

## Another one for the collection - mespinoza (pysa) ransomware

By f0wL

Published: 2019-12-14 · Archived: 2026-04-05 21:05:33 UTC

Back in October of 2019 the Mespinoza Ransomware family first surfaced via Malspam. On the 14th of December it returned with a new extension .pysa so let's see if any changes have been made.

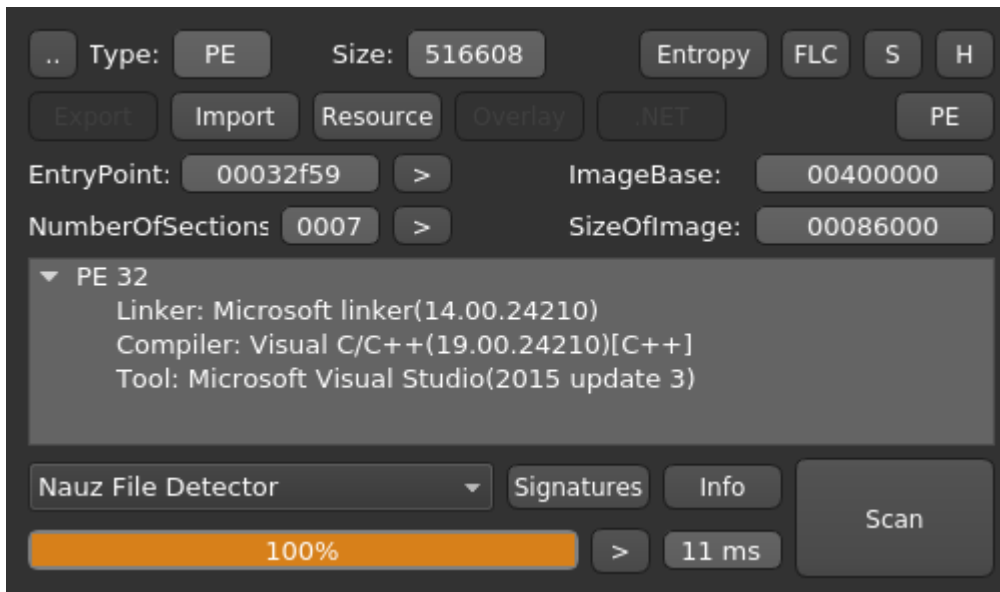
Fun Fact: The Extension "pysa" is probably derived from the Zanzibari Coin with the same name. Apparently it's quite popular with collectors. But enough of the pocket change, so let me put my two cents in on this sample :D



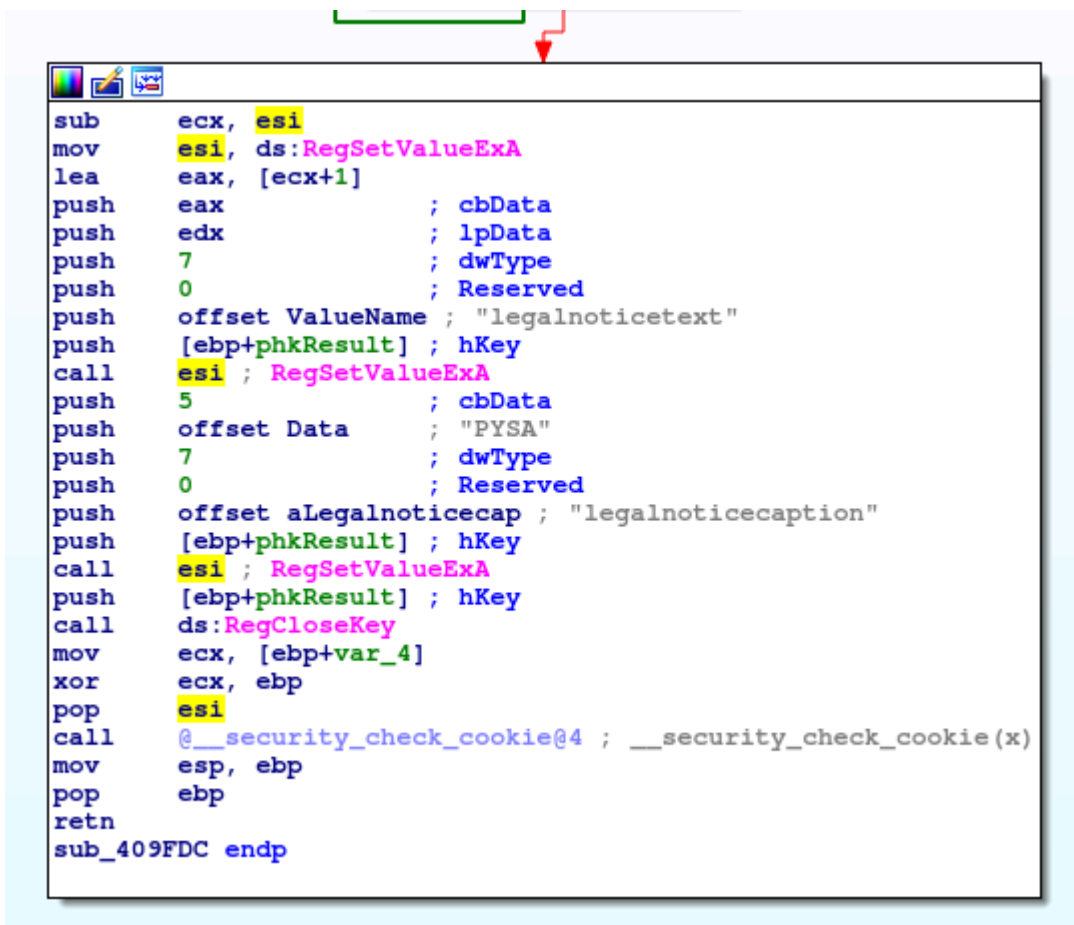
***A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f\$cking careful. Also check with your local laws as owning malware binaries/sources might be illegal depending on where you live.***

Mespinoza (.pysa) @ [AnyRun](#) | [VirusTotal](#) | [HybridAnalysis](#) --> sha256  
a18c85399cd1ec3f1ec85cd66ff2e97a0dcf7ccb17ecf697a5376da8eda4d327

As always: Running Detect it easy on the executable:



One of the first things it will do is modify the SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System Registry Key to set the following values. Unfortunately I couldn't confirm this action in a sandbox with RegShot yet.



To retain basic functions of the Operating System Mespinoza will spare certain directories related directly to Windows and critical files.

```
push edi
push eax
lea eax, [ebp+var_1004]
mov [ebp+var_127C], offset aWindows ; ":\Windows\"
push 400h
push eax
mov [ebp+var_1278], offset aBoot ; "\\Boot\"
mov [ebp+var_1274], offset aBootsect ; "\\BOOTSECT"
mov [ebp+var_1270], offset aPagefile ; "\\pagefile"
mov [ebp+var_126C], offset aSystemVolumeIn ; "\\System Volume Information\"
mov [ebp+var_1268], offset aBootmgr ; "bootmgr"
mov [ebp+var_1264], offset aRecovery ; "\\Recovery"
mov [ebp+var_1260], offset aMicrosoft ; "\\Microsoft"
call sub_43F351
lea eax, [ebp+var_1004]
push eax
lea eax, [ebp+FileName]
push offset aS ; "%s\*.*)"
push eax ; LPWSTR
call ds:wsprintfW
add esp, 18h
lea eax, [ebp+FindFileData]
push eax ; lpFindFileData
lea eax, [ebp+FileName]
push eax ; lpFileName
call ds:FindFirstFileW
mov edi, eax
mov [ebp+var_125C], edi
cmp edi, 0FFFFFFFh
jz loc_4096ED
```

```
push ebx
mov ebx, [ebp+arg_4]
push esi
xor esi, esi
mov [ebp+var_1258], esi
```

It will also specifically look for SQL related processes. I will have to confirm this with a debugger, but most of the time database processes are killed by Ransomware to disrupt the service and make the files available for encryption.

```
lea eax, [ebp+FileName]
push offset aSql_0 ; "SQL"
push eax
call sub_435EF8
pop ecx
pop ecx
test eax, eax
jz short loc_4096CC
```

Of course Mespinoza won't stop with the system drive so it will check for connected removable media or shared network drives. *GetDriveTypeW* will tell it which type of media the selected device belongs to.

```
push    104h          ; nBufferLength
mov     [ebp+var_48], 1
call   ds:GetLogicalDriveStringsW
test   eax, eax
jz     loc_408FC4

cmovnb eax, [ebp+lpRootPathName]
push   eax           ; lpRootPathName
call   ds:GetDriveTypeW
cmp    eax, 3
jnz   short loc_408FA2
```

Up until now I have not seen a ransomware sample running *verclsid.exe*, so let's investigate: `{0B2C9183-C9FA-4C53-AE21-C900B0C39965}` corresponds to `C:\Windows\system32\SearchFolder.dll` and `{0C733A8A-2A1C-11CE-ADE5-00AA0044773D}` matches the CLSID of `IDBProperties` which is part of the Microsoft SQL Server.

```
C:\Windows\system32\verclsid.exe" /S /C {0B2C9183-C9FA-4C53-AE21-C900B0C39965} /I {0C733A8A-2A1C-11CE-ADE5-00AA0044773D}
```

After looking at a string dump I found this hex string which is probably the key blob. I'll try to verify this with *x32dbg* later.

```
30820220300D06092A864886F70D01010105000382020D003082020802820201009CC3A0141B5488CD31B7D2DD49F92214830
```

Turns out that the encrypted key is appended to the end of each file affected by the ransomware (which is a common tactic for some strains).

```
000C:E860 DE D2 1B E4 5B 97 49 21 06 AD A0 FA 48 07 C4 F1 P0.ä[.I!..úH.Äñ
000C:E870 1F A5 71 FF D9 33 31 36 37 32 42 33 44 41 45 42 .¥qÿÜ31672B3DAEB
000C:E880 32 43 38 44 33 36 33 39 38 36 42 37 41 38 44 35 2C8D363986B7A8D5
000C:E890 36 45 46 43 43 30 35 33 41 42 45 41 43 43 38 35 6EFCC053ABEACC85
000C:E8A0 31 33 37 34 35 31 33 36 37 32 43 32 45 36 37 41 1374513672C2E67A
000C:E8B0 36 30 37 46 41 34 37 35 41 34 30 41 39 30 37 45 607FA475A40A907E
000C:E8C0 44 39 45 45 32 34 32 44 30 43 46 37 42 35 42 31 D9EE242D0CF7B5B1
000C:E8D0 30 30 44 41 32 30 45 32 41 41 42 36 39 33 34 31 00DA20E2AAB69341
000C:E8E0 34 42 33 46 39 42 39 35 42 31 36 38 33 37 45 35 4B3F9B95B16837E5
000C:E8F0 36 44 32 35 32 38 41 30 42 46 46 32 42 32 30 43 6D2528A0BFF2B20C
000C:E900 41 36 41 32 35 45 32 34 32 33 32 31 38 30 35 31 A6A25E2423218051
000C:E910 45 36 44 37 41 43 46 30 30 44 35 34 30 37 37 30 E6D7ACF00D540770
000C:E920 37 31 31 30 36 37 33 43 46 44 45 41 30 46 32 39 7110673CFDEA0F29
000C:E930 36 34 33 31 33 43 32 31 45 43 37 43 44 36 30 44 64313C21EC7CD60D
000C:E940 38 30 43 30 32 33 46 33 44 35 37 42 42 33 38 41 80C023F3D57BB38A
000C:E950 35 39 32 41 46 46 37 34 45 43 34 39 42 36 32 30 592AFF74EC49B620
000C:E960 45 30 33 39 42 45 46 32 34 41 36 42 35 45 35 38 E039BEF24A6B5E58
000C:E970 32 41 37 45 36 43 43 31 45 38 39 44 30 38 33 42 2A7E6CC1E89D083B
000C:E980 42 46 43 33 43 31 36 46 44 37 44 39 39 45 38 35 BFC3C16FD7D99E85
000C:E990 41 33 44 36 32 42 37 30 44 44 44 33 31 44 31 38 A3D62B70DDD31D18
000C:E9A0 35 34 31 36 33 30 32 43 46 36 43 30 41 34 30 46 5416302CF6C0A40F
000C:E9B0 46 42 36 46 31 35 31 36 30 44 35 30 30 38 41 30 FB6F15160D5008A0
000C:E9C0 37 41 39 37 34 42 35 43 34 44 38 32 33 31 30 35 7A974B5C4D823105
000C:E9D0 38 44 43 31 41 31 45 39 41 30 42 41 44 42 45 42 8DC1A1E9A0BADBEB
000C:E9E0 46 30 32 42 32 43 45 30 33 31 37 45 36 42 37 36 F02B2CE0317E6B76
000C:E9F0 38 36 46 45 39 36 44 43 36 46 34 44 39 34 31 30 86FE96DC6F4D9410
000C:EA00 41 41 44 43 41 44 33 42 44 41 41 44 35 34 44 30 AADCAD3BDAAD54D0

Offset: 000C:F075 Selection: 000C:E875 - 000C:F074 (2,048 bytes)
```

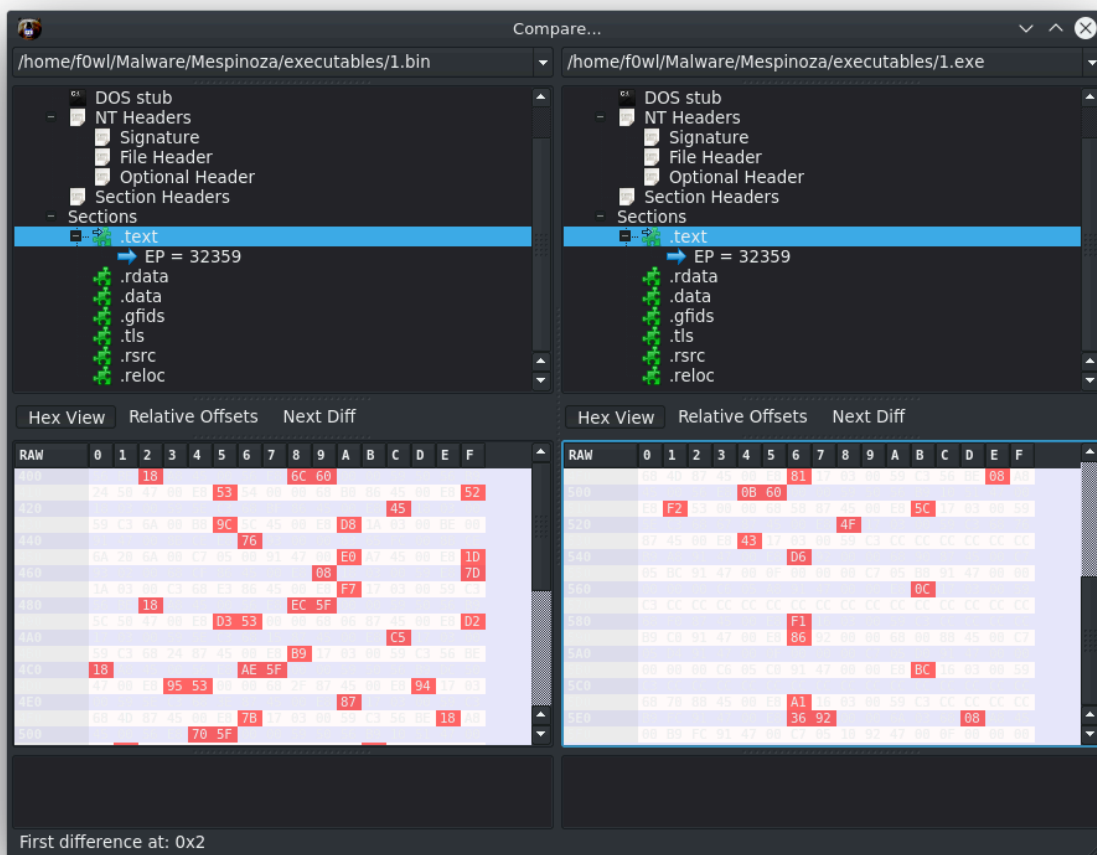
As this article is work in progress I will update it as soon as I can. As I did not see the Malware deleting the Volume Shadow Copies until now, so one option for possible victims would be to run [Photorec](#) or [Recuva](#) to check for recoverable files.

### Update 22.01.2020:

There's a new version of the Mespinoza / .pysa Variant compiled on the 18th of January:

```
Mespinoza (.pysa) @ AnyRun --> `sha256
e9662b468135f758a9487a1be50159ef57f3050b753de2915763b4ed78839ead
```

In the screenshot below you can see a comparison of the old sample (1.exe) and the new one (1.bin). Except for a few minor changes the two samples are mostly identical:



The public Key used by the criminals is still the same (converted from hex to raw, key blob located in the binary):

```
MIICIDANBgkqhkiG9w0BAQEFAAOCAg0AMIICCAKCAgEA6dYN+TogNihncAJNXRhtUeyj7EQ/BIGbupIM
q5PRI3a1+HqMXEk5vdb3NhzFBUoVhY/jTEE71fLTwHM73q9PrgovaYS18HeXZaU+HkqjF70fu4Qf+SDk
oPxcubX4cFYV1r97z9vcFgFehzk+9CofEnHWEo2N656QGRXe00PaJX/riiL672KHZMDNKzfZQnmpMHL+
KzeyJaaPVVz7V9qCckjT+IT26xtG2jY5tggeplLQfB6ExxaoJ1j0GapQMIZ3k6F1AtBmfcNvyu3cW29a
bIOcsu1QRzfq6iSau2xx0ZaRz0l3vgU79PCLtsGw7BNPtKZdDL9dA879aKWLDBIizc3lg4Iphxdf5MOT
mpQR0kst3ky0ieNLIjEayewyRQ788o3qs8k9SS+89CD916AMEVqRcQH8ugBv5ocs0xAf+2bHe13ogIRc
iTz9ALTvTMSqhNptEBP/z+lIhuMTs2MrJRTaQLpVHUilqAcQuLm8AHIYdGmBXEvUqPjRIo+L9Jb+P1XU
cXYHvOZUBV0VFS0oyQeqiBeaYS+PhCV6TmTRHsH/8XkPt/eGxm3Dk4feYNaZ5a9uQKYc9Akt6G0N+P8T
7zobyAWfQNqGFJhklh6JEAJw58XCJNdmETT68kfwQ+XFB4caUHessaJ369lprAj4TjDUFfYkkm74ntG
4nVtL+sCARE===
```

The Ransomnote contents stayed the same, except for the contact email addresses. Here are the contents of 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:

raingemaximo@protonmail.com

gareth.mckie3l@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.

## MITRE ATT&CK

*T1215* --> Kernel Modules and Extensions --> Persistence

*T1045* --> Software Packing --> Defense Evasion

*T1012* --> Query Registry --> Discovery

*T1114* --> Email Collection --> Collection

## IOCs

### Mespinoza (pysa)

1.exe --> SHA256: a18c85399cd1ec3f1ec85cd66ff2e97a0dcf7ccb17ecf697a5376da8eda4d327  
SSDEEP: 12288:aVchT6oi+0e0+0eNhBBhbBpi0Tn5CjG6c4dX0s0jKf:aVc1Jiin5yGpMIj

File size: 504.50 KB

## Associated Files

Readme.README

%temp%\update.bat

## E-Mail Addresses

aireyeric@protonmail[.]com  
ellershaw.kiley@protonmail[.]com

Used in previous campaigns:

mespinoza980@protonmail[.]com  
alanson\_street8@protonmail[.]com  
lambchristoffer@protonmail[.]com

## Ransomnote

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.

---

Source: <https://dissectingmalwa.re/another-one-for-the-collection-mespinoza-pysa-ransomware.html>