A "Project.exe" that should have stayed in a drawer - MZRevenge / MaMo434376

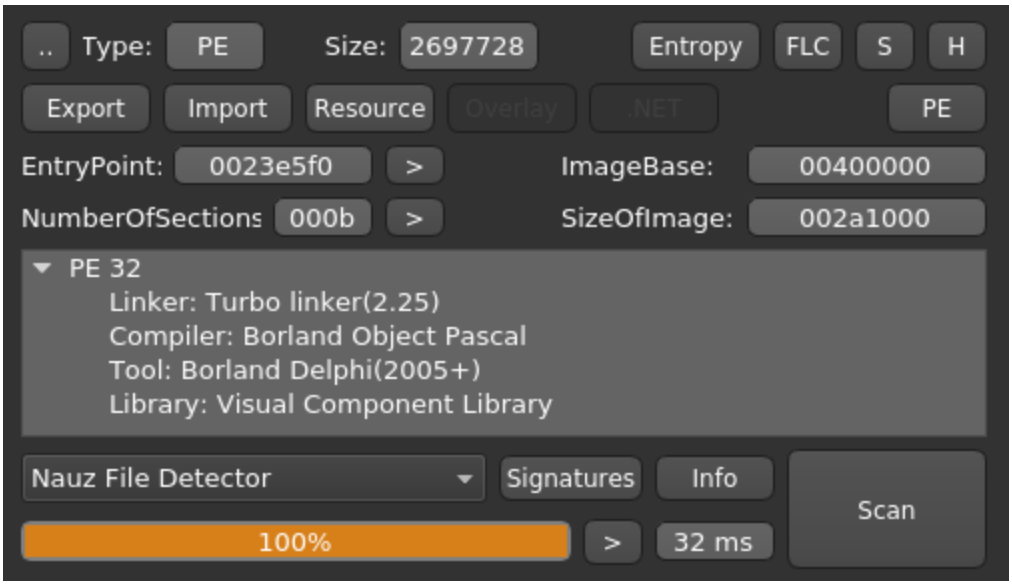
dissectingmalwa.re/a-projectexe-that-should-have-stayed-in-a-drawer-mzrevenge-mamo434376.html

Wed 11 December 2019 in Ransomware

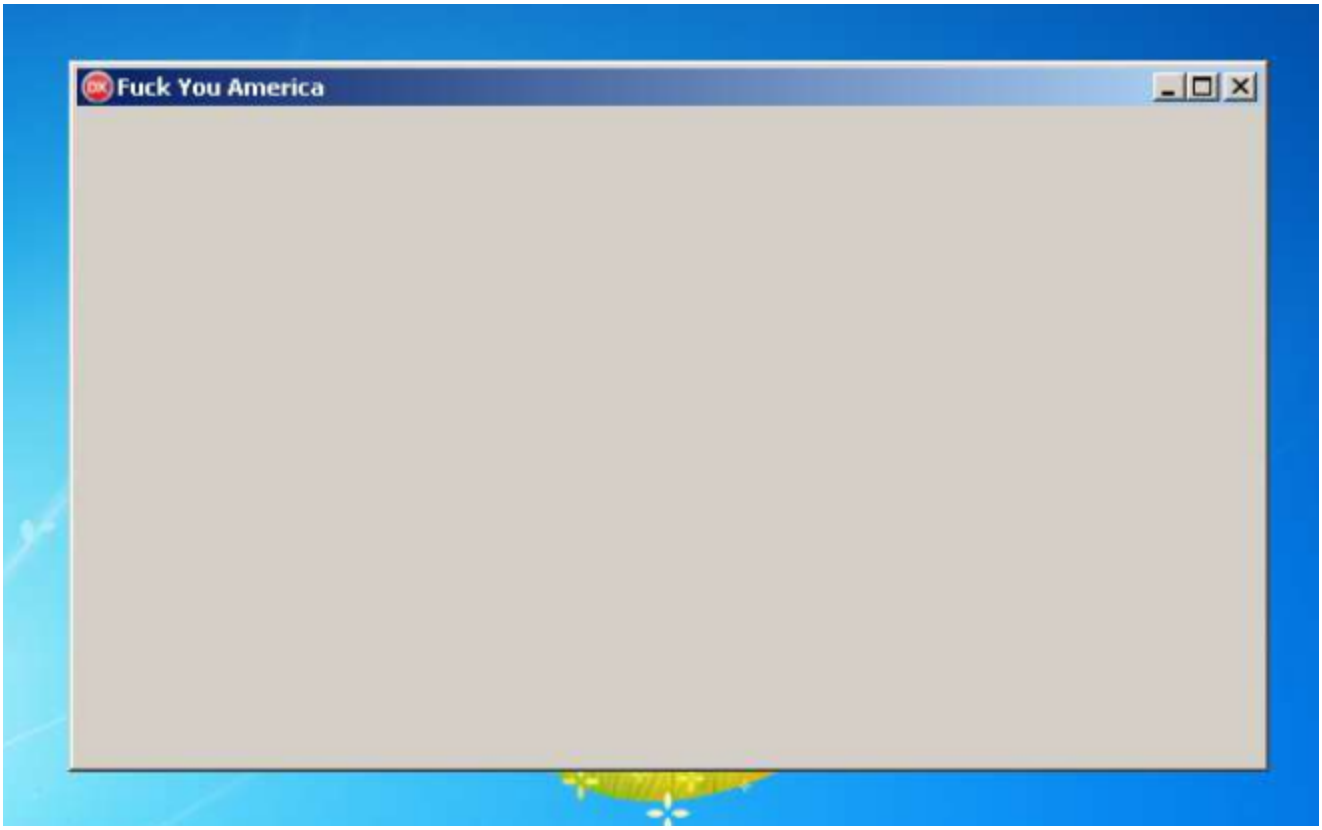
I first read about this strain on Twitter but it didn't seem like a big thing. Turns out I Was wrong: In the last 3 days I collected over 35 samples :O

Searching for "Project.exe" on AnyRun yields more than a healthy list of results all matching this strain.

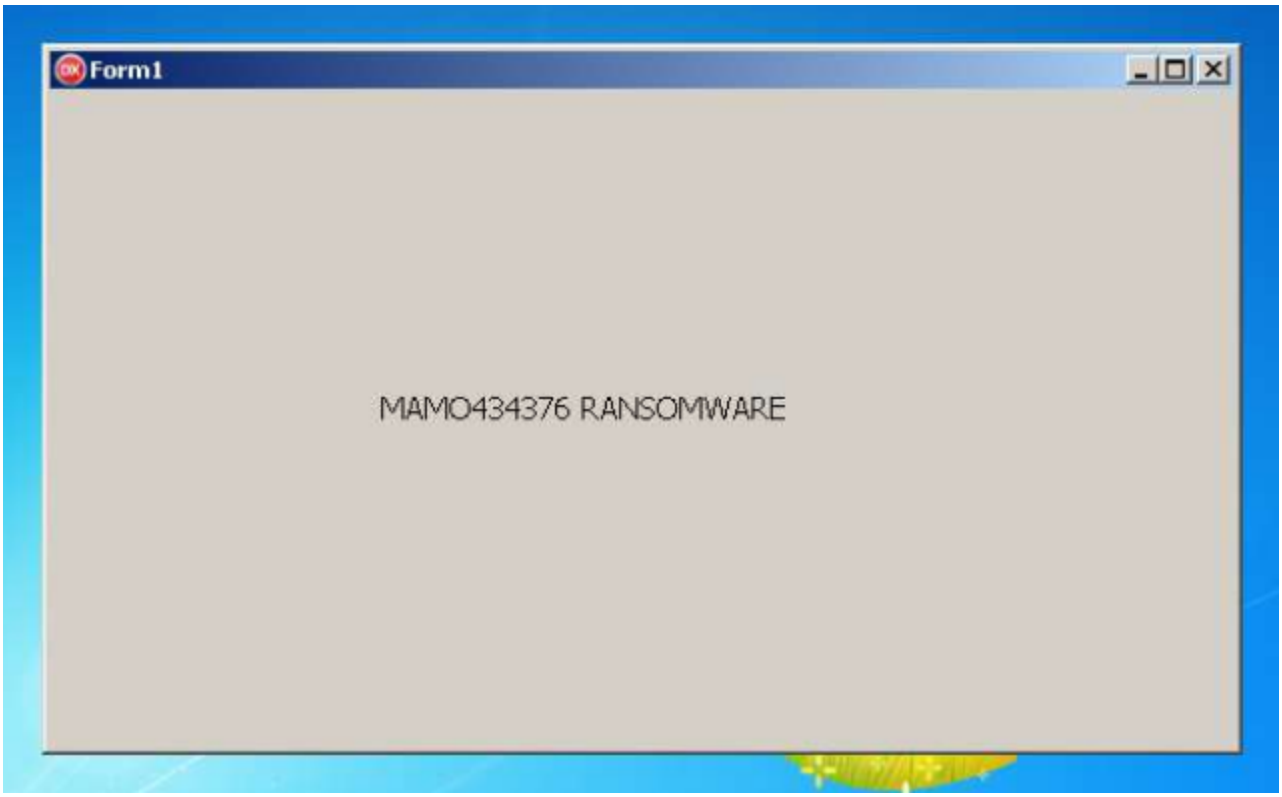
Oh would you look at that: Looks like we have a Borland Delphi application here 🧐



Yep, it's that ugly it definitely is Deplhi :D And the criminals seem to have a very strong opinion about the Land of the Free but no arguments to back it up (since the rest of the form is empty).



The other strain uses a similar Form Window but actually displays its name in there (but they saved on the Window Title).



MZ Revenge and MaMo add these extensions to encrypted files respectively: *.MZ173801* and *.MaMo434376*. It seems to drop the Ransomnotes into the Library Folders, once into %appdata%\Microsoft\Windows\Recent and into the root of every (unmounted) storage device.

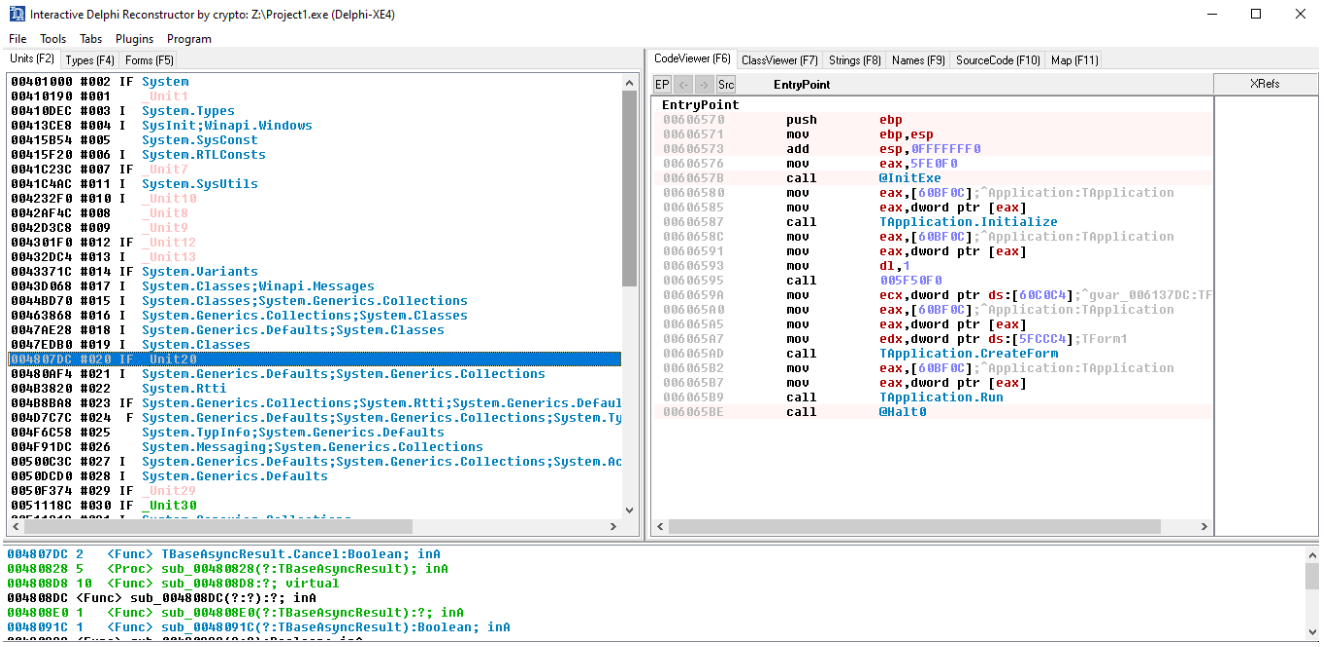
+34944ms	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\Read_ME_PLS.txt	
	Size:	578 b
	MD5:	D352855FB01E04E00E8E6844A0C5301E
+34944ms	C:\Users\admin\Pictures\Read_ME_PLS.txt	
	Size:	578 b
	MD5:	D352855FB01E04E00E8E6844A0C5301E
+34944ms	C:\Users\admin\Music\Read_ME_PLS.txt	
	Size:	578 b
	MD5:	D352855FB01E04E00E8E6844A0C5301E
+34944ms	C:\Users\admin\Videos\Read_ME_PLS.txt	
	Size:	578 b
	MD5:	D352855FB01E04E00E8E6844A0C5301E
+34944ms	C:\Users\admin\Documents\Read_ME_PLS.txt	
	Size:	578 b
	MD5:	D352855FB01E04E00E8E6844A0C5301E
+34944ms	C:\Users\admin\Desktop\Read_ME_PLS.txt	
	Size:	578 b
	MD5:	D352855FB01E04E00E8E6844A0C5301E
+34944ms	C:\Users\admin\Downloads\Read_ME_PLS.txt	
	Size:	578 b
	MD5:	D352855FB01E04E00E8E6844A0C5301E

TIL: The *MZP* Magic tells you that the PE was built in Pascal. Therefore the error message is different as well, normally you would expect to see **This program cannot be run in DOS mode** here.

```
0000:0000 4D 5A 50 00  02 00 00 00  04 00 0F 00  FF FF 00 00  MZP.........ÿÿ..
0000:0010 B8 00 00 00  00 00 00 00  40 00 1A 00  00 00 00 00  ¸.......@.......
0000:0020 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0000:0030 00 00 00 00  00 00 00 00  00 00 00 00  00 01 00 00  ................
0000:0040 BA 10 00 0E  1F B4 09 CD  21 B8 01 4C  CD 21 90 90  º....´.Í!¸.LÍ!..
0000:0050 54 68 69 73  20 70 72 6F  67 72 61 6D  20 6D 75 73  This program mus
0000:0060 74 20 62 65  20 72 75 6E  20 75 6E 64  65 72 20 57  t be run under W
0000:0070 69 6E 33 32  0D 0A 24 37  00 00 00 00  00 00 00 00  in32..$7........
```

Because loading a Delphi executable into IDA or Ghidra can be very painful to look at I'll try out a tool I haven't used before. It is called "Interactive Delphi Reconstructor" (IDR in short) and the setup is trivial. Just clone the Git Repository and download the Knowledge Base files linked at the bottom and extract + paste them into the source folder.

For those playing along at home it should look something like this after the auto-analysis finished:



Looking at the Strings tab I noticed this weird GUID *{43826d1e-e718-42ee-bc55-a1e261c37bfe}*. I'll have to investigate further to say for sure, but looking at this Document for the CIA Vault7 Leaks this might be part of an UAC bypass.

I also grabbed the extension list the ransomware uses. It will target the following extensions:

```
.txt;.doc;.docx;.intex;.pdf;.zip;.rar;.onetoc;.css;.lnk;.xlsx;.ppt;.pptx;.odt;.jpg;.bm
zip;.ace;.arj;.bz2;.myi;.cab;.gzip;.lzh;.tar;.uue;.xz;.z;.001;.mpg;.odg;.core;.crproj;
```

As suspected by @Hildakrypt on Twitter the creators of the turkish KesLan Ransomware might also have built MZ Revenge / MaMo.

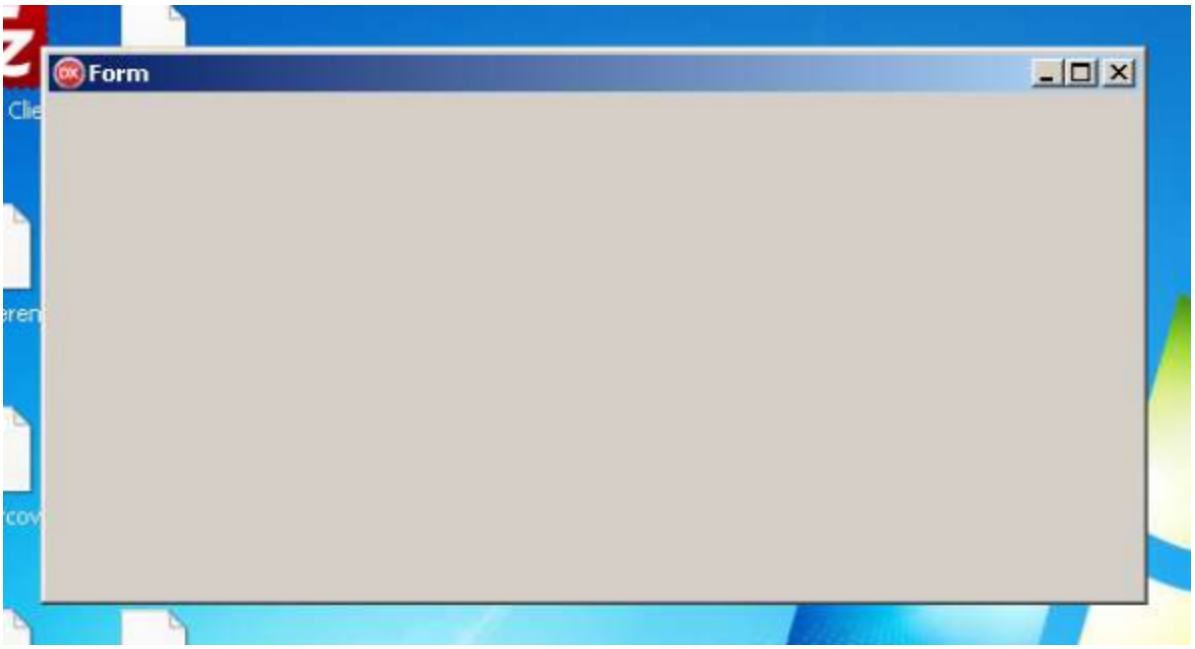
> The #KesLan and #MZREVENGE #Ransomware authors are the same person, the canonical name is #MaMo434376 (as refered in the code) cc @BleepinComputer @demonslay335 @GrujaRS @raby_mr @Amigo_A_ pic.twitter.com/HQCuTWgJoH
>
> — HILDACRYPT (@HILDAKRYPT) December 11, 2019

Update 15.12.2019:

A new Version of this strain was found to be appending *.aes* to encrypted files. This time there is no ransomnote though, so let's see if this is a malfunction or intentional.

The Any.Run Analysis can be found here.

Visually this sample resembles the look of the "MZ Revenge 1.0" strain with an empty Form and the red DX icon.



MITRE ATT&CK

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

T1045 --> Software Packing --> Defense Evasion

T1056 --> Input Capture --> Credential Access

T1012 --> Query Registry --> Discovery

T1124 --> System Time Discovery --> Discovery

T1083 --> File and Directory Discovery --> Discovery

T1076 --> Remote Desktop Protocol --> Lateral Movement

T1056 --> Input Capture --> Collection

T1115 --> Clipboard Data --> Collection

IOCs

MZRevenge / MaMo434376

```
"MZ Revenge 1.0":

7a92a80e742dbcb0d30948dbf6c4d7a6236a5692c5864a1276cfc84d5c71e375
00c84efdebc555191ec91999a7f85c4ab0a6e7236dc477c7e4eb487152211336
a90c73a86a2771f6bff2cfc34d5798b71603da49105342a0a00324b7b6c63018
6907a7689375a06c4f3d5c9d99074c9242342c0e813e669a03a07899740dcfa8
f9cb03dbec628694f81c015b6799e3305f4941dab95d6f67343ef2c2dd2fb891
734a6461eed16f83a355d22ecea28c993ef350a9ea925e2a68caea404f1c0a42
be880ab3f9b4f9cd967fdca899446241e962b3de8c938ed58b69d419b1b6168a
62b129f041cb6b3ebf16f084295f6ffb818db67254eaadeadc906e3d2aecc415
75b6e08e9a0ec989d4936dbbca7dc4ae5cf05ee0f4a7bc4ebccbf5bc81ac9518
32c666ae39cced01978d43a878b4708cb4f4e7051c6d22f9a11c35ce6176151d
184a63ae5c09e4963fc915f9957302ec5b0bd52b2e86049f45a75613f8d9f552
00144748f68a6fe3a7cd98539043698a49fd1e020a6465d5f6e07542712ec014
d8cff0354008b6fd2ea362d33609099eaedc13c5c7c759e2ad9ad998e0b00cda
56ee5c88648365f5269e1ab0d6b00634f7d9fd9f08c91a45c7cb601d5073feb4
3e0c4925102b2b4f1d93193000907c30731163b0e756d37c2a3b4dda1f938794
ca15b28914dc22461fbf8f213047673de7a0434d7ca0d8b796c1a6038f169e23
265e0746692b5301156e4bbd19a9aa62961e333f04fc26d71a64f7739705ee7b
a90c73a86a2771f6bff2cfc34d5798b71603da49105342a0a00324b7b6c63018
859c4b2306ea6a20fdbc4cdbdb28aa500e9928e57ae2ba13fbfb729cc465b6b0
ec70974046fbbd1461ef4b181f8a08270ffaede196c02f1e25e6c7807c29db6a
45d7884b61a6b38356ee18b3814fae0e88715ac004e9df4417d47522203e2a89
648cec145362a52c89c155bf5034eaedee9dd8c90e458dd8c0e1a25ad96e577e
13bcd9a3c09560357b1decc640971f2cc8c1ac58275c317c4266751aefafd29b
d95bd4077537edd5922861977ab3be873532ff2717b0dba916abc9465481cb0e
b02ee036ac32a3b7425a57ff1cf68f2fc46a5f2d7bdea6be78efd574f9761c53
9f28d3d3b8f6078c98d5831a3f1996c28fc14209f2240cc87bf70d20ffac371f
1d5a8d924766f8aba0839ca747b0076b8b3718544c43e9ed32afd33f7fdd3c73
4af2825b70fa4006d56a1faf40062e4a614dfa3de79a197bc268cd708709d4ec
3f35a62f5e2fcb8f74d3aecae7de4bd9834c9400d33a716b74bbe28cf156f142
0b7974582bb4e9c7de0c04618f307e7cbb4bba644c99f165be54117abeb32d43
91d490cabd6776df1bcf26fa17cf9a13663bd79c1b5087ea718248f602d8df0e

"MaMo434376":

3276ab52336b9bc944717cfee706301326addf339891092fb0697d7b93960fa4
10e37630cb1d050911f0c6c094d9c8218622887695960e35f98a596a2ed4de8d
bbfa50b69c3ce9274f8c207dc6eb9caee6e55481440dfde23b85e9aa891ae53d
02101d26f1ac2b3a9188489e4d2f4eeef648916c6a346d3318c36c2622754cbc
bbb26303554c109d62b6f340045c04083ce04d5b6d94ac3a221223187a977072
d7d908991970c971bcc0239654e437c22a987160422c70a838a016c5770caa72

Version 2:

70733389c89b4358f04575226a8ce60c4511018c98731a2ff7f556c29447e4a4
```

Registry Keys

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
--> DisableTaskMgr = 1

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
--> UNCAsIntranet = 0
```

E-Mail Addresses

helpdesk_mz@aol[.]com

Ransomnote V1

```
ATTENTION!

Don*t worry, you can return all your files!
All your files like photos, databases, documents and other important are encrypted
with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for
you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
Price of private key and decrypt software is $300.
Discount 50% available if you contact us first 72 hours, thats price for you is $150.
Please note that you*ll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don*t get answer more than 6 hours.


e-mail address to send your file and To get this software you need write on my e-
mail:
helpdesk_mz@aol.com

Your Decryption Key (DO NOT WIPE OR CHANGE THIS SWITCH!) :
[redacted]
```

Ransomnote V2

```
---> MZ REVENGE 1.0 <---

Dont worry, some of your files have extension .MZ173801 and they are encrypted.

In confirmatiom, that we have private decryption key,
We can provide test decryption for 1 file (png,jpg,bmp,gif).
Its a business, if we cant provide full decryption, other people wont trust us.

There is no way to decrypt your files without our help.
Dont trust anyone. Even your cat.

Main mail: helpdesk_mz@aol.com

Dont change decryption key below!!!

MZ DECRYPTION KEY:
[redacted]
```