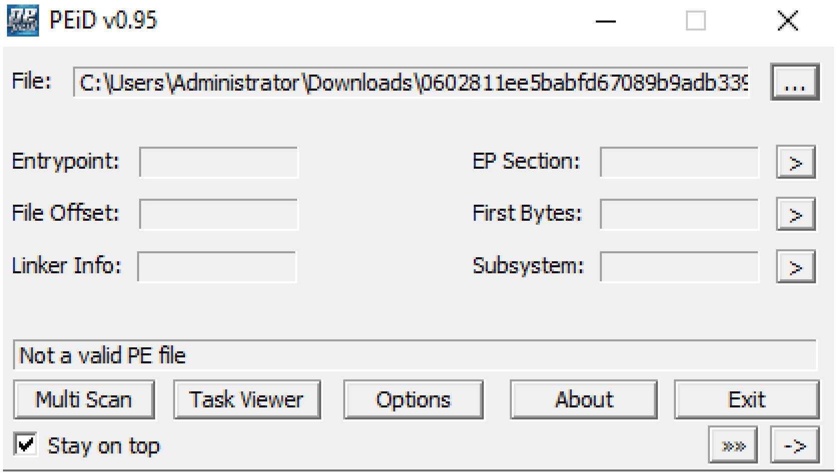
OUTPUT:

PeiD:



PEiD v0.95

File: C:\Users\Administrator\Downloads\0602811ee5babfd67089b9adb339

Entrypoint:

EP Section:

File Offset:

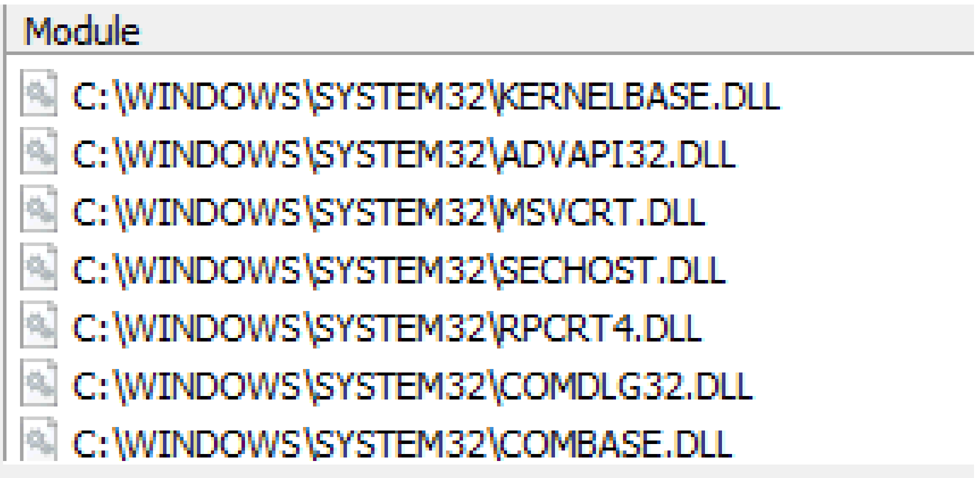
First Bytes:

Linker Info:

Subsystem:

Not a valid PE file

☑ Stay on top



Module

C:\WINDOWS\SYSTEM32\KERNELBASE.DLL

C:\WINDOWS\SYSTEM32\ADVAPI32.DLL

C:\WINDOWS\SYSTEM32\MSVCRT.DLL

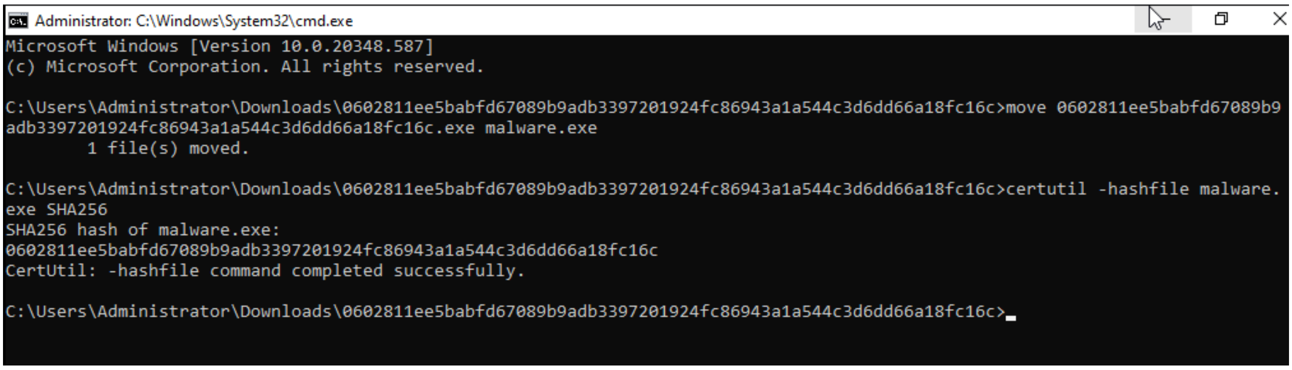
C:\WINDOWS\SYSTEM32\SECHOST.DLL

C:\WINDOWS\SYSTEM32\RPCRT4.DLL

C:\WINDOWS\SYSTEM32\COMDLG32.DLL

C:\WINDOWS\SYSTEM32\COMBASE.DLL

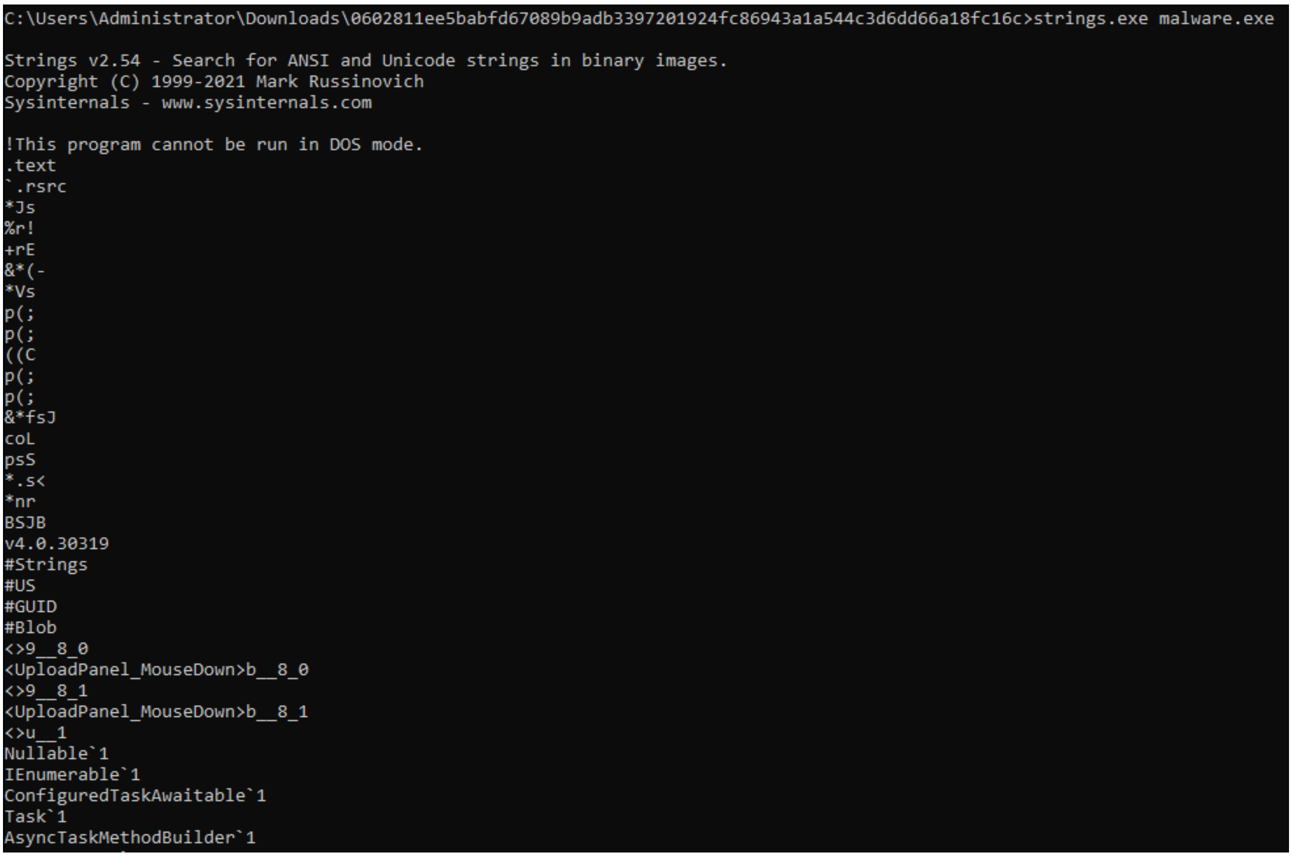
Hash:



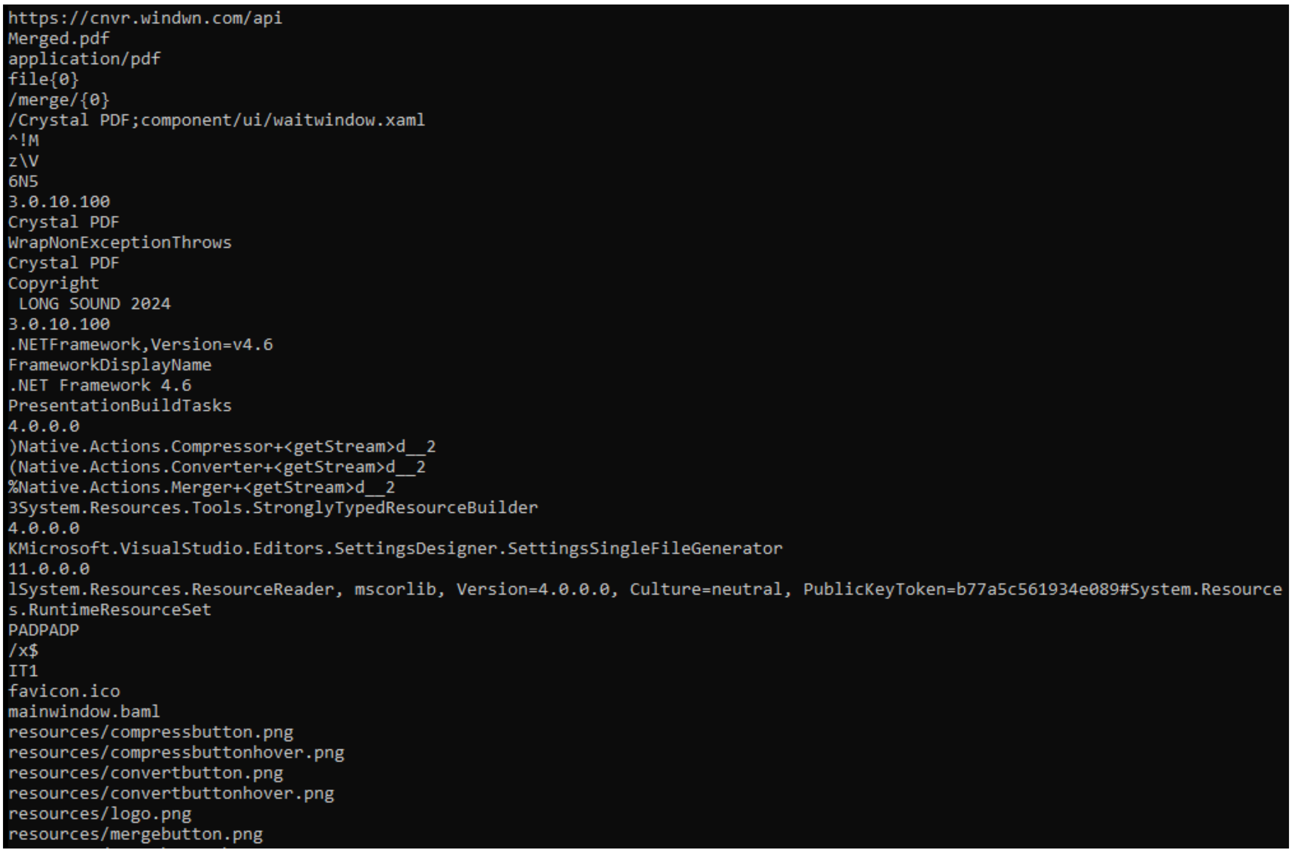
Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads\0602811ee5babfd67089b9adb3397201924fc86943a1a544c3d6dd66a18fc16c>move 0602811ee5babfd67089b9
adb3397201924fc86943a1a544c3d6dd66a18fc16c.exe malware.exe
        1 file(s) moved.

C:\Users\Administrator\Downloads\0602811ee5babfd67089b9adb3397201924fc86943a1a544c3d6dd66a18fc16c>certutil -hashfile malware.
exe SHA256
SHA256 hash of malware.exe:
0602811ee5babfd67089b9adb3397201924fc86943a1a544c3d6dd66a18fc16c
CertUtil: -hashfile command completed successfully.

C:\Users\Administrator\Downloads\0602811ee5babfd67089b9adb3397201924fc86943a1a544c3d6dd66a18fc16c>
```

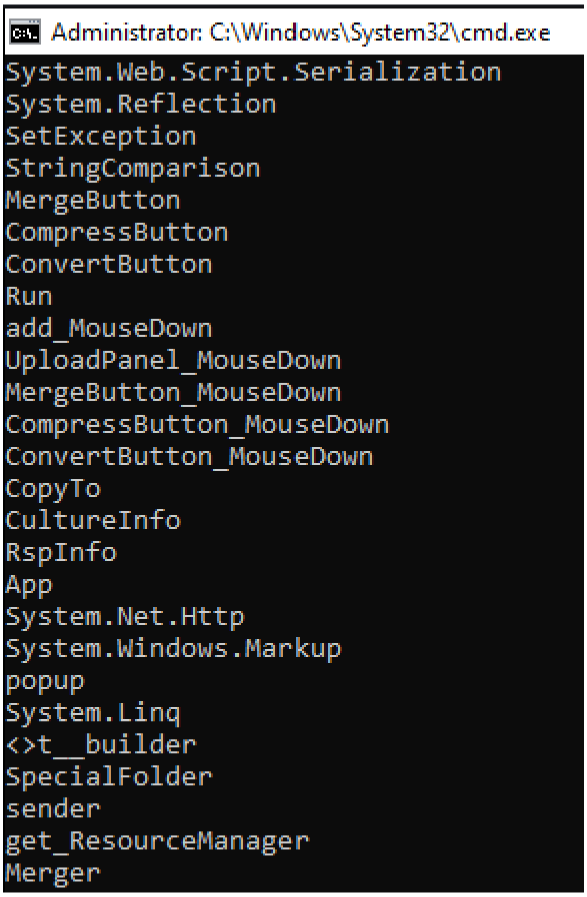
Strings:



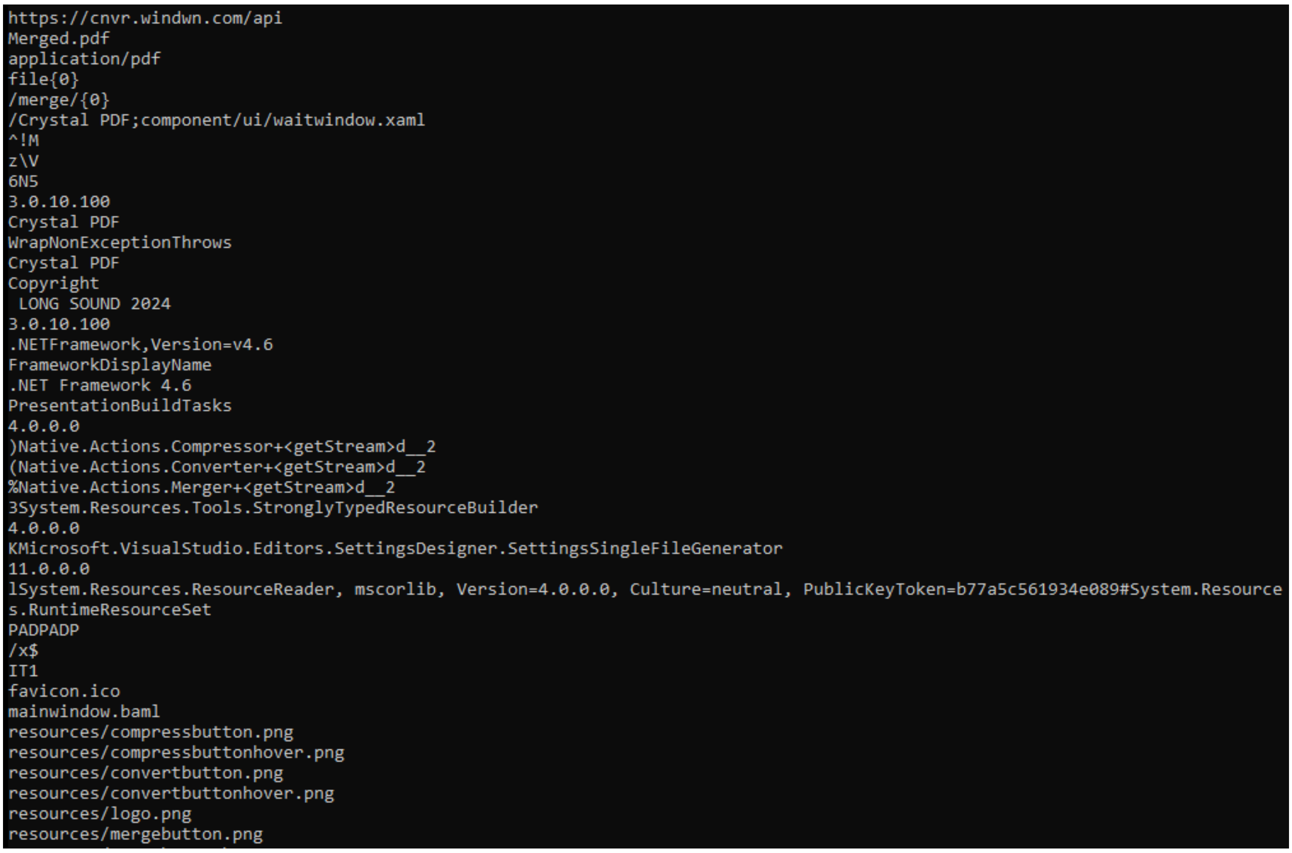
```
C:\Users\Administrator\Downloads\0602811ee5babfd67089b9adb3397201924fc86943a1a544c3d6dd66a18fc16c>strings.exe malware.exe

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.
.text
`.rsrc
*Js
%r!
+rE
&*(-
*Vs
p(;
p(;
((C
p(;
p(;
&*fsJ
coL
psS
*.s<
*nr
BSJB
v4.0.30319
#Strings
#US
#GUID
#Blob
<>9__8_0
<UploadPanel_MouseDown>b__8_0
<>9__8_1
<UploadPanel_MouseDown>b__8_1
<>u__1
Nullable`1
IEnumerable`1
ConfiguredTaskAwaitable`1
Task`1
AsyncTaskMethodBuilder`1
```



```
https://cnvr.windwn.com/api
Merged.pdf
application/pdf
file{0}
/merge/{0}
/Crystal PDF;component/ui/waitwindow.xaml
^!M
z\V
6N5
3.0.10.100
Crystal PDF
WrapNonExceptionThrows
Crystal PDF
Copyright
 LONG SOUND 2024
3.0.10.100
.NETFramework,Version=v4.6
FrameworkDisplayName
.NET Framework 4.6
PresentationBuildTasks
4.0.0.0
)Native.Actions.Compressor+<getStream>d__2
(Native.Actions.Converter+<getStream>d__2
%Native.Actions.Merger+<getStream>d__2
3System.Resources.Tools.StronglyTypedResourceBuilder
4.0.0.0
KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
11.0.0.0
lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resource
s.RuntimeResourceSet
PADPADP
/x$
IT1
favicon.ico
mainwindow.baml
resources/compressbutton.png
resources/compressbuttonhover.png
resources/convertbutton.png
resources/convertbuttonhover.png
resources/logo.png
resources/mergebutton.png
```



```
System.Web.Script.Serialization
System.Reflection
SetException
StringComparison
MergeButton
CompressButton
ConvertButton
Run
add_MouseDown
UploadPanel_MouseDown
MergeButton_MouseDown
CompressButton_MouseDown
ConvertButton_MouseDown
CopyTo
CultureInfo
RspInfo
App
System.Net.Http
System.Windows.Markup
popup
System.Linq
<>t__builder
SpecialFolder
sender
get_ResourceManager
Merger
```



```
https://cnvr.windwn.com/api
Merged.pdf
application/pdf
file{0}
/merge/{0}
/Crystal PDF;component/ui/waitwindow.xaml
^!M
z\V
6N5
3.0.10.100
Crystal PDF
WrapNonExceptionThrows
Crystal PDF
Copyright
 LONG SOUND 2024
3.0.10.100
.NETFramework,Version=v4.6
FrameworkDisplayName
.NET Framework 4.6
PresentationBuildTasks
4.0.0.0
)Native.Actions.Compressor+<getStream>d__2
(Native.Actions.Converter+<getStream>d__2
%Native.Actions.Merger+<getStream>d__2
3System.Resources.Tools.StronglyTypedResourceBuilder
4.0.0.0
KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
11.0.0.0
lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resource
s.RuntimeResourceSet
PADPADP
/x$
IT1
favicon.ico
mainwindow.baml
resources/compressbutton.png
resources/compressbuttonhover.png
resources/convertbutton.png
resources/convertbuttonhover.png
resources/logo.png
resources/mergebutton.png
```