

Scarabey

Archived: 2026-04-10 02:32:04 UTC

Scarabey Ransomware

Scarab-Scarabey Ransomware

Scarab-Russian Ransomware

(шифровальщик-вымогатель, деструктор)

(первоисточник)

Этот крипто-вымогатель шифрует данные пользователей с помощью AES-256 (режим CBC), а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: **Scarabey**. Написан на Delphi без упаковки в C++ которая используется в оригинальном Scarab.

[Для вас подготовлен видеообзор одной из версий >>](#)

© Генеалогия: [Scarab](#) > Scarabey

К зашифрованным файлам добавляется расширение **.scarab**

Позже стали добавляться расширения **.oneway**, **.omerta**, **.rent**, **.mvp** и другие. Цель: запутать идентификацию и исследователей.

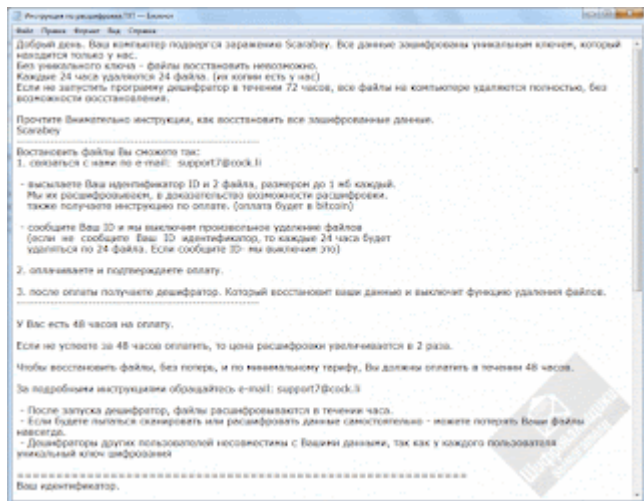


Логотип шифровальщика разработан на этом сайте ID-Ransomware.RU

Стилизация выполнена в виде скарабея, держащего глобус с Россией.

Активность этого крипто-вымогателя пришла на начало декабря 2017 г. Ориентирован на русскоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа написана на русском языке и называется: **Инструкция по расшифровке.TXT**



Содержание записки о выкупе:

Добрый день. Ваш компьютер подвергся заражению Scarabeu. Все данные зашифрованы уникальным ключом, который находится только у нас.

Без уникального ключа - файлы восстановить невозможно.

Каждые 24 часа удаляются 24 файла. (их копии есть у нас)

Если не запустить программу дешифратор в течении 72 часов, все файлы на компьютере удаляются полностью, без возможности восстановления.

Прочтите Внимательно инструкции, как восстановить все зашифрованные данные.

Scarabeu

Восстановить файлы Вы сможете так:

1. связаться с нами по e-mail: support7@cock.li
 - высылаете Ваш идентификатор ID и 2 файла, размером до 1 мб каждый. Мы их расшифровываем, в доказательство возможности расшифровки. также получаете инструкцию по оплате. (оплата будет в bitcoin)
 - сообщите Ваш ID и мы выключим произвольное удаление файлов (если не сообщите Ваш ID идентификатор, то каждые 24 часа будет удаляться по 24 файла. Если сообщите ID- мы выключим это)
2. оплачиваете и подтверждаете оплату.
3. после оплаты получаете дешифратор. Который восстановит ваши данные и выключит функцию удаления файлов.

У Вас есть 48 часов на оплату.

Если не успеете за 48 часов оплатить, то цена расшифровки увеличивается в 2 раза.

Чтобы восстановить файлы, без потерь, и по минимальному тарифу, Вы должны оплатить в течении 48 часов.

За подробными инструкциями обращайтесь e-mail: support7@cock.li

- После запуска дешифратор, файлы расшифровываются в течении часа.

- Если будете пытаться сканировать или расшифровать данные самостоятельно - можете потерять Ваши файлы навсегда.

- Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования

=====

Ваш идентификатор.

+4IAAAAAAAAAAgIUuHZLHEQA1***lwAxNEiDVrkUqanFasK=hC212=ky

----- P.S. -----

Если у Вас нет биткойнов

* Здесь вы можете обменять любые электронные деньги - <https://bestchange.ru>
это список обменников.

* Приобретите криптовалюту Bitcoin удобным способом:

https://localbitcoins.com/ru/buy_bitcoins (Visa/MasterCard, QIWI Visa Wallet и др.)

- Не имеет смысла устраивать панику.

- Каждое нецензурное слово в наш адрес равняется + 50\$ к оплате.

- Жалобами заблокировав e-mail, Вы лишаете возможность остальных, расшифровать свои компьютеры.

Остальных, у кого также зашифрованы компьютеры Вы лишаете ЕДИНСТВЕННОЙ НАДЕЖДЫ расшифровать. НАВСЕГДА.

- Просто войдите с нами в контакт, оговорим условия расшифровки файлов и доступной оплаты, в дружественной обстановке.

Ваш идентификатор.

+4IAAAAAAAAAAgIUuHZLHEQA1***lwAxNEiDVrkUqanFasK=hC212=ky

Перевод записки на русский язык:

Уже сделан вымогателями. Примечательно, что кроме банальной ошибки в слове "ключем" в тексте немало других ошибок, что говорит не в пользу грамотности составителей вымогательского текста. Да, похоже, что их было несколько, кто-то добавлял текст, кто-то удалял слова. Отсюда множественные ошибки с пунктуацией и лексикой.

Технические детали

Распространяется путём взлома через незащищенную конфигурацию RDP. Также может распространяться с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов (Necurs и других), эксплойтов, веб-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на [вводной странице блога](#).

!!! Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы сделайте резервное копирование важных файлов по [методу 3-2-1](#).

► Удаляет теньные копии файлов, отключает функции восстановления и исправления Windows на этапе загрузки командами:

```
cmd.exe /c wbadmIn DELETE SYSTEMSTATEBACKUP -keepVersions:0
```

```
cmd.exe /c wmic SHADOWCOPY DELETE
```

```
cmd.exe /c vssadmIn Delete Shadows /All /Quiet
```

```
cmd.exe /c bcdedit /set {default} recoveryenabled No
```

```
cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

Особенности:

- По названию записка о выкупе аналогична тем, что использовались в обновлениях крипто-вымогателей [Amnesia](#) и [Amnesia-2](#). Но по детекту это одна из разновидностей [Scarab Ransomware](#), ориентированная на русскоязычных пользователей.
- Кроме шифрования файлов также производится их выборочное удаление, отсюда вторая характеристика — деструктор.
- Scarabeу ориентирован на российских пользователей и распространяется через RDP и ручную установку на серверы и системы.

Список файловых расширений, подвергающихся шифрованию:

Большинство типов файлов, кроме тех, что нужны для работы системы.

Это наверняка будут документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:

Инструкция по расшифровке.TXT

sevnz.exe

svhosts.exe

<random>.exe

Расположения:

\Desktop\ -> Инструкция по расшифровке.TXT

\Downloads\ -> Инструкция по расшифровке.TXT

\Documents\ -> Инструкция по расшифровке.TXT

\User_folders\ -> Инструкция по расшифровке.TXT
C:\Windows\HhSm\svhosts.exe
\%APPDATA%\ ->
\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
uSjBVNE = "%Application Data%\sevnz.exe
См. ниже результаты анализов.

Сетевые подключения и связи:

Email: support7@cock.li
См. ниже в обновлениях другие адреса и контакты.

Результаты анализов:

Гибридный анализ >>
[VirusTotal анализ >>](#)
Другой анализ >>

Степень распространённости: **высокая**.
Подробные сведения собираются регулярно.

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

Scarab Family (семейство Scarab):

- [Scarab \(ScarabLocker\)](#) - июнь-август 2017, ноябрь 2017
- [Scarab-Scorpio \(Scorpio\)](#) - июль 2017
- [Scarab-Jackie](#) - октябрь 2017
- [Scarab-Russian \(Scarabey\)](#) - декабрь 2017
- [Scarab-Decrypts](#) - март 2018
- [Scarab-Crypto](#) - март 2018
- [Scarab-Amnesia](#) - март 2018
- [Scarab-Please](#) - март 2018
- [Scarab-XTBL](#) - апрель 2018
- [Scarab-Oblivion](#) - апрель 2018
- [Scarab-Horsia](#) - май 2018
- [Scarab-Walker](#) - май 2018
- [Scarab-Osk](#) - май 2018
- [Scarab-Rebus](#) - май 2018

[Scarab-DiskDoctor](#) - июнь 2018

[Scarab-Danger](#) - июнь 2018

[Scarab-Crypt000](#) - июнь 2018

[Scarab-Bitcoin](#) - июнь 2018

[Scarab-Bomber](#) - июнь 2018

[Scarab-Omerta](#) - июнь-июль 2018

[Scarab-Bin](#) - июль 2018

[Scarab-Recovery](#) - июль 2018

[Scarab-Turkish](#) - июль 2018

[Scarab-Barracuda](#) - июль 2018

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

Обновление от 23 декабря 2017:

Оригинальное название: **Scarabey**

Расширение: **.scarab**

Записка: Инструкция по расшифровке.ТХТ (текст аналогичен, email новый)

Email: Support56@cock.li

Файл: sevnz.exe

Те же деструктивные функции. Смотрите видеообзор в блоке ссылок ниже.

Результаты анализов: [НА](#) + [VT](#)

Обновление от 25 января 2018:

Расширение: **.scarab**

Записка: Инструкция по расшифровке.ТХТ

Email: helper023@cock.li

Обновление от 25 апреля 2018:

Расширение: **.scarab**

Email: decrypt014@cock.li

Записка: Инструкция по расшифровке файлов.ТХТ

Скриншот записки о выкупе >>

Без уникального ключа - файлы восстановить невозможно.

Каждые 24 часа удаляются 24 файла. (их копии есть у нас)

Если не запустить программу дешифратор в течении 72 часов, все файлы на компьютере удаляются полностью, без возможности восстановления.

Прочтите Внимательно инструкции, как восстановить все зашифрованные данные.

Scarabey

Восстановить файлы Вы сможете так:

1. связаться с нами по e-mail: locker87@cock.li

- высылаете Ваш идентификатор ID и 2 файла, размером до 1 мб каждый.

Мы их расшифровываем, в доказательство возможности расшифровки.

также получаете инструкцию по оплате. (оплата будет в bitcoin)

- сообщите Ваш ID и мы выключим произвольное удаление файлов

(если не сообщите Ваш ID идентификатор, то каждые 24 часа будет удаляться по 24 файла. Если сообщите ID- мы выключим это)

2. оплачиваете и подтверждаете оплату.

3. после оплаты получаете дешифратор. Который восстановит ваши данные и выключит функцию удаления файлов.

У Вас есть 48 часов на оплату.

Если не успеете за 48 часов оплатить, то цена расшифровки увеличивается в 2 раза.

Чтобы восстановить файлы, без потерь, и по минимальному тарифу, Вы должны оплатить в течении 48 часов.

За подробными инструкциями обращайтесь e-mail: locker87@cock.li

- После запуска дешифратор, файлы расшифровываются в течении часа.

- Если будете пытаться сканировать или расшифровать данные самостоятельно - можете потерять Ваши файлы навсегда.

- Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования

=====

Ваш идентификатор.

+4IAAAAAAACA3z8gH***nlxkOlw

----- P.S. -----

Если у Вас нет биткойнов

* Здесь вы можете обменять любые электронные деньги - <https://bestchange.ru>
это список обменников.

* Приобретите криптовалюту Bitcoin удобным способом:

https://localbitcoins.com/ru/buy_bitcoins (Visa/MasterCard, QIWI Visa Wallet и др.)

- Не имеет смысла устраивать панику.

- Каждое нецензурное слово в наш адрес равняется + 50\$ к оплате.

- Жалобами заблокировав e-mail, Вы лишаете возможность остальных, расшифровать свои компьютеры.
Остальных, у кого также зашифрованы компьютеры Вы лишаете **ЕДИНСТВЕННОЙ НАДЕЖДЫ**

(если не сообщите Ваш ID идентификатор, то каждые 24 часа будет удаляться по 24 файла. Если сообщите ID- мы выключим это)

2. оплачиваете и подтверждаете оплату.
3. после оплаты получаете дешифратор. Который восстановит ваши данные и выключит функцию удаления файлов.

У Вас есть 48 часов на оплату.

Если не успеете за 48 часов оплатить, то цена расшифровки увеличивается в 2 раза.

Чтобы восстановить файлы, без потерь, и по минимальному тарифу, Вы должны оплатить в течении 48 часов.

За подробными инструкциями обращайтесь e-mail: Scarab@horsefucker.org

- После запуска дешифратор, файлы расшифровываются в течении часа.
- Если будете пытаться сканировать или расшифровать данные самостоятельно - можете потерять Ваши файлы навсегда.
- Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования

Ваш идентификатор.

+4IAAAAAAACp0O7oHZ***7xN=gHyM3XqjucXdDk

Обновление от 18 июня 2018:

Расширение: .oneway

Email: ibm15@horsefucker.org

Записки могут называться: Как расшифровать файлы oneway.TXT

или Инструкция по расшифровке файлов oneway.TXT

Статус: Файлы можно дешифровать.



► Содержание записки:

Напишите на почту - ibm15@horsefucker.org

=====

ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!

Ваш личный идентификатор

+4IAAAAAAASDeOZH***5YTVClk5rnLn7aBk

Ваши документы, фотографии, базы данных и другие важные файлы были зашифрованы.

Каждые 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.

Каждые 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)

Для расшифровки данных:

Напишите на почту - ibm15@horsefucker.org

*В письме указать Ваш личный идентификатор

*Прикрепите 2 файла до 1 мб для тестовой расшифровки.

мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.

-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.

-Написав нам на почту вы получите дальнейшие инструкции по оплате.

В ответном письме Вы получите программу для расшифровки.

После запуска программы-дешифровщика все Ваши файлы будут восстановлены.

Внимание!

* Не пытайтесь удалить программу или запускать антивирусные средства

* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных

* Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования

* Не пытайтесь найти решение на стороне, это 100% развод. Никто кроме нас расшифровать не может.

=====

Если связаться через почту не получается

* Зарегистрируйтесь на сайте <http://bitmsg.me> (сервис онлайн отправки Bitmessage)

* Напишите письмо на адрес BM-2cXv1tCz4mRNE52UyDZ7DWDdVfUf5ed6GB с указанием Вашей почты и личного идентификатора

Ваш личный идентификатор

+4IAAAAAAASDeOZH***5YTVClk5rnLn7aBk

Обновление от 19-20 июня 2018:

Файлы можно было дешифровать, если они были зашифрованы до 18 июня 2018 года.

В июне 2018 злоумышленники, распространяющие шифровальщики семейства Scarab, обновили основной крипто-конструктор.

В предыдущих версиях Scarab-шифровальщиков был Trojan.Encoder.18000 (по классификации Dr.Web).

Файлы можно было дешифровать.


```

Иструкция по расшифровке файла.TXT
Напишите на почту - ibm15@horsefucker.org
=====
Ваш личный идентификатор
AQAAAAAAACccD.`TeThDhNADA***A}U&Aj)kl
Кажде 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.
Кажде 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)
Для расшифровки данных:
Напишите на почту - ibm15@horsefucker.org
*В письме указать Ваш личный идентификатор
*Прикрепите 2 файла до 1 мб для тестовой расшифровки.
мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.
-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.
-Написав нам на почту вы получите дальнейшие инструкции по оплате.
В ответном письме Вы получите программу для расшифровки.
После запуска программы-дешифровщика все Ваши файлы будут восстановлены.
Внимание!
* Не пытайтесь удалить программу или запускать антивирусные средства
* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных
* Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования
* Не пытайтесь найти решение на стороне, это 100% развод. Никто кроме нас расшифровать не может.
=====
Если сводились через почту не получайте
* Загрузите программу на сайте http://521eag.me (скажем омаде отправки @521eag)
* Напишите письмо на адрес ibm15@horsefucker.org с указанием Вашей почты и
личного идентификатора
Ваш личный идентификатор
AQAAAAAAACccD.`TeThDhNADA***A}U&Aj)kl
Кажде 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.
Кажде 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)
Для расшифровки данных:
Напишите на почту - ibm15@horsefucker.org
*В письме указать Ваш личный идентификатор
*Прикрепите 2 файла до 1 мб для тестовой расшифровки.
мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.
-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.
-Написав нам на почту вы получите дальнейшие инструкции по оплате.
В ответном письме Вы получите программу для расшифровки.
После запуска программы-дешифровщика все Ваши файлы будут восстановлены.
Внимание!
* Не пытайтесь удалить программу или запускать антивирусные средства
* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных
* Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования
* Не пытайтесь найти решение на стороне, это 100% развод. Никто кроме нас расшифровать не может.
=====

```

► Содержание записки:

Напишите на почту - ibm15@horsefucker.org

ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!

Ваш личный идентификатор
;AQAAAAAAACccD.`TeThDhNADA***A}U&Aj)kl

Ваши документы, фотографии, базы данных и другие важные файлы были зашифрованы.

Каждые 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.

Каждые 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)

Для расшифровки данных:

Напишите на почту - ibm15@horsefucker.org

*В письме указать Ваш личный идентификатор

*Прикрепите 2 файла до 1 мб для тестовой расшифровки.

мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.

-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.

-Написав нам на почту вы получите дальнейшие инструкции по оплате.

В ответном письме Вы получите программу для расшифровки.

После запуска программы-дешифровщика все Ваши файлы будут восстановлены.

Внимание!

- * Не пытайтесь удалить программу или запускать антивирусные средства
- * Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных
- * Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования
- * Не пытайтесь найти решение на стороне, это 100% развод. Никто кроме нас расшифровать не может.

=====

Если связаться через почту не получается

* Зарегистрируйтесь на сайте <http://bitmsg.me> (сервис онлайн отправки Bitmessage)

* Напишите письмо на адрес BM-2cXv1tCz4mRNE52UyDZ7DWDdVfUf5ed6GB с указанием Вашей почты

и

личного идентификатора

Ваш личный идентификатор

;AQAAAAAACCcD.`TeTHDhNADA***A}U&Aj)kl

Обновление от 16 августа 2018:

Расширение: **.rent**

Записка: Инструкция по расшифровке файлов Rent.TXT

Email: diven@cock.li или другой

Bitmessage: BM-2cXv1tCz4mRNE52UyDZ7DWDdVfUf5ed6GB

Статус: Файлы зашифрованы иначе, но обнаружив ключ, их можно дешифровать.



► Содержание записки:

Напишите на почту - diven@cock.li

=====

ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!

Ваш личный идентификатор

+4IAAAAAAADv7HAE***oRTWlw

Ваши документы, фотографии, базы данных и другие важные файлы были зашифрованы.

Каждые 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.

Каждые 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)

Для расшифровки данных:

Напишите на почту - diven@cock.li

*В письме указать Ваш личный идентификатор

*Прикрепите 2 файла до 1 мб для тестовой расшифровки.

мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.

-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.

-Написав нам на почту вы получите дальнейшие инструкции по оплате.

В ответном письме Вы получите программу для расшифровки.

После запуска программы-дешифровщика все Ваши файлы будут восстановлены.

Внимание!

* Не пытайтесь удалить программу или запускать антивирусные средства

* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных

* Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования

* Не пытайтесь найти решение на стороне, это 100% развод. Никто кроме нас расшифровать не может.

=====

Если связаться через почту не получается

* Зарегистрируйтесь на сайте <http://bitmsg.me> (сервис онлайн отправки Bitmessage)

* Напишите письмо на адрес VM-2cXv1tCz4mRNE52UyDZ7DWDdvfUf5ed6GB с указанием Вашей почты и

личного идентификатора

Ваш личный идентификатор

+4IAAAAAAADv7HAE***oRTWlw

Обновление от 23 августа 2018:

Расширение: .omerta

Email: xvalera228@protonmail.com

[Топик на форуме >>](#)

Статус: Файлы зашифрованы иначе, но обнаружив ключ, их можно дешифровать.

Обновление от 10 сентября 2018:

[Пост в Твиттере >>](#)

Расширение: .mvp

Файлы переименовываются.

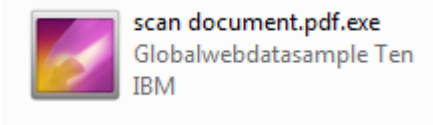
Пример заш-файла: 3oIoZu+32IciG9rHroIoFpy3rN1ICT5DHxSHTZCU7M9xXkWzydDXCq+M.mvp

Записка: Как расшифровать файлы.TXT

Email: thermal@lock.li



Файлы: scan document.pdf.exe, systems.exe



Mutex: STOPSCARABSTOPSCARABSTOPSCARABSTOPSCARABSTOPSCARAB

На файле написано: Globalwebdatasample Ten

Фальш-имя: T668f Authentication

Фальш-копирайт: IBM (c) 2015 Company

Результаты анализов: [VT](#)

Статус: Файлы зашифрованы иначе, но обнаружив ключ, их можно дешифровать.

Обновление от 23 сентября 2018:

Расширение: .omerta

Файлы переименованы.

Записка: Инструкция по расшифровки omerta.TXT

Email: thermal@cock.li

Статус: Файлы зашифрованы иначе, но обнаружив ключ, их можно дешифровать.



► Содержание записки:

Напишите на почту - thermal@cock.li

=====

ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!

Ваш личный идентификатор

;AQAAAAAAACgrkr-Le***PeA~jn)+#aI~[P

Ваши документы, фотографии, базы данных и другие важные файлы были зашифрованы.

Каждые 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.

Каждые 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)

Для расшифровки данных:

Напишите на почту - thermal@cock.li

*В письме указать Ваш личный идентификатор

*Прикрепите 2 файла до 1 мб для тестовой расшифровки.

мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.

-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.

-Написав нам на почту вы получите дальнейшие инструкции по оплате.

В ответном письме Вы получите программу для расшифровки.

После запуска программы-дешифровщика все Ваши файлы будут восстановлены.

Внимание!

* Не пытайтесь удалить программу или запустить антивирусные средства

* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных

* Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования

* Не пытайтесь найти решение на стороне, это 100% развод. Никто кроме нас расшифровать не может.

=====

Ваш личный идентификатор
;AQAaaaaaacgrkr-Le***PeA~jn)+#aI~[P

Обновление от 17 декабря 2018:

[Пост на форуме >>](#)

Расширение: .omerta

Email: alices@mail2tor.com

Другие email вымогателей (февраль 2019): alices@cock.li, bin420@cock.li

VM-2cTx9M1bfonGRN31Rw3F7h7MFYomEWoGJ1

Записка: Инструкция по расшифровке файлов.txt



► Содержание записки:

Напишите на почту - alices@mail2tor.com

=====

ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!

Ваш личный идентификатор

pAQAAAAAAABpG9LdH***SnX=cteKU0RY3

Ваши документы, фотографии, базы данных и другие важные файлы были зашифрованы.

Каждые 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.

Каждые 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)

Для расшифровки данных:

Напишите на почту - alices@mail2tor.com

*В письме указать Ваш личный идентификатор

*Прикрепите 2 файла до 1 мб для тестовой расшифровки.

мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.

-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.

-Написав нам на почту вы получите дальнейшие инструкции по оплате.

Если связаться через почту не получается

* Зарегистрируйтесь на сайте <http://bitmsg.me> (сервис онлайн отправки Bitmessage)

* Напишите письмо на адрес VM-2cTx9M1bfonGRN31Rw3F7h7MFYomEWOgJ1 с указанием Вашей почты и личного идентификатора

Внимание!

* Не пытайтесь удалить программу или запускать антивирусные средства

* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных

* Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования

=====

Ваш личный идентификатор

pAQAAAAAAABpG9LdH***SnX=cteKU0RY3

Обновление от 1 февраля 2019:

Расширение: **.secure**

Записка: Расшифровать файлы и работать дальше.TXT

Расшифровать файлы и работать дальше.TXT.secure

Особенность: Записка о выкупе тоже получает расширение .secure

Email: secure32@sock.li

Файл EXE: [osk.exe](#)



► **Содержание записки:**

Напишите на почту - secure32@sock.li

=====

ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!

Ваш личный идентификатор pAQAAAAAAACazRP***Shoh+8DfAk

Ваши документы, фотографии, базы данных и другие важные файлы были зашифрованы.

Каждые 24 часа удаляются 24 файла, необходимо прислать свой идентификатор чтоб мы отключили эту функцию.

Каждые 24 часа стоимость расшифровки данных увеличивается на 30% (через 72 часа сумма фиксируется)

Для расшифровки данных:

Напишите на почту - secure32@cock.li

*В письме указать Ваш личный идентификатор

*Прикрепите 2 файла до 1 мб для тестовой расшифровки. мы их расшифруем, в качестве доказательства, что ТОЛЬКО МЫ можем их расшифровать.

-Чем быстрее вы сообщите нам свой идентификатор, тем быстрее мы выключим произвольное удаление файлов.

-Написав нам на почту вы получите дальнейшие инструкции по оплате.

В ответном письме Вы получите программу для расшифровки.

Запустите инструмент на вашем компьютере и безопасно расшифруйте все ваши данные.

Мы гарантируем: 100% успешное восстановление всех ваших файлов 100% гарантию соответствия 100% безопасный и надежный сервис

Внимание!

* Не пытайтесь удалить программу или запустить антивирусные средства

* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных

* Дешифраторы других пользователей несовместимы с Вашими данными, так как у каждого пользователя уникальный ключ шифрования =====

Ваш личный идентификатор `pAQAAAAAACazRP***Shoh+8DfAk`

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===



Внимание!

Файлы в некоторых случаях можно дешифровать!

Изучите моё руководство в статье [SCARAB DECODER](#)

Или прочтите инфу по [ссылке](#). Мой перевод [рядом](#).

Or ask for help using [this link](#). My translation [beside](#).



Read to links:

[Tweet on Twitter](#)

[ID Ransomware](#) (ID under Scarab)

Write-up, [Topic of Support](#)

 [Video review](#)

Ett fel inträffade.

Det går inte att köra JavaScript.



Thanks:

Andrew Ivanov, Alex Svirid

GrujaRS, Michael Gillespie, S!Ri, Emmanuel_ADC-Soft

ANY.RUN, Intezer Analyze

всем пострадавшим из топиков поддержки на англоязычных и русскоязычных форумах

© Amigo-A (Andrew Ivanov): All blog articles.

Source: <https://id-ransomware.blogspot.com/2017/12/scarabey-ransomware.html>