BRANDEFENSE
CYBER THREAT INTELLIGENCE

Pandora Ransomware Technical Analysis

Author : Threat Intelligence Team

Date : 20.12.2022

Report ID : BD20221208

Brandefense
Digital Risk Protection Platform

info@brandefense.com

+90 850 303 85 35

Contents

1 Introduction

Report Reference Number	BD20221201
Prepared by	PARS
Analysis Date	01.12.2022
Report Date	04.12.2022

Ransomware attacks have become an increasingly common and costly threat to businesses, government agencies, and other organizations. According to a 2021 report from Cybersecurity Ventures, ransomware attacks are expected to cost businesses over $11.5 billion in damages in 2021 alone.

As we move into the last quarter of the year, it's important to remain vigilant against ransomware threats, even if they are frequently in the news. Last year saw a number of high-profile ransomware operations, including LockBit 3.0, and BlackMatter. These groups continue to evolve their tactics and techniques, and it's important to stay informed about their activities. In this report, we will focus on Pandora ransomware, examining their methods and impact on businesses and organizations.

The Pandora ransomware was discovered in February 2022. Pandora ransomware targets corporate networks for financial gain and uses double extortion to increase pressure on the victim.

After infiltrating the target system, appends the ".pandora" file extension to the encrypted files and a ransom note named `"Restore_My_Files.txt"` is left in each encrypted directory with instructions on how to recover the data.

1.1 Scope

In the "Scope" section, hashes of the analyzed "Pandora Ransomware" sample are given.

File Name	1f172321dfc7445019313cbed4d5f3718a6c0638f2f310918665754a9e117733.exe
MD5	f25e25832dad770c5f989c986770f9e6
SHA-1	2565983f765b76a183de4b6ee793b4903e40c505
SHA256	1f172321dfc7445019313cbed4d5f3718a6c0638f2f310918665754a9e117733

2 Executive Summary

In recent years, Pandora has made headlines for its use of advanced techniques such as double extortion, where it not only encrypts victims' data but also threatens to leak sensitive information unless a ransom is paid. These tactics have made Pandora a particularly feared and reviled group among cybersecurity experts.

One of the key tactics that sets Pandora apart is its use of double extortion, where it not only encrypts victims' data but also threatens to leak sensitive information unless a ransom is paid. This has made Pandora a particularly feared and reviled group among cybersecurity experts, as it puts pressure on organizations to pay the ransom in order to protect their reputation and customer trust.

In addition to double extortion, Pandora has also been known to use other advanced techniques such as exploiting vulnerabilities and using custom encryption algorithms to evade detection. The group is also known for its highly targeted attacks, often conducting extensive research on its victims before launching an attack.

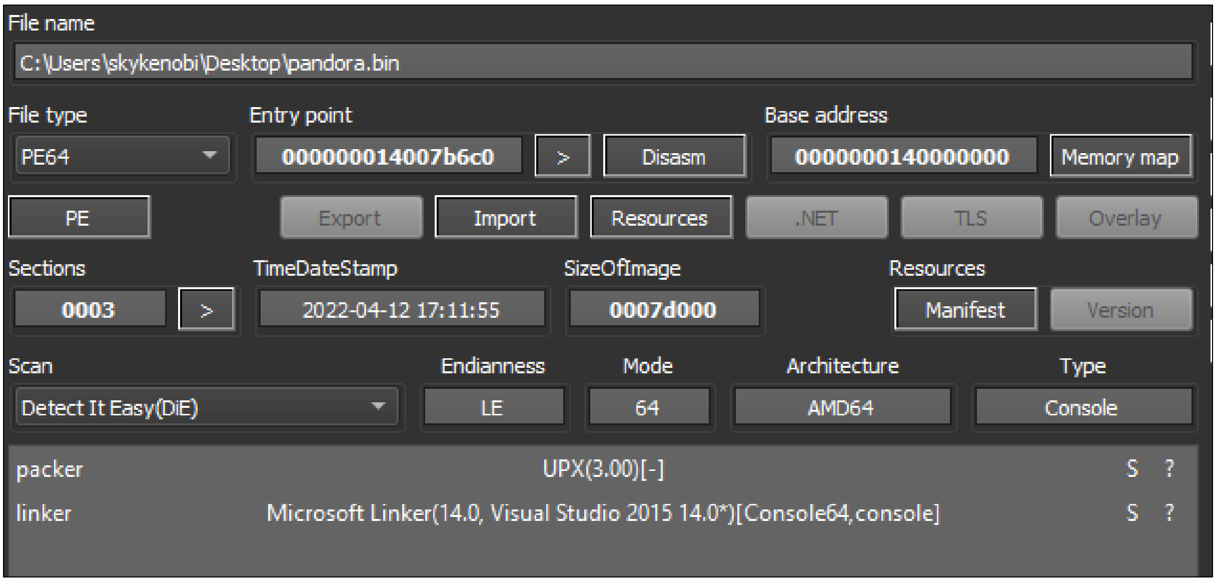
Despite the efforts of law enforcement and cybersecurity firms to disrupt its operations, Pandora remains a formidable threat. In this report, we provide a comprehensive overview of Pandora's history, tactics, and impact, as well as recommendations for organizations seeking to protect themselves from ransomware attacks. This includes measures such as regularly backing up data, implementing robust cybersecurity protocols, and staying up-to-date with the latest threats and vulnerabilities.

3 Technical Analysis

This section covers technical findings discovered during analysis.

3.1 Packing Method

The Pandora sample is packed with a modified UPX packer as seen in the image below.



File name: C:\Users\skykenobi\Desktop\pandora.bin

File type: PE64

Entry point: 000000014007b6c0

Base address: 0000000140000000

Sections: 0003

TimeDateStamp: 2022-04-12 17:11:55

SizeOfImage: 0007d000

Scan: Detect It Easy(DiE)

Endianness: LE

Mode: 64

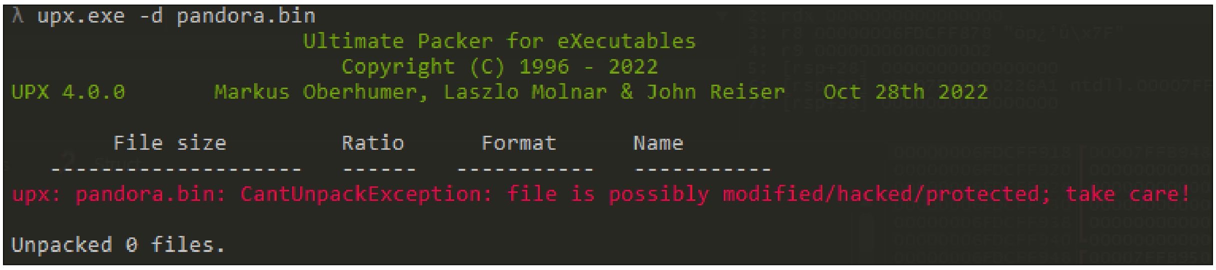
Architecture: AMD64

Type: Console

```
packer      UPX(3.00)[-]                                                          S  ?
linker      Microsoft Linker(14.0, Visual Studio 2015 14.0*)[Console64,console]   S  ?
```

Figure 1: Detect It Easy output

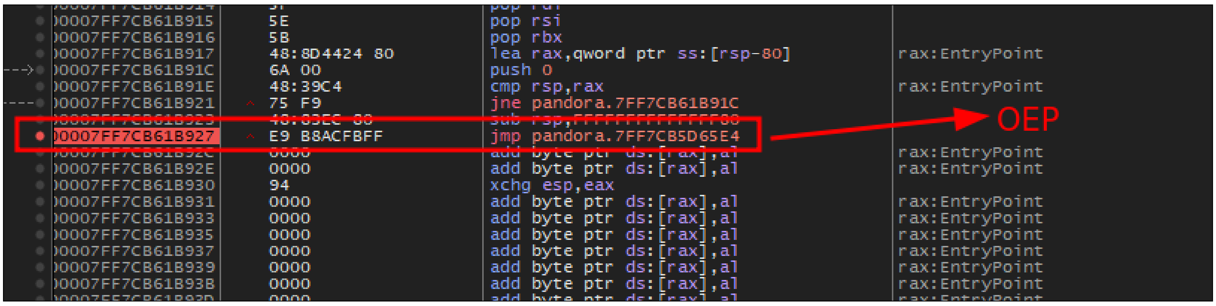
Although it seems to be packed with UPX, the standard UPX unpacker does not work.



```
λ upx.exe -d pandora.bin
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2022
UPX 4.0.0       Markus Oberhumer, Laszlo Molnar & John Reiser   Oct 28th 2022

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: pandora.bin: CantUnpackException: file is possibly modified/hacked/protected; take care!

Unpacked 0 files.
```

Figure 2: The standard UPX unpacker

The jmp instruction at the end from the entrypoint shows OEP.



```
00007FF7CB61B915    5E              pop rsi
00007FF7CB61B916    5B              pop rbx
00007FF7CB61B917    48:8D4424 80    lea rax,qword ptr ss:[rsp-80]          rax:EntryPoint
00007FF7CB61B91C    6A 00           push 0
00007FF7CB61B91E    48:39C4         cmp rsp,rax                            rax:EntryPoint
00007FF7CB61B921    75 F9           jne pandora.7FF7CB61B91C
00007FF7CB61B923    48:83EC 80      sub rsp,FFFFFFFFFFFFFF80
00007FF7CB61B927    E9 B8ACFBFF     jmp pandora.7FF7CB5D65E4
00007FF7CB61B92C    0000            add byte ptr ds:[rax],al               rax:EntryPoint
00007FF7CB61B92E    0000            add byte ptr ds:[rax],al               rax:EntryPoint
00007FF7CB61B930    94              xchg esp,eax
00007FF7CB61B931    0000            add byte ptr ds:[rax],al               rax:EntryPoint
00007FF7CB61B933    0000            add byte ptr ds:[rax],al               rax:EntryPoint
00007FF7CB61B935    0000            add byte ptr ds:[rax],al               rax:EntryPoint
00007FF7CB61B937    0000            add byte ptr ds:[rax],al               rax:EntryPoint
00007FF7CB61B939    0000            add byte ptr ds:[rax],al               rax:EntryPoint
00007FF7CB61B93B    0000            add byte ptr ds:[rax],al               rax:EntryPoint
```

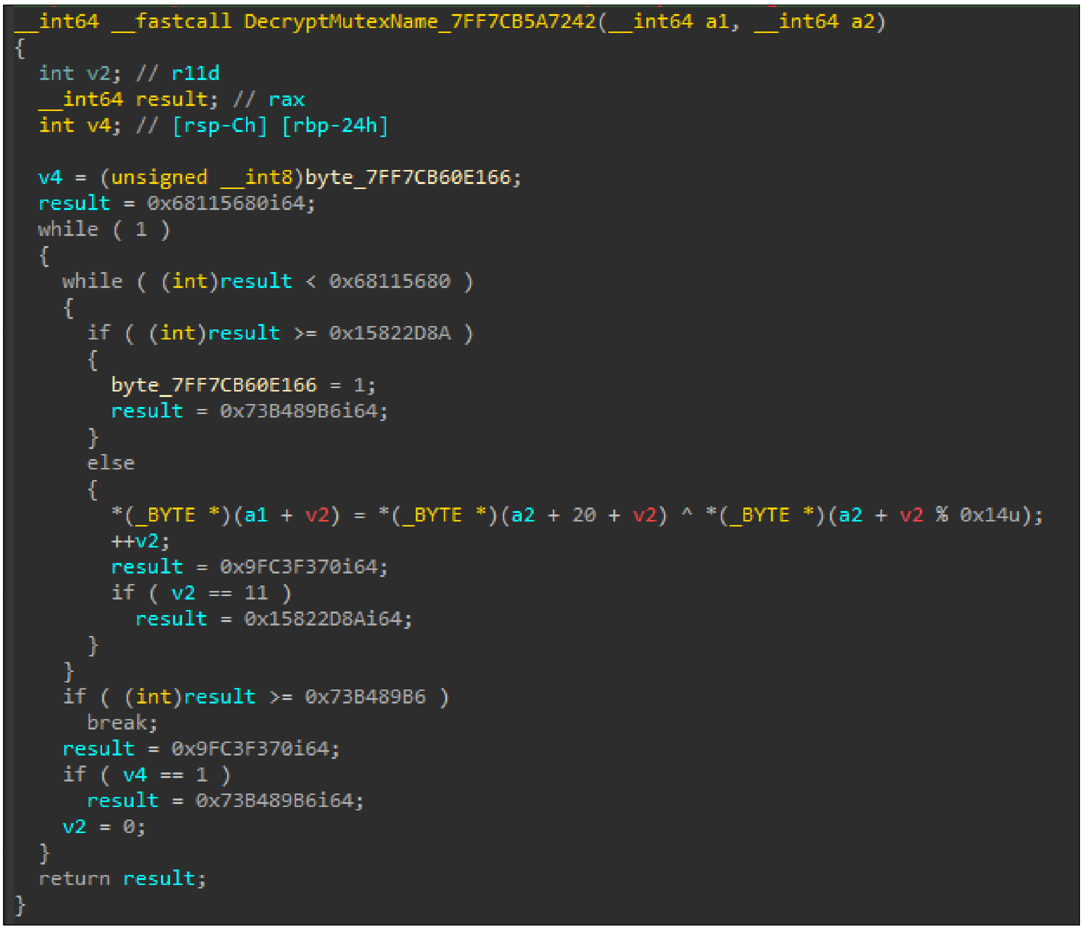
Figure 3: Unpacking the sample

3.2 Obfuscation Techniques

After unpacking the sample, the malware has several obfuscation techniques. Because of obfuscation, disassemble tools cannot give a clean output. In this section, the obfuscation techniques of the malware will be discussed.

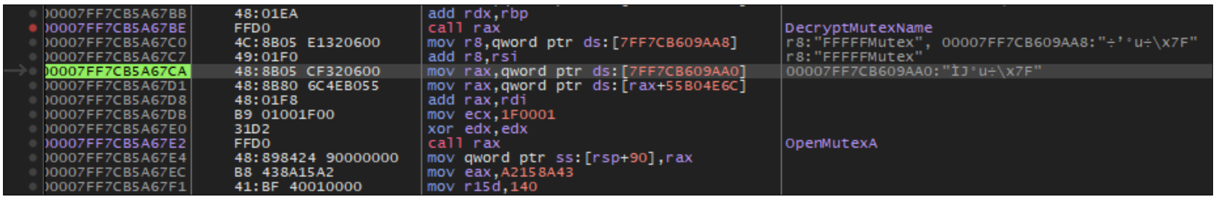
3.2.1 Encrypted Strings

The Pandora ransomware dynamically decrypts some strings like mutex name, public key to make static analysis more difficult.



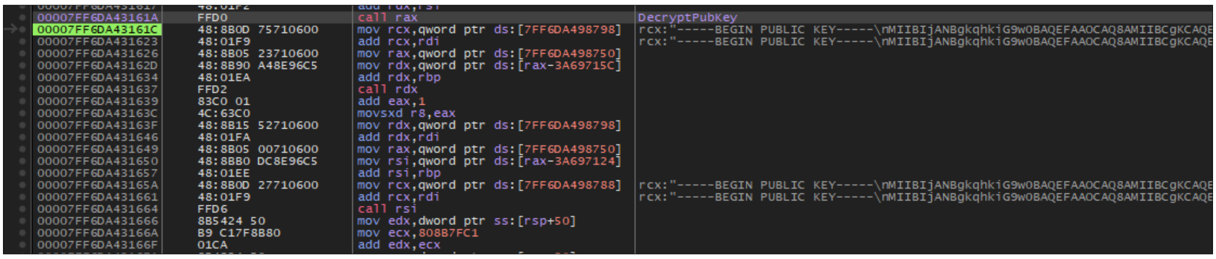
```
__int64 __fastcall DecryptMutexName_7FF7CB5A7242(__int64 a1, __int64 a2)
{
  int v2; // r11d
  __int64 result; // rax
  int v4; // [rsp-Ch] [rbp-24h]

  v4 = (unsigned __int8)byte_7FF7CB60E166;
  result = 0x68115680i64;
  while ( 1 )
  {
    while ( (int)result < 0x68115680 )
    {
      if ( (int)result >= 0x15822D8A )
      {
        byte_7FF7CB60E166 = 1;
        result = 0x73B489B6i64;
      }
      else
      {
        *(_BYTE *)(a1 + v2) = *(_BYTE *)(a2 + 20 + v2) ^ *(_BYTE *)(a2 + v2 % 0x14u);
        ++v2;
        result = 0x9FC3F370i64;
        if ( v2 == 11 )
          result = 0x15822D8Ai64;
      }
    }
    if ( (int)result >= 0x73B489B6 )
      break;
    result = 0x9FC3F370i64;
    if ( v4 == 1 )
      result = 0x73B489B6i64;
    v2 = 0;
  }
  return result;
}
```

Figure 4: Decrypting Mutex name



```
00007FF7CB5A67BB   48:01EA            add rdx,rbp
00007FF7CB5A67BE   FFD0               call rax                                     DecryptMutexName
00007FF7CB5A67C0   4C:8B05 E1320600   mov r8,qword ptr ds:[7FF7CB609AA8]           r8:"FFFFFMutex", 00007FF7CB609AA8:"÷'°u÷\x7F"
00007FF7CB5A67C7   49:01F0            add r8,rsi                                   r8:"FFFFFMutex"
00007FF7CB5A67CA   48:8B05 CF320600   mov rax,qword ptr ds:[7FF7CB609AA0]          00007FF7CB609AA0:"İJ°u÷\x7F"
00007FF7CB5A67D1   48:8B80 6C4EB055   mov rax,qword ptr ds:[rax+55B04E6C]
00007FF7CB5A67D8   48:01F8            add rax,rdi
00007FF7CB5A67DB   B9 01001F00        mov ecx,1F0001
00007FF7CB5A67E0   31D2               xor edx,edx
00007FF7CB5A67E2   FFD0               call rax                                     OpenMutexA
00007FF7CB5A67E4   48:898424 90000000 mov qword ptr ss:[rsp+90],rax
00007FF7CB5A67EC   B8 438A15A2        mov eax,A2158A43
00007FF7CB5A67F1   41:BF 40010000     mov r15d,140
```

Figure 5: Decrypting Mutex name



```
00007FF6DA43161A   FFD0               call rax                              DecryptPubKey
00007FF6DA43161C   48:8B0D 75710600   mov rcx,qword ptr ds:[7FF6DA498798]   rcx:"-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE
00007FF6DA431623   48:01F9            add rcx,rdi                           rcx:"-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE
00007FF6DA431626   48:8B05 23710600   mov rax,qword ptr ds:[7FF6DA498750]
00007FF6DA43162D   48:8B90 A48E96C5   mov rdx,qword ptr ds:[rax-3A69715C]
00007FF6DA431634   48:01EA            add rdx,rbp
00007FF6DA431637   FFD2               call rdx
00007FF6DA431639   83C0 01            add eax,1
00007FF6DA43163C   4C:63C0            movsxd r8,eax
00007FF6DA43163F   48:8B15 52710600   mov rdx,qword ptr ds:[7FF6DA498798]
00007FF6DA431646   48:01FA            add rdx,rdi
00007FF6DA431649   48:8B05 00710600   mov rax,qword ptr ds:[7FF6DA498750]
00007FF6DA431650   48:8BB0 DC8E96C5   mov rsi,qword ptr ds:[rax-3A697124]
00007FF6DA431657   48:01EE            add rsi,rbp
00007FF6DA43165A   48:8B0D 27710600   mov rcx,qword ptr ds:[7FF6DA498788]   rcx:"-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE
00007FF6DA431661   48:01F9            add rcx,rdi                           rcx:"-----BEGIN PUBLIC KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE
00007FF6DA431664   FFD6               call rsi
00007FF6DA431666   8B5424 50          mov edx,dword ptr ss:[rsp+50]
00007FF6DA43166A   B9 C17F8B80        mov ecx,808B7FC1
00007FF6DA43166F   01CA               add edx,ecx
```

Figure 6: Decrypting public key

3.2.2 Control-Flow Flattening

Control-Flow Flattening is an obfuscation technique that makes static analysis difficult by hiding the normal flow of the program. The following image shows the graph of the Main function of the program.

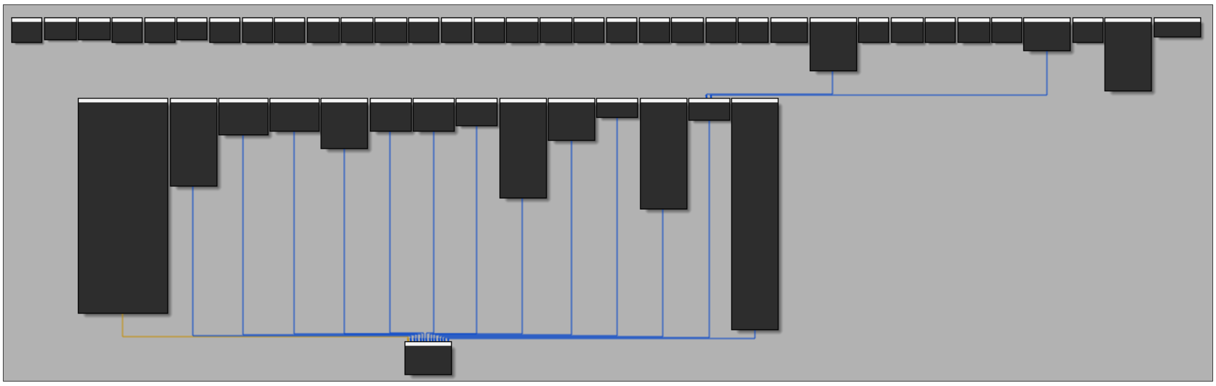
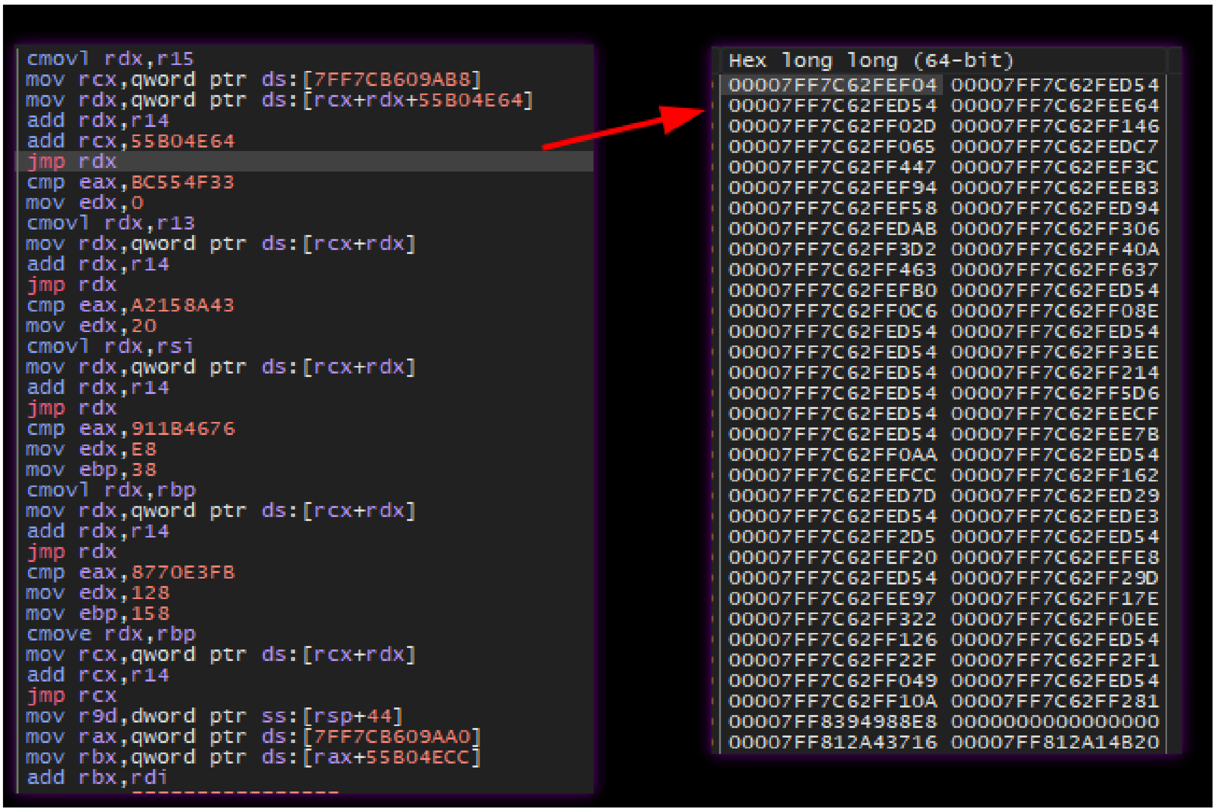


Figure 7: Control-Flow Flattening

3.2.2.1 Function Call Obfuscation

Pandora Ransomware calls functions with registers instead of using direct addresses. It stores a table of function addresses in memory.



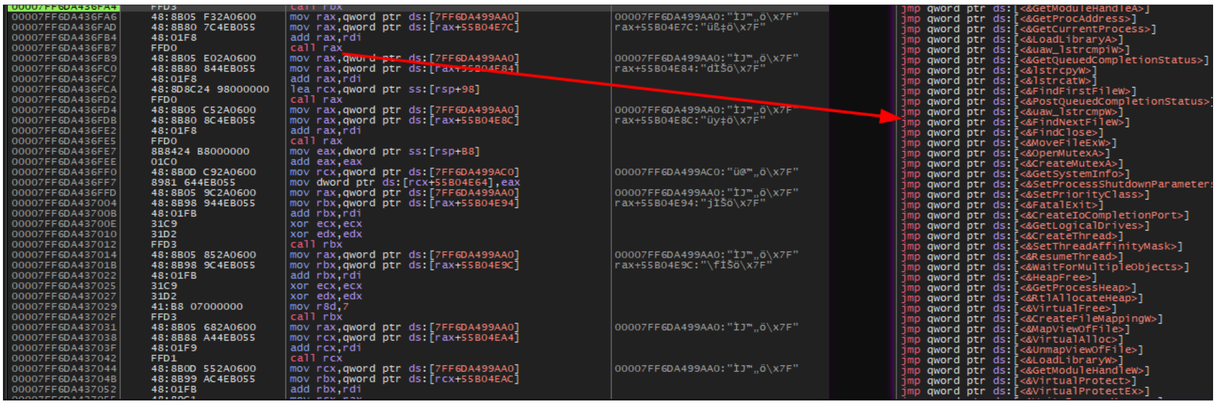
```
cmovl rdx,r15
mov rcx,qword ptr ds:[7FF7CB609AB8]
mov rdx,qword ptr ds:[rcx+rdx+55B04E64]
add rdx,r14
add rcx,55B04E64
jmp rdx
cmp eax,BC554F33
mov edx,0
cmovl rdx,r13
mov rdx,qword ptr ds:[rcx+rdx]
add rdx,r14
jmp rdx
cmp eax,A2158A43
mov edx,20
cmovl rdx,rsi
mov rdx,qword ptr ds:[rcx+rdx]
add rdx,r14
jmp rdx
cmp eax,911B4676
mov edx,E8
mov ebp,38
cmovl rdx,rbp
mov rdx,qword ptr ds:[rcx+rdx]
add rdx,r14
jmp rdx
cmp eax,8770E3FB
mov edx,128
mov ebp,158
cmove rdx,rbp
mov rcx,qword ptr ds:[rcx+rdx]
add rcx,r14
jmp rcx
mov r9d,dword ptr ss:[rsp+44]
mov rax,qword ptr ds:[7FF7CB609AA0]
mov rbx,qword ptr ds:[rax+55B04ECC]
add rbx,rdi
```

```
Hex long long (64-bit)
00007FF7C62FEF04 00007FF7C62FED54
00007FF7C62FED54 00007FF7C62FEE64
00007FF7C62FF02D 00007FF7C62FF146
00007FF7C62FF065 00007FF7C62FEDC7
00007FF7C62FF447 00007FF7C62FEF3C
00007FF7C62FEF94 00007FF7C62FEEB3
00007FF7C62FEF58 00007FF7C62FED94
00007FF7C62FEDAB 00007FF7C62FF306
00007FF7C62FF3D2 00007FF7C62FF40A
00007FF7C62FF463 00007FF7C62FF637
00007FF7C62FEFB0 00007FF7C62FED54
00007FF7C62FF0C6 00007FF7C62FF08E
00007FF7C62FED54 00007FF7C62FED54
00007FF7C62FED54 00007FF7C62FF3EE
00007FF7C62FED54 00007FF7C62FF214
00007FF7C62FED54 00007FF7C62FF5D6
00007FF7C62FED54 00007FF7C62FEECF
00007FF7C62FED54 00007FF7C62FEE7B
00007FF7C62FF0AA 00007FF7C62FED54
00007FF7C62FEFCC 00007FF7C62FF162
00007FF7C62FED7D 00007FF7C62FED29
00007FF7C62FED54 00007FF7C62FEDE3
00007FF7C62FF2D5 00007FF7C62FED54
00007FF7C62FEF20 00007FF7C62FEFE8
00007FF7C62FED54 00007FF7C62FF29D
00007FF7C62FEE97 00007FF7C62FF17E
00007FF7C62FF322 00007FF7C62FF0EE
00007FF7C62FF126 00007FF7C62FED54
00007FF7C62FF22F 00007FF7C62FF2F1
00007FF7C62FF049 00007FF7C62FED54
00007FF7C62FF10A 00007FF7C62FF281
00007FF8394988E8 0000000000000000
00007FF812A43716 00007FF812A14B20
```

Figure 8: Control-Flow Flattening

3.2.2.2 Windows API Call Obfuscation

It keeps the address of each Windows API in a table. It dynamically resolves addresses and calls again with register.



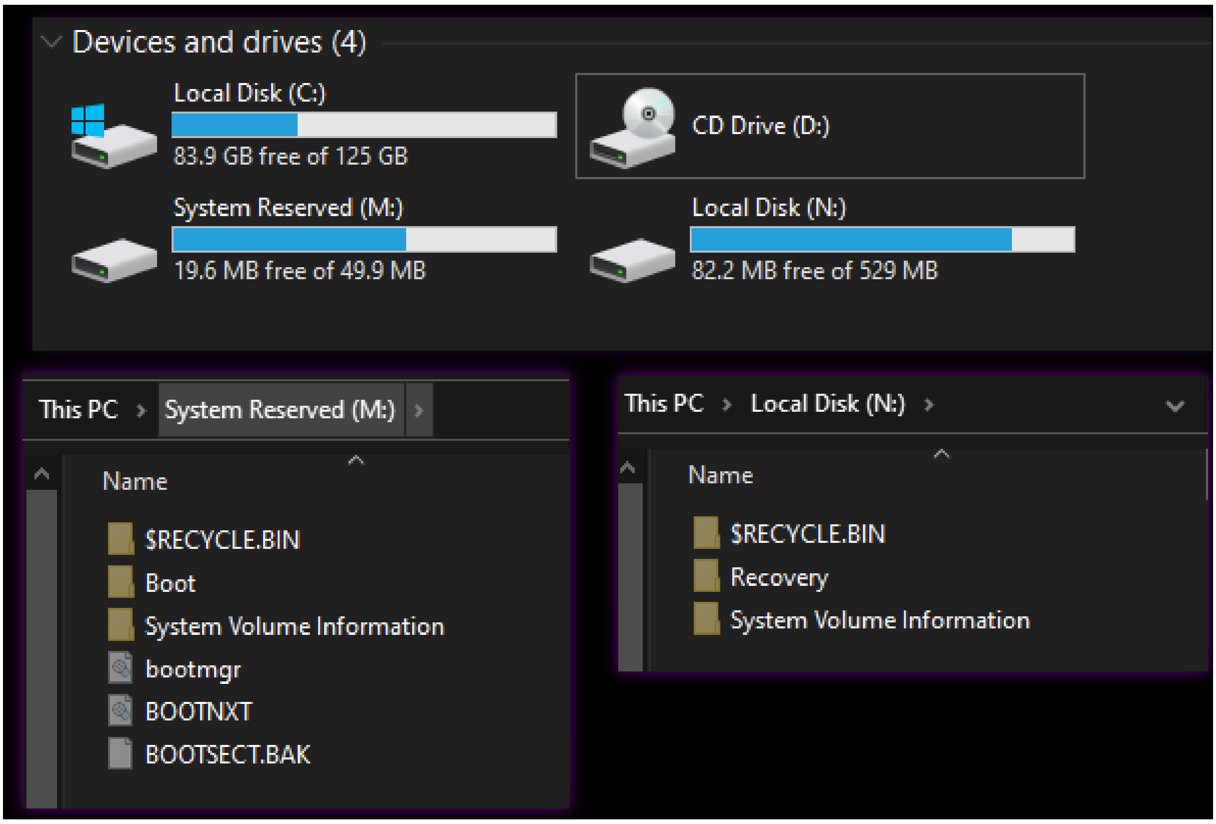
```
00007FF6DA436FA4   FFD3                 call rbx
00007FF6DA436FA6   48:8B05 F32A0600     mov rax,qword ptr ds:[7FF6DA499AA0]     00007FF6DA499AA0:"İJ™„ö\x7F"
00007FF6DA436FAD   48:8B80 7C4EB055     mov rax,qword ptr ds:[rax+55B04E7C]     rax+55B04E7C:"üß‡ö\x7F"
00007FF6DA436FB4   48:01F8              add rax,rdi
00007FF6DA436FB7   FFD0                 call rax
00007FF6DA436FB9   48:8B05 E02A0600     mov rax,qword ptr ds:[7FF6DA499AA0]     00007FF6DA499AA0:"İJ™„ö\x7F"
00007FF6DA436FC0   48:8B80 844EB055     mov rax,qword ptr ds:[rax+55B04E84]     rax+55B04E84:"dİŠö\x7F"
00007FF6DA436FC7   48:01F8              add rax,rdi
00007FF6DA436FCA   48:8D8C24 98000000   lea rcx,qword ptr ss:[rsp+98]
00007FF6DA436FD2   FFD0                 call rax
00007FF6DA436FD4   48:8B05 C52A0600     mov rax,qword ptr ds:[7FF6DA499AA0]     00007FF6DA499AA0:"İJ™„ö\x7F"
00007FF6DA436FDB   48:8B80 8C4EB055     mov rax,qword ptr ds:[rax+55B04E8C]     rax+55B04E8C:"üy‡ö\x7F"
00007FF6DA436FE2   48:01F8              add rax,rdi
00007FF6DA436FE5   FFD0                 call rax
00007FF6DA436FE7   8B8424 B8000000      mov eax,dword ptr ss:[rsp+B8]
00007FF6DA436FEE   01C0                 add eax,eax
00007FF6DA436FF0   48:8B0D C92A0600     mov rcx,qword ptr ds:[7FF6DA499AC0]     00007FF6DA499AC0:"ü@™„ö\x7F"
00007FF6DA436FF7   8981 644EB055        mov dword ptr ds:[rcx+55B04E64],eax
00007FF6DA436FFD   48:8B05 9C2A0600     mov rax,qword ptr ds:[7FF6DA499AA0]     00007FF6DA499AA0:"İJ™„ö\x7F"
00007FF6DA437004   48:8B98 944EB055     mov rbx,qword ptr ds:[rax+55B04E94]     rax+55B04E94:"jİŠö\x7F"
00007FF6DA43700B   48:01FB              add rbx,rdi
00007FF6DA43700E   31C9                 xor ecx,ecx
00007FF6DA437010   31D2                 xor edx,edx
00007FF6DA437012   FFD3                 call rbx
00007FF6DA437014   48:8B05 852A0600     mov rax,qword ptr ds:[7FF6DA499AA0]     00007FF6DA499AA0:"İJ™„ö\x7F"
00007FF6DA43701B   48:8B98 9C4EB055     mov rbx,qword ptr ds:[rax+55B04E9C]     rax+55B04E9C:"\fİŠö\x7F"
00007FF6DA437022   48:01FB              add rbx,rdi
00007FF6DA437025   31C9                 xor ecx,ecx
00007FF6DA437027   31D2                 xor edx,edx
00007FF6DA437029   41:B8 07000000       mov r8d,7
00007FF6DA43702F   FFD3                 call rbx
00007FF6DA437031   48:8B05 682A0600     mov rax,qword ptr ds:[7FF6DA499AA0]     00007FF6DA499AA0:"İJ™„ö\x7F"
00007FF6DA437038   48:8B88 A44EB055     mov rcx,qword ptr ds:[rax+55B04EA4]
00007FF6DA43703F   48:01F9              add rcx,rdi
00007FF6DA437042   FFD1                 call rcx
00007FF6DA437044   48:8B0D 552A0600     mov rcx,qword ptr ds:[7FF6DA499AA0]     00007FF6DA499AA0:"İJ™„ö\x7F"
00007FF6DA43704B   48:8B99 AC4EB055     mov rbx,qword ptr ds:[rcx+55B04EAC]
00007FF6DA437052   48:01FB              add rbx,rdi
```

```
jmp qword ptr ds:[<&GetModuleHandleA>]
jmp qword ptr ds:[<&GetProcAddress>]
jmp qword ptr ds:[<&GetCurrentProcess>]
jmp qword ptr ds:[<&LoadLibraryA>]
jmp qword ptr ds:[<&uaw_lstrcmpiW>]
jmp qword ptr ds:[<&GetQueuedCompletionStatus>]
jmp qword ptr ds:[<&lstrcpyW>]
jmp qword ptr ds:[<&lstrcatW>]
jmp qword ptr ds:[<&FindFirstFileW>]
jmp qword ptr ds:[<&PostQueuedCompletionStatus>]
jmp qword ptr ds:[<&uaw_lstrcmpW>]
jmp qword ptr ds:[<&FindNextFileW>]
jmp qword ptr ds:[<&FindClose>]
jmp qword ptr ds:[<&MoveFileExW>]
jmp qword ptr ds:[<&OpenMutexA>]
jmp qword ptr ds:[<&CreateMutexA>]
jmp qword ptr ds:[<&GetSystemInfo>]
jmp qword ptr ds:[<&SetProcessShutdownParameters
jmp qword ptr ds:[<&SetPriorityClass>]
jmp qword ptr ds:[<&FatalExit>]
jmp qword ptr ds:[<&CreateIoCompletionPort>]
jmp qword ptr ds:[<&GetLogicalDrives>]
jmp qword ptr ds:[<&CreateThread>]
jmp qword ptr ds:[<&SetThreadAffinityMask>]
jmp qword ptr ds:[<&ResumeThread>]
jmp qword ptr ds:[<&WaitForMultipleObjects>]
jmp qword ptr ds:[<&HeapFree>]
jmp qword ptr ds:[<&GetProcessHeap>]
jmp qword ptr ds:[<&RtlAllocateHeap>]
jmp qword ptr ds:[<&VirtualFree>]
jmp qword ptr ds:[<&CreateFileMappingW>]
jmp qword ptr ds:[<&MapViewOfFile>]
jmp qword ptr ds:[<&VirtualAlloc>]
jmp qword ptr ds:[<&UnmapViewOfFile>]
jmp qword ptr ds:[<&LoadLibraryW>]
jmp qword ptr ds:[<&GetModuleHandleW>]
jmp qword ptr ds:[<&VirtualProtect>]
jmp qword ptr ds:[<&VirtualProtectEx>]
```

Figure 9: Control-Flow Flattening

3.3 Setting New Volumes

Pandora ransomware creates 2 new volumes to prevent OS corruption before encryption.



Devices and drives (4)

Local Disk (C:)
83.9 GB free of 125 GB

CD Drive (D:)

System Reserved (M:)
19.6 MB free of 49.9 MB

Local Disk (N:)
82.2 MB free of 529 MB

This PC › System Reserved (M:) ›

Name
- $RECYCLE.BIN
- Boot
- System Volume Information
- bootmgr
- BOOTNXT
- BOOTSECT.BAK

This PC › Local Disk (N:) ›

Name
- $RECYCLE.BIN
- Recovery
- System Volume Information

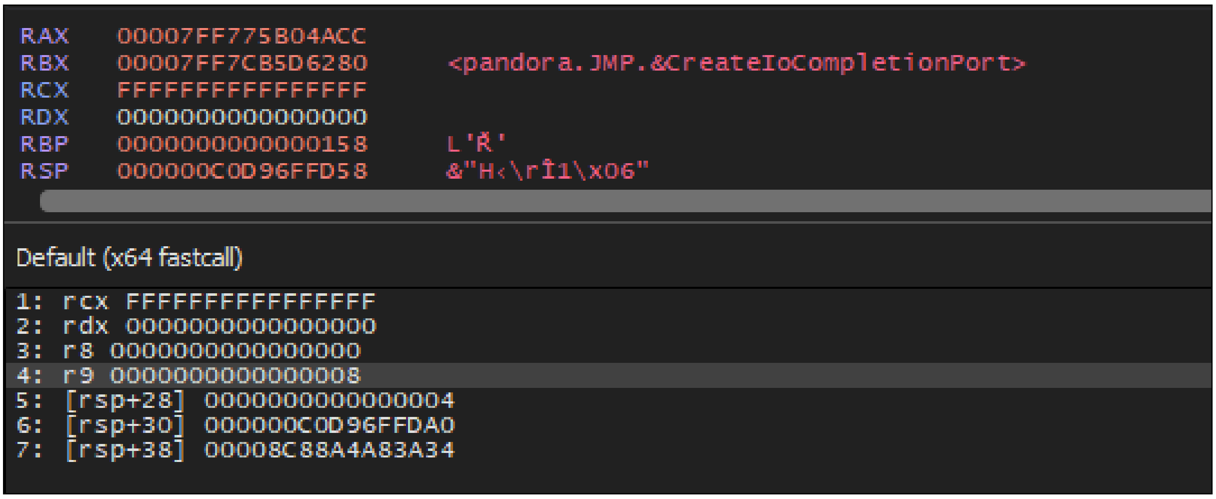
Figure 10: New volumes

Windows APIs used:

- FindFirstVolumeW
- GetVolumePathNamesForVolumeNameW
- SetVolumeMountPointW
- FindNextVolumeW
- FindVolumeClose

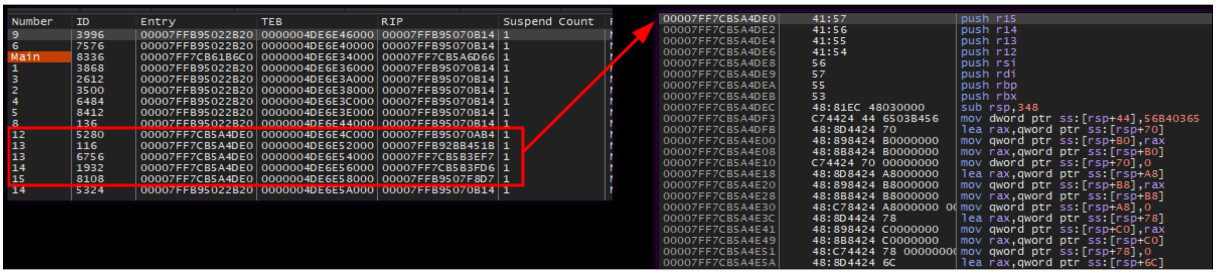
3.4 Multi-Threading

Pandora Ransomware uses multiple threads to speed up the encryption process. It uses Windows' IO Completion Ports concept for Multiple Thread management.



```
RAX    00007FF775B04ACC
RBX    00007FF7CB5D6280      <pandora.JMP.&CreateIoCompletionPort>
RCX    FFFFFFFFFFFFFFFF
RDX    0000000000000000
RBP    0000000000000158      L'Ř'
RSP    000000C0D96FFD58      &"H‹\rÎ1\x06"

Default (x64 fastcall)
1: rcx FFFFFFFFFFFFFFFF
2: rdx 0000000000000000
3: r8 0000000000000000
4: r9 0000000000000008
5: [rsp+28] 0000000000000004
6: [rsp+30] 000000C0D96FFDA0
7: [rsp+38] 00008C88A4A83A34
```

Figure 11: Create IO Completion



```
Number  ID    Entry             TEB               RIP               Suspend Count
9       3996  00007FFB95022B20  0000004DE6E46000  00007FFB95070B14  1
6       7576  00007FFB95022B20  0000004DE6E40000  00007FFB95070B14  1
Main    8336  00007FF7CB61B6C0  0000004DE6E34000  00007FF7CB5A6D66  1
1       3868  00007FFB95022B20  0000004DE6E36000  00007FFB95070B14  1
3       2612  00007FFB95022B20  0000004DE6E3A000  00007FFB95070B14  1
2       3500  00007FFB95022B20  0000004DE6E38000  00007FFB95070B14  1
4       6484  00007FFB95022B20  0000004DE6E3C000  00007FFB95070B14  1
5       8412  00007FFB95022B20  0000004DE6E3E000  00007FFB95070B14  1
8       136   00007FFB95022B20  0000004DE6E44000  00007FFB95070B14  1
12      5280  00007FF7CB5A4DE0  0000004DE6E4C000  00007FFB95070AB4  1
13      116   00007FF7CB5A4DE0  0000004DE6E52000  00007FFB92BB451B  1
13      6756  00007FF7CB5A4DE0  0000004DE6E54000  00007FF7CB5B3EF7  1
14      1932  00007FF7CB5A4DE0  0000004DE6E56000  00007FF7CB5B3FD6  1
15      8108  00007FF7CB5A4DE0  0000004DE6E58000  00007FFB9507F8D7  1
14      5324  00007FFB95022B20  0000004DE6E5A000  00007FFB95070B14  1
```

```
00007FF7CB5A4DE0   41:57                  push r15
00007FF7CB5A4DE2   41:56                  push r14
00007FF7CB5A4DE4   41:55                  push r13
00007FF7CB5A4DE6   41:54                  push r12
00007FF7CB5A4DE8   56                     push rsi
00007FF7CB5A4DE9   57                     push rdi
00007FF7CB5A4DEA   55                     push rbp
00007FF7CB5A4DEB   53                     push rbx
00007FF7CB5A4DEC   48:81EC 48030000       sub rsp,348
00007FF7CB5A4DF3   C74424 44 6503B456     mov dword ptr ss:[rsp+44],56B40365
00007FF7CB5A4DFB   48:8D4424 70           lea rax,qword ptr ss:[rsp+70]
00007FF7CB5A4E00   48:898424 B0000000     mov qword ptr ss:[rsp+B0],rax
00007FF7CB5A4E08   48:8B8424 B0000000     mov rax,qword ptr ss:[rsp+B0]
00007FF7CB5A4E10   C74424 70 00000000     mov dword ptr ss:[rsp+70],0
00007FF7CB5A4E18   48:8D8424 A8000000     lea rax,qword ptr ss:[rsp+A8]
00007FF7CB5A4E20   48:898424 B8000000     mov qword ptr ss:[rsp+B8],rax
00007FF7CB5A4E28   48:8B8424 B8000000     mov rax,qword ptr ss:[rsp+B8]
00007FF7CB5A4E30   48:C78424 A8000000 00  mov qword ptr ss:[rsp+A8],0
00007FF7CB5A4E3C   48:8D4424 78           lea rax,qword ptr ss:[rsp+78]
00007FF7CB5A4E41   48:898424 C0000000     mov qword ptr ss:[rsp+C0],rax
00007FF7CB5A4E49   48:8B8424 C0000000     mov rax,qword ptr ss:[rsp+C0]
00007FF7CB5A4E51   48:C74424 78 0000000   mov qword ptr ss:[rsp+78],0
00007FF7CB5A4E5A   48:8D4424 6C           lea rax,qword ptr ss:[rsp+6C]
```

Figure 12: Created threads for encryption

Windows APIs used:

- CreateThread
- SetThreadAffinityMask
- ResumeThread
- CreateIoCompletionPort
- GetQueuedCompletionStatus
- PostQueuedCompletionStatus
- WaitForMultipleObjects

3.5 Encryption

Before Pandora encrypts a file, it checks the directories and files in the list to prevent operating system corruption. It does not encrypt when it comes to a directory or file in the list.

AppData	Boot	Windows	Windows.old
Tor Browser	Internet Explorer	Google	Opera
Opera Software	Mozilla	Mozilla Firefox	$Recycle.Bin
ProgramData	All Users	autorun.inf	boot.ini
bootfont.bin	bootsect.bak	bootmgr	bootmgr.efi
bootmgfw.efi	desktop.ini	iconcache.db	ntldr
ntuser.dat	ntuser.dat.log	ntuser.ini	thumbs.db
Program Files	Program Files (x86)	#recycle	

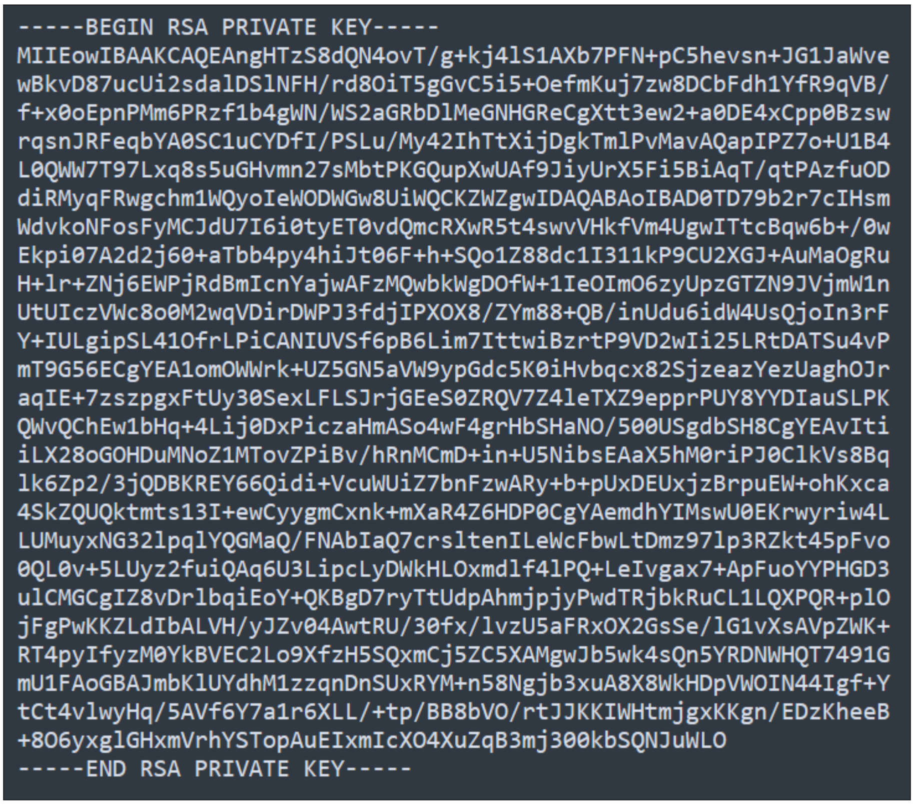
Table 1: Folders and files

Each target file is compared to the following list of file extensions. If the file's extension is in the list, the file is not encrypted.

.hta	.exe	.dll	.cpl	.idx	.ocx
.ini	.cab	.cur	.drv	.sys	.pandora
.hlp	.icl	.icns	.ico	.spl	

Table 2: Extensions

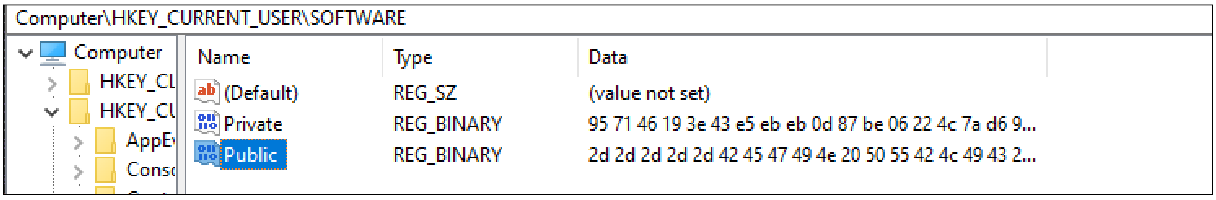
Pandora Ransomware uses RSA for asymmetric encryption. The RSA private key is dynamically decrypted.



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAngHTzS8dQN4ovT/g+kj4lS1AXb7PFN+pC5hevsn+JG1JaWve
wBkvD87ucUi2sdalDSlNFH/rd8OiT5gGvC5i5+OefmKuj7zw8DCbFdh1YfR9qVB/
f+x0oEpnPMm6PRzf1b4gWN/WS2aGRbDlMeGNHGReCgXtt3ew2+a0DE4xCpp0Bzsw
rqsnJRFeqbYA0SC1uCYDfI/PSLu/My42IhTtXijDgkTmlPvMavAQapIPZ7o+U1B4
L0QWW7T97Lxq8s5uGHvmn27sMbtPKGQupXwUAf9JiyUrX5Fi5BiAqT/qtPAzfuOD
diRMyqFRwgchm1WQyoIeWODWGw8UiWQCKZWZgwIDAQABAoIBAD0TD79b2r7cIHsm
WdvkoNFosFyMCJdU7I6i0tyET0vdQmcRXwR5t4swvVHkfVm4UgwITtcBqw6b+/0w
Ekpi07A2d2j60+aTbb4py4hiJt06F+h+SQo1Z88dc1I311kP9CU2XGJ+AuMaOgRu
H+lr+ZNj6EWPjRdBmIcnYajwAFzMQwbkWgDOfW+1IeOImO6zyUpzGTZN9JVjmW1n
UtUIczVWc8o0M2wqVDirDWPJ3fdjIPXOX8/ZYm88+QB/inUdu6idW4UsQjoIn3rF
Y+IULgipSL41OfrLPiCANIUVSf6pB6Lim7IttwiBzrtP9VD2wIi25LRtDATSu4vP
mT9G56ECgYEA1omOWWrk+UZ5GN5aVW9ypGdc5K0iHvbqcx82SjzeazYezUaghOJr
aqIE+7zszpgxFtUy30SexLFLSJrjGEeS0ZRQV7Z4leTXZ9epprPUY8YYDIauSLPK
QWvQChEw1bHq+4Lij0DxPiczaHmASo4wF4grHbSHaNO/500USgdbSH8CgYEAvIti
iLX28oGOHDuMNoZ1MTovZPiBv/hRnMCmD+in+U5NibsEAaX5hM0riPJ0ClkVs8Bq
lk6Zp2/3jQDBKREY66Qidi+VcuWUiZ7bnFzwARy+b+pUxDEUxjzBrpuEW+ohKxca
4SkZQUQktmts13I+ewCyygmCxnk+mXaR4Z6HDP0CgYAemdhYIMswU0EKrwyriw4L
LUMuyxNG32lpqlYQGMaQ/FNAbIaQ7crsltenILeWcFbwLtDmz97lp3RZkt45pFvo
0QL0v+5LUyz2fuiQAq6U3LipcLyDWkHLOxmdlf4lPQ+LeIvgax7+ApFuoYYPHGD3
ulCMGCgIZ8vDrlbqiEoY+QKBgD7ryTtUdpAhmjpjyPwdTRjbkRuCL1LQXPQR+plO
jFgPwKKZLdIbALVH/yJZv04AwtRU/30fx/lvzU5aFRxOX2GsSe/lG1vXsAVpZWK+
RT4pyIfyzM0YkBVEC2Lo9XfzH5SQxmCj5ZC5XAMgwJb5wk4sQn5YRDNWHQT7491G
mU1FAoGBAJmbKlUYdhM1zzqnDnSUxRYM+n58Ngjb3xuA8X8WkHDpVWOIN44Igf+Y
tCt4vlwyHq/5AVf6Y7a1r6XLL/+tp/BB8bVO/rtJJKKIWHtmjgxKKgn/EDzKheeB
+8O6yxglGHxmVrhYSTopAuEIxmIcXO4XuZqB3mj300kbSQNJuWLO
-----END RSA PRIVATE KEY-----
```

Figure 13: RSA private key

Private and public keys also stored in the registry under `HKCU\textbackslash SOFTWARE\textbackslash[ Private, Public]`.

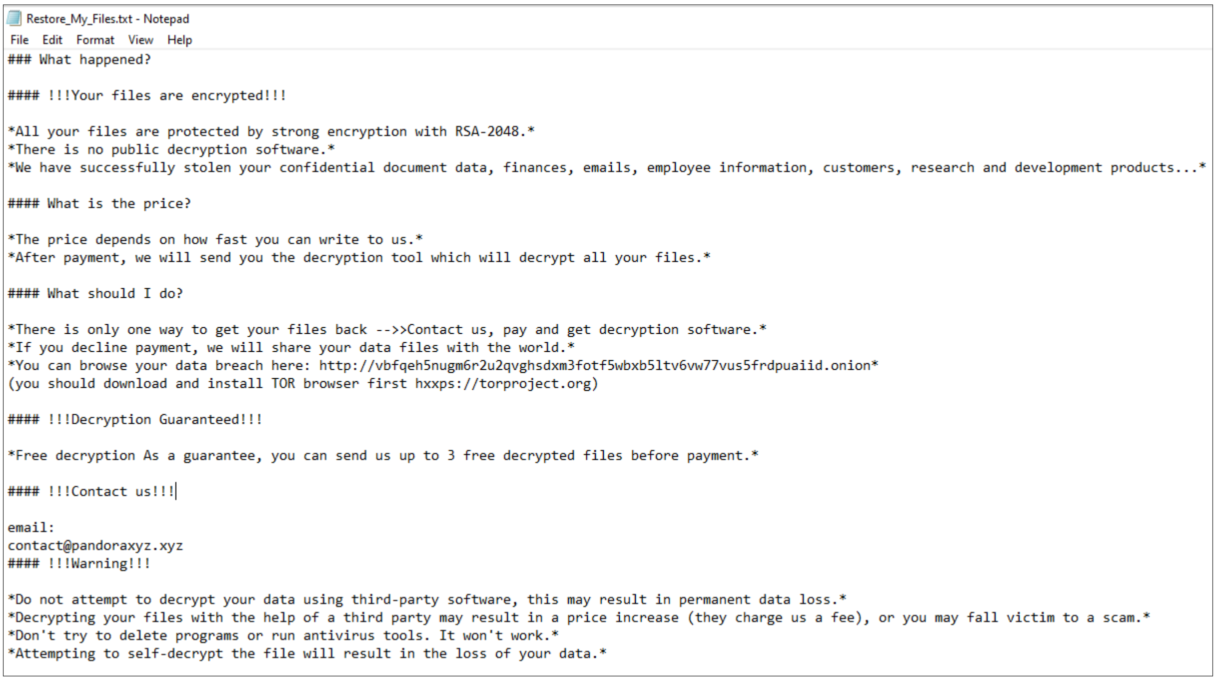


Computer\HKEY_CURRENT_USER\SOFTWARE

Name	Type	Data
(Default)	REG_SZ	(value not set)
Private	REG_BINARY	95 71 46 19 3e 43 e5 eb eb 0d 87 be 06 22 4c 7a d6 9...
Public	REG_BINARY	2d 2d 2d 2d 2d 42 45 47 49 4e 20 50 55 42 4c 49 43 2...

Figure 14: Registry keys

Pandora ransomware creates a ransom note named `"Restore_My_Files.txt"` for each encrypted folder.



```
### What happened?

#### !!!Your files are encrypted!!!

*All your files are protected by strong encryption with RSA-2048.*
*There is no public decryption software.*
*We have successfully stolen your confidential document data, finances, emails, employee information, customers, research and development products...*

#### What is the price?

*The price depends on how fast you can write to us.*
*After payment, we will send you the decryption tool which will decrypt all your files.*

#### What should I do?

*There is only one way to get your files back -->>Contact us, pay and get decryption software.*
*If you decline payment, we will share your data files with the world.*
*You can browse your data breach here: http://vbfqeh5nugm6r2u2qvghsdxm3fotf5wbxb5ltv6vw77vus5frdpuaiid.onion*
(you should download and install TOR browser first hxxps://torproject.org)

#### !!!Decryption Guaranteed!!!

*Free decryption As a guarantee, you can send us up to 3 free decrypted files before payment.*

#### !!!Contact us!!!

email:
contact@pandoraxyz.xyz
#### !!!Warning!!!

*Do not attempt to decrypt your data using third-party software, this may result in permanent data loss.*
*Decrypting your files with the help of a third party may result in a price increase (they charge us a fee), or you may fall victim to a scam.*
*Don't try to delete programs or run antivirus tools. It won't work.*
*Attempting to self-decrypt the file will result in the loss of your data.*
```

Figure 15: Ransom note

Unlike other ransomware, it does not change the desktop background.

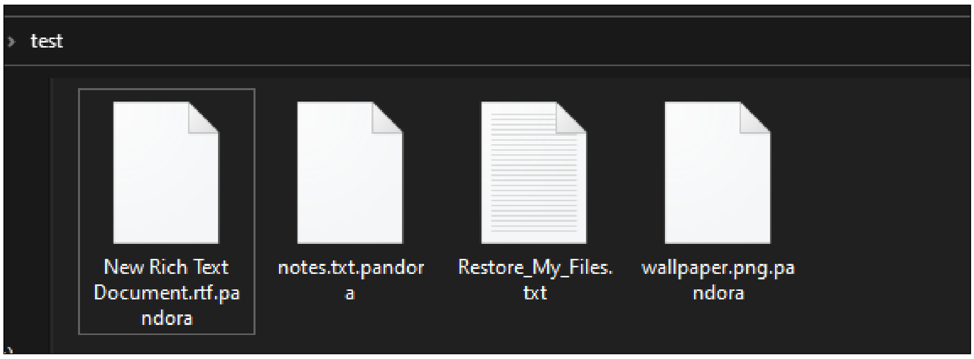
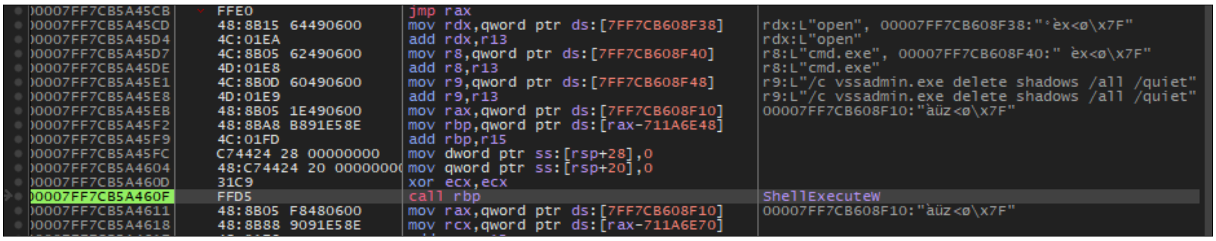


Figure 16: Encrypted folder

3.6 Deleting Shadow Copies

Like a lot of other ransomware, Pandora deletes the Windows Shadow Copies.



```
)0007FF7CB5A45CB   FFE0                    jmp rax
)0007FF7CB5A45CD   48:8B15 64490600        mov rdx,qword ptr ds:[7FF7CB608F38]   rdx:L"open", 00007FF7CB608F38:"°èx<ø\x7F"
)0007FF7CB5A45D4   4C:01EA                 add rdx,r13                           rdx:L"open"
)0007FF7CB5A45D7   4C:8B05 62490600        mov r8,qword ptr ds:[7FF7CB608F40]    r8:L"cmd.exe", 00007FF7CB608F40:" èx<ø\x7F"
)0007FF7CB5A45DE   4D:01E8                 add r8,r13                            r8:L"cmd.exe"
)0007FF7CB5A45E1   4C:8B0D 60490600        mov r9,qword ptr ds:[7FF7CB608F48]    r9:L"/c vssadmin.exe delete shadows /all /quiet"
)0007FF7CB5A45E8   4D:01E9                 add r9,r13                            r9:L"/c vssadmin.exe delete shadows /all /quiet"
)0007FF7CB5A45EB   48:8B05 1E490600        mov rax,qword ptr ds:[7FF7CB608F10]   00007FF7CB608F10:"àüz<ø\x7F"
)0007FF7CB5A45F2   48:8BA8 B891E58E        mov rbp,qword ptr ds:[rax-711A6E48]
)0007FF7CB5A45F9   4C:01FD                 add rbp,r15
)0007FF7CB5A45FC   C74424 28 00000000      mov dword ptr ss:[rsp+28],0
)0007FF7CB5A4604   48:C74424 20 0000000(   mov qword ptr ss:[rsp+20],0
)0007FF7CB5A460D   31C9                    xor ecx,ecx
)0007FF7CB5A460F   FFD5                    call rbp                              ShellExecuteW
)0007FF7CB5A4611   48:8B05 F8480600        mov rax,qword ptr ds:[7FF7CB608F10]   00007FF7CB608F10:"àüz<ø\x7F"
)0007FF7CB5A4618   48:8B88 9091E58E        mov rcx,qword ptr ds:[rax-711A6E70]
```

Figure 17: Ransom note

4 Conclusion

Pandora ransomware is more advanced than the average malware with its anti-analysis techniques. It increases the pressure on the victim to pay money with the double extortion method.

Here are our recommendations against ransomware and other malware threats.

- Emails sent from outside the corporation must not be opened outside of the sandbox environment.
- The IOCs given at the end of the report should be added to the security products.
- Critical data should be backed up regularly to minimize ransomware threats.
- Threat actors should not be paid to recover encrypted files.
- In order not to be affected by vulnerabilities, operating systems, used programs and security products should be kept up to date.
- Password policies, hardening of the systems used should be done well.

4.1 YARA Rule

```
rule Pandora_ransom_packed{
  strings:
      $main_func = {53 56 57 55 48 8D 35 ?5 ?? FC FF 48
      8D BE 00 ?0 FB FF 57 31 DB 31 C9 48 83 CD FF E8 50}
      $UPX = {33 2E 30 30 00 55 50 58 21} // 3.00.UPX!
  condition:
      uint16(0) == 0x5a4d and all of them
}
```

```
rule Pandora_ransomware_unpacked {
  strings:
      $Mutex_decryption = {3D ?? ?? ?? ?? 75 ?? 48 8B
      5C 24 08 49 63 FB 89 FE 49 0F AF F0 48 C1 EE 24
      C1 E6 ?? 8D 34 ?? 89 F8 29 F0 0F B6 04 02 32 04
      3B 88 04 39}
      $decryption_xor = {4D 63 D2 44 89 D0 83 E0 0F 0F
      B6 04 02 43 32 04 13 42 88 04 11}
      $str1 = "Restore_My_Files.txt" wide ascii
      $str2 = ".pandora" wide ascii

     condition:
      uint16(0) == 0x5a4d and ($Mutex_decryption or
      $decryption_xor) and ($str1 and $str2)
}
```

4.2 MITRE ATT&CK Techniques

Tactic	Tactic ID	Technique	Technique ID
Initial Access	TA0001	Supply Chain Compromise	T1195
Execution	TA0002	Command and Scripting Interpreter	T1509
Persistence	TA0003	System Information Discovery	T1082
Defense Evasion	TA0005	Modify Registry Impair Defenses: Disable or Modify Tools Obfuscated Files or Information	T112 T1562.001 T1027
Discovery	TA0007	System Information Discovery File and Directory Discovery	T1082 T1083
Exfiltration	TA0010	Ingress Tool Transfer Exfiltration Over C2 Channel	T1105 T1041
Impact	TA0040	Inhibit System Recovery Data Encrypted for Impact	T1490 T1486

4.3 IoC

Hash(SHA256)	Description
1f172321dfc7445019313cbed4d5f3718a6c0638f2f310918665754a9e117733	Pandora Ransomware Executable
627ede421ee51a7153ee896f657169665c1e9f79ef0ba4af1f6450d816900cbb	Pandora Ransomware Executable
5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b	Pandora Ransomware Executable