

Telegram, «Касперский» и троян-шифровальщик за 5000

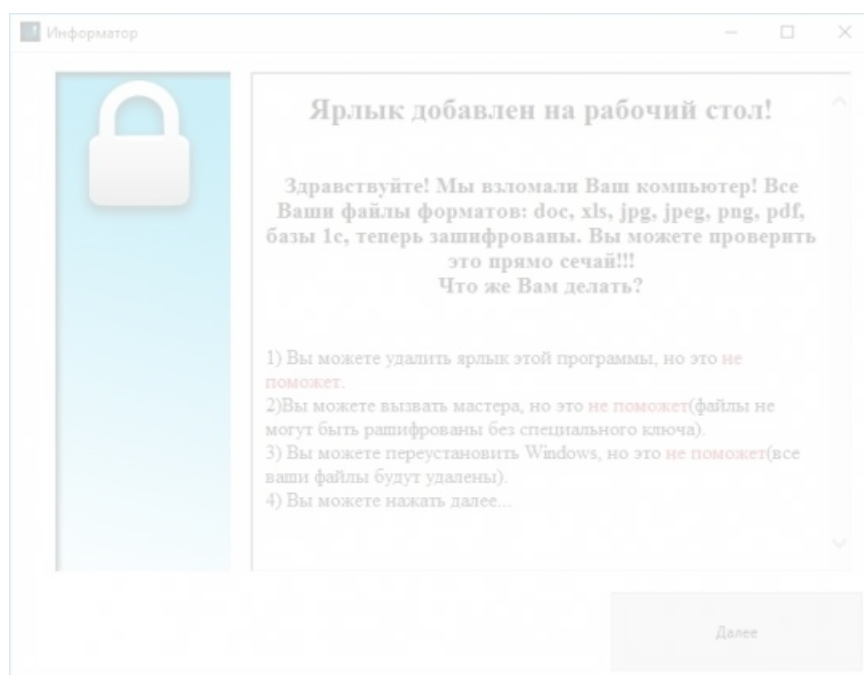
Российские мошенники создали новый вирус. Он относится к группе шифровальщиков и распространяется через популярное приложение Telegram. Об обнаружении вируса, использующего протокол мессенджера Telegram, заявила «Лаборатория Касперского».

Вредоносное ПО шифрует находящиеся на вашем устройстве файлы – от документов до фотографий, после чего вывешивает на рабочий стол окно с требованием оплатить за ключ для расшифровки. Авторы вредоноса уверяют: без их помощи вернуть файлы в первоначальный вид невозможно, даже переустановив систему заново.

Троянец написан на Delphi и имеет размер более 3Мб. После запуска вредоносное ПО генерирует ключ для шифрования файлов и идентификатор заражения `infection_id`.

Далее вирус связывается со своими создателями с помощью публично доступного Telegram Bot API. Для этого они заранее создали «бот Telegram», получив при этом от серверов Telegram уникальный токен, который однозначно идентифицирует вновь созданного бота, и поместили его в тело вируса, чтобы он мог использовать API Telegram.

Вирус ищет на дисках файлы заданных расширений и шифрует их. Затем зловард скачивает дополнительный модуль Xhelp.exe и запускает его. Этот модуль – его назвали «Информатор» – сообщает жертве о произошедшем, а также выдвигает требования выкупа. Сумма составляет 5000 руб, а в качестве методов оплаты предлагаются Qiwi и Яндекс.Деньги.

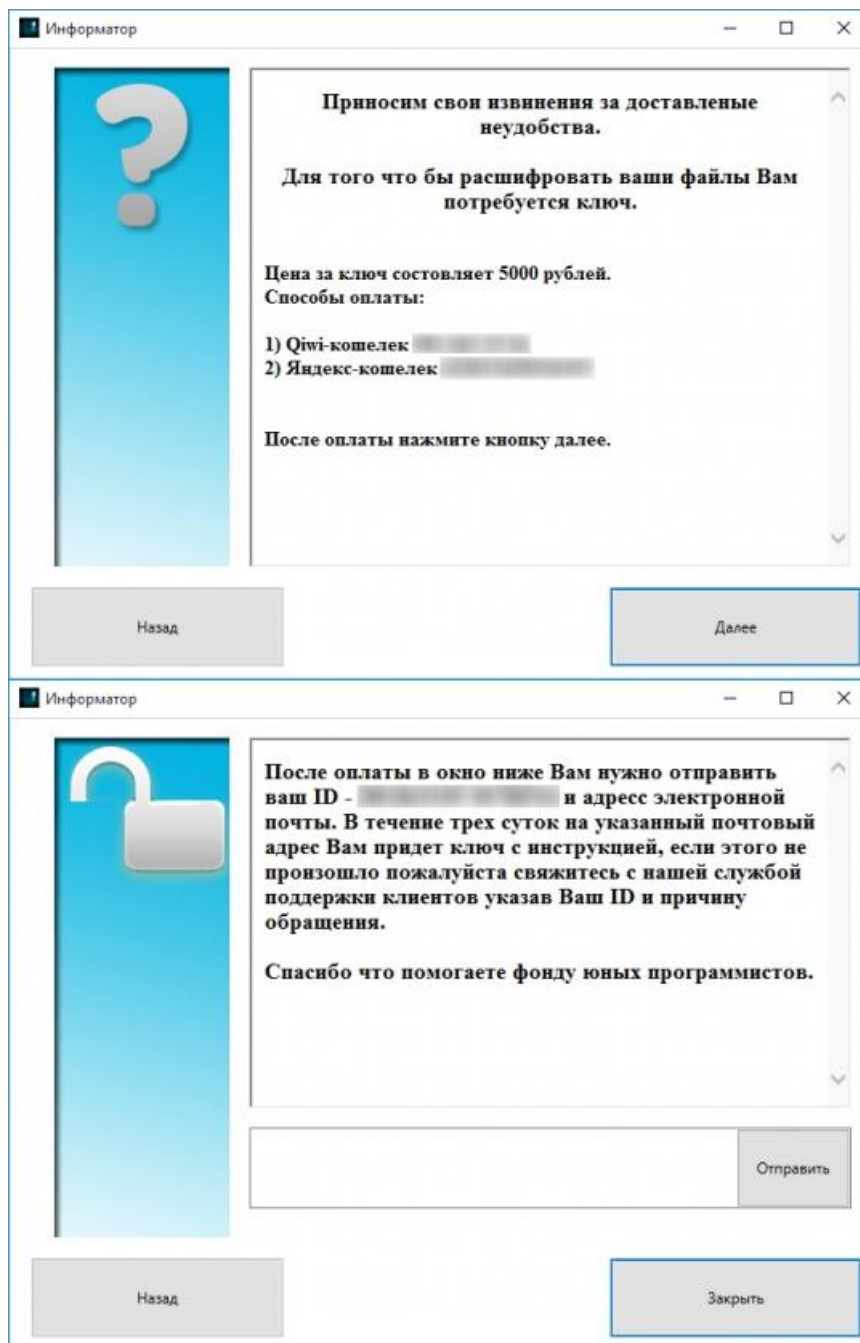


Связь жертвы со злоумышленниками осуществляется через поле ввода в интерфейсе «Информатора».

В блоге «Лаборатории Касперского» опубликованы имена файлов, под которыми можно обнаружить зловреда на вашем гаджете.

Специалисты компании просят пользователей, столкнувшихся с этим вирусом, не платить злоумышленникам, а обратиться в службу поддержки «Лаборатории», где помогут расшифровать зараженные файлы.

При этом нигде не сообщается, как уберечь свой смартфон от заражения...



Автор: Алина Саратова
📌 16

© SmartBabr

НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР

👁 3038

10.11.2016, 16:42

URL: <https://babr24.com/?ADE=271107>

Bytes: 2751 / 1869

Версия для печати

Скачать PDF

👍 Пореккомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

newsbabr@gmail.com

Автор текста: **Алина
Саратова.**

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)