Mespinoza, Pysa

id-ransomware.blogspot.com/2019/10/mespinoza-ransomware.html

Mespinoza Ransomware

Pysa Ransomware

Mespinoza (Pysa) Doxware

Mespinoza (Pysa) Hand-Ransomware

(шифровальщик-вымогатель, публикатор) (первоисточник)
Translation into English

Этот крипто-вымогатель шифрует данные на ПК бизнес-пользователей и компаний с помощью AES, а затем требует написать на email вымогателей, чтобы узнать как заплатить выкуп и вернуть файлы. Оригинальное название: в записке не указано. На файле написано: 1.exe, 51.exe или что-то еще.

Вымогатели, распространяющие Mespinoza-Pysa, стали угрожать опубликовать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — публикатор). Как известно из других Ransomware, для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов. Об этих акциях вымогателей сообщалось в СМИ. На момент публикации статьи, не было известно о публикациях украденных данных, вымогатели только угрожали.

Обнаружения:
DrWeb -> Trojan.Encoder.30075, Trojan.Encoder.30386, Trojan.Encoder.30815
BitDefender -> Gen:Heur.Ransom.REntS.Gen.1, Gen:Variant.Ransom.Dee.1
Kaspersky -> UDS:DangerousObject.Multi.Generic, HEUR:Trojan-Ransom.Win32.Encoder.gen

TrendMicro -> Ransom.Win32.LOCKERGOGA.AF, Ransom.Win32.MESPINOZA.A

© Генеалогия: Vurten > Mespinoza, Pysa

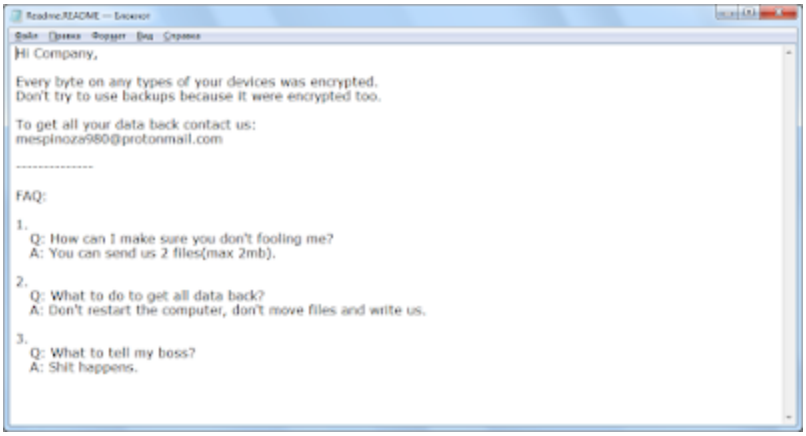
Изображение — логотип статьи

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

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 октябрь 2019 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

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


Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
mespinoza980@protonmail.com

FAQ:

1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).

2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.

3.
Q: What to tell my boss?
A: Shit happens.

Содержание записки о выкупе:
Hi Company,
Every byte on any types of your devices was encrypted.

Don't try to use backups because it were encrypted too.
To get all your data back contact us:
mespinoza980@protonmail.com

FAQ:
1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).
2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.
3.
Q: What to tell my boss?
A: Shit happens.

Перевод записки на русский язык:
Привет компания,
Каждый байт на любых типах ваших устройств был зашифрован.
Не пытайтесь использовать резервные копии, потому что они тоже зашифрованы.
Чтобы получить все свои данные, свяжитесь с нами:
mespinoza980@protonmail.com

ВОПРОСЫ-ОТВЕТЫ:
1.
Q: Как я могу убедиться, что ты не обманешь меня?
A: Вы можете отправить нам 2 файла (не более 2 МБ).
2.
B: Что нужно сделать, чтобы вернуть все данные?
A: Не перезагружайте компьютер, не перемещайте файлы и пишите нам.
3.
Q: Что сказать моему боссу?
A: Дерьмо случается.

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**.

➤ Может останавливать процессы антивирусных программ и Windows Defender, чтобы потом беспрепятственно шифровать файлы.

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.README
<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: mespinoza980@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 >>

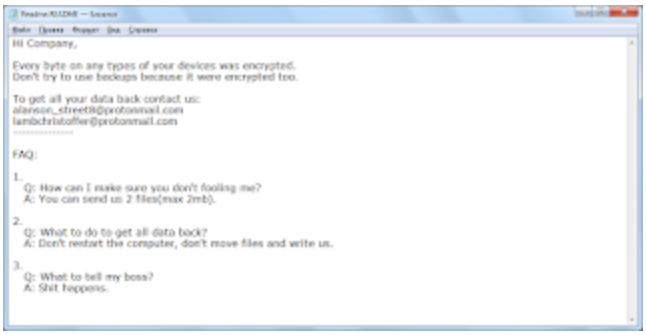
Степень распространённости: низкая.
Подробные сведения собираются регулярно. Присылайте образцы.

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

Vurten Ransomware - апрель 2018
Mespinoza Ransomware - октябрь 2019
Pysa Ransomware - декабрь 2019 - январь 2020 и позже

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

Вариант от 10 ноября 2019:
DrWeb -> Trojan.Encoder.30075
Пост в Твиттере >>
Топик на форуме >>
Расширение: .locked
Записка: Readme.README
Email: alanson_street8@protonmail.com, lambchristoffer@protonmail.com
Файлы: 51.exe %supdater.bat
Результаты анализов: **VT** + **HA** + **IA** + **AR**

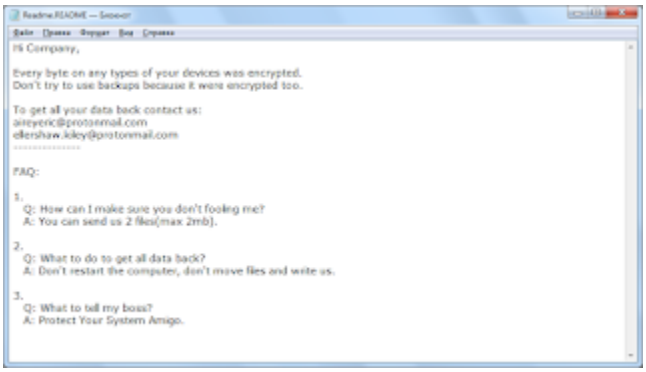


➤ Содержание записки:
Hi Company,
Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
alanson_street8@protonmail.com
lambchristoffer@protonmail.com

FAQ:
1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).
2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.
3.
Q: What to tell my boss?
A: Shit happens.

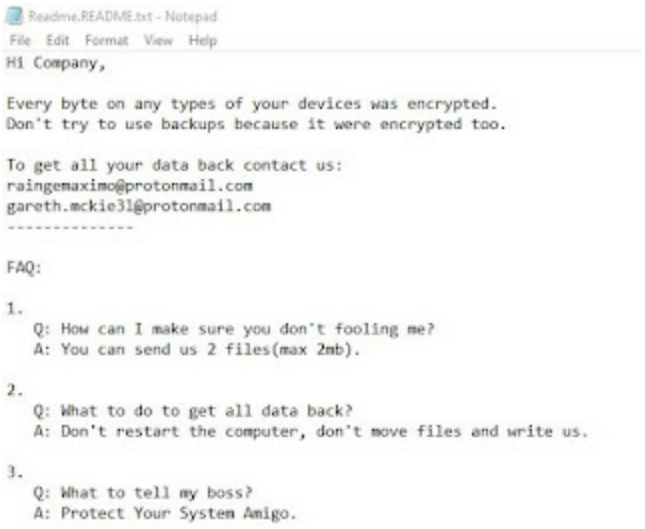
Вариант от 14 декабря 2019:
DrWeb -> Trojan.Encoder.30386
Пост в Твиттере >>
Расширение: **.pysa**
Этимология для PYSA: "**P**rotect **Y**our **S**ystem **A**migo".
Записка: Readme.README
Email: aireyeric@protonmail.com, ellershaw.kiley@protonmail.com
Результаты анализов: **VT** + **AR**



➤ Содержание записки:
Hi Company,
Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.
To get all your data back contact us:
aireyeric@protonmail.com
ellershaw.kiley@protonmail.com

FAQ:
1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).
2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.
3.
Q: What to tell my boss?
A: Protect Your System Amigo.

Вариант от 22 января 2020:
DrWeb -> Trojan.Encoder.30815
Пост в Твиттере >>
Расширение: .pysa
Записка: Readme.README
Email: raingemaximo@protonmail.com
gareth.mckie31@protonmail.com
Мьютекс: **Pysa**
Результаты анализов: **VT** + **VMR**
Этот вариант распространяется с помощью грубых атак на консоли управления и аккаунты Active Directory и PowerShell-скриптов.
код Pysa Ransomware Ransom.Win32.LOCKERGOGA.AF, довольно специфичный и короткий по сравнению с другими вымогателями.


Readme.README.txt - Notepad
File Edit Format View Help
Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
raingemaximo@protonmail.com
gareth.mckie31@protonmail.com

FAQ:

1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).

2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.

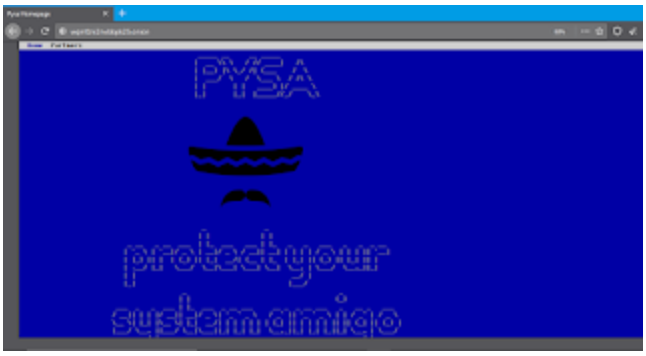
3.
Q: What to tell my boss?
A: Protect Your System Amigo.

Вариант от 18 марта 2020 года:
Расширение: **.newversion**

Фактически обновленный вариант Pysa Ransomware, который был представлен ранее - в конце декабря 2019 и в январе 2020.
Некоторые подробности см. в статье >>

=== 2021 ===

Вариант от 5 января 2021:
DrWeb -> Trojan.Encoder.32290
Сообщение >>
Расширение: **.pysa**
Записка: Readme.README.txt
Дата компиляции: 1 декабря 2020.
Результаты анализов: **VT** + **HA**



С марта 2020 участились атаки вымогателей с использованием Pysa Ransomware на американские и канадские правительственные учреждения, образовательные учреждения, частные компании и сектор здравоохранения. По последним данным,

вымогатели специально нацелены на высшее образование и общеобразовательные школы K-12 (название включает 12 лет начального и среднего образования).
ФБР рекомендует не выплачивать выкуп вымогателям, поскольку уступка их требованиям, скорее всего, профинансирует их будущие атаки в этой и других областях.
ФБР понимает ущерб, который образовательные учреждения могут понести после таких атак, и призывает их как можно скорее сообщать об атаках в местное отделение ФБР или в Центр жалоб на преступления в Интернете (IC3), независимо от решения платить выкуп или нет.

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

Read to links:

Tweet on Twitter: **myTweet**
ID Ransomware (ID as Mespinoza)
Write-up, **Topic of Support**
*

Thanks:

Michael Gillespie, quietman7
Andrew Ivanov (author)
GrujaRS
to the victims who sent the samples