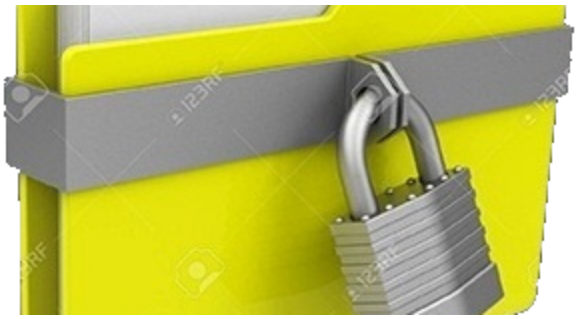
ChernoLocker

id-ransomware.blogspot.com/2019/12/chernolocker-ransomware.html



ChernoLocker Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES-256, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: Adobe Acrobat Activation Patch.exe, Mobdro For PC.exe или что-то еще.

Обнаружения:
DrWeb -> Trojan.Encoder.30403
BitDefender -> Trojan.GenericKD.32833226
Symantec -> ML.Attribute.HighConfidence
Malwarebytes -> Ransom.FileCryptor
Microsoft -> Ransom:Win32/Genasom

© Генеалогия: выясняется, явное родство с кем-то не доказано.

Изображение из экрана вымогателя — логотип статьи

К зашифрованным файлам добавляется одно из следующих расширений:
(.CHERNOLOCKER)
(.chernolocker)
(.filelockergprotonmail.ch)
.(filelocker£protonmail.ch)

```
"(.CHERNOLOCKER)",
"(.chernolocker)",
"(.filelocker@protonmail.ch)",
".(filelocker@protonmail.ch)"
```

Внимание! Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришлась на начало середину декабря 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

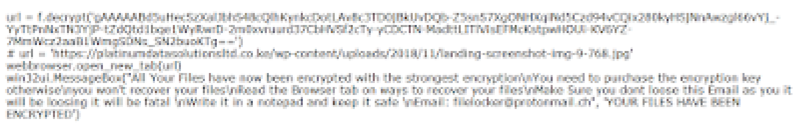
Запиской с требованием выкупа выступает изображение, загружаемое онлайн:

Содержание записки о выкупе:
FILES IN YOUR COMPUTER HAVE BEEN LOCKED!
YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN LOCKED
WITH THE STRONGEST ENCRYPTION AND UNIQUE KEY GENERATED FOR THIS COMPUTER.
PRIVATE DECRYPTION KEY STORED STORED ON A SECRET SERVER AND NOBODY WILL DECRYPT YOUR FILES UNTIL YOU PAY AND OBTAIN THE PRIVATE DECRYPTION KEY.
THE SERVER WILL ELIMINATE THE KEY AFTER 14 DAYS.

PURCHASE THE DECRYPTION KEY, NOW
YOU CAN CONTACT ME VIA FILELOCKER@PROTONMAIL.CH

Перевод записки на русский язык:
ФАЙЛЫ НА ВАШЕМ КОМПЬЮТЕРЕ ЗАБЛОКИРОВАНЫ!
ВАШИ ДОКУМЕНТЫ, ФОТО, БАЗЫ ДАННЫХ И ДРУГИЕ ВАЖНЫЕ ФАЙЛЫ ЗАБЛОКИРОВАНЫ
С САМЫМ НАДЕЖНЫМ ШИФРОВАНИЕМ И УНИКАЛЬНЫМ КЛЮЧОМ, СГЕНЕРИРОВАННЫМ ДЛЯ ЭТОГО КОМПЬЮТЕРА.
ЗАКРЫТЫЙ КЛЮЧ ДЕШИФРОВАНИЯ ХРАНИТСЯ НА СЕКРЕТНОМ СЕРВЕРЕ И НИКТО
НЕ РАСШИФРУЕТ ВАШИ ФАЙЛЫ, ПОКА ВЫ НЕ ЗАПЛАТИТЕ И НЕ ПОЛУЧИТЕ ЗАКРЫТЫЙ КЛЮЧ ДЕШИФРОВАНИЯ.
СЕРВЕР УДАЛИТ КЛЮЧ ЧЕРЕЗ 14 ДНЕЙ.
КУПИТЕ КЛЮЧ РАСШИФРОВКИ, СЕЙЧАС
ВЫ МОЖЕТЕ НАПИСАТЬ МНЕ НА FILELOCKER@PROTONMAIL.CH

Для того, чтобы это отобразить, используется скрипт, скомпилированный на Python, который отображает окно сообщения после шифрования и открывает заготовленное онлайн-изображение в браузере.



Содержание этого сообщения:
YOUR FILES HAVE BEEN ENCRYPTED
All Your Files have now been encrypted with the strongest encryption
You need to purchase the encryption key otherwise you won't recover your files
Read the Browser tab on ways to recover your files
Make Sure you dont loose this Email as you it will be loosing it will be fatal
Write it in a notepad and keep it safe
Email: filelocker@protonmail.ch

Перевод на русский язык:
Ваши файлы были зашифрованы
Все ваши файлы зашифрованы с самым сильным шифрованием
Вам надо купить ключ шифрования, иначе не сможете вернуть файлы
Прочтите в Браузере о способах возврата ваших файлов
Постарайтесь не потерять этот Email, т.к. эта потеря будет фатальной
Запишите это в блокнот и сохраните
Email: filelocker@protonmail.ch

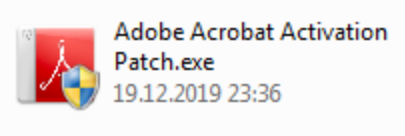
Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инжектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на вводной странице блога.

Нужно всегда использовать Актуальную антивирусную защиту!!!
Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу **3-2-1**.

Список файловых расширений, подвергающихся шифрованию:
Это документы MS Office, OpenOffice, PDF, текстовые файлы, базы данных, фотографии, музыка, видео, файлы образов, архивы и пр.

Файлы, связанные с этим Ransomware:
Adobe Acrobat Activation Patch.exe



Mobdro For PC.exe
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
Online Image: xxxxs://platinumdatasolutionsltd.co.ke/wp-content/uploads/2018/11/landing-screenshot-img-9-768.jpg

Записи реестра, связанные с этим Ransomware:
См. ниже результаты анализов.

Сетевые подключения и связи:
Email: filelocker@protonmail.ch
BTC:
См. ниже в обновлениях другие адреса и контакты.
См. ниже результаты анализов.

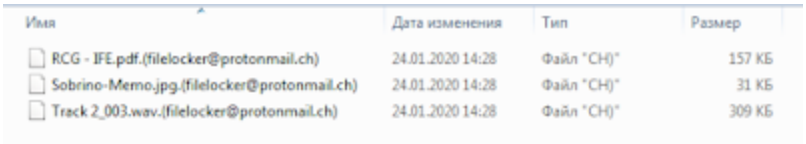
Результаты анализов:
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>** **VT>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
꩜ JOE Sandbox analysis >>

Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Обновление от 22 января 2020:
Топик на форуме >>
Расширение: **.(filelocker@protonmail.ch)**



Имя	Дата изменения	Тип	Размер
RCG - IFE.pdf.(filelocker@protonmail.ch)	24.01.2020 14:28	Файл "CH)"	157 КБ
Sobrino-Memo.jpg.(filelocker@protonmail.ch)	24.01.2020 14:28	Файл "CH)"	31 КБ
Track 2_003.wav.(filelocker@protonmail.ch)	24.01.2020 14:28	Файл "CH)"	309 КБ

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

Внимание!

```
Для зашифрованных файлов есть дешифровщик
Скачать Emsisoft Decrypter для дешифровки >>
Прочтите подробную инструкцию перед запуском.
```

Thanks:

S!Ri, Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples