строки в распакованном сэмпле

Как видно, Trojan-Ransom.Win32.Cryakl.bo охотится не только за файлами «офисных» форматов, но и за архивами, образами дисков и файлами популярных программ резервного копирования. Причем последние появились лишь в свежих версиях зловреда. В целом, это ещё раз подтверждает важное правило – бэкапы необходимо хранить **вне компьютера.**

После запуска троянец копирует себя из папки, куда был загружен, в папку *C:Program Files (x86)temp под именем winrar.exe* и производит запуск свежесозданного объекта. Дальнейшие действия в системе выполняются уже новой копией.

Получив управление, новая копия Trojan-Ransom.Win32.Cryakl.bo первым делом прописывается в автозагрузку компьютера жертвы. Для этого она использует ключ реестра:

HKLMSOFTWAREMicrosoftWindowsCurrentVersionRun

где создает параметр с названием: *progrmma*

Этот трюк необходим на случай, если процесс шифрования по каким-либо причинам будет прерван. Например, если пользователь выключит компьютер. Тогда при следующей загрузке компьютера, шифровальщик вновь получит управление.

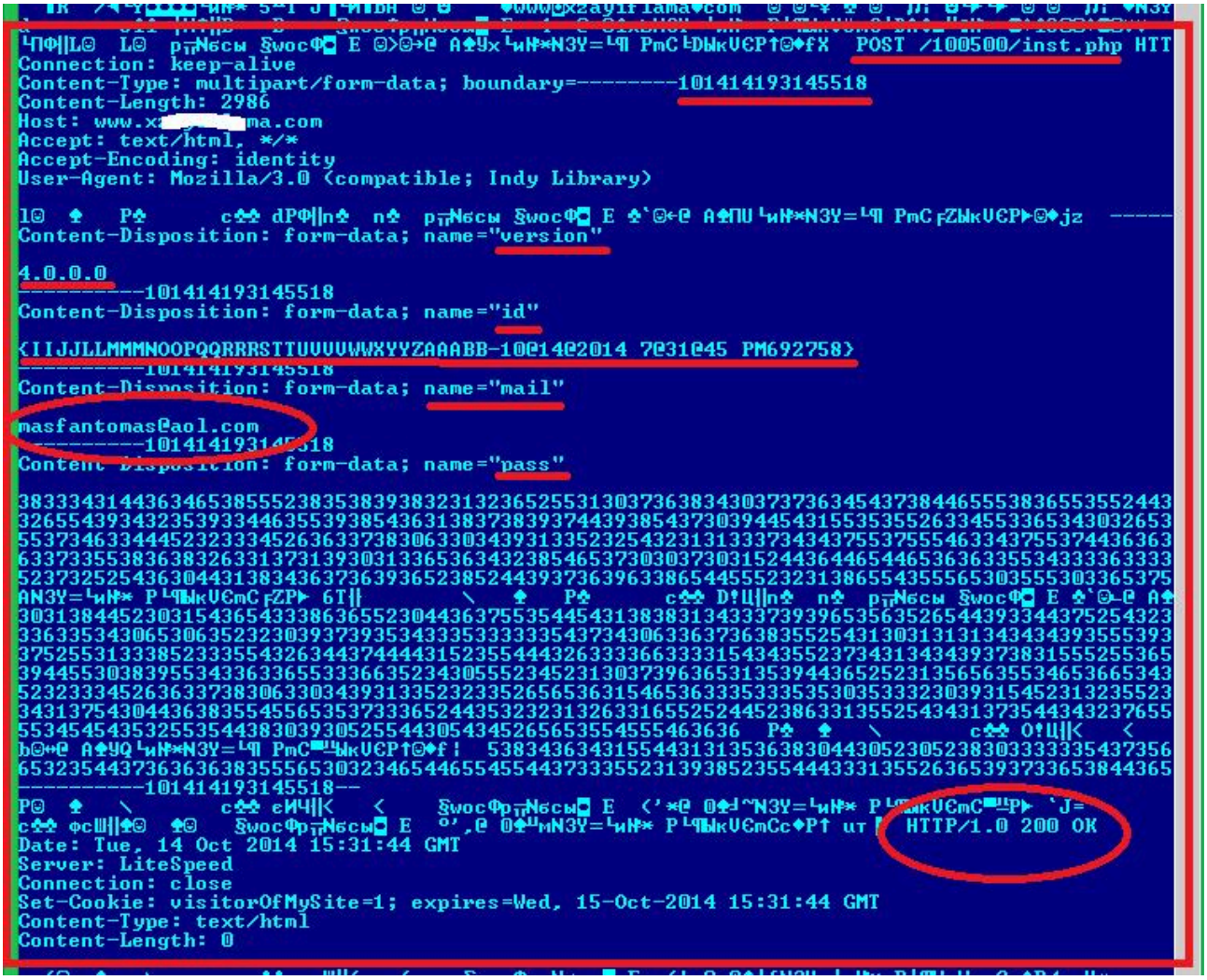
Однако в случае перезагрузки компьютера, перед Trojan-Ransom.Win32.Cryakl.bo возникнет другая проблема: часть данных пользователя уже зашифрована и необходимо продолжить шифрование с теми же параметрами, какие были использованы до перезагрузки. Иначе файлы пользователя окажутся зашифрованными несогласовано, и расшифровать их окажется затруднительно даже для злоумышленника. Следовательно, зловреду необходимо где-то сохранить нужную информацию так, чтобы она могла пережить перезагрузку компьютера. Для этих целей Trojan-Ransom.Win32.Cryakl.bo создаёт в той же папке файл с неприметным названием:

C:Program Files (x86)temptemp056.tmp

На разных этапах работы троянца в этот файл помещается различная «служебная» информация о выбранных параметрах шифрования.

Связь с хозяевами

Теперь всё вроде бы готово для начала шифрования. Однако само по себе оно будет лишено для злоумышленников смысла, если они не смогут расшифровать данные (например, в случае, если жертва попросит в качестве доказательства расшифровать пару файлов). Поэтому перед началом шифрования зловред оповещает своих хозяев о проделанной работе, посылая особый POST-запрос к серверу злоумышленников. В этом заключается первое отличие Trojan-Ransom.Win32.Cryakl.bo от ранних образцов этого семейства, которые посылали сведения на адрес электронной почты по протоколу SMTP.



POST-запрос Trojan-Ransom.Win32.Cryakl.bo к серверу злоумышленников и ответ сервера

Структура POST-запроса специально выбрана так, чтобы облегчить автоматическое добавление информации в базу данных злоумышленников. Она включает следующие поля:

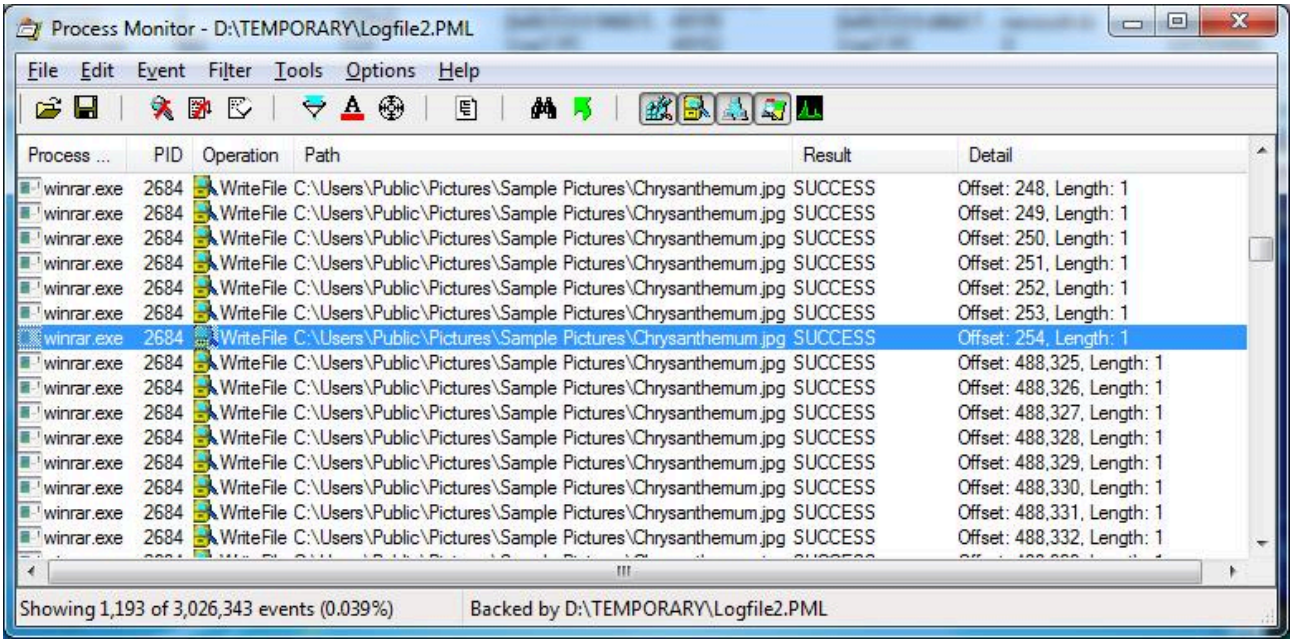
- Идентификатор: в качестве идентификатора используется метка времени.
- Version: значение 4.0.0.0 подтверждает наши прежние догадки о том, что семейство зловредов прошло некоторую «эволюцию» в своём развитии.
- ID: представляет собой составную структуру, включающую в себя два идентификатора, а также текущую дату и время.
- Pass: включает в себя видоизменённый ключ, который в дальнейшем будет использоваться для шифрования данных жертвы.

На скриншоте также видно, что сервер подтверждает приём данных сообщением с кодом ответа «200» — это означает, что данные успешно приняты.

Шифрование

Далее троянец рекурсивно ищет файлы нужных форматов и шифрует их. В отличие от ранних представителей семейства Trojan-Ransom.Win32.Cryakl.bo шифрует сразу 255 байт от начала файла.

Первые образцы, напомним, использовали блок в 29 байт от начала файла.



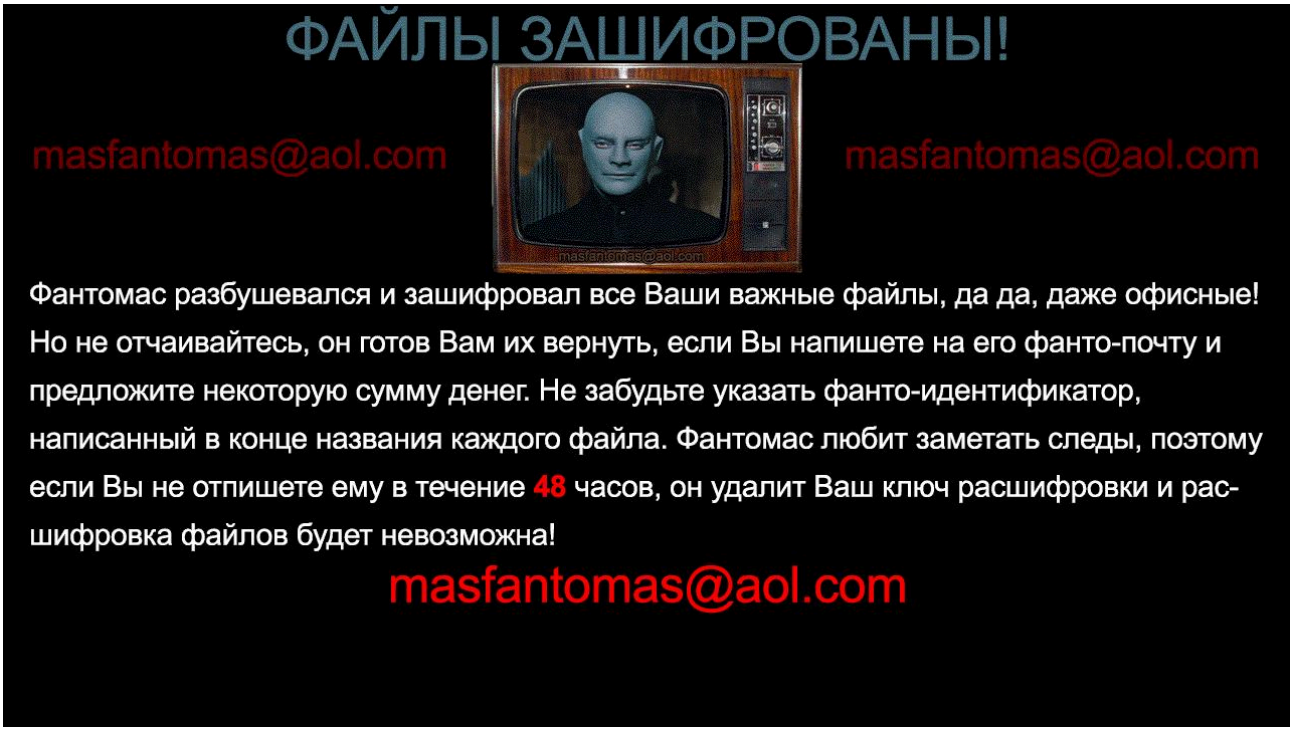
Процесс шифрования файлов

Однако, структура в конце файла осталась прежней и всё ещё содержит информацию о начальном блоке в 29 байт.

Структура в конце зашифрованного файла

Впрочем, блок 0-255 байт в структуре также присутствует.

После окончания шифрования Trojan-Ransom.Win32.Cryakl.bo меняет картинку на рабочем столе пользователя на обращение от имени знаменитого ретро-злодея Фантомаса. Французский мастер преступления идет в ногу со временем: являясь владельцем электронной «фанто-почты», он способен расшифровать файлы, зашифрованные вредоносной программой. Естественно, не бесплатно.



По сравнению с предыдущими посланиями срок, выделенный жертве на ответ, значительно уменьшен – до 48 часов. Также обратите внимание на то, что злоумышленник не указывает, какую конкретно сумму он хочет получить за свою «помощь». Не исключено, что она варьируется в зависимости от количества и качества зашифрованных файлов. Например, в одном из случаев заражения зловредом из семейства Cryakl злоумышленники запросили 1000 долларов. Но перед этим, по словам жертвы, удаленно подключились с зараженному компьютеру и удалили все резервные копии. Коварство, достойное Фантомаса!

Защита

К сожалению, расшифровать обработанные Cryakl файлы на данный момент невозможно. Поэтому в случае отсутствия резервной копии затронутых файлов жертвам троянца приходится прощаться с данными или же соглашаться на требования вымогателей. После выплаты требуемой суммы пострадавшему присылают утилиту-дешифратор и текстовый файлик с ключом, который подходит только этому пользователю. Впрочем, получение рабочего ключа, равно как и отклика от злоумышленников, не гарантировано.

Мы рекомендуем заранее позаботиться о безопасности данных:

- Сделать резервные копии важных файлов и разместить их на отдельном носителе либо на другом компьютере.
- Игнорировать письма с подозрительными вложениями и ссылками, даже если они якобы присланы арбитражным судом или иным официальным органом. В случае возникновения каких-либо

сомнений стоит связаться с приславшей письмо организацией по телефону или электронной почте, указанной на официальном сайте.

- Установить современное антивирусное ПО.

Дополнительную защиту могут обеспечить такие специализированные технологии, как Cryptoprotection, входящая в состав Kaspersky System Watcher. System Watcher анализирует системные события и позволяет «откатить» вредоносные изменения. В частности, в случае обнаружения подозрительной попытки доступа к персональным файлам пользователя, он немедленно создает их локальную резервную копию. Если окажется, что попытка изменения файла была инициирована вредоносной программой, например, шифровальщиком, защитное решение удаляет ее, а Cryptoprotection автоматически заменяет модифицированные файлы сделанной ранее копией.

http://www.youtube.com/watch?v=BwjdZgreCVs

Технология Cryptoprotection работает в домашних и корпоративных продуктах «Лаборатории Касперского».
