SepSys

SepSys Ransomware

(шифровальщик-вымогатель) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные пользователей с помощью AES, а затем требует выкуп в 100$ в BTC, чтобы вернуть файлы. Оригинальное название: sepSys. На файле написано: нет данных. Получатель криптовалюты: Silicon Venom.

Обнаружения:
DrWeb -> Trojan.Encoder.31095
BitDefender -> Trojan.GenericKD.42682853, Gen:Variant.Razy.618273
Emsisoft -> Trojan-Ransom.SepSys (A)
ESET-NOD32 -> Win64/Filecoder.BM, A Variant Of Win64/Filecoder.BM
Fortinet -> W32/Ransom.FVG!tr
Kaspersky -> Trojan.Win32.Zudochka.ebg
Malwarebytes -> Ransom.SepSys
Microsoft -> Ransom:Win32/SepSys!MTB
Qihoo-360 -> Trojan.Generic
Rising -> Ransom.SepSys!1.C30A (CLOUD)
TrendMicro -> Ransom.Win64.SEPSYS.A, Ransom_Filecoder.R002C0DC520, Ransom_Henasome.R002C0DDB20

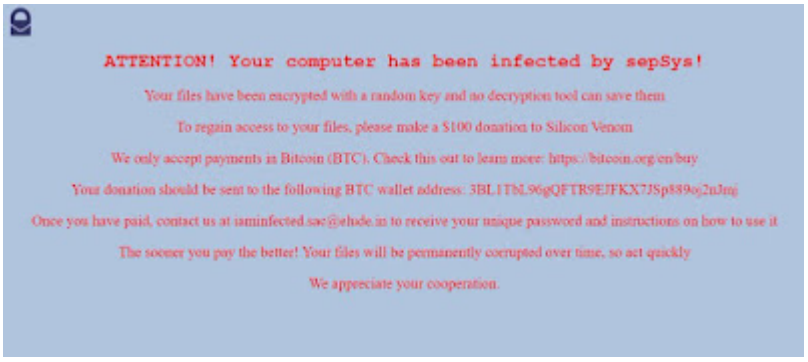
© Генеалогия: ??? > SepSys > Silvertor

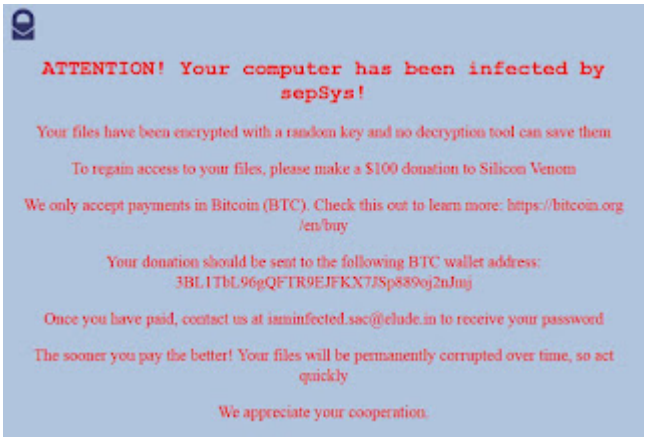
Изображение — логотип статьи

К зашифрованным файлам добавляется расширение: **.sepsys** **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 вторую половину февраля 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **README.html**





Содержание записки о выкупе:
ATTENTION! Your computer has been infected by sepSys!
Your files have been encrypted with a random key and no decryption tool can save them
To regain access to your files, please make a $100 donation to Silicon Venom
We only accept payments in Bitcoin (BTC). Check this out to learn more: https://bitcoin.org/en/buy
Your donation should be sent to the following BTC wallet address: 3BL1TbL96gQFTR9EJFKX7JSp889oj2nJmj
Once you have paid, contact us at iaminfected.sac@elude.in to receive your unique password and instructions on how to use it
The sooner you pay the better! Your files will be permanently corrupted over time, so act quickly

We appreciate your cooperation.

Перевод записки на русский язык:
ВНИМАНИЕ! Ваш компьютер был заражен sepSys!
Ваши файлы зашифрованы случайным ключом, и никакой инструмент расшифровки не может их сохранить
Чтобы вернуть доступ к вашим файлам, пожертвуйте 100$ на Silicon Venom
Мы принимаем платежи только в биткойнах (BTC). Проверьте это, чтобы узнать больше: https://bitcoin.org/en/buy
Ваше пожертвование должно быть отправлено на следующий адрес BTC-кошелька: 3BL1TbL96gQFTR9EJFKX7JSp889oj2nJmj
После оплаты пишите нам на адрес iaminfected.sac@elude.in, чтобы получить уникальный пароль и инструкции по его использованию.
Чем раньше вы заплатите, тем лучше! Ваши файлы будут повреждены, поэтому действуйте быстро
Мы ценим ваше сотрудничество.

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**.

➤ Использует Windows PowerShell для атаки. Это в очередной раз подтверждает вредоносность этой технологии Microsoft.

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:
README.html

destructy-1.0.exe
<random>.exe - случайное название вредоносного файла

Расположения:
\Desktop\ ->
\User_folders\ ->
\%TEMP%\ ->
C:\ProgramData\README.html

Оригинальное название проекта:
C:\Users\tinop\Documents\Experiments\virusTests\sepSys1-0\target\debug\deps\sepSys1_0-ebd9526c88434a09.pdb

Прочее:
Desktoppasswordhere.txtajsndhcuyofklqwghftdgcbsmdfkiops.sepsyssepsyssrc\main.rs

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

Сетевые подключения и связи:
URL - IP: http://www.myip.ch/
URL - icon: https://2no.co/3mAp64
Email: iaminfected.sac@elude.in
BTC: 3BL1TbL96gQFTR9EJFKX7JSp889oj2nJmj
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 ===

SepSys Ransomware - февраль 2020

Silvertor Ransomware - июль 2020

RedRoman Ransomware - ноябрь 2020

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

Обновление от 25 апреля 2020:
Пост в Твиттере >>
Расширение: .sepsys
Выдает себя за SMBGhoster_1.2.exe
Результаты анализов: **VT**

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

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

Thanks:
GrujaRS, MalwareHunterTeam
Andrew Ivanov (author)

```
***
to the victims who sent the samples
```
