ChinaJm

Archived: 2026-04-05 16:17:46 UTC

ChinaJm Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES+RSA, а затем требует написать на email вымогателей, чтобы узнать как заплатить выкуп и вернуть файлы. Оригинальное название: в записке не указано. На файле написано: 简易抽奖小程序-SIGN.exe

Обнаружения:
DrWeb -> Trojan.Encoder.30799
BitDefender -> Gen:Variant.Mikey.110458
ESET-NOD32 -> A Variant Of Win32/Filecoder.OAW
Malwarebytes -> ***
Rising -> Trojan.Zudochka!8.106DC (CLOUD)
Symantec -> Downloader
TrendMicro -> TROJ_GEN.R002C0PG320

To AV vendors! Want to be on this list regularly or be higher on the list? Contact me!
AV вендорам! Хотите быть в этом списке регулярно или повыше? Сообщите мне!

© Генеалогия: Barack Obama's EBBV и другие >> ChinaJm > Pojie

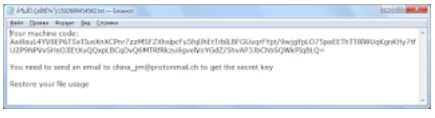
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.China**

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 конец февраля - начало марта 2020 г. Ориентирован на китайскоязычных и англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **Á³ÏµÎÒ,ÇëÎðÉ¾³ý1582689454562.txt**



Содержание записки о выкупе:
Your machine code:
Aai8auL4YV8EP6TSaTIueXnXCPnr7zzMSFZXhslpcFu5fqlJhEtTrbILBFGUvqrFYpt/9wjgYpLO75paEEThTT8lWUqKgnKHy7tfU2P9NPVvSHsOJIEt
You need to send an email to china_jm@protonmail.ch to get the secret key
Restore your file usage

Перевод записки на русский язык:
Код вашей машины:
Aai8auL4YV8EP6TSaTIueXnXCPnr7zzMSFZXhslpcFu5fqlJhEtTrbILBFGUvqrFYpt/9wjgYpLO75paEEThTT8lWUqKgnKHy7tfU2P9NPVvSHsOJIEt
Вам нужно отправить email на адрес china_jm@protonmail.ch, чтобы получить секретный ключ
Вернуть использование вашего файла

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**.

➤ По данным сервиса IntezerAnalyze содержит код майнера криптовалюты CoinMiner, значит шифровальщик может быть прикрытием установки майнера.

➤ Использует чужие электронные подписи для исполняемого файла.

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:
简易抽奖小程序-SIGN.exe
Á³ÏµÎÒ,ÇëÎðÉ¾³ý1582689454562.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\Users\User\AppData\Local\Temp\简易抽奖小程序-SIGN.exe

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

Мьютексы:
См. ниже результаты анализов.

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

Результаты анализов:
🔻 **Triage analysis >>**
Ⓗ **Hybrid analysis >>**
Σ VirusTotal analysis >>
🐞 **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 ===

Ещё не было обновлений этого варианта.

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

Read to links:
Tweet on Twitter + Tweet + myTweet
ID Ransomware (ID as ChinaJm)
Write-up, Topic of Support
*

Thanks:
dnwls0719, Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples
