SilentDeath

id-ransomware.blogspot.com/2020/07/silentdeath-ransomware.html

SilentDeath Ransomware

(шифровальщик-вымогатель) (первоисточник)
Translation into English

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

Обнаружения:
DrWeb ->
BitDefender ->
ALYac ->
Avira (no cloud) ->
ESET-NOD32 ->
Malwarebytes ->
Rising ->
Symantec ->
TrendMicro ->

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: ??? >> SilentDeath

Изображение — логотип статьи

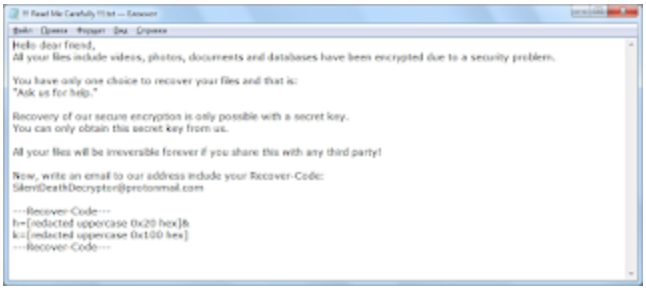
К зашифрованным файлам добавляется расширение: **.SilentDeath**

Этимология названия:
Silent Death ("Тихая смерть") — это название известной игры от Iron Crown Enterprise с космическими битвами.

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 июля 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **!!! Read Me Carefully !!!.txt**



Содержание записки о выкупе:
Hello dear friend,
All your files include videos, photos, documents and databases have been encrypted due to a security problem.
You have only one choice to recover your files and that is:
"Ask us for help."

Recovery of our secure encryption is only possible with a secret key.
You can only obtain this secret key from us.
All your files will be irreversible forever if you share this with any third party!
Now, write an email to our address include your Recover-Code:
SilentDeathDecryptor@protonmail.com
---Recover-Code---
h=[redacted uppercase 0x20 hex]&
k=[redacted uppercase 0x100 hex]
---Recover-Code---

Перевод записки на русский язык:
Здравствуй, дорогой друг,
Все твои файлы, включая видео, фотографии, документы и базы данных, зашифрованы из-за проблем с безопасностью.
У тебя есть только один шанс восстановить твои файлы:
"Просите у нас помощь".
Восстановить наше безопасное шифрование можно только с секретным ключом.
Вы можете получить этот секретный ключ только от нас.
Все ваши файлы будут необратимыми навсегда, если вы поделитесь этим с какой-либо третьей стороной!
Теперь напишите письмо на наш адрес, включив свой код восстановления:
SilentDeathDecryptor@protonmail.com
---Recover-Code---
h=[знаки в верхнем регистре 0x20 hex]&
k=[знаки в верхнем регистре 0x100 hex]
---Recover-Code---

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:
!!! Read Me Carefully !!!.txt - название файла с требованием выкупа
<random>.exe - случайное название вредоносного файла

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

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

Мьютексы:
См. ниже результаты анализов.

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

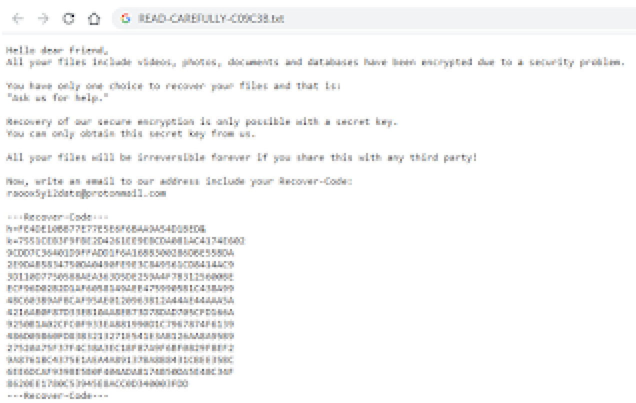
Результаты анализов:
Ⓗ Hybrid analysis >>
Σ VirusTotal analysis >>
🐞 Intezer analysis >>
⋟ ANY.RUN analysis >>
⧖ VMRay analysis >>
Ⓥ VirusBay samples >>
 MalShare samples >>
👽 AlienVault analysis >>
🔃 CAPE Sandbox analysis >>
⟲ JOE Sandbox analysis >>

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

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

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

Вариант от 7 сентября 2020:
Расширение: .SilentDeath
Записка: READ-CAREFULLY-C09C3B.txt
Email: raoox5y12date@protonmail.com


Hello dear friend,
All your files include videos, photos, documents and databases have been encrypted due to a security problem.

You have only one choice to recover your files and that is:
"Ask us for help."

Recovery of our secure encryption is only possible with a secret key.
You can only obtain this secret key from us.

All your files will be irreversible forever if you share this with any third party!

Now, write an email to our address include your Recover-Code:
raoox5y12date@protonmail.com

---Recover-Code---
[illegible]
---Recover-Code---

➤ Содержание записки:

You have only one choice to recover your files and that is:
"Ask us for help."
Recovery of our secure encryption is only possible with a secret key.
You can only obtain this secret key from us.
All your files will be irreversible forever if you share this with any third party!
Now, write an email to our address include your Recover-Code:
raoox5y12date@protonmail.com
---Recover-Code---
h=FE4DE10BB77E77E5E6F6BAA9A54D1BED&
k=7551CEB3F9FBE2D4261EE9EBCDA081AC4174E602
***
---Recover-Code---

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

Thanks:

Michael Gillespie
Andrew Ivanov (author)
***
to the victims who sent the samples