Cuba

Cuba Ransomware

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные корпоративной сети с помощью AES, а затем требует выкуп в # BTC, чтобы вернуть файлы. Оригинальное название: в записке не указано. На файле написано: нет данных.

Обнаружения:
DrWeb -> Trojan.Encoder.30823, Trojan.Encoder.30979, Trojan.Encoder.31964, Trojan.Encoder.33101
BitDefender -> Trojan.GenericKD.32976553, Gen:Variant.Johnnie.215261
Avira (no cloud) -> TR/FileCoder.xacls, HEUR/AGEN.1041333
ESET-NOD32 -> Win32/Filecoder.OAE
McAfee -> RDN/Generic.dx
Rising -> Ransom.Gen!8.DE83 (CLOUD), Trojan.Filecoder!8.68 (CLOUD)
Tencent -> Win32.Trojan.Gen.Hryu, Win32.Trojan.Gen.Pdlp
VBA32 -> BScope.TrojanDownloader.Deyma
Symantec -> Downloader

© Генеалогия: Buran ? >> Cuba

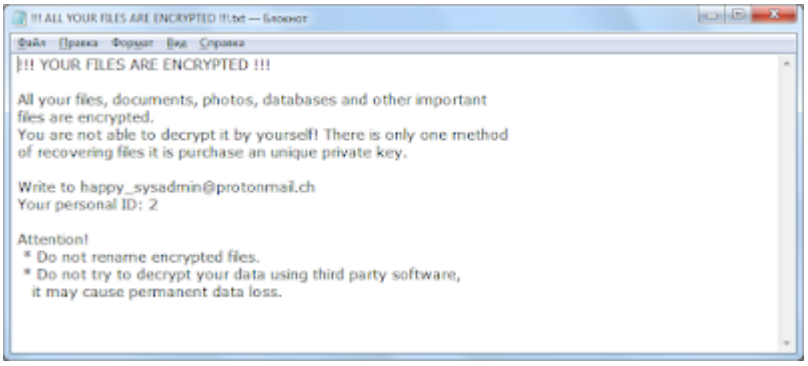
Изображение — только логотип статьи

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

Также используется файловый маркер **FIDEL.CA** **Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Ранняя активность этого крипто-вымогателя пришлась на конец декабря 2019 - начало 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT**



Содержание записки о выкупе:

!!! YOUR FILES ARE ENCRYPTED !!!
All your files, documents, photos, databases and other important
files are encrypted.
You are not able to decrypt it by yourself! There is only one method
of recovering files it is purchase an unique private key.
Write to happy_sysadmin@protonmail.ch
Your personal ID: 2
Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software,
it may cause permanent data loss.

Перевод записки на русский язык:

!!! Ваши файлы зашифрованы !!!
Все ваши файлы, документы, фотографии, базы данных и другие важные файлы зашифрованы.
Вы не можете расшифровать это сами! Есть только один способ восстановления файлов - это покупка уникального закрытого ключа.
Пишите на адрес happy_sysadmin@protonmail.ch
Ваш личный ID: 2
Внимание!
* Не переименовывайте зашифрованные файлы.
* Не пытайтесь расшифровать ваши данные с помощью сторонних программ,

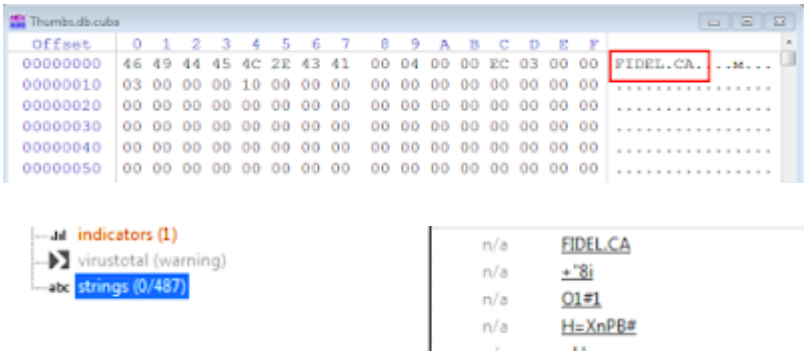
это может вызвать постоянную потерю данных.

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**.

➤ Скриншоты демонстрируют заголовок **FIDEL.CA** в коде зашифрованных файлов. Без сомнения вымогатели использовали это известное имя неслучайно. Это могло быть сделано ради эпатажа.



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:
!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->

Записи реестра, связанные с этим Ransomware:

См. ниже результаты анализов.

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

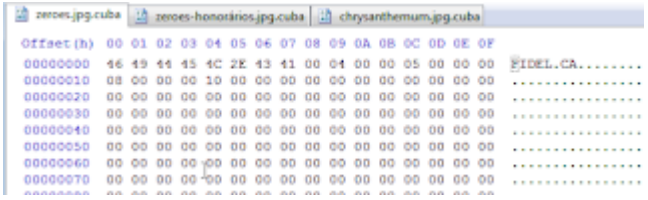
Результаты анализов (из первого обновления ниже):
Ⓗ **Hybrid analysis >>**
Σ **VirusTotal analysis >>**
🐞 **Intezer analysis >>**
⋟ **ANY.RUN analysis >>**
⧖ **VMRay analysis >>**
Ⓥ VirusBay samples >>
⩓ MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

Степень распространённости: **средняя**.
Подробные сведения собираются регулярно. Присылайте образцы.

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

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

Вариант от 22 января 2020:
Расширение: .cuba
Записка: !!FAQ for Decryption!!.txt
Email: iracomp4@protonmail.ch
Результаты анализов: **VT** + **VMR**



➤ Содержание записки:

Good day. All your files are encrypted. Fop decryption contact us.

Write here iracomp4@protonmail.ch

We also inform that your databases, ftp server and file server were downloaded by us to our servers.

* Do not rename encrypted files.

* Do not try to decrypt your data using third party software,

it may cause permanent data loss.

Вариант от 10 февраля 2020:

Сообщение >>

Расширение: .cuba

Записка: !!FAQ for Decryption!!.txt

Email: iracomp2@protonmail.ch

Результаты анализов: **VT** + **VMR**

➤ Обнаружения:

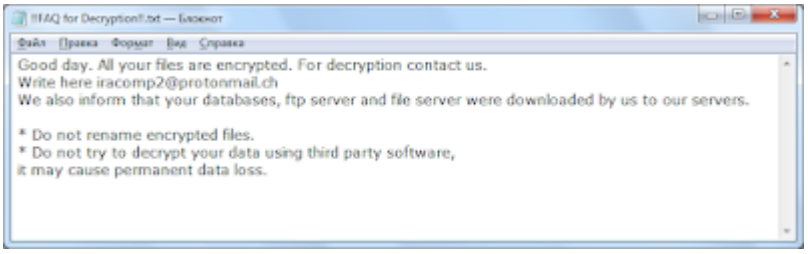
DrWeb -> Trojan.Encoder.30979

BitDefender -> Gen:Variant.Johnnie.215261

Avira (no cloud) -> HEUR/AGEN.1041333

Rising -> Trojan.Filecoder!8.68 (CLOUD)

Tencent -> Win32.Trojan.Gen.Pdlp



➤ Содержание записки:

Good day. All your files are encrypted. For decryption contact us.

Write here iracomp2@protonmail.ch

We also inform that your databases, ftp server and file server were downloaded by us to our servers.

* Do not rename encrypted files.

* Do not try to decrypt your data using third party software,

it may cause permanent data loss.

Вариант от 14 марта 2020:

Расширение: .cuba

Записка: !!FAQ for Decryption!!.txt

➤ Содержание записки:

Good day. All your files are encrypted. For decryption contact us.

Write here iracomp2@protonmail.ch

We also inform that your databases, ftp server and file server were downloaded by us to our servers.

* Do not rename encrypted files.

* Do not try to decrypt your data using third party software,

it may cause permanent data loss.

Вариант от 4 июня 2020:

Расширение: .cuba

Записка: !!FAQ for Decryption!!.txt

Email: mrddnet_support@protonmail.ch

Файл: CC.exe

➤ Содержание записки:

Good day. All your files are encrypted. For decryption contact us.

Write here mrddnet_support@protonmail.ch

We also inform that your databases, ftp server and file server were downloaded by us to our servers.

* Do not rename encrypted files.

* Do not try to decrypt your data using third party software,

it may cause permanent data loss.

➤ Обнаружения:

DrWeb -> Trojan.Encoder.31964

Avast/AVG -> Win32:Malware-gen

Avira (no cloud) -> TR/AD.ZDlder.wtwnt

BitDefender -> Trojan.GenericKD.43285712

ESET-NOD32 -> A Variant Of Generik.CGSYLIU

Kaspersky -> Trojan-Ransom.Win32.Encoder.jcd

Malwarebytes -> Ransom.Fidel

McAfee -> RDN/Akbot

Microsoft -> Trojan:Win32/CryptInject!MSR

Rising -> Trojan.Kryptik!1.C427 (CLOUD)

Symantec -> ML.Attribute.HighConfidence

Tencent -> Win32.Trojan.Encoder.Eek

TrendMicro -> Possible_SMHPQAKBOTTH

Вариант от 10 июля 2020:

Сообщение >>

Расширение: .cuba

Записка: !!FAQ for Decryption!!.txt

Email: achtung_admin@protonmail.com

Файл EXE: kalt.exe

Мьютекс: Global\SvcctrlStartEvent_A3752DX

➤ Содержание записки:

Good day. All your files are encrypted. For decryption contact us.

Write here achtung_admin@protonmail.com

We also inform that your databases, ftp server and file server were downloaded by us to our servers.

* Do not rename encrypted files.

* Do not try to decrypt your data using third party software,

it may cause permanent data loss.

Результаты анализов: **VT** + **IA** + **HA** + **TG**

➤ Обнаружения:

DrWeb -> Trojan.MulDrop4.25343

BitDefender -> Gen:Heur.Mint.Titirez.1.23

ESET-NOD32 -> A Variant Of Win32/Kryptik.HEPB

Kaspersky -> Trojan-Ransom.Win32.Gen.xpi

Malwarebytes -> Trojan.MalPack.GS

Microsoft -> Trojan:Win32/Ymacco.AAE9

Rising -> Ransom.Gen!8.DE83 (CLOUD)
Symantec -> ML.Attribute.HighConfidence
TrendMicro -> Ransom_Gen.R011C0GG820

Вариант от 3 августа 2020:

Сообщение >>

Расширение: .cuba

Email: aam_sysadmin@protonmail.com

Результаты анализов: **VT** + **IA** + **TG**

➤ Содержание записки:

Good day. All your files are encrypted. For decryption contact us.
Write here aam_sysadmin@protonmail.com
We also inform that your databases, ftp server and file server were downloaded by us to our servers.
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software,
it may cause permanent data loss.

Вариант от 13 ноября 2020:

Расширение: .cuba

Записка: !!FAQ for Decryption!!.txt

Email: helpadmin2@protonmail.com, helpadmin2@cock.li

Результаты анализов: **VT** + **IA** + **VMR**

Email-адреса других вариантов:

under_amur@protonmail.ch

fedelsupportagent@cock.li

admin@cuba-supp.com

cuba_support@exploit.im

=== 2021 ===

Вариант от 20 января 2021:

Расширение: .cuba

Записка: !!FAQ for Decryption!!.txt

Email: LR_FWS_H2M_ET@protonmail.ch

Tor-URL: http://cuba4mp6ximo2zlo.onion/

➤ Содержание записки:

Good day. All your files are encrypted. For decryption contact us.

Write here LR_FWS_H2M_ET@protonmail.ch

We also inform that your databases, ftp server and file server were downloaded by us to our servers.

Check our platform: http://cuba4mp6ximo2zlo.onion/

* Do not rename encrypted files.

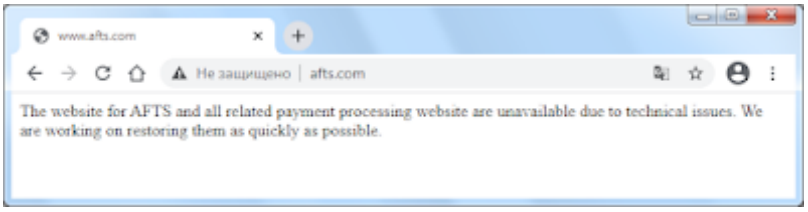
* Do not try to decrypt your data using third party software,

it may cause permanent data loss.

Вымогатели создали сайт, использующий фотографии Фиделя Кастро.

Обновление от 18 февраля 2021:

Атака Cuba Ransomware на широко используемую в США службу автоматического перевода средств (ATFS) стала причиной официальных уведомлений об утечке данных из многих городов и агентств в Калифорнии и Вашингтоне (США). Эти города, использующие AFTS для обработки платежей или проверки адресов, вынуждены были раскрыть потенциальные утечки данных. AFTS находится в Сиэтле, штат Вашингтон. Их сайт до сих пор в дауне.



Ниже мы перечислим некоторые города и агентства, которые выпустили уведомление об утечке данных. Вероятность того, что их будет больше, очень велика. Вот этот список:

Департамент автотранспортных средств Калифорнии

Город Киркленд, Вашингтон

Город Линвуд, Вашингтон

Город Монро, Вашингтон

Город Сиэтл, Вашингтон

Компания водоснабжения в Лейквуде, Вашингтон

Пристань в Эверетте, Вашингтон

и другие.

=== 2022 ===

Вариант от 7 февраля 2022:

Расширение: .cuba

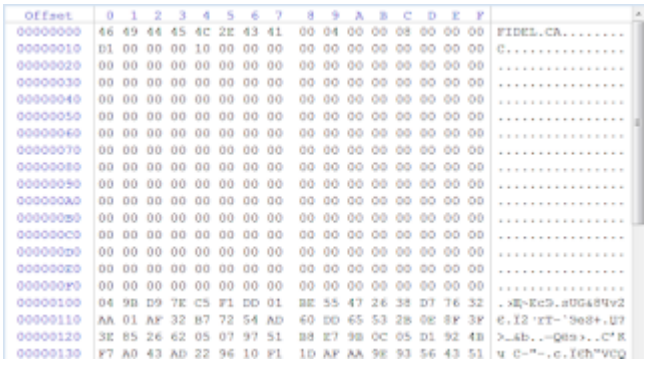
Записка: !! READ ME !!.txt

Email: belingmor@cock.li, admin@cuba-supp.com

Jabber: cuba_support@exploit.im

Tor-URL: hxxx://cuba4ikm4jakjgmkezytyawtdgr2xymvy6nvzgw5cglswg3si76icnqd.onion/

Результаты анализов: **VT** + **AR**



Обновления мая-июня 2022:

Обновление 1 декабря 2022:

ФБР: cuba Ransomware получила 60 миллионов долларов от более чем 100 пострадавших.

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

Read to links:
myMessage + Message
ID Ransomware (ID as Cuba)
Write-up, Topic of Support
*

Thanks:
Andrew Ivanov (author), Michael Gillespie
quietman7, sayso, Dmitry Bestuzhev
Marc Rivero López, xiaopao
to the victims who sent the samples
