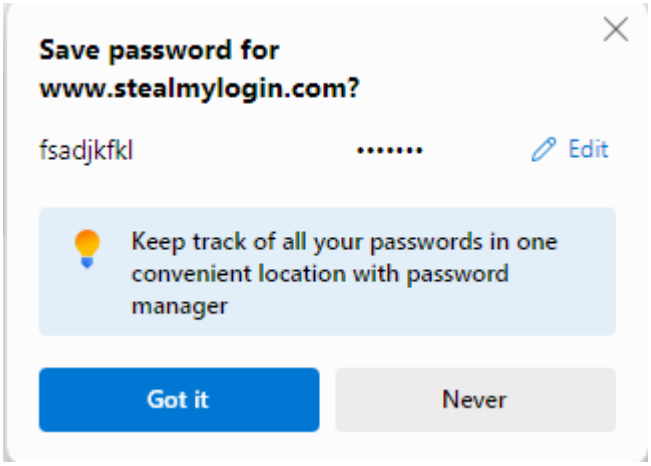
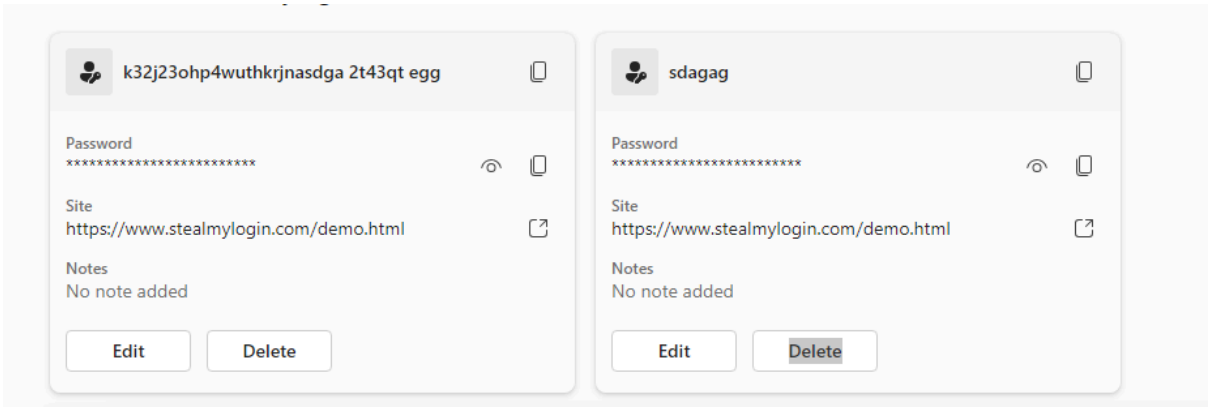
Question 1

Browser password database in MS Edge.
Let's create some credentials to be stored in the database.





Now we enter the password credentials database editor in the browser, and we will try to Edit and change this entries to locate the database.
We will look for edge process in ProcMon:

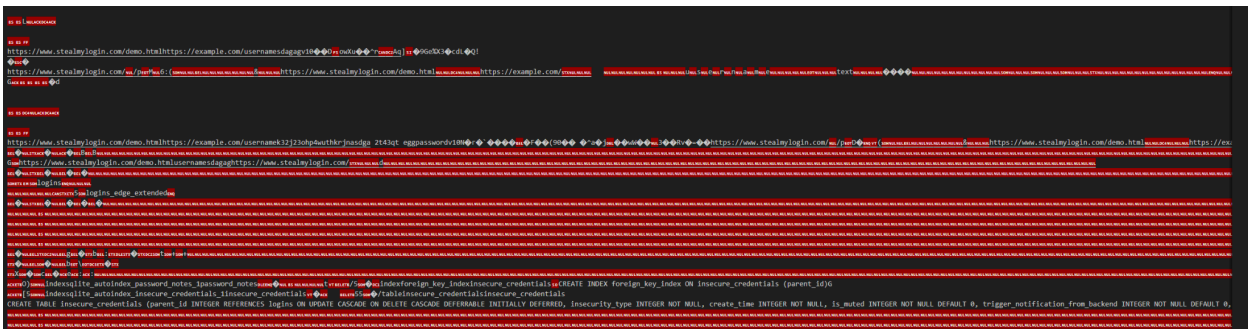
Process Name	PID	Operation	Path	Result	Detail
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\GPUCache\data_1	SUCCESS	Offset: 8,192, Length: 296
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\DawnCache\data_1	SUCCESS	Offset: 8,192, Length: 296
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,671, Length: 2
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,673, Length: 1
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,674, Length: 24
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,698, Length: 2
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,700, Length: 1
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,701, Length: 4
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,705, Length: 2
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,707, Length: 1
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,708, Length: 24
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,732, Length: 2
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,734, Length: 1
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,735, Length: 24
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Desired Access: Generic Read/Write, Delete, Disposition: Create, Optio
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Rep
msedge.exe	7100	QueryBasicInfor...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	CreationTime: 2/15/2024 9:23:42 AM, LastAccessTime: 2/15/2024 9:2
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	
msedge.exe	7100	QueryDirectory	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: Default, 2: Defa
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Offset: 0, Length: 61,514, Priority: Normal
msedge.exe	7100	FlushBuffersFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Offset: 0, Length: 65,536, I/O Flags: Non-cached, Paging I/O, Synchror
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	PRIVILEGE NOT ...	Desired Access: Write Data/Add File, Read EA, Read Attributes, Delete
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	Desired Access: Write Data/Add File, Read EA, Read Attributes, Delete
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Desired Access: Generic Read/Write, Delete, Write DAC, Write Owner,
msedge.exe	7100	QueryBasicInfor...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	CreationTime: 2/12/2024 7:29:07 AM, LastAccessTime: 2/15/2024 9:2
msedge.exe	7100	QueryBasicInfor...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	CreationTime: 2/15/2024 9:23:42 AM, LastAccessTime: 2/15/2024 9:2
msedge.exe	7100	SetBasicInform...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	CreationTime: 2/12/2024 7:29:07 AM, LastAccessTime: 0, LastWriteTim
msedge.exe	7100	QueryAttributeI...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, C
msedge.exe	7100	QueryRemotePr...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	INVALID PARAME...	
msedge.exe	7100	QuerySecurityFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	Information: Owner, DACL, Label, Attribute
msedge.exe	7100	QueryRemotePr...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	INVALID PARAME...	
msedge.exe	7100	QuerySecurityFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Information: Attribute
msedge.exe	7100	QueryRemotePr...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	INVALID PARAME...	
msedge.exe	7100	QuerySecurityFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Information: Owner
msedge.exe	7100	QueryBasicInfor...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	CreationTime: 2/12/2024 7:29:07 AM, LastAccessTime: 2/15/2024 9:2
msedge.exe	7100	QueryNameInfo...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Name: \Users\user\AppData\Local\Microsoft\Edge\User Data\Default
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Open Repars
msedge.exe	7100	QueryRemotePr...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	INVALID PARAME...	
msedge.exe	7100	QuerySecurityFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Information: DACL, DACL Unprotected
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	
msedge.exe	7100	QueryRemotePr...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	INVALID PARAME...	
msedge.exe	7100	QuerySecurityFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Information: Owner, Group, DACL, DACL Unprotected
msedge.exe	7100	SetSecurityFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Information: DACL, DACL Unprotected
msedge.exe	7100	QueryStreamInf...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	0: ::$DATA
msedge.exe	7100	FileSystemControl	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Control: FSCTL_DELETE_OBJECT_ID
msedge.exe	7100	FileSystemControl	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	OBJECTID NOT F...	Control: FSCTL_GET_OBJECT_ID
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF581c94.TMP	SUCCESS	Desired Access: Generic Write, Read Attributes, Delete, Disposition: Cre
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF581c94.TMP	SUCCESS	
msedge.exe	7100	QueryBasicInfor...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	CreationTime: 2/12/2024 7:29:07 AM, LastAccessTime: 2/15/2024 9:2
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Desired Access: Write Data/Add File, Synchronize, Disposition: Open, C
msedge.exe	7100	SetRenameInfo...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	Flags: FILE_RENAME_REPLACE_IF_EXISTS, FILE_RENAME_SUPPF
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	
msedge.exe	7100	QueryBasicInfor...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	CreationTime: 2/12/2024 7:29:07 AM, LastAccessTime: 2/15/2024 9:2
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	Desired Access: Write Data/Add File, Synchronize, Disposition: Open, C
msedge.exe	7100	SetRenameInfo...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\224f5ca8-b0d0-4546-86ec-7806921a192e.tmp	SUCCESS	Flags: FILE_RENAME_REPLACE_IF_EXISTS, FILE_RENAME_SUPPF
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default	SUCCESS	
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF581c94.TMP	SUCCESS	
msedge.exe	7100	FileSystemControl	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	Control: FSCTL_WRITE_USN_CLOSE_RECORD
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	SUCCESS	
msedge.exe	7100	CreateFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF581c94.TMP	SUCCESS	Desired Access: Read Attributes, Delete, Disposition: Open, Options: No
msedge.exe	7100	QueryAttributeT...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF581c94.TMP	SUCCESS	Attributes: A, ReparseTag: 0x0
msedge.exe	7100	SetDispositionI...	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF581c94.TMP	SUCCESS	Flags: FILE_DISPOSITION_DELETE, FILE_DISPOSITION_POSIX_SEI
msedge.exe	7100	CloseFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF581c94.TMP	SUCCESS	
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,759, Length: 2
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,761, Length: 1
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,762, Length: 24
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,786, Length: 2
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,788, Length: 1
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,789, Length: 4
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,793, Length: 2
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,795, Length: 1
msedge.exe	7100	WriteFile	C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13352491205023539	SUCCESS	Offset: 130,796, Length: 24

We see a lot of entries to a specific location in the folder:
C:\Users\user\App Data\Local\Microsoft\Edge\User Data\Default\....

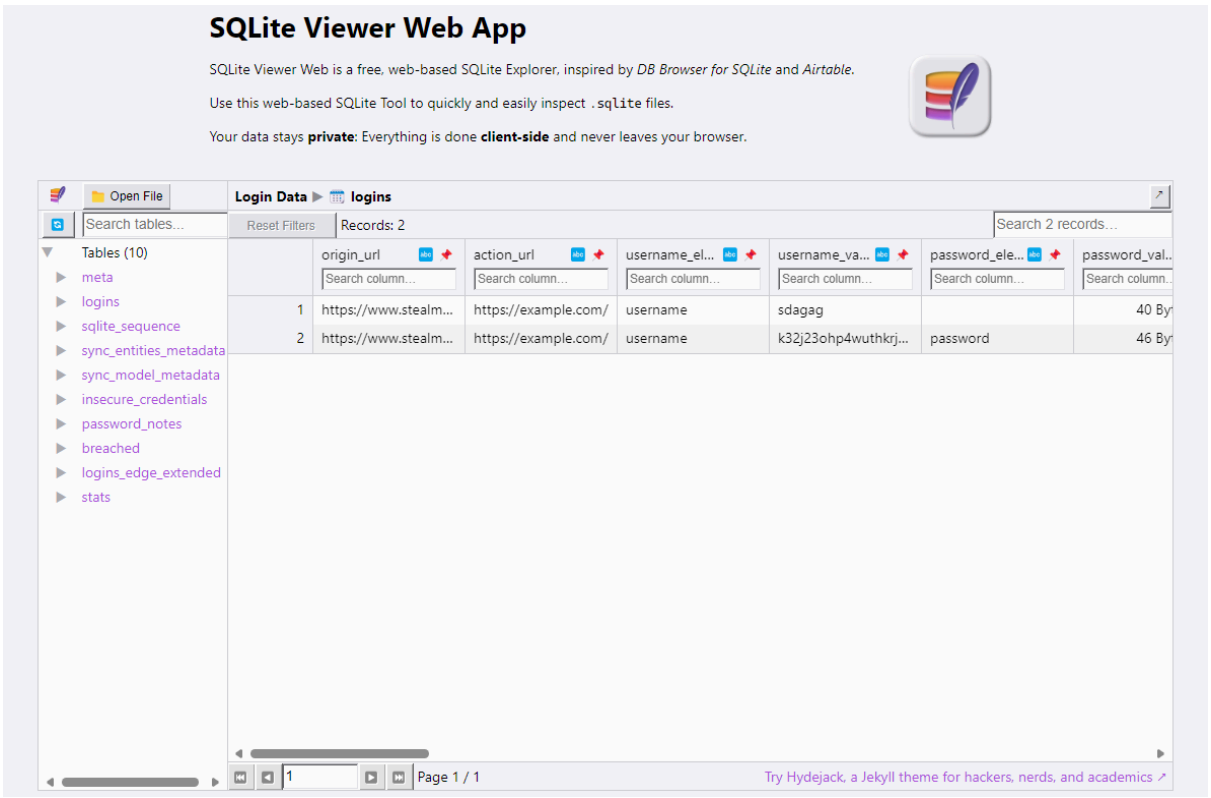
Let's view the last modified files in the Explorer after updating a password in the browser:

Name	Date modified	Type	Size
Login Data	2/15/2024 9:26 AM	File	50 KB
Login Data-journal	2/15/2024 9:26 AM	File	0 KB

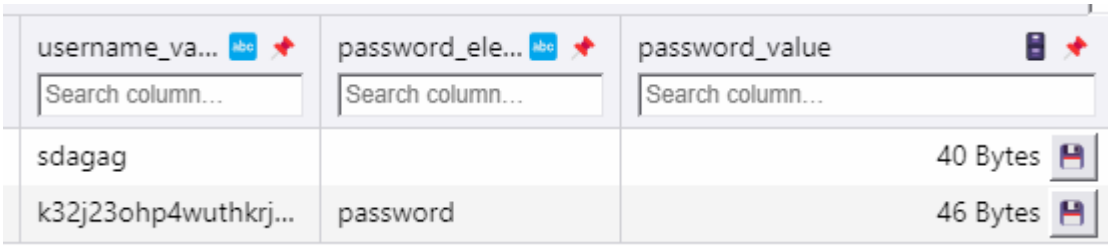
We locate the "Login Data" file that was just modified.
Let's view its contents:



We see some links to the website that we registered to create some credentials.
This file looks like a binary but includes some SQL, it's and SQLite database! Let's open this file online:



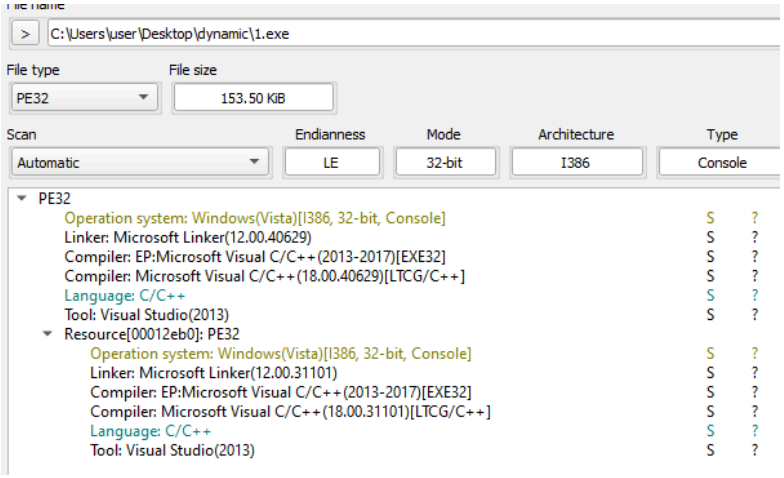
We can spot right away a table with credentials "logins"
this table has the usernames we created, and passwords.



The passwords are encrypted.
With a lookup on the MS docs, it is encrypted with local stored encryption key. so **an attacker could extract the encryption key to decrypt the passwords and gain plain text!**
Very nice!

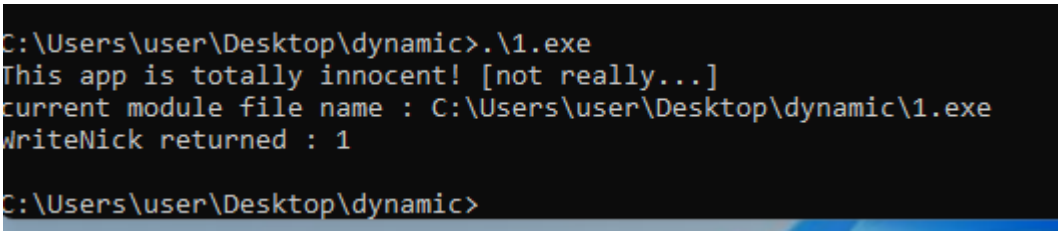
Question 2
Sample dynamic analysis

Sample 1



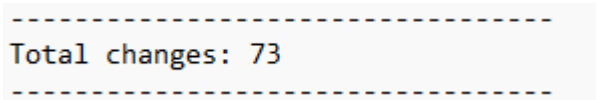
PE32 file that was compiled with Visual Studio 2013

Let's run the program and see what happens:

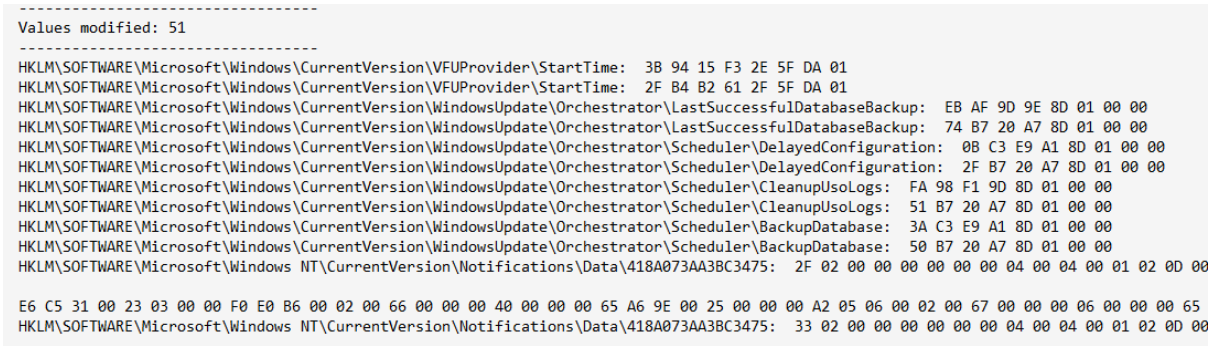


The application printed "This app is totally innocent! [not really…]"
So we can infer that it's a malware, let's see what it did.

First we will use Regshot to compare the registry before and after the program has been run.
And we see that there were some changes, keys added and deleted, values changes…



73 total changes.



A lot of unclear values that have been added

Let's see in process monitor what this malware did.

2:19:3...	1.exe	7052	Process Start		SUCCESS	Parent PID: 3664, ...
2:19:3...	1.exe	7052	Thread Create		SUCCESS	Thread ID: 1772
2:19:3...	1.exe	7052	Load Image	C:\Users\user\Desktop\dynamic\1.exe	SUCCESS	Image Base: 0xde0...
2:19:3...	1.exe	7052	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc...
2:19:3...	1.exe	7052	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77c...

At the start it loaded ntdll.dll, already suspicious.

2:19:3...	1.exe	7052	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77c...
2:19:3...	1.exe	7052	CreateFile	C:\Windows\Prefetch\1.EXE-D9EEC90C.pf	NAME NOT FOUND	Desired Access: G...
2:19:3...	1.exe	7052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	REPARSE	Desired Access: R...
2:19:3...	1.exe	7052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	Desired Access: R...
2:19:3...	1.exe	7052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\ACP	SUCCESS	Type: REG_SZ, Le...
2:19:3...	1.exe	7052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\OEMCP	SUCCESS	Type: REG_SZ, Le...
2:19:3...	1.exe	7052	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	
2:19:3...	1.exe	7052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
2:19:3...	1.exe	7052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
2:19:3...	1.exe	7052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80
2:19:3...	1.exe	7052	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
2:19:3...	1.exe	7052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
2:19:3...	1.exe	7052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
2:19:3...	1.exe	7052	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
2:19:3...	1.exe	7052	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
2:19:3...	1.exe	7052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
2:19:3...	1.exe	7052	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
2:19:3...	1.exe	7052	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\57a6ed1a-79f7-5011-b242-4784e5620cf7	NAME NOT FOUND	Length: 528
2:19:3...	1.exe	7052	QueryNameInfo...	C:\Windows\System32\ntdll.dll	SUCCESS	Name: \Windows\...

Here we see the Registry accesses that Regshot spotted.

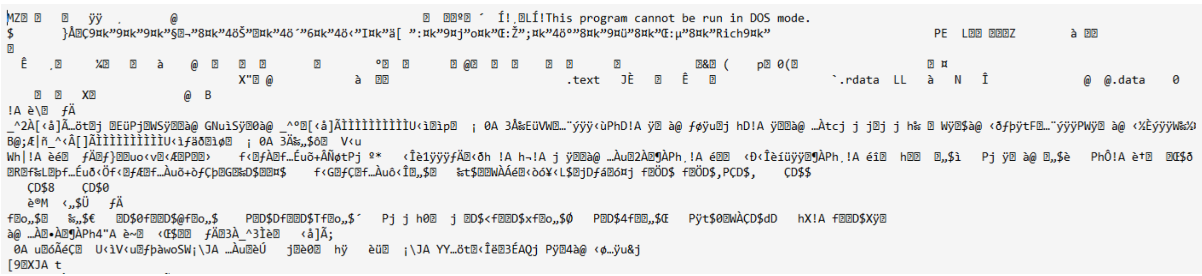
2:19:3...	1.exe	7052	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\000604xx	SUCCESS	Type: REG_SZ, Length: 26, Data: kernel32.dll
2:19:3...	1.exe	7052	QueryNameInfo...	C:\Users\user\Desktop\dynamic\1.exe	SUCCESS	Name: \Users\user\Desktop\dynamic\1.exe
2:19:3...	1.exe	7052	CreateFile	C:\Users\user\Desktop\dynamic	SUCCESS	Desired Access: Read Data/List Directory, Synchronize,...
2:19:3...	1.exe	7052	QueryDirectory	C:\Users\user\Desktop\dynamic\Clones	NO SUCH FILE	FileInformationClass: FileBothDirectoryInformation, Filter: ...
2:19:3...	1.exe	7052	CloseFile	C:\Users\user\Desktop\dynamic	SUCCESS	
2:19:3...	1.exe	7052	CreateFile	C:\Users\user\Desktop\dynamic\Clones	SUCCESS	Desired Access: Read Data/List Directory, Synchronize,...
2:19:3...	1.exe	7052	CloseFile	C:\Users\user\Desktop\dynamic\Clones	SUCCESS	
2:19:3...	1.exe	7052	CreateFile	C:\Users\user\Desktop\dynamic\1.exe	SUCCESS	Desired Access: Generic Read, Disposition: OpenIf, Opti...
2:19:3...	1.exe	7052	CreateFile	C:\Users\user\Desktop\dynamic	SUCCESS	Desired Access: Read Data/List Directory, Synchronize,...
2:19:3...	1.exe	7052	QueryDirectory	C:\Users\user\Desktop\dynamic\1.exe	SUCCESS	FileInformationClass: FileBothDirectoryInformation, Filter: ...
2:19:3...	1.exe	7052	ReadFile	C:\Users\user\Desktop\dynamic\1.exe	SUCCESS	Offset: 0, Length: 157,184, Priority: Normal
2:19:3...	1.exe	7052	CloseFile	C:\Users\user\Desktop\dynamic\1.exe	SUCCESS	
2:19:3...	1.exe	7052	CreateFile	C:\Users\user\Desktop\dynamic\Clones\Nick.jpg	SUCCESS	Desired Access: Generic Read/Write/Execute, Dispositi...
2:19:3...	1.exe	7052	WriteFile	C:\Users\user\Desktop\dynamic\Clones\Nick.jpg	SUCCESS	Offset: 0, Length: 158,184, Priority: Normal
2:19:3...	1.exe	7052	CloseFile	C:\Users\user\Desktop\dynamic\Clones\Nick.jpg	SUCCESS	

At the end it creates a Clones directory and saves Nick.jpg to it.

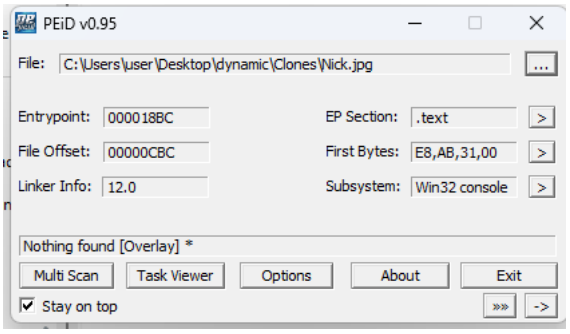
Nick.jpg

It looks like we don't support this file format.

The Nick.jpg is not supported image format. Let's open it with a notepad.

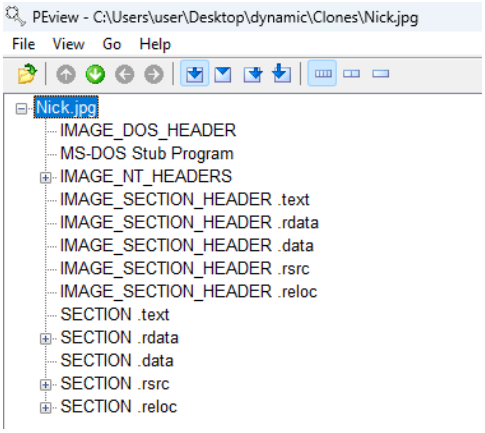


The is actually a PE. (we can see the DOS header)



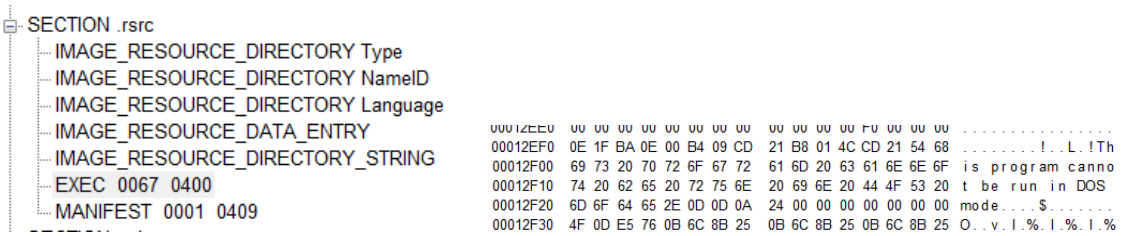
However PEiD doesn't spot it as PE.

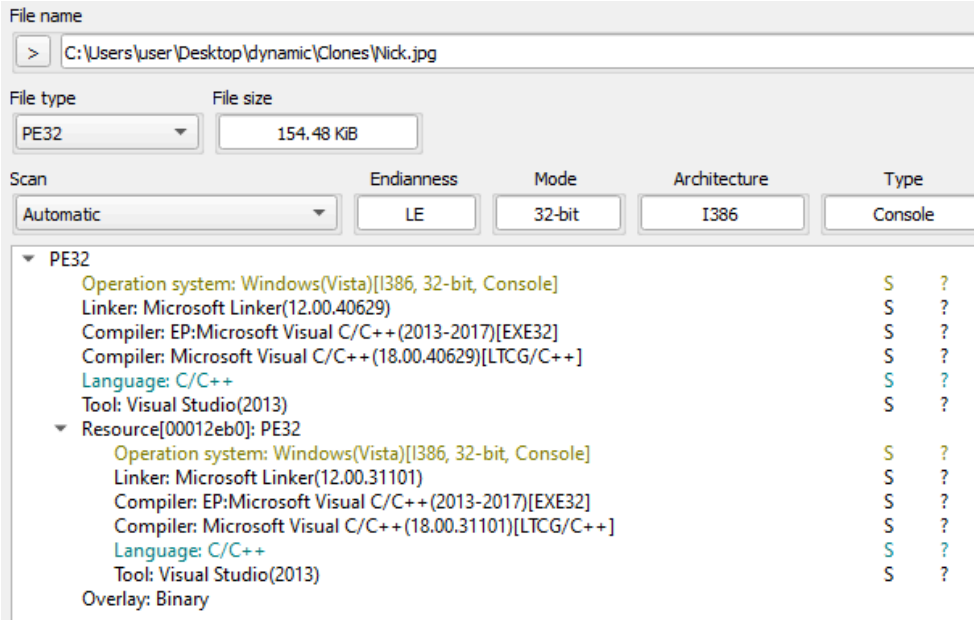
We can still open it in PEview:



That PE was compiled in 2017.
In the rdata section in the import address table we can see, Is DebuggerPresent.
That malware tries to evade forensics.

Inside the resource section appears to be another PE





In DiE it appears that the Nick.jpg is a copy of the 1.exe file itself, they share similar structure and approximately the same size.
Let's try to run Nick.jpg via changing it to Nick.exe.

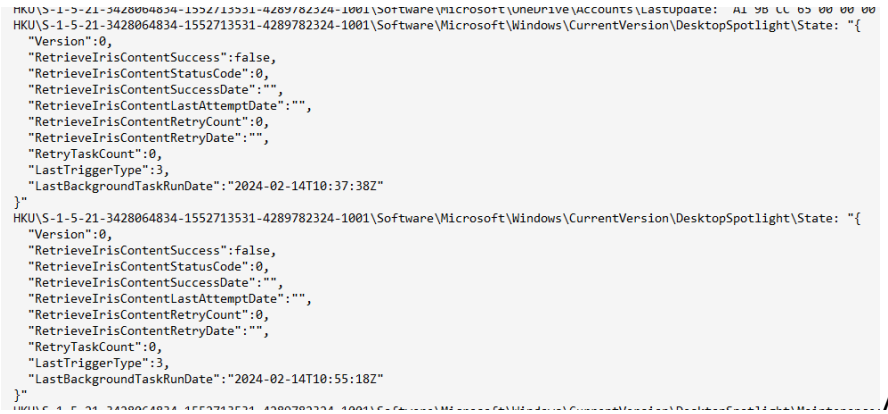
It appear to run the same program but now it added output of: "createprocess returned: 1" seems like it did something different this time.

```
C:\Users\user\Desktop\dynamic\Clones>.\Nick.exe
This app is totally innocent! [not really...]
current module file name : C:\Users\user\Desktop\dynamic\Clones\Nick.exe
WriteNick returned : 1
CreateProcess returned : 1
```

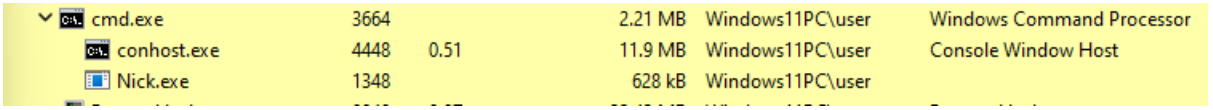
Again RegShot shows that the registry was changed:

```
-----------------------------------
Total changes: 43
-----------------------------------
```

And the Process Monitor confirms it.

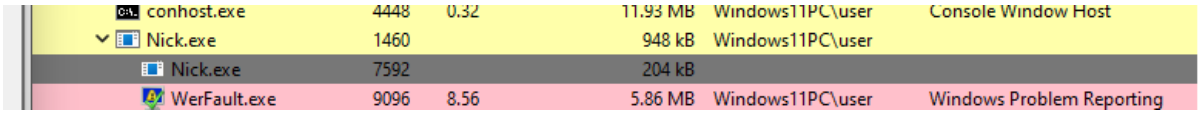


Appear to be some kind of BackgroundTask to run scheduled to run in 8 hours from now.
If we run the program the second time it appear to do just hang:

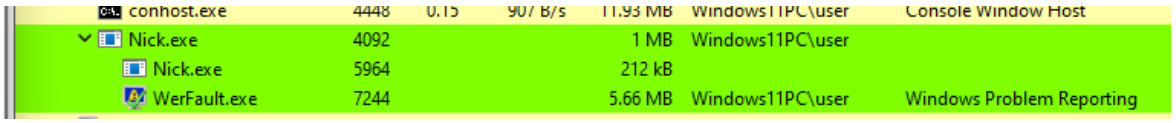



```
C:\Users\user\Desktop\dynamic\Clones>.\Nick.exe
This app is totally innocent! [it really is]
```

If we try to run the clone of the clone it seems that he gets some error:



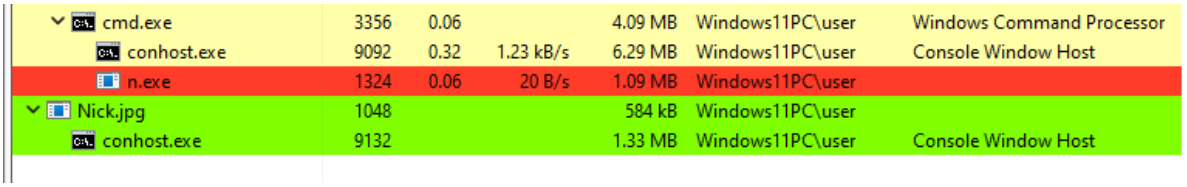
And if we run it multiple times only one Clone is created.




```
C:\Users\user\Desktop\dynamic\Clones\Clones\Clones>.\Nick.exe
This app is totally innocent! [not really...]
current module file name : C:\Users\user\Desktop\dynamic\Clones\Clones\Clones\Nick.exe
WriteNick returned : 1
```

It doesn't create the process again.
The second Nick appears to be special, he runs some process only once and hangs on later runs. the rest of the Clones as we go further are seems to be same and just continue to copy itself.

The second Clone creates a process "Nick.jpg" for couple of milliseconds and closes.



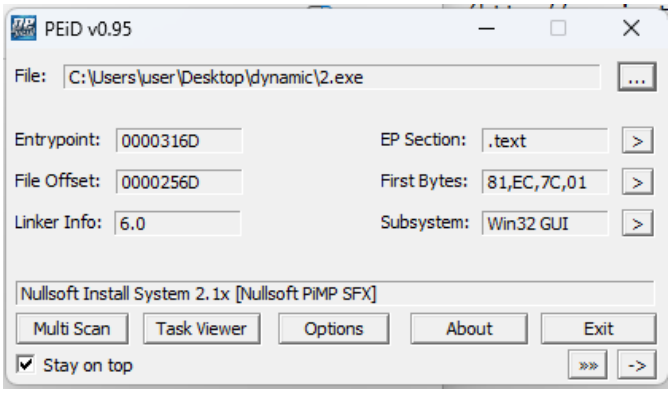
Nick.jpg the special process that starts from the **first Clone** appears to change the Nick.exe itself, that's probably why Nick.exe hangs after the second run.

After restart and change of time I didn't notice anything new.

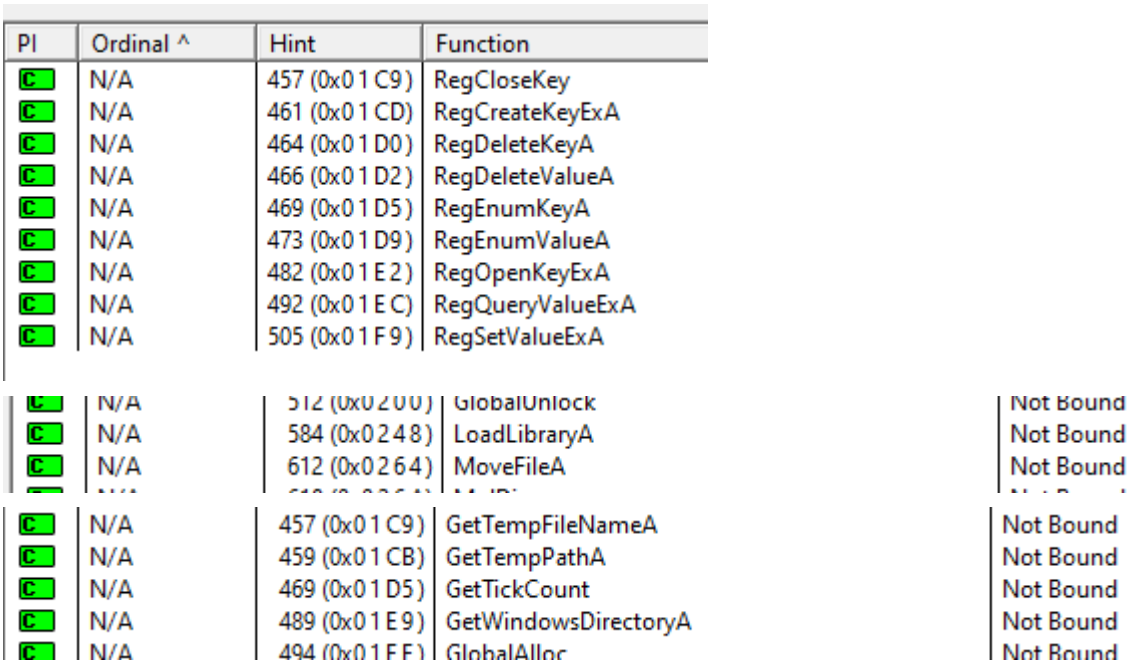
Conclusion 1

Looks like a worm that replicates itself and ensures only to be run once, probably so it won't reinfect a computer multiple times. Didn't spot any try to go out to the network or to jump to an adjacent computer. Didn't try to establish a connection to a C2 server.
Changes the registry probably for persistence.

Sample 2

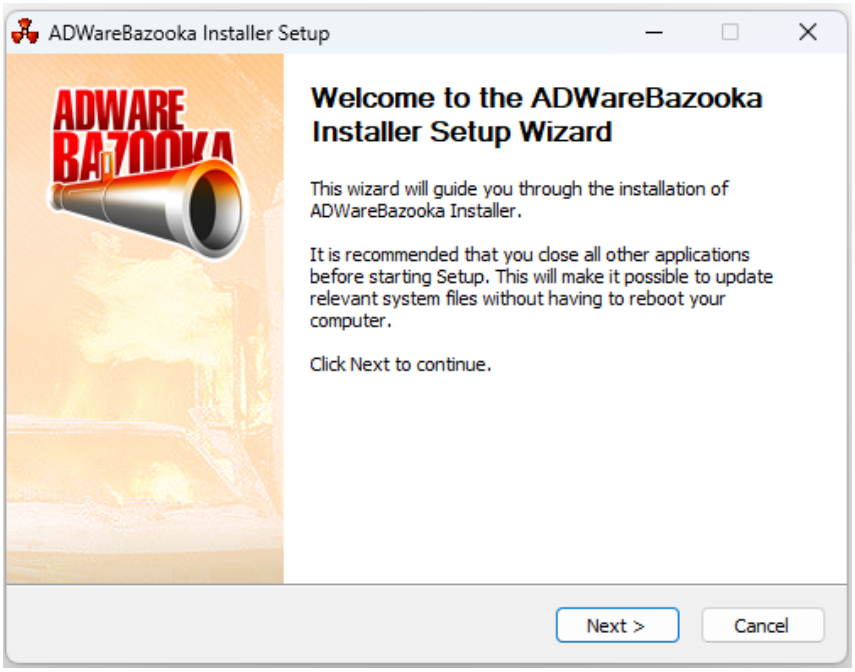


This file is an installer.
In the dependency walker we see registry access:

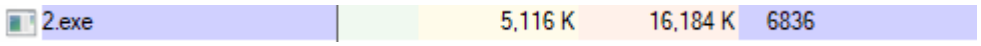


PI	Ordinal ^	Hint	Function	
C	N/A	457 (0x01C9)	RegCloseKey	
C	N/A	461 (0x01CD)	RegCreateKeyExA	
C	N/A	464 (0x01D0)	RegDeleteKeyA	
C	N/A	466 (0x01D2)	RegDeleteValueA	
C	N/A	469 (0x01D5)	RegEnumKeyA	
C	N/A	473 (0x01D9)	RegEnumValueA	
C	N/A	482 (0x01E2)	RegOpenKeyExA	
C	N/A	492 (0x01EC)	RegQueryValueExA	
C	N/A	505 (0x01F9)	RegSetValueExA	
C	N/A	512 (0x0200)	GlobalUnlock	Not Bound
C	N/A	584 (0x0248)	LoadLibraryA	Not Bound
C	N/A	612 (0x0264)	MoveFileA	Not Bound
C	N/A	457 (0x01C9)	GetTempFileNameA	Not Bound
C	N/A	459 (0x01CB)	GetTempPathA	Not Bound
C	N/A	469 (0x01D5)	GetTickCount	Not Bound
C	N/A	489 (0x01E9)	GetWindowsDirectoryA	Not Bound
C	N/A	494 (0x01EE)	GlobalAlloc	Not Bound

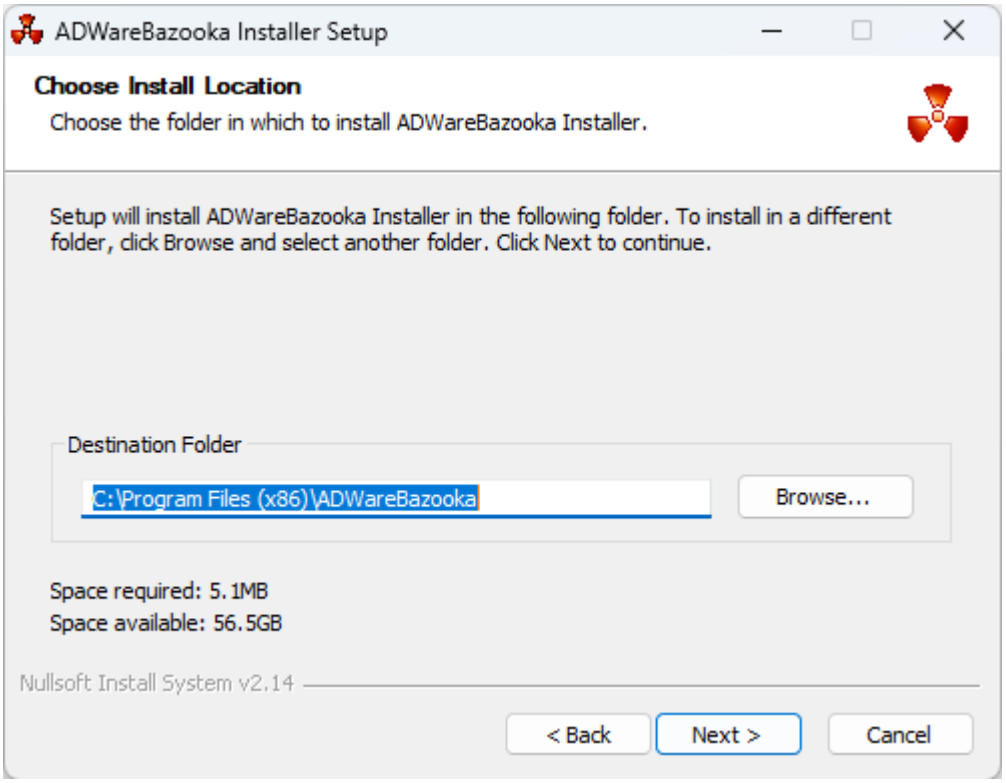
We also see loadlibrary and gettickcount.
Let's Run the program and analyze it with ProcMon, RegShot and ProcessExplorer:



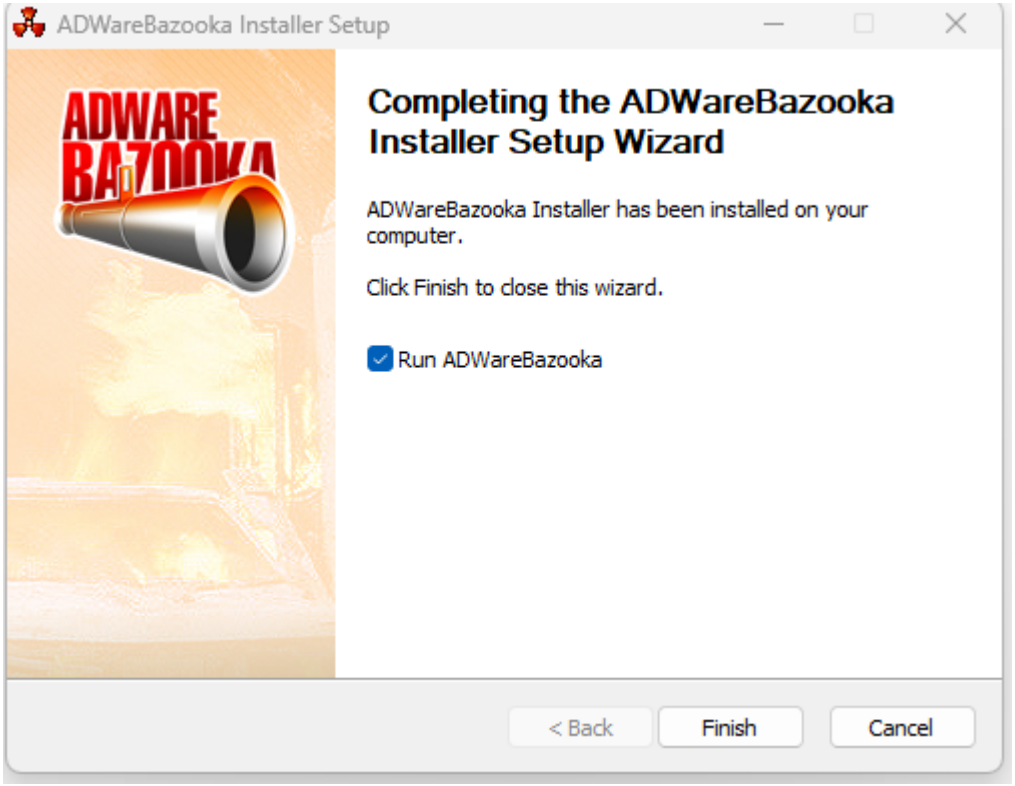
Installation window pops up,



And we can see the process is up.

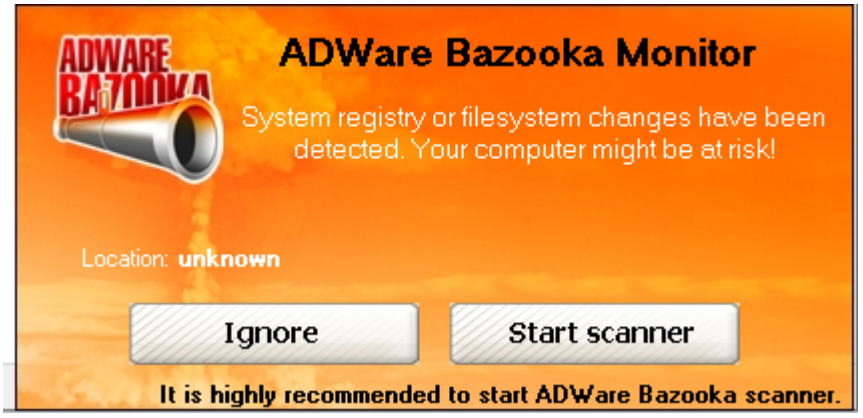


Let’s try to install in the Default location.



2.exe	1.06	5,616 K	21,156 K	6836
adwarebazooka_monitor....	< 0.01	7,484 K	17,696 K	4212

At the finish of installation another child process opens up.



This window appears on the bottom right corner of the screen and suggests a scan.

After clicking on finish and running ADWareBazooka, another screen appears, and another process starts:

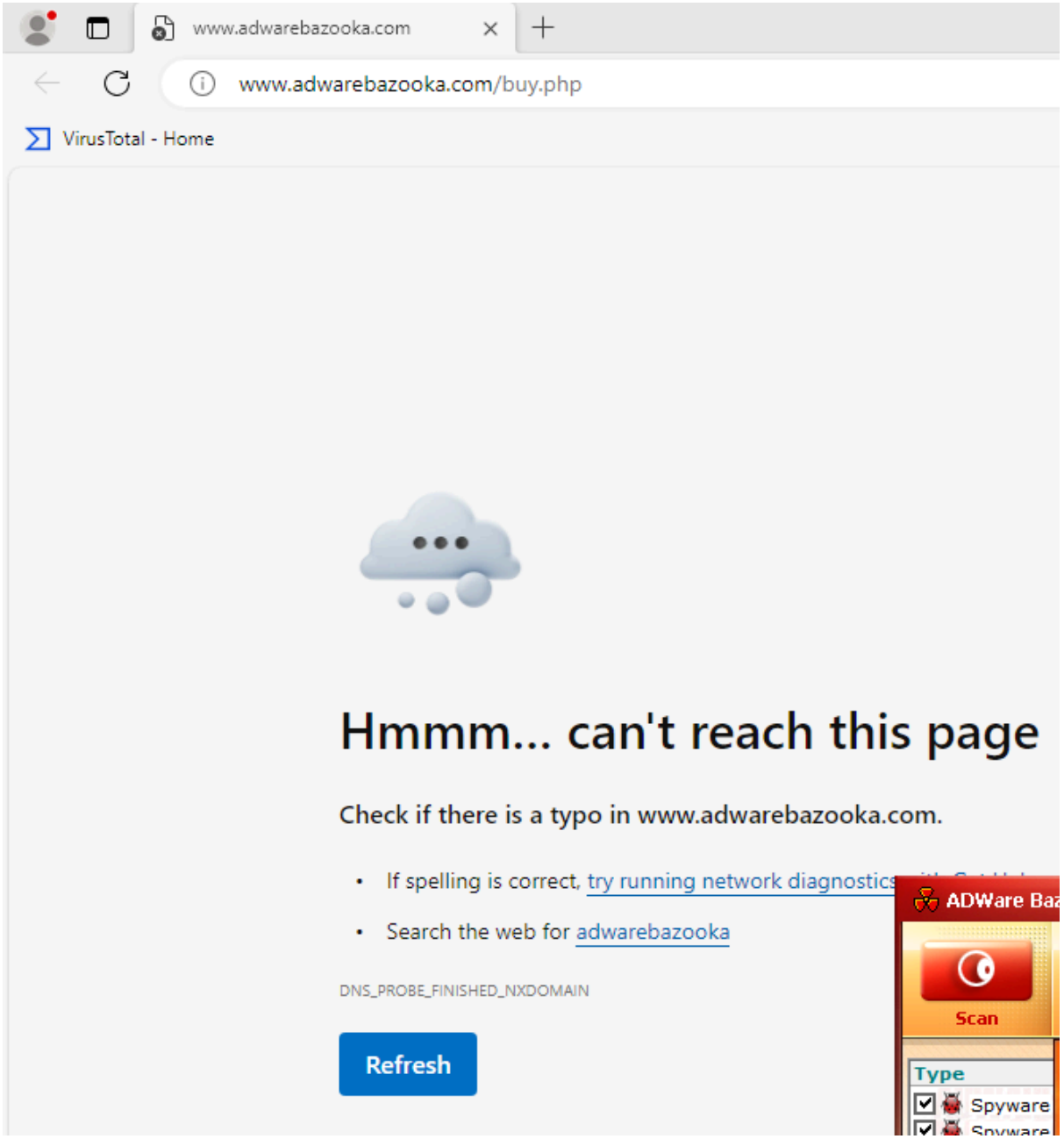
adwarebazooka_monitor.exe	< 0.01	7,336 K	17,736 K	4212
adwarebazooka.exe	< 0.01	15,416 K	30,292 K	7548

We see a window that started a scan
and showing us “Spyware”.

After clicking “Ok” let’s try to press “Remove”


ADWare Bazooka
Scan
Settings
Privacy
Recovery
Tools
Live update
Register
Type
Spyware
Spyware
Spyware
In order to activate all the features of ADWare Bazooka you should register the program with product key.
Please enter your name and product key into the fileds below.
Your e-mail
A
Product Key
Ok
Cancel
Buy now!
5/2024
Monitor:
Enabled
Save log
Save susp.
Select all
Select none
Remove


ADWare Bazooka
Scan
Settings
Privacy
Recovery
Tools
Live update
Register
Type
Spyware
Spyware
Spyware
In order to activate all the features of ADWare Bazooka you should register the program with product key.
Please enter your name and product key into the fileds below.
Your e-mail
mail@mail.com
Product Key
5k2n5klj53j453l4;5bl
Ok
Cancel
Buy now!
5/2024
Monitor:
Enabled
Save log
Save susp.
Select all
Select none
Remove



It seems that it tried to connect to www.adwarebazooka.com

Let's close the window:

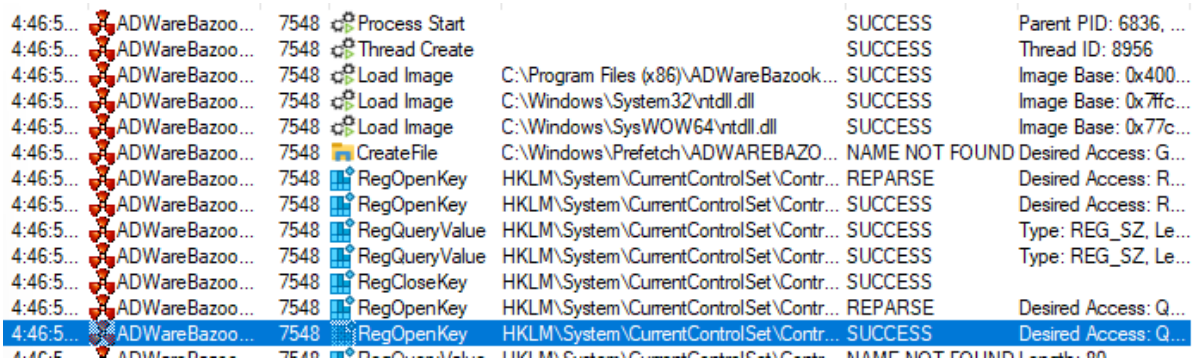
adwarebazooka_monitor.exe	< 0.01	7,352 K	17,428 K	4212
adwarebazooka.exe	< 0.01	15,952 K	35,904 K	7548

And those processes still remain in background.
Let's look on the registry via RegShot:

```
HKU\S-1-5-18\Software\Microsoft\Window

----------------------------------
Total changes: 373704
----------------------------------
```

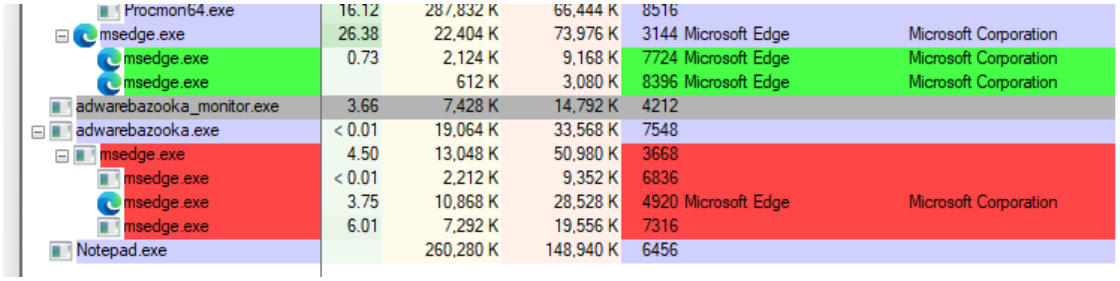
Wow! a lot of changes have been made!
Let's analyze the events in ProcMon



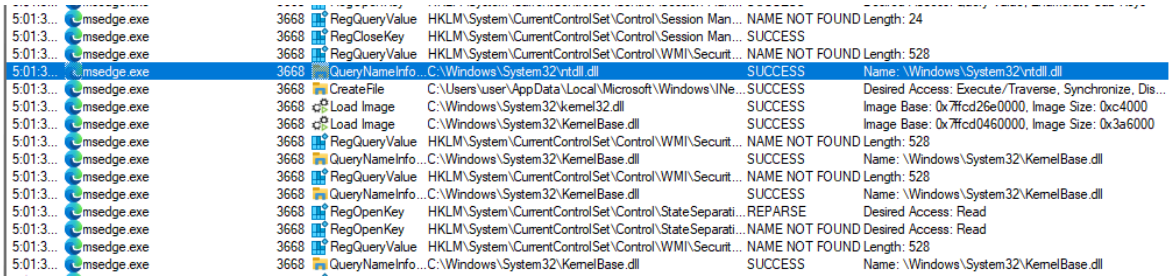
4:46:5...	ADWareBazoo...	7548	Process Start		SUCCESS	Parent PID: 6836, ...
4:46:5...	ADWareBazoo...	7548	Thread Create		SUCCESS	Thread ID: 8956
4:46:5...	ADWareBazoo...	7548	Load Image	C:\Program Files (x86)\ADWareBazook...	SUCCESS	Image Base: 0x400...
4:46:5...	ADWareBazoo...	7548	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc...
4:46:5...	ADWareBazoo...	7548	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77c...
4:46:5...	ADWareBazoo...	7548	CreateFile	C:\Windows\Prefetch\ADWAREBAZO...	NAME NOT FOUND	Desired Access: G...
4:46:5...	ADWareBazoo...	7548	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
4:46:5...	ADWareBazoo...	7548	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
4:46:5...	ADWareBazoo...	7548	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
4:46:5...	ADWareBazoo...	7548	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
4:46:5...	ADWareBazoo...	7548	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
4:46:5...	ADWareBazoo...	7548	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
4:46:5...	ADWareBazoo...	7548	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...

Straight away from the start it tries to open the registry.

When we press the “Buy” msedge.exe opens for a second under the process tree, and then closes pretty fast and opens as an individual process:



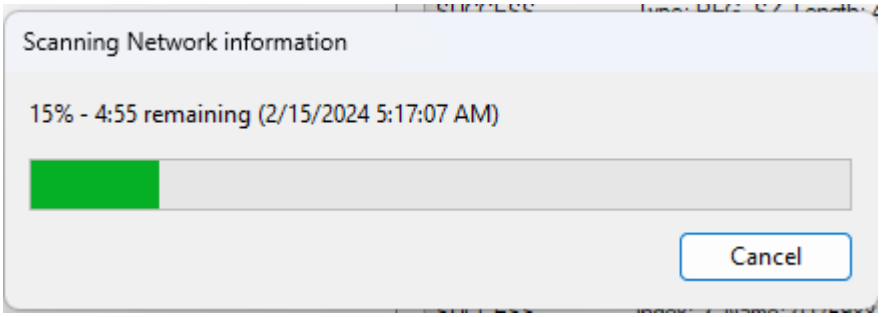
Procmon64.exe	16.12	287,832 K	66,444 K	8516		
msedge.exe	26.38	22,404 K	73,976 K	3144	Microsoft Edge	Microsoft Corporation
msedge.exe	0.73	2,124 K	9,168 K	7724	Microsoft Edge	Microsoft Corporation
msedge.exe		612 K	3,080 K	8396	Microsoft Edge	Microsoft Corporation
adwarebazooka_monitor.exe	3.66	7,428 K	14,792 K	4212		
adwarebazooka.exe	< 0.01	19,064 K	33,568 K	7548		
msedge.exe	4.50	13,048 K	50,980 K	3668		
msedge.exe	< 0.01	2,212 K	9,352 K	6836		
msedge.exe	3.75	10,868 K	28,528 K	4920	Microsoft Edge	Microsoft Corporation
msedge.exe	6.01	7,292 K	19,556 K	7316		
Notepad.exe		260,280 K	148,940 K	6456		



5:01:3...	msedge.exe	3668	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Man...	NAME NOT FOUND Length: 24
5:01:3...	msedge.exe	3668	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Man...	SUCCESS
5:01:3...	msedge.exe	3668	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Securit...	NAME NOT FOUND Length: 528
5:01:3...	msedge.exe	3668	QueryNameInfo...	C:\Windows\System32\ntdll.dll	SUCCESS Name: \Windows\System32\ntdll.dll
5:01:3...	msedge.exe	3668	CreateFile	C:\Users\user\AppData\Local\Microsoft\Windows\INe...	SUCCESS Desired Access: Execute/Traverse, Synchronize, Dis...
5:01:3...	msedge.exe	3668	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS Image Base: 0x7ffcd26e0000, Image Size: 0xc4000
5:01:3...	msedge.exe	3668	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS Image Base: 0x7ffcd0460000, Image Size: 0x3a6000
5:01:3...	msedge.exe	3668	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Securit...	NAME NOT FOUND Length: 528
5:01:3...	msedge.exe	3668	QueryNameInfo...	C:\Windows\System32\KernelBase.dll	SUCCESS Name: \Windows\System32\KernelBase.dll
5:01:3...	msedge.exe	3668	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Securit...	NAME NOT FOUND Length: 528
5:01:3...	msedge.exe	3668	QueryNameInfo...	C:\Windows\System32\KernelBase.dll	SUCCESS Name: \Windows\System32\KernelBase.dll
5:01:3...	msedge.exe	3668	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparati...	REPARSE Desired Access: Read
5:01:3...	msedge.exe	3668	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparati...	NAME NOT FOUND Desired Access: Read
5:01:3...	msedge.exe	3668	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Securit...	NAME NOT FOUND Length: 528
5:01:3...	msedge.exe	3668	QueryNameInfo...	C:\Windows\System32\KernelBase.dll	SUCCESS Name: \Windows\System32\KernelBase.dll

It queries Ntdll.dll and opens the registry.
after this it makes a lot of changes to the registry.

Let’s check what did it do in the network in procmon:



there was a TCP connection to some IP via the browser via :

Process Name	PID	Operation	Path	Result	Detail
msedge.exe	7724	TCP Connect	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, r...
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 293, startime: 184877, endtime: 184877, seq...
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 99, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 99, seqnum: 0, connid: 0
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 364, startime: 184894, endtime: 184894, seq...
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1460, seqnum: 0, connid: 0
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1460, seqnum: 0, connid: 0
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1460, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 4096, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 284, seqnum: 0, connid: 0
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1460, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1460, seqnum: 0, connid: 0
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 532, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 532, seqnum: 0, connid: 0
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 74, startime: 184911, endtime: 184911, seqn...
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1210, startime: 184914, endtime: 184914, se...
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 3715, startime: 184914, endtime: 184914, se...
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 103, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 103, seqnum: 0, connid: 0
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 841, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 841, seqnum: 0, connid: 0
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1210, startime: 185080, endtime: 185080, se...
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 3715, startime: 185080, endtime: 185080, se...
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 841, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 841, seqnum: 0, connid: 0
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 1210, startime: 185333, endtime: 185333, se...
msedge.exe	7724	TCP Send	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 3715, startime: 185333, endtime: 185333, se...
msedge.exe	7724	TCP TCPCopy	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 841, seqnum: 0, connid: 0
msedge.exe	7724	TCP Receive	Windows11PC:50585 -> 20.42.65.92:https	SUCCESS	Length: 841, seqnum: 0, connid: 0

Command Line:

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\user\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=pt

54 "--annotation=prod=Microsoft Edge" --annotation=ver=121.0.2277.112 --initial-client-data=0x258,0x25c,0x260,0x254,0x280,0x7ffcb676bf98,0x7ffcb676bfa4,0x7ffcb676bfb0

Maybe it tries to exfiltrate the data it collected in the registry…

Let's restart the computer.

adwarebazooka_monitor.exe		2,936 K	8,984 K	6360 The SpyGuard Monitor	thespyguard.com
adwarebazooka_monitor....	Susp...	460 K	24 K	6412	
WerFault.exe		6,044 K	24,568 K	2180 Windows Problem Reporting	Microsoft Corporation

and we see the process pops up and closes after that.

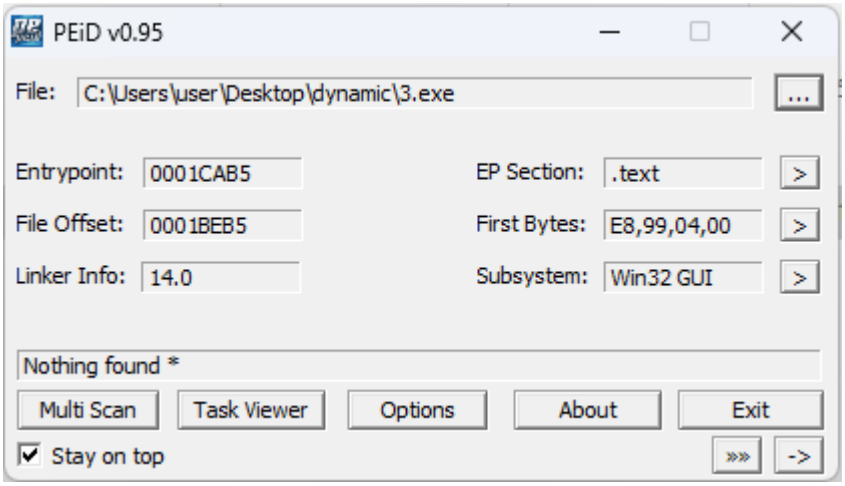
the malware gained persistence.

Conclusion 2

Looks like a Trojan that advertises itself as an Antivirus/ Anti Adware but requests payment for services it doesn't provide. (Because there is no real malware on my VM and it still demanded payment for clearing the "viruses")
Gained persistence and installed itself on the computer. Could be exfiltrating data through the browser.

Sample 3

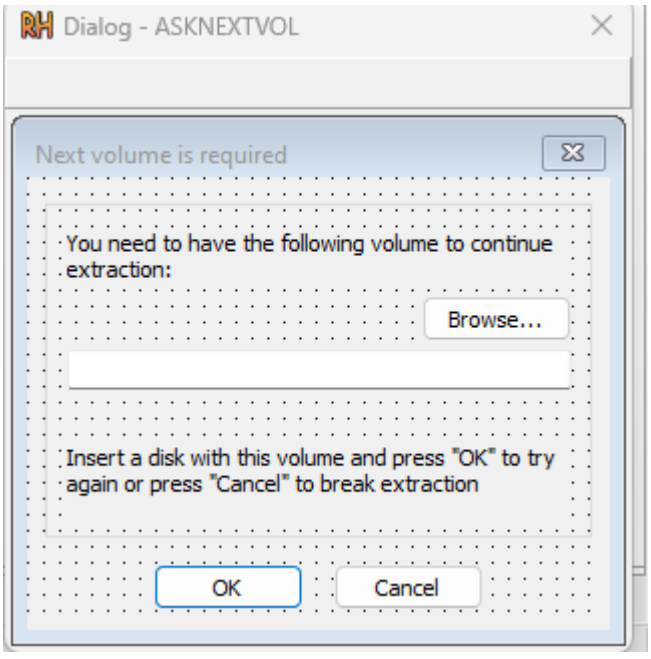
We can see that sample 3 uses some kind of packing. PEiD didn't successfully identify the packer.



In PEview we observe the following imported functions:

0002E564	0003867E	Hint/Name RVA	0273 GetSystemInfo
0002E568	0003868E	Hint/Name RVA	04EF VirtualProtect
0002E56C	000386A0	Hint/Name RVA	04F1 VirtualQuery
0002E570	000386B0	Hint/Name RVA	033D LoadLibraryExA
0002E574	000386C2	Hint/Name RVA	0304 IsProcessorFeaturePresent
0002E578	000386DE	Hint/Name RVA	0300 IsDebuggerPresent

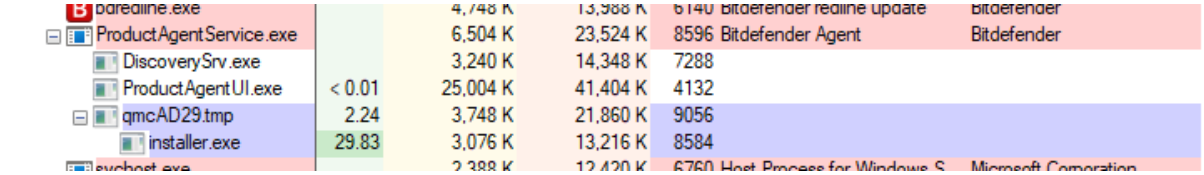
It uses Virtual protect to change permissions, LoadLibrary and checks IsDebuggerPresent.
In the resource section we see a lot of Icons and dialog windows such as:



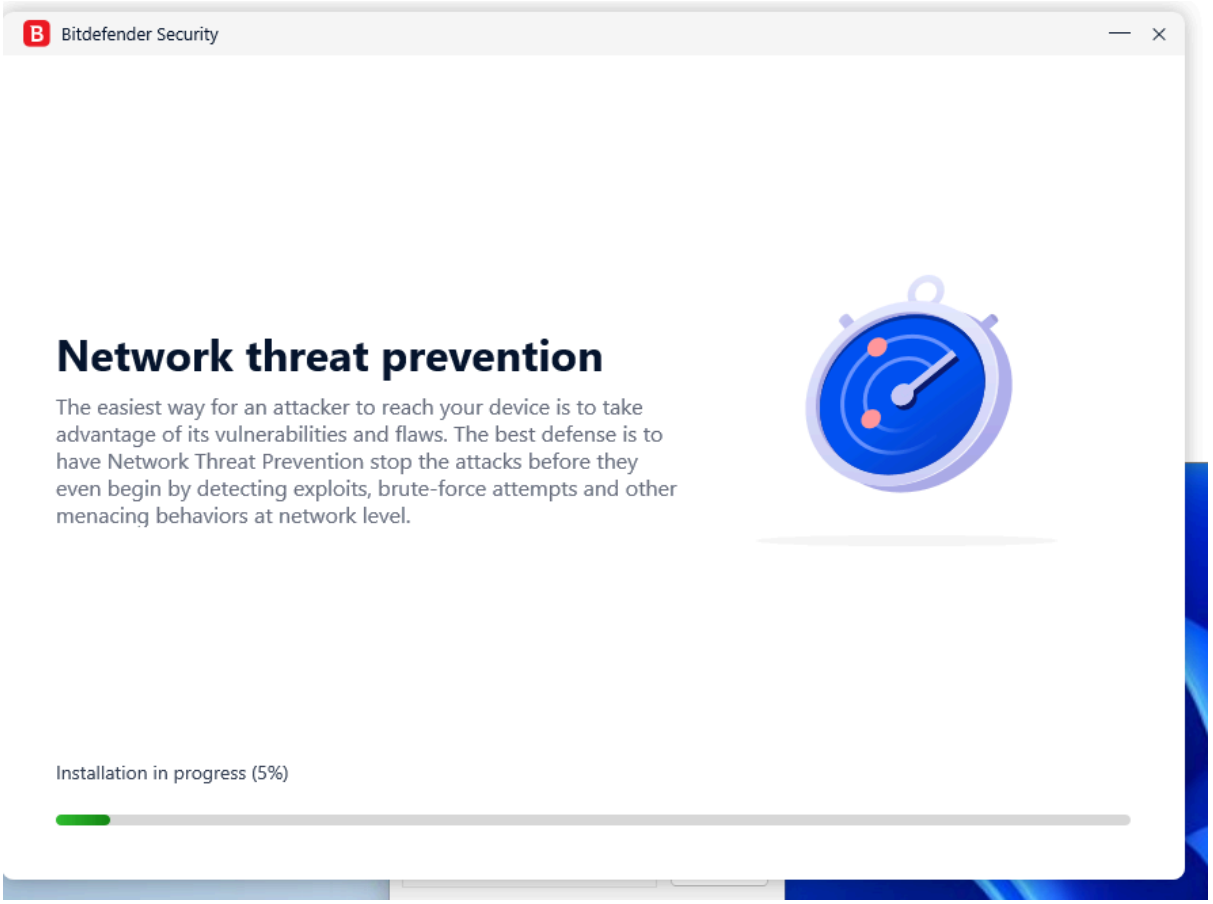
Let's continue with running the sample and analyzing it.

This is the window that opens up, and it appears to download 708MB from the Internet.
It runs as a service:

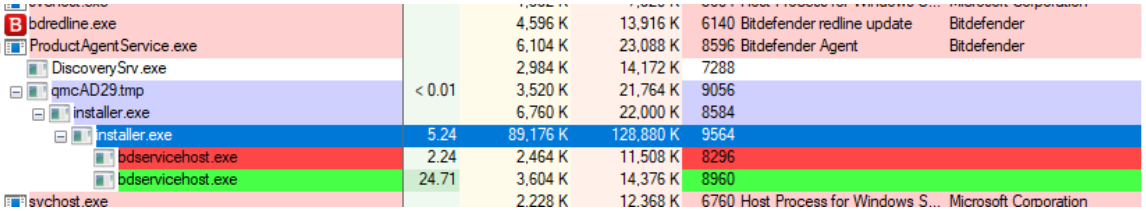
under winit.exe under services.exe



also there appears another ProductAgentService.exe

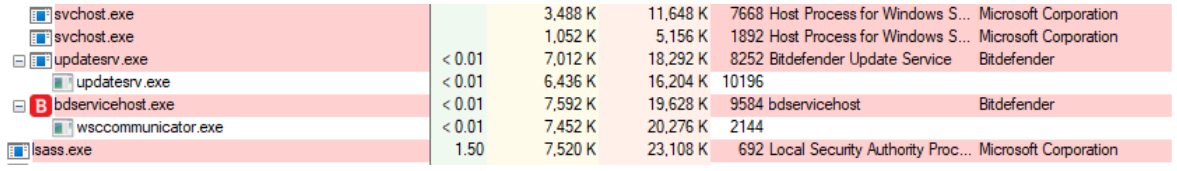


After that a installation phase beggins.

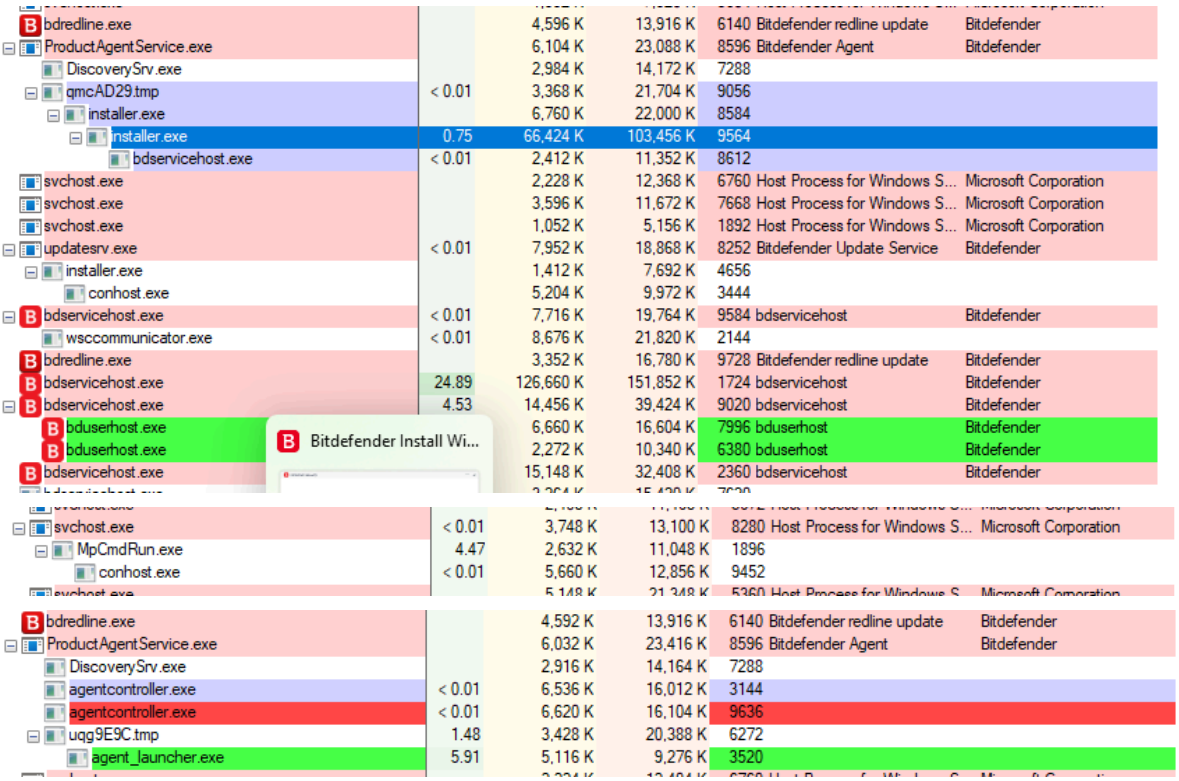


A lot of processes under the services.exe start to pop up including the installer.exe

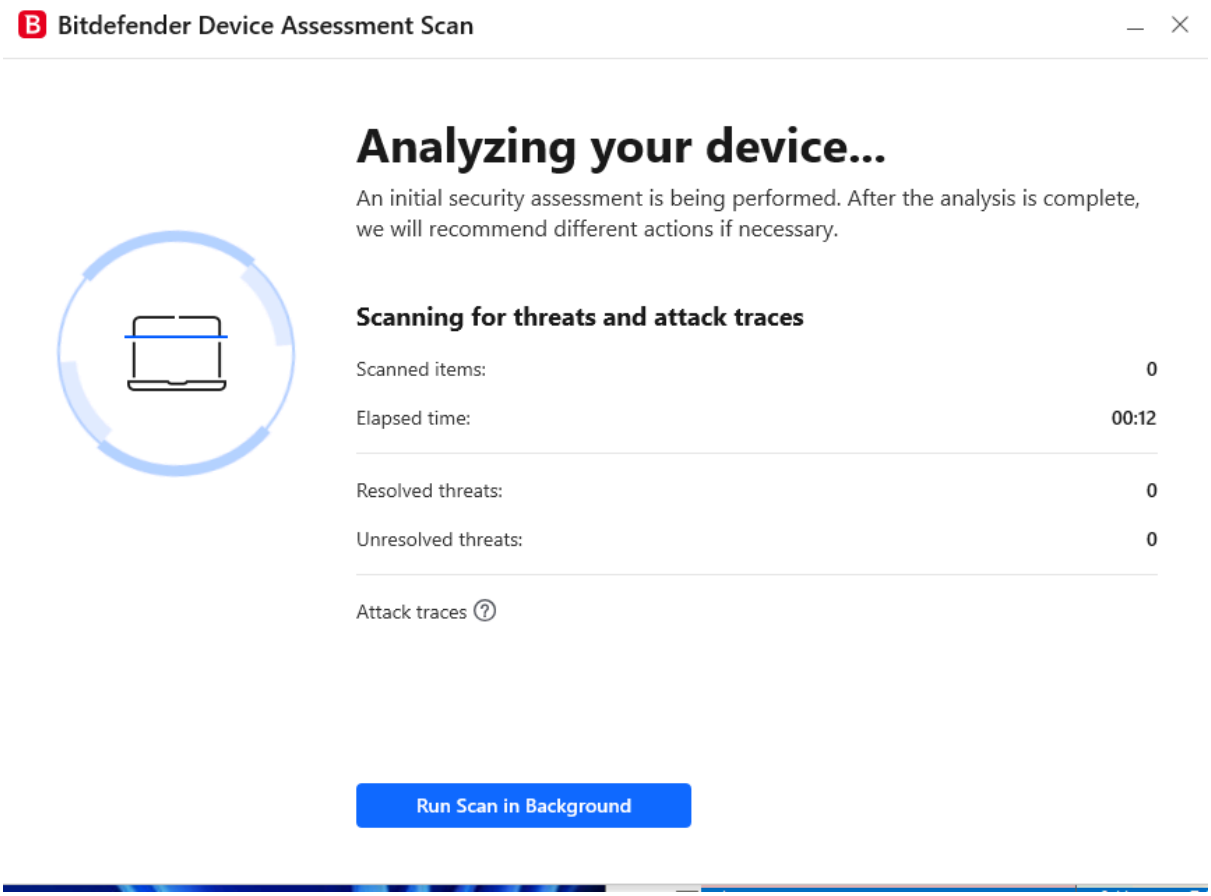
Additional like updatesrv.exe appear too, and also bdservicehost.exe with wscommunicator.exe which is suspicious name. could be C2 channel.



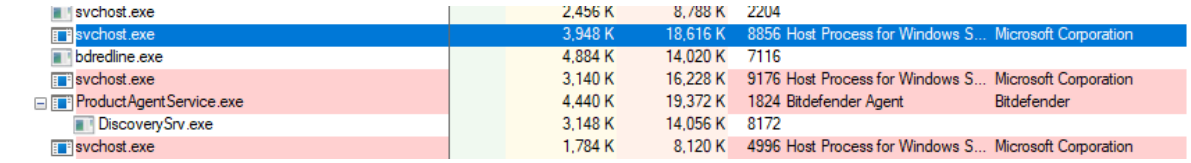
All those are signed by “Bitdefender” company.



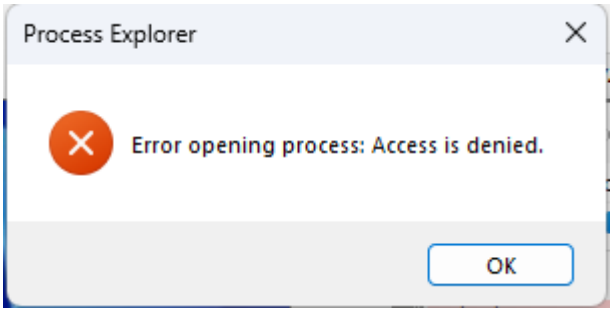
After that more services launch such as a lot of bdservicehost.exe and ProductAgentService.exe…

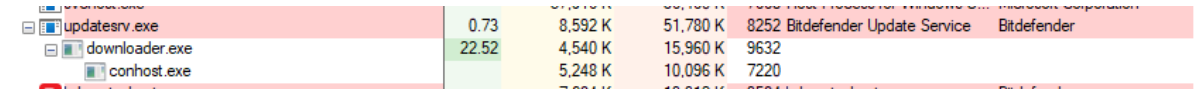


We start a scan with the tool. It appears that it's an antivirus.



When we try to close the services we get an Access is denied error. It is not closing very eagerly.

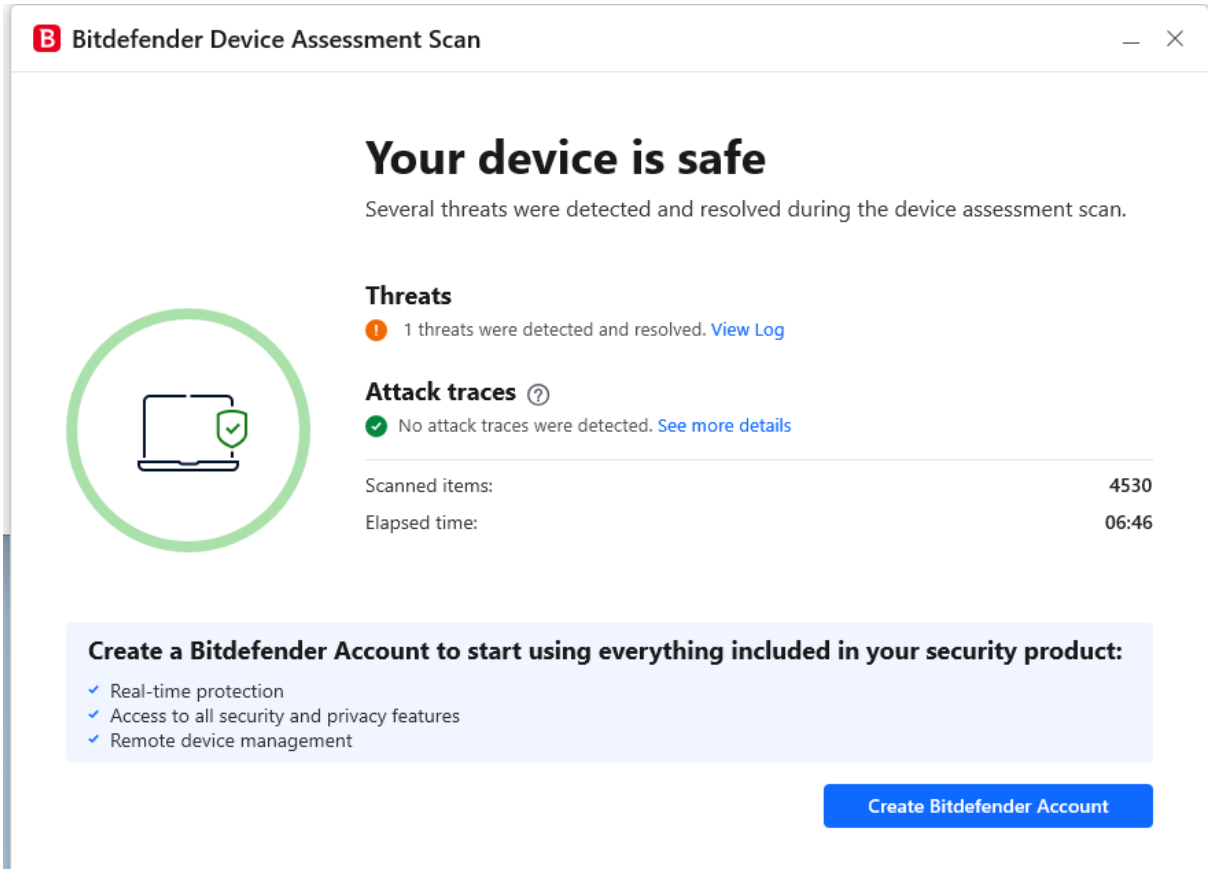




We also sometimes see updatesrv.exe pop up, thich spawns downloader.exe which downloads probably stuff from the internet.

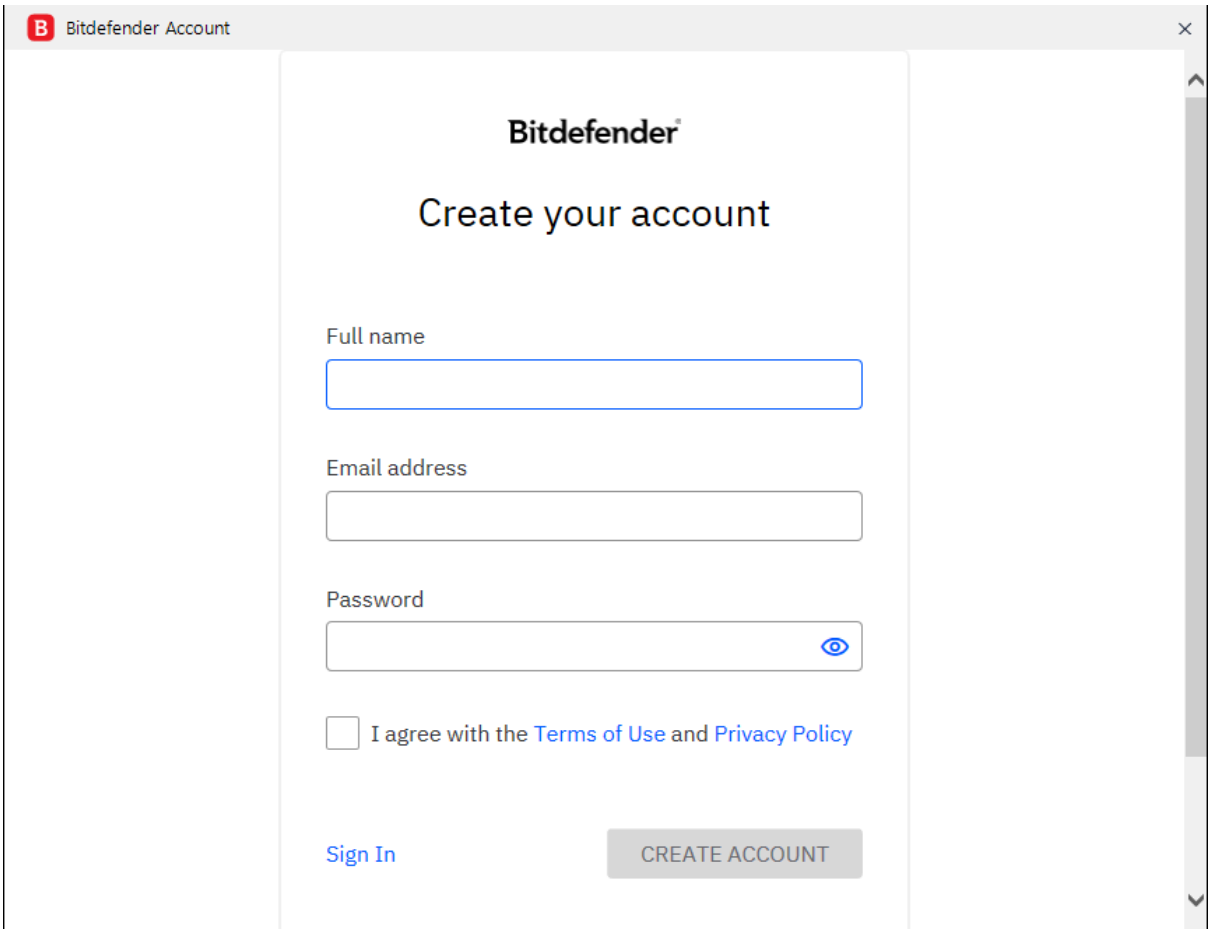
```
---------------------------------
Total changes: 3743
---------------------------------
```

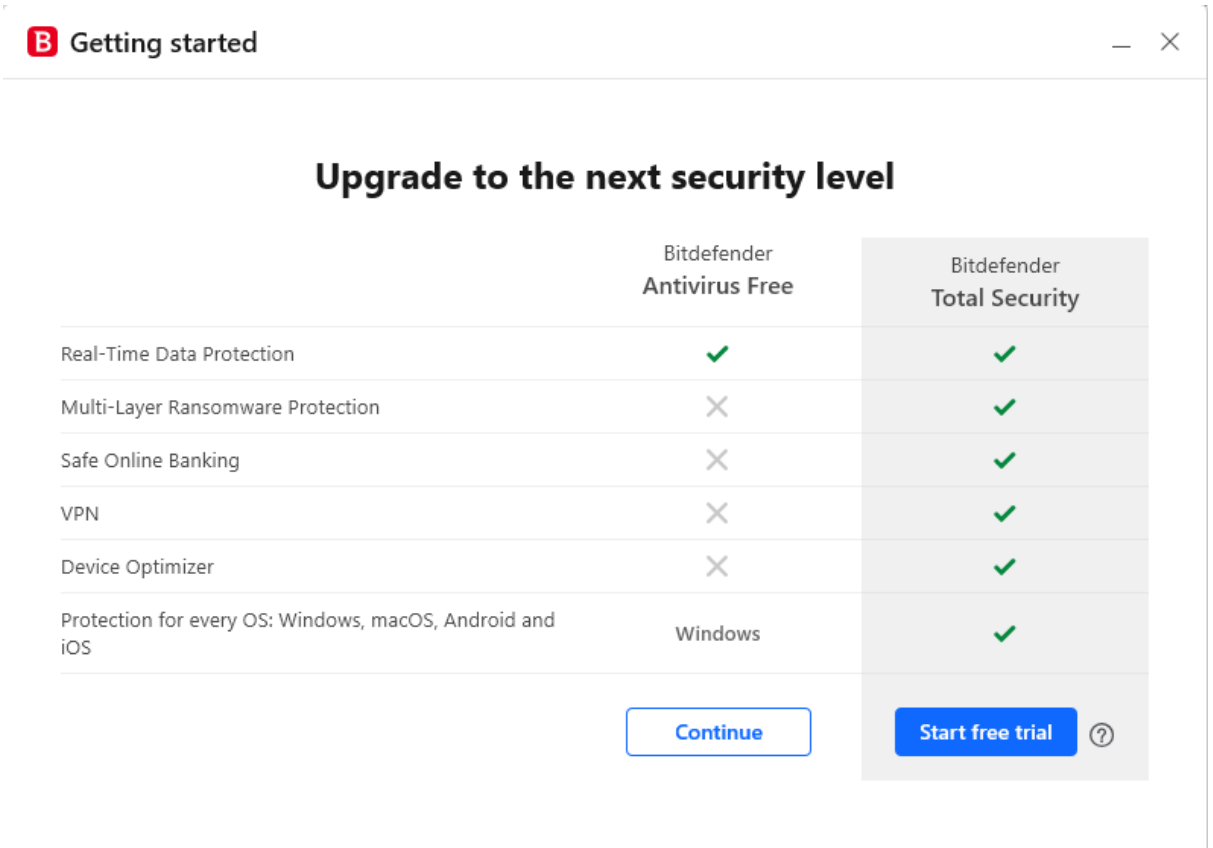
In the Regshot we suresly see that it changed a lot of values in the registry.

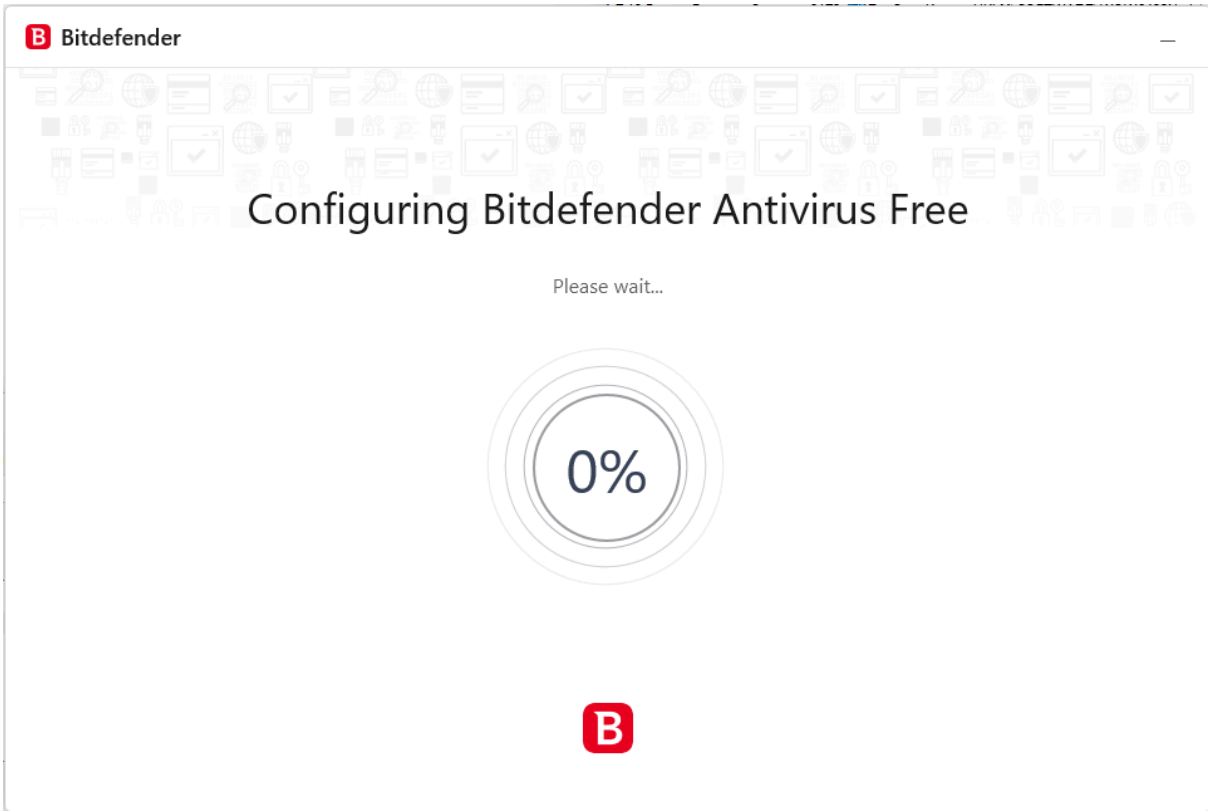


Bitdefender writes that I'm safe (but not from this "Antivirus" probably 🙂)

We can create our account and continue with the free version.







updatesrv.exe	< 0.01	8,276 K	18,100 K	9052	Bitdefender Update Service	Bitdefender
downloader.exe	5.00	7,080 K	18,800 K	1700		
conhost.exe		5,188 K	9,636 K	6724		
svchost.exe		3,548 K	10,108 K	6128		

We see a lot of traffic going out and in, and it even tries to contact the router that is behind in another subnet.

7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 40, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 40, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 82, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 94, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 49, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 49, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 43, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 43, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 52, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Send	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 52, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 65, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 77, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 59, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 71, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 68, seqnu...
7:17:4...	bdservicehost.exe	1724	UDP Receive	Windows11PC:61324 -> 10.100.102.1:d...	SUCCESS	Length: 80, seqnu...
7:17:4...	bdservicehost.exe	9020	UDP Send	Windows11PC:61325 -> 10.100.102.1:d...	SUCCESS	Length: 40, seqnu...
7:17:4...	bdservicehost.exe	9020	UDP Send	Windows11PC:61325 -> 10.100.102.1:d...	SUCCESS	Length: 40, seqnu...

All communication was with UDP, no TCP… maybe it tries to avoid detection that way.

7:13:3...	ProductAgentService.exe	8596	UDP Receive	Windows11PC:59996 -> 10.100.102.1:d...	SUCCESS	Length: 59, seqnu...
7:13:3...	installer.exe	3368	UDP Send	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 40, seqnu...
7:13:3...	installer.exe	3368	UDP Receive	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 82, seqnu...
7:13:3...	installer.exe	3368	UDP Send	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 49, seqnu...
7:13:3...	installer.exe	3368	UDP Send	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 43, seqnu...
7:13:3...	installer.exe	3368	UDP Send	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 52, seqnu...
7:13:3...	installer.exe	3368	UDP Receive	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 65, seqnu...
7:13:3...	installer.exe	3368	UDP Receive	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 59, seqnu...
7:13:3...	installer.exe	3368	UDP Receive	Windows11PC:59997 -> 10.100.102.1:d...	SUCCESS	Length: 68, seqnu...
7:13:3...	svchost.exe	1736	UDP Send	Windows11PC:60700 -> 10.100.102.1:d...	SUCCESS	Length: 46, seqnu...

7:13:4...	svchost.exe	2928	UDP Send	Windows11PC:ssdp -> ff02::c:ssdp	SUCCESS	Length: 428, seqn...
7:13:4...	svchost.exe	2928	UDP Receive	ff02::c:ssdp -> Windows11PC:ssdp	SUCCESS	Length: 428, seqn...
7:13:4...	svchost.exe	2928	UDP Send	Windows11PC:ssdp -> 239.255.255.250...	SUCCESS	Length: 447, seqn...
7:13:4...	svchost.exe	2928	UDP Receive	239.255.255.250:ssdp -> Windows11PC...	SUCCESS	Length: 447, seqn...
7:13:4...	svchost.exe	2928	UDP Send	Windows11PC:ssdp -> ff02::c:ssdp	SUCCESS	Length: 437, seqn...
7:13:4...	svchost.exe	2928	UDP Receive	ff02::c:ssdp -> Windows11PC:ssdp	SUCCESS	Length: 437, seqn...
7:13:4...	svchost.exe	2928	UDP Send	Windows11PC:ssdp -> 239.255.255.250...	SUCCESS	Length: 486, seqn...
7:13:4...	svchost.exe	2928	UDP Receive	239.255.255.250:ssdp -> Windows11PC...	SUCCESS	Length: 486, seqn...
7:13:4...	svchost.exe	2928	UDP Send	Windows11PC:ssdp -> ff02::c:ssdp	SUCCESS	Length: 476, seqn...
7:13:4...	svchost.exe	2928	UDP Receive	ff02::c:ssdp -> Windows11PC:ssdp	SUCCESS	Length: 476, seqn...
7:13:4...	svchost.exe	2928	UDP Send	Windows11PC:ssdp -> 239.255.255.250...	SUCCESS	Length: 488, seqn...
7:13:4...	svchost.exe	2928	UDP Receive	239.255.255.250:ssdp -> Windows11PC...	SUCCESS	Length: 488, seqn...
7:13:4...	svchost.exe	2928	UDP Send	Windows11PC:ssdp -> ff02::c:ssdp	SUCCESS	Length: 478, seqn...
7:13:4...	svchost.exe	2928	UDP Receive	ff02::c:ssdp -> Windows11PC:ssdp	SUCCESS	Length: 478, seqn...
7:13:4...	svchost.exe	1736	UDP Send	Windows11PC:60700 -> 10.100.102.1:d...	SUCCESS	Length: 42, seqnu...
7:13:4...	svchost.exe	1736	UDP Receive	Windows11PC:60700 -> 10.100.102.1:d...	SUCCESS	Length: 95, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 82, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 94, seqnu...
7:19:5...	installer.exe	1052	UDP Send	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 49, seqnu...
7:19:5...	installer.exe	1052	UDP Send	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 49, seqnu...
7:19:5...	installer.exe	1052	UDP Send	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 43, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 65, seqnu...
7:19:5...	installer.exe	1052	UDP Send	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 43, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 77, seqnu...
7:19:5...	installer.exe	1052	UDP Send	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 52, seqnu...
7:19:5...	installer.exe	1052	UDP Send	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 52, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 59, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 71, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 68, seqnu...
7:19:5...	installer.exe	1052	UDP Receive	Windows11PC:61334 -> 10.100.102.1:d...	SUCCESS	Length: 80, seqnu...

It even communicated with the router in my home??
The VM is in NAT so it shouldn't see the router…

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b66f:5837:25d9:77ea%4
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2
```

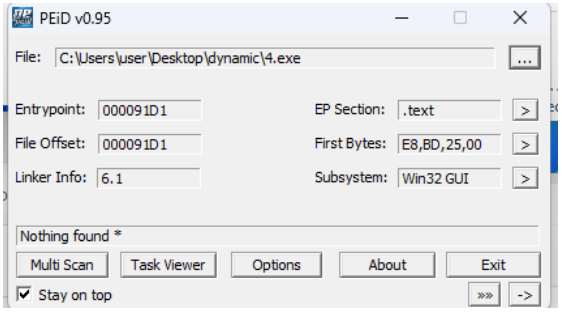
???
After restart we see that the services boot up again and the malware gained persistence.

svchost.exe		2,712 K	8,160 K	1928 Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,708 K	7,964 K	1088 Host Process for Windows S...	Microsoft Corporation
bdservicehost.exe	5.44	540,288 K	440,892 K	1404 bdservicehost	Bitdefender
bdservicehost.exe	< 0.01	14,900 K	26,160 K	1184 bdservicehost	Bitdefender
VBoxService.exe		2,664 K	6,824 K	2196 VirtualBox Guest Additions S...	Oracle and/or its affiliates
svchost.exe		2,396 K	8,048 K	2204 Host Process for Windows S...	Microsoft Corporation
bdservicehost.exe		32,344 K	56,772 K	2280 bdservicehost	Bitdefender
bdagent.exe	< 0.01	48,696 K	35,224 K	9884 Bitdefender agent	Bitdefender
bdservicehost.exe		14,780 K	33,276 K	2292 bdservicehost	Bitdefender
bdntwrk.exe		8,240 K	18,752 K	3912	

There is a lot of processes from Bitdefender now and it seems like a virus that infected the whole PC and have a good persistence on the machine.

Conclusion 3
It is a trojan that is selling itself as an antivirus. could be even a real antivirus with a backdoor installed inside it so it will be more convincing. installed itself and gained persistence, not easily removed. the processes cannot be closed by the user because it gives "denied access error". Could exfiltrate data through the connections it made and also download more malware and spyware after the installation or during it.

Sample 4



We ran PEiD and it found nothing so it could be packed.

000000E6	0006	Number of Sections	
000000E8	4B4C9998	Time Date Stamp	2010/01/12 Tue 15:47:36 UTC
000000EC	00000000	Pointer to Symbol Table	
000000F0	00000000	Number of Symbols	
000000F4	00E0	Size of Optional Header	
000000F6	0102	Characteristics	

This sample is stamped with 2010.

00010018	0002D12E	Hint/Name RVA	04B2 CryptHashData
0001001C	0002D13E	Hint/Name RVA	06AB SetTokenInformation
00010020	0002D154	Hint/Name RVA	05E0 OpenProcessToken
00010024	0002D168	Hint/Name RVA	049D CryptCreateHash
00010028	0002D17A	Hint/Name RVA	04AE CryptGetHashParam
0001002C	0002D18E	Hint/Name RVA	0667 RegSetValueExW
00010030	0002D1A0	Hint/Name RVA	0656 RegQueryValueExA
00010034	0002D1B4	Hint/Name RVA	0630 RegDeleteValueA
00010038	0002D1C6	Hint/Name RVA	0666 RegSetValueExA
0001003C	0002D1D8	Hint/Name RVA	0621 RegCreateKeyExA
00010040	0002D1EA	Hint/Name RVA	0619 RegCloseKey
00010044	0002D1F8	Hint/Name RVA	0649 RegOpenKeyExA
00010048	0002D208	Hint/Name RVA	049A CryptAcquireContextA
0001004C	0002D220	Hint/Name RVA	04AB CryptGenRandom
00010050	0002D232	Hint/Name RVA	04B5 CryptReleaseContext
00010054	0002D248	Hint/Name RVA	04A4 CryptEncrypt
00010058	0002D258	Hint/Name RVA	04B7 CryptSetKeyParam
0001005C	0002D26C	Hint/Name RVA	04B4 CryptImportKey
00010060	0002D27E	Hint/Name RVA	04A1 CryptDestroyKey

We see in PEview a lot of crypto functions and Registry.

000100D8	0002D48A	Hint/Name RVA	0245 GetProcAddress
000100DC	0002D49C	Hint/Name RVA	02A9 GetVolumeNameForVolumeMountPointA
000100E0	0002D4C0	Hint/Name RVA	01C2 GetCurrentProcess

GetProcAddress is seen

00010198	0002D81A	Hint/Name RVA	04C1 TerminateProcess
0001019C	0002D82E	Hint/Name RVA	0301 IsDebuggerPresent

IsDebuggerPresent is here as well

000101AC	0002D884	Hint/Name RVA	04C7 TlsFree
000101B0	0002D88E	Hint/Name RVA	04C9 TlsSetValue
000101B4	0002D89C	Hint/Name RVA	04C8 TlsGetValue
000101B8	0002D8AA	Hint/Name RVA	04C6 TlsAlloc
000101BC	0002D8B6	Hint/Name RVA	02CD HeapAlloc

TLS function it can be used for network communication.

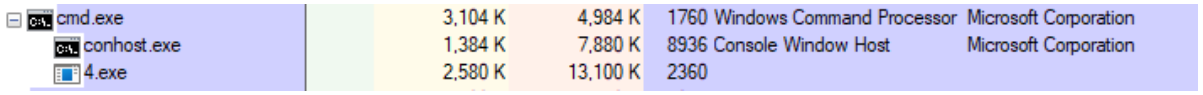
00010248	0002DAFC	Hint/Name RVA	010D InternetOpenA
0001024C	0002DB0C	Hint/Name RVA	00E1 InternetCloseHandle
00010250	0002DB22	Hint/Name RVA	0122 InternetSetOptionA
00010254	0002DB38	Hint/Name RVA	00CD HttpOpenRequestA
00010258	0002DB4C	Hint/Name RVA	0113 InternetQueryOptionA
0001025C	0002DB64	Hint/Name RVA	00D2 HttpSendRequestExA
00010260	0002DB7A	Hint/Name RVA	0135 InternetWriteFile
00010264	0002DB8E	Hint/Name RVA	00CB HttpEndRequestA
00010268	0002DBA0	Hint/Name RVA	00D1 HttpSendRequestA
0001026C	0002DBB4	Hint/Name RVA	00CF HttpQueryInfoA
00010270	0002DBC6	Hint/Name RVA	00E9 InternetCrackUrlA
00010274	0002DBDA	Hint/Name RVA	0115 InternetReadFile
00010278	0002DBEE	Hint/Name RVA	00E7 InternetConnectA
0001027C	00000000	End of Imports	wininet.dll

And as expected HTTP and Internet functions are here.

Let’s run this sample.

```
----------------------------------
Total changes: 40451
----------------------------------
```

The registry changed a lot, and no visible process is up. The file itself is deleted, did it just delete itself?



After rerun and running it with cmd it looks like it appears as regular process and doesn't do much…

—----------

In further investigation it loaded ntdll, changed the registry and started 2 processes:

Time ...	Process Name	PID	Operation	Path	Result	Detail
2:14:3...	4.exe	7356	Process Start		SUCCESS	Parent PID: 4432, ...
2:14:3...	4.exe	7356	Thread Create		SUCCESS	Thread ID: 8180
2:14:3...	4.exe	7356	Load Image	C:\Users\user\Desktop\dynamic\4.exe	SUCCESS	Image Base: 0x4f0...
2:14:3...	4.exe	7356	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc...
2:14:3...	4.exe	7356	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77c...
2:14:3...	4.exe	7356	CreateFile	C:\Windows\Prefetch\4.EXE-13EFF89...	NAME NOT FOUND	Desired Access: G...
2:14:3...	4.exe	7356	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...

2 processes are created:

2:14:3...	4.exe	7356	Load Image	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS	Image Base: 0x74420000, Image Size: 0x29000
2:14:3...	4.exe	7356	Process Create	C:\Users\user\AppData\Local\Temp\svchost.exe	SUCCESS	PID: 7724, Command line: C:\Users\user\AppData\Local\Temp\svchost.exe
2:14:3...	4.exe	7356	Process Create	C:\Windows\SYSTEM32\cmd.exe	SUCCESS	PID: 6572, Command line: cmd.exe /C del /Q /F "C:\Users\user\AppData\Local\Temp\sysF1...
2:14:3...	4.exe	7356	Thread Exit		SUCCESS	Thread ID: 5816, User Time: 0.0000000, Kernel Time: 0.0156250

4.exe created a cmd.exe which run:
cmd.exe /C del /Q /F “C:\Users\user\AppData\Local\Temp\sysF1A0.tmp
PID: 6572

Time ...	Process Name	PID	Operation	Path	Result	Detail
2:14:3...	cmd.exe	6572	Process Start		SUCCESS	Parent PID: 7356, Command line: cmd.exe /C del /Q /F "C:\Users\user\AppData\Local\Temp...
2:14:3...	cmd.exe	6572	Thread Create		SUCCESS	Thread ID: 5680
2:14:3...	cmd.exe	6572	Load Image	C:\Windows\System32\cmd.exe	SUCCESS	Image Base: 0x7ff73e440000, Image Size: 0x6a000
2:14:3...	cmd.exe	6572	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffcd30f0000, Image Size: 0x217000
2:14:3...	cmd.exe	6572	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	REPARSE	Desired Access: Read
2:14:3...	cmd.exe	6572	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	Desired Access: Read
2:14:3...	cmd.exe	6572	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\ACP	SUCCESS	Type: REG_SZ, Length: 10, Data: 1252
2:14:3...	cmd.exe	6572	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\OEMCP	SUCCESS	Type: REG_SZ, Length: 8, Data: 437
2:14:3...	cmd.exe	6572	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	

Which changes the registry and deletes files…
This cmd process opens another process with PID 5756

2:14:3...	cmd.exe	6572	Process Create	C:\Windows\System32\Conhost.exe	SUCCESS	PID: 5756, Command line: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Which runs the command \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

4.exe also starts svchost.exe
It tries to fake a system process!
PID: 7724

procexp.exe		4,512 K	12,920 K	2676 Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	4.54	23,792 K	52,008 K	4364 Sysinternals Process Explorer	Sysinternals - www.sysinter...
svchost.exe		2,780 K	13,508 K	7724	

Let’s filter to search what is PID 7724 is
It loads ntdll and makes changes to the registry.

Time ...	Process Name	PID	Operation	Path	Result	Detail
2:14:3...	svchost.exe	7724	Process Start		SUCCESS	Parent PID: 7356, Command line: C:\Users\user\AppData\Local\Temp\svchost.exe, Current d...
2:14:3...	svchost.exe	7724	Thread Create		SUCCESS	Thread ID: 5820
2:14:3...	svchost.exe	7724	Load Image	C:\Users\user\AppData\Local\Temp\svchost.exe	SUCCESS	Image Base: 0x6c0000, Image Size: 0x2e000
2:14:3...	svchost.exe	7724	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffcd30f0000, Image Size: 0x217000
2:14:3...	svchost.exe	7724	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77c50000, Image Size: 0x1b1000
2:14:3...	svchost.exe	7724	CreateFile	C:\Windows\Prefetch\SVCHOST.EXE-90080CD9.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attribut...
2:14:3...	svchost.exe	7724	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	REPARSE	Desired Access: Read
2:14:3...	svchost.exe	7724	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	Desired Access: Read
2:14:3...	svchost.exe	7724	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\ACP	SUCCESS	Type: REG_SZ, Length: 10, Data: 1252
2:14:3...	svchost.exe	7724	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\OEMCP	SUCCESS	Type: REG_SZ, Length: 8, Data: 437
2:14:3...	svchost.exe	7724	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	

And the more interesting is the network connections it tries to establish:

2:14:3...	svchost.exe	7724	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x77aa0000, Image Size: 0x9c000
2:14:3...	svchost.exe	7724	TCP Reconnect	Windows11PC:49888 -> echo509.dedicatedpanel.com:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:14:3...	svchost.exe	7724	TCP Reconnect	Windows11PC:49888 -> echo509.dedicatedpanel.com:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:14:4...	svchost.exe	7724	TCP Reconnect	Windows11PC:49888 -> echo509.dedicatedpanel.com:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:14:4...	svchost.exe	7724	TCP Reconnect	Windows11PC:49888 -> echo509.dedicatedpanel.com:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:14:5...	svchost.exe	7724	TCP Disconnect	Windows11PC:49888 -> echo509.dedicatedpanel.com:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:14:5...	svchost.exe	7724	TCP Connect	Windows11PC:49892 -> ip.cishost.ru:http	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tsopt: 0, wsopt: 0, rcvwin: 65535, rcvwinscale: 0
2:14:5...	svchost.exe	7724	TCP Send	Windows11PC:49892 -> ip.cishost.ru:http	SUCCESS	Length: 216, startime: 34606, endtime: 34606, seqnum: 0, connid: 0
2:14:5...	svchost.exe	7724	TCP TCPCopy	Windows11PC:49892 -> ip.cishost.ru:http	SUCCESS	Length: 326, seqnum: 0, connid: 0
2:14:5...	svchost.exe	7724	TCP Receive	Windows11PC:49892 -> ip.cishost.ru:http	SUCCESS	Length: 326, seqnum: 0, connid: 0
2:14:5...	svchost.exe	7724	TCP Reconnect	Windows11PC:49893 -> xray730.startdedicated.net:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:14:5...	svchost.exe	7724	TCP Reconnect	Windows11PC:49893 -> xray730.startdedicated.net:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:15:0...	svchost.exe	7724	TCP Reconnect	Windows11PC:49893 -> xray730.startdedicated.net:http	SUCCESS	Length: 0, seqnum: 0, connid: 0
2:15:1...	svchost.exe	7724	TCP Reconnect	Windows11PC:49893 -> xray730.startdedicated.net:http	SUCCESS	Length: 0, seqnum: 0, connid: 0

Looks like this one is trying to connect to some domains in russia and two other weird ones.

Let’s simulate the network with inetsim:

procexp.exe		4,512 K	14,796 K	2676 Sysinternals Pr
procexp64.exe	< 0.01	24,020 K	48,268 K	4364 Sysinternals Pr
svchost.exe		2,820 K	13,760 K	6044

Time ...	Process Name	PID	Operation	Path	Result	Detail
2:26:3...	svchost.exe	6044	TCP Reconnect	Windows11PC:50105 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:26:4...	svchost.exe	6044	TCP Reconnect	Windows11PC:50105 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:26:4...	svchost.exe	6044	TCP Reconnect	Windows11PC:50105 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:26:5...	svchost.exe	6044	TCP Reconnect	Windows11PC:50105 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:26:5...	svchost.exe	6044	TCP Disconnect	Windows11PC:50105 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:26:5...	svchost.exe	6044	TCP Connect	Windows11PC:50106 -> 31.41.47.37:http	SUCCESS	Length: 0, mss: 14...
2:26:5...	svchost.exe	6044	TCP Send	Windows11PC:50106 -> 31.41.47.37:http	SUCCESS	Length: 216, starti...
2:26:5...	svchost.exe	6044	TCP TCPCopy	Windows11PC:50106 -> 31.41.47.37:http	SUCCESS	Length: 326, seqn...
2:26:5...	svchost.exe	6044	TCP Receive	Windows11PC:50106 -> 31.41.47.37:http	SUCCESS	Length: 326, seqn...
2:27:0...	svchost.exe	6044	TCP Reconnect	Windows11PC:50107 -> 85.25.138.187:...	SUCCESS	Length: 0, seqnum:...
2:27:0...	svchost.exe	6044	TCP Reconnect	Windows11PC:50107 -> 85.25.138.187:...	SUCCESS	Length: 0, seqnum:...
2:27:0...	svchost.exe	6044	TCP Reconnect	Windows11PC:50107 -> 85.25.138.187:...	SUCCESS	Length: 0, seqnum:...
2:27:1...	svchost.exe	6044	TCP Reconnect	Windows11PC:50107 -> 85.25.138.187:...	SUCCESS	Length: 0, seqnum:...
2:27:2...	svchost.exe	6044	TCP Disconnect	Windows11PC:50107 -> 85.25.138.187:...	SUCCESS	Length: 0, seqnum:...
2:27:3...	svchost.exe	6044	TCP Reconnect	Windows11PC:50108 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:27:3...	svchost.exe	6044	TCP Reconnect	Windows11PC:50108 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:27:3...	svchost.exe	6044	TCP Reconnect	Windows11PC:50108 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:27:4...	svchost.exe	6044	TCP Reconnect	Windows11PC:50108 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:27:5...	svchost.exe	6044	TCP Disconnect	Windows11PC:50108 -> 188.138.88.18...	SUCCESS	Length: 0, seqnum:...
2:28:0...	svchost.exe	6044	TCP Disconnect	Windows11PC:50106 -> 31.41.47.37:http	SUCCESS	Length: 0, seqnum:...
2:28:0...	svchost.exe	6044	TCP Connect	Windows11PC:50111 -> 31.41.47.37:http	SUCCESS	Length: 0, mss: 14...
2:28:0...	svchost.exe	6044	TCP Send	Windows11PC:50111 -> 31.41.47.37:http	SUCCESS	Length: 216, starti...
2:28:0...	svchost.exe	6044	TCP TCPCopy	Windows11PC:50111 -> 31.41.47.37:http	SUCCESS	Length: 326, seqn...
2:28:0...	svchost.exe	6044	TCP Receive	Windows11PC:50111 -> 31.41.47.37:http	SUCCESS	Length: 326, seqn...
2:28:1...	svchost.exe	6044	TCP Reconnect	Windows11PC:50112 -> 85.25.138.187:...	SUCCESS	Length: 0, seqnum:...

Let's try to scan those servers:

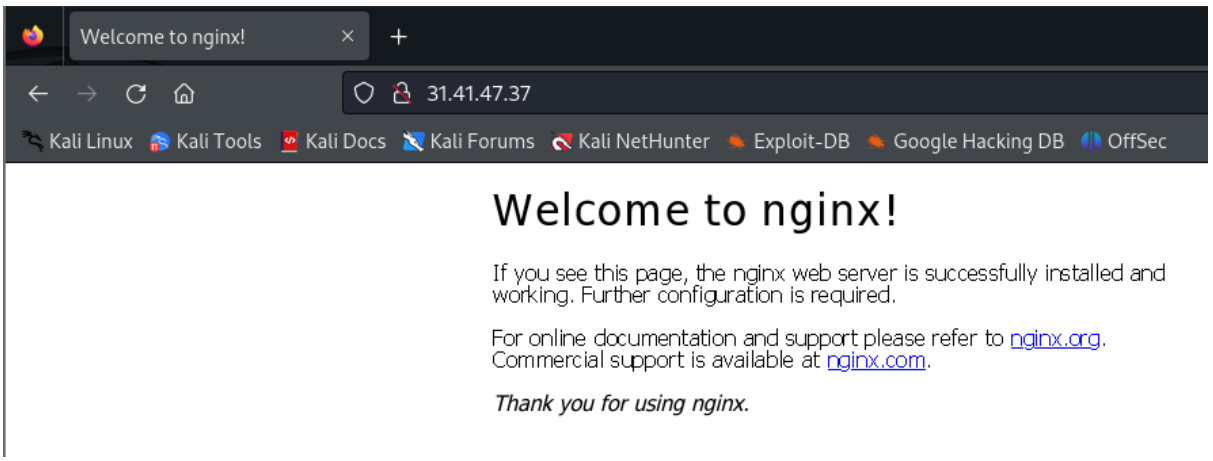
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 31.41.47.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 12:31 IST
Nmap scan report for ip.cishost.ru (31.41.47.37)
Host is up (0.11s latency).
Not shown: 992 closed tcp ports (reset)
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
25/tcp  filtered smtp
80/tcp  open     http
110/tcp open     pop3
143/tcp open     imap
993/tcp open     imaps
995/tcp open     pop3s

Nmap done: 1 IP address (1 host up) scanned in 8.18 seconds
```

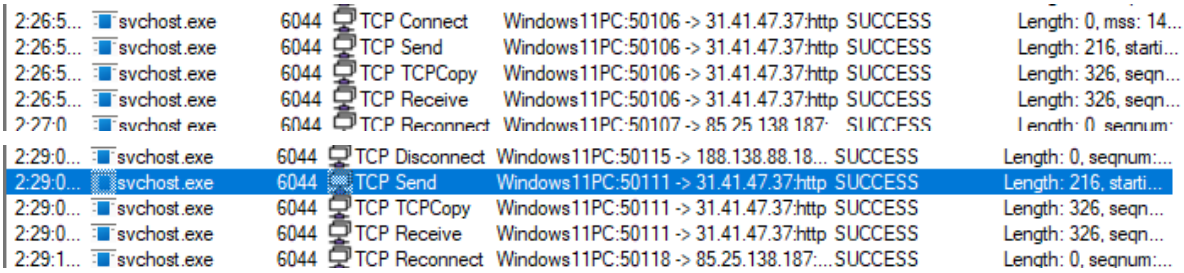
The first server seems to be up, the malware send there a RCPCopy request. exfiltrated data probably or tried to connect to the C2 channel.

```
TRACEROUTE (using port 1025/tcp)
HOP RTT       ADDRESS
1   3.10 ms   10.100.102.1
2   6.67 ms   85-250-208-1.bb.netvision.net.il (85.250.208.1)
3   6.28 ms   192.168.254.5
4   ...
5   6.48 ms   agr1-hfa-Hun4-0-7-ibc-hfa-data.nta.nv.net.il (212.143.229.200)
6   6.10 ms   core2-2-2-vl200-hfa.hfa.nv.net.il (212.143.7.239)
7   7.11 ms   gw2-0-1-core1.hfa.hfa.nv.net.il (212.143.7.245)
8   63.79 ms  gw2-hu-4-2.lnd.nv.net.il (212.143.12.22)
9   70.24 ms  10.10.30.1
10  78.45 ms  spb-ivc-cr1.rascom.ru (195.66.226.51)
11  ...
12  103.27 ms msk-3v-cr1.be4.rascom.as20764.net (80.64.96.125)
13  103.53 ms macomnet-rascom-gw1.as20764.net (80.64.101.10)
14  101.06 ms ncc-8Q.TenE-0-0-0.macomnet.net (195.128.64.72)
15  100.32 ms GUPKIN-22-DCH-05202-Macom.MAcomnet.NET (195.128.65.217)
16  106.17 ms ip.cishost.ru (31.41.47.37)
```

Via the traceroute we see that at the end it connected to a russian server ip.cishost.ru
In the port 80 we have an open webserver with the default screen:



The other two seem to be down
To this server multiple requests have been sent:




```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 85.25.138.187
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 12:30 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.22 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 188.138.88.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 12:32 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.21 seconds
```

Let's set up apatedns to redirect the 31.41.47.37 to our kali machine:

3:24:4...	svchost.exe	10868	TCP Send	Windows11PC:50999 -> 37.47.41.31.in-...	SUCCESS	Length: 216, starti...
3:24:4...	svchost.exe	10868	TCP TCPCopy	Windows11PC:50999 -> 37.47.41.31.in-...	SUCCESS	Length: 326, seqn...
3:24:4...	svchost.exe	10868	TCP Receive	Windows11PC:50999 -> 37.47.41.31.in-...	SUCCESS	Length: 326, seqn...
3:25:0...	svchost.exe	10868	TCP Reconnect	Windows11PC:51050 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:25:0...	svchost.exe	10868	TCP Reconnect	Windows11PC:51050 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:25:0...	svchost.exe	10868	TCP Reconnect	Windows11PC:51050 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:25:1...	svchost.exe	10868	TCP Reconnect	Windows11PC:51050 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Disconnect	Windows11PC:51050 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51062 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51062 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51062 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51062 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Disconnect	Windows11PC:51062 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51065 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51065 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51065 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51065 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Disconnect	Windows11PC:51065 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51067 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51067 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51067 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51067 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Disconnect	Windows11PC:51067 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:2...	svchost.exe	10868	TCP Reconnect	Windows11PC:51068 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:3...	svchost.exe	10868	TCP Reconnect	Windows11PC:51068 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:3...	svchost.exe	10868	TCP Reconnect	Windows11PC:51068 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:3...	svchost.exe	10868	TCP Reconnect	Windows11PC:51068 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:3...	svchost.exe	10868	TCP Disconnect	Windows11PC:51068 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:25:3...	svchost.exe	10868	TCP Reconnect	Windows11PC:51071 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...

now it's connected to our machine

Time ...	Process Name	PID	Operation	Path	Result	Detail
3:40:1...	4.exe	4368	TCP Reconnect	Windows11PC:50225 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:40:1...	4.exe	4368	TCP Reconnect	Windows11PC:50225 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:40:1...	4.exe	4368	TCP Reconnect	Windows11PC:50225 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:40:2...	4.exe	4368	TCP Reconnect	Windows11PC:50225 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:40:3...	4.exe	4368	TCP Disconnect	Windows11PC:50225 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:40:3...	4.exe	4368	TCP Reconnect	Windows11PC:50232 -> 187.138.25.85....	SUCCESS	Length: 0, seqnum:...
3:40:3...	4.exe	8520	TCP Reconnect	Windows11PC:50233 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:40:3...	4.exe	4368	TCP Reconnect	Windows11PC:50232 -> 187.138.25.85....	SUCCESS	Length: 0, seqnum:...
3:40:3...	4.exe	8520	TCP Reconnect	Windows11PC:50233 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...
3:40:3...	4.exe	4368	TCP Reconnect	Windows11PC:50232 -> 187.138.25.85....	SUCCESS	Length: 0, seqnum:...
3:40:3...	4.exe	8520	TCP Reconnect	Windows11PC:50233 -> 184.88.138.18...	SUCCESS	Length: 0, seqnum:...

```
2024-02-16 13:40:34  HTTP connection, method: POST, URL: http://xgliacigulmjum.nl/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:40:48  HTTP connection, method: GET, URL: http://www.msftconnecttest.com/connecttest.txt,
file name: /var/lib/inetsim/http/fakefiles/sample.txt
2024-02-16 13:40:51  HTTP connection, method: POST, URL: http://ejpcvdmkrjsjvn.in/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:40:51  HTTP connection, method: POST, URL: http://rypsrq.eu/main.php, file name: /var/lib/
inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:40:51  HTTP connection, method: POST, URL: http://fomfotiqo.in/main.php, file name: /var/l
ib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:40:51  HTTP connection, method: POST, URL: http://wbofelmd.nl/main.php, file name: /var/li
b/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:40:51  HTTP connection, method: POST, URL: http://kqovdubeptl.fr/main.php, file name: /var
/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:40:51  HTTP connection, method: POST, URL: http://xgliacigulmjum.nl/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:13  HTTP connection, method: POST, URL: http://ejpcvdmkrjsjvn.in/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:14  HTTP connection, method: POST, URL: http://rypsrq.eu/main.php, file name: /var/lib/
inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:14  HTTP connection, method: POST, URL: http://fomfotiqo.in/main.php, file name: /var/l
ib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:14  HTTP connection, method: POST, URL: http://wbofelmd.nl/main.php, file name: /var/li
b/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:14  HTTP connection, method: POST, URL: http://kqovdubeptl.fr/main.php, file name: /var
/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:14  HTTP connection, method: POST, URL: http://xgliacigulmjum.nl/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:16  HTTP connection, method: POST, URL: http://ejpcvdmkrjsjvn.in/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:16  HTTP connection, method: POST, URL: http://rypsrq.eu/main.php, file name: /var/lib/
inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:16  HTTP connection, method: POST, URL: http://fomfotiqo.in/main.php, file name: /var/l
ib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:16  HTTP connection, method: POST, URL: http://wbofelmd.nl/main.php, file name: /var/li
b/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:16  HTTP connection, method: POST, URL: http://kqovdubeptl.fr/main.php, file name: /var
/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:16  HTTP connection, method: POST, URL: http://xgliacigulmjum.nl/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:41:34  HTTP connection, method: GET, URL: http://www.msftconnecttest.com/connecttest.txt,
file name: /var/lib/inetsim/http/fakefiles/sample.txt
2024-02-16 13:41:34  Last simulated date in log file
```

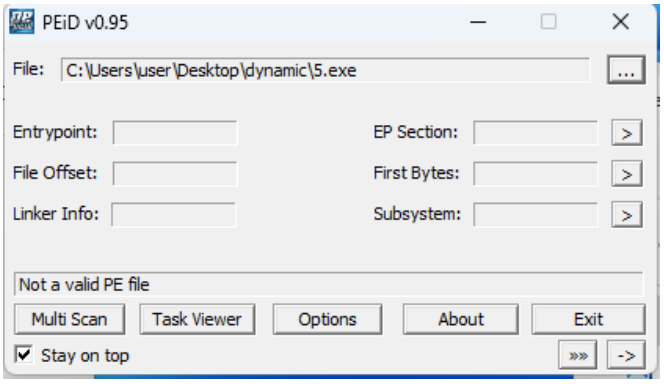
and we receive some HTTP POST requests, meaning it could exfiltrate data to this HTTP server after infection.

Conclusion 4

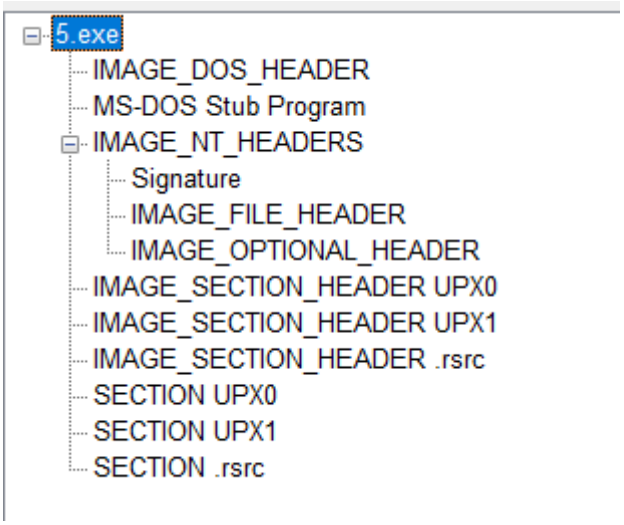
Seems like russian spyware, it infects the computer and runs as svchost.exe process to seem like an OS process. however it connects to a remote C2 channel and seems to exfiltrate data from our computer to this server via HTTP POST requests.

Sample 5

This sample is “not valid PE file” if we use PEiD



However in PEview we still can view it's contents



Looks like it's packed with UPX.

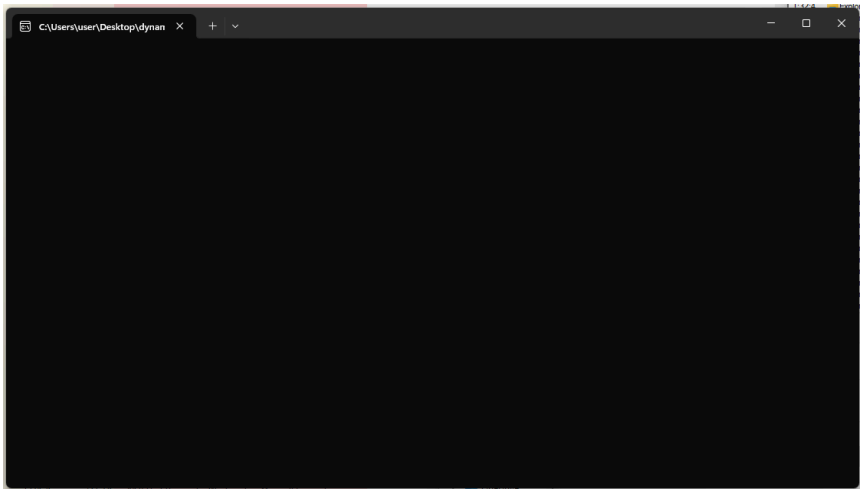
000000FC	8664	Machine	IMAGE_FILE_MACHINE_AMD64
000000FE	0003	Number of Sections	
00000100	5F2E9A62	Time Date Stamp	2020/08/08 Sat 12:28:18 UTC
00000104	00000000	Pointer to Symbol Table	

Let's run the process and view what it does:

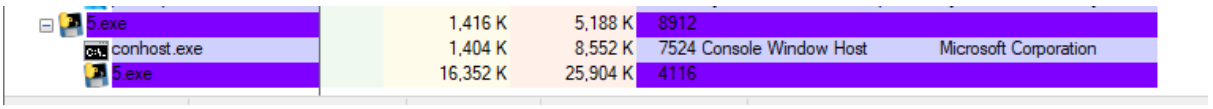
Our process pops up with PID 8912, straight away it opens a conhost.exe (terminal) with PID 7524.

Procmon64.exe	27.55	68,316 K	49,164 K	8240		
procexp.exe		4,512 K	12,864 K	2676 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
procexp64.exe	0.73	23,788 K	51,752 K	4364 Sysinternals Process Explorer	Sysinternals - www.sysinter...	
5.exe	1.45	1,416 K	5,024 K	8912		
conhost.exe		1,404 K	8,552 K	7524 Console Window Host	Microsoft Corporation	

A terminal pops up on screen:

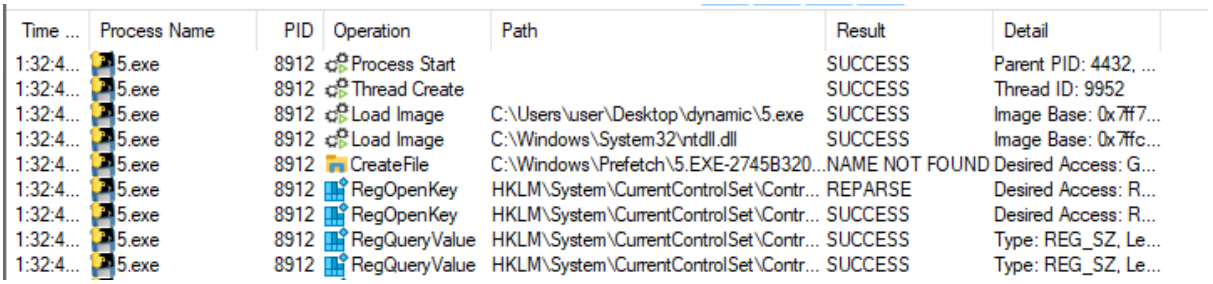


After a few seconds a second second child process 5.exe opens up with PID 4116, he is bigger in size, thus it could be the unpacked version of the first one which is packed as we have seen.



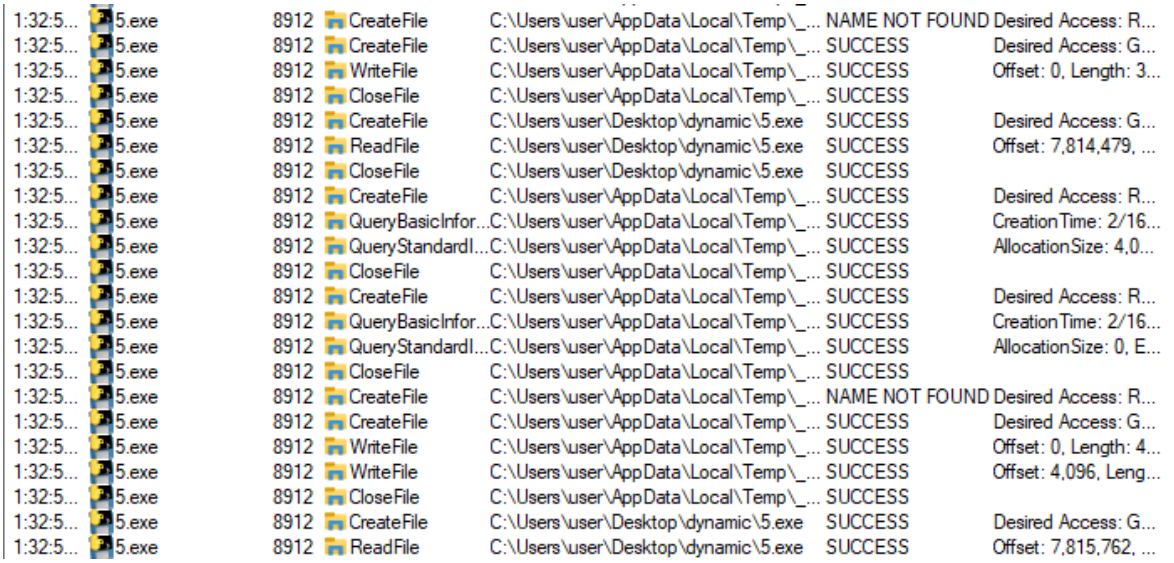
5.exe	1,416 K	5,188 K	8912	
conhost.exe	1,404 K	8,552 K	7524 Console Window Host	Microsoft Corporation
5.exe	16,352 K	25,904 K	4116	

Let's view PID 8912 in procmon:



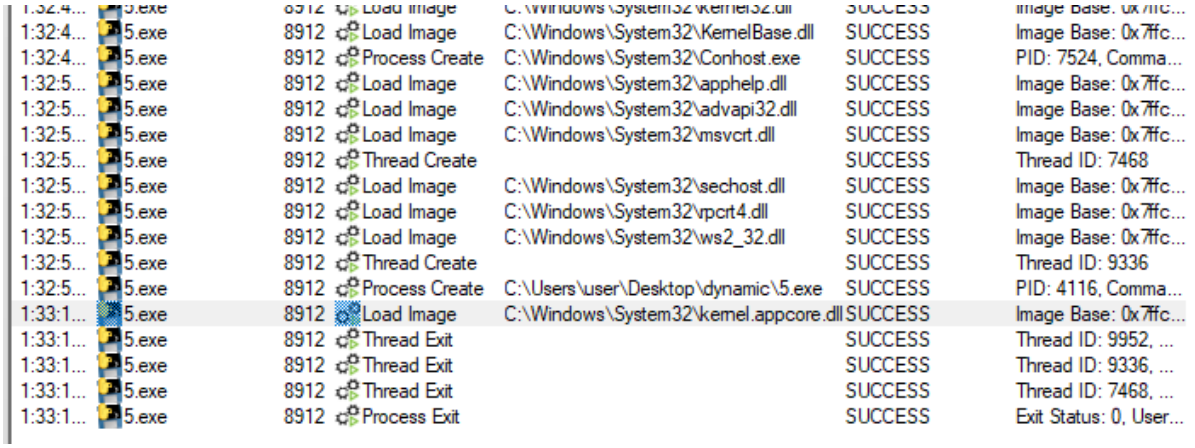
Time ...	Process Name	PID	Operation	Path	Result	Detail
1:32:4...	5.exe	8912	Process Start		SUCCESS	Parent PID: 4432, ...
1:32:4...	5.exe	8912	Thread Create		SUCCESS	Thread ID: 9952
1:32:4...	5.exe	8912	Load Image	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	Image Base: 0x7ff7...
1:32:4...	5.exe	8912	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc...
1:32:4...	5.exe	8912	CreateFile	C:\Windows\Prefetch\5.EXE-2745B320...	NAME NOT FOUND	Desired Access: G...
1:32:4...	5.exe	8912	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
1:32:4...	5.exe	8912	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
1:32:4...	5.exe	8912	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
1:32:4...	5.exe	8912	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...

opens up ntdll.dll and start to query the registry.



1:32:5...	5.exe	8912	CreateFile	C:\Users\user\AppData\Local\Temp_...	NAME NOT FOUND	Desired Access: R...
1:32:5...	5.exe	8912	CreateFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Desired Access: G...
1:32:5...	5.exe	8912	WriteFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Offset: 0, Length: 3...
1:32:5...	5.exe	8912	CloseFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	
1:32:5...	5.exe	8912	CreateFile	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	Desired Access: G...
1:32:5...	5.exe	8912	ReadFile	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	Offset: 7,814,479, ...
1:32:5...	5.exe	8912	CloseFile	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	
1:32:5...	5.exe	8912	CreateFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Desired Access: R...
1:32:5...	5.exe	8912	QueryBasicInfor...	C:\Users\user\AppData\Local\Temp_...	SUCCESS	CreationTime: 2/16...
1:32:5...	5.exe	8912	QueryStandardI...	C:\Users\user\AppData\Local\Temp_...	SUCCESS	AllocationSize: 4,0...
1:32:5...	5.exe	8912	CloseFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	
1:32:5...	5.exe	8912	CreateFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Desired Access: R...
1:32:5...	5.exe	8912	QueryBasicInfor...	C:\Users\user\AppData\Local\Temp_...	SUCCESS	CreationTime: 2/16...
1:32:5...	5.exe	8912	QueryStandardI...	C:\Users\user\AppData\Local\Temp_...	SUCCESS	AllocationSize: 0, E...
1:32:5...	5.exe	8912	CloseFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	
1:32:5...	5.exe	8912	CreateFile	C:\Users\user\AppData\Local\Temp_...	NAME NOT FOUND	Desired Access: R...
1:32:5...	5.exe	8912	CreateFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Desired Access: G...
1:32:5...	5.exe	8912	WriteFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Offset: 0, Length: 4...
1:32:5...	5.exe	8912	WriteFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Offset: 4,096, Leng...
1:32:5...	5.exe	8912	CloseFile	C:\Users\user\AppData\Local\Temp_...	SUCCESS	
1:32:5...	5.exe	8912	CreateFile	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	Desired Access: G...
1:32:5...	5.exe	8912	ReadFile	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	Offset: 7,815,762, ...

It uses Temp a lot, probably to unpack itself.



1:32:4...	5.exe	8912	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffc...
1:32:4...	5.exe	8912	Process Create	C:\Windows\System32\Conhost.exe	SUCCESS	PID: 7524, Comma...
1:32:5...	5.exe	8912	Load Image	C:\Windows\System32\apphelp.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	8912	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	8912	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	8912	Thread Create		SUCCESS	Thread ID: 7468
1:32:5...	5.exe	8912	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	8912	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	8912	Load Image	C:\Windows\System32\ws2_32.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	8912	Thread Create		SUCCESS	Thread ID: 9336
1:32:5...	5.exe	8912	Process Create	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	PID: 4116, Comma...
1:33:1...	5.exe	8912	Load Image	C:\Windows\System32\kernel.appcore.dll	SUCCESS	Image Base: 0x7ffc...
1:33:1...	5.exe	8912	Thread Exit		SUCCESS	Thread ID: 9952, ...
1:33:1...	5.exe	8912	Thread Exit		SUCCESS	Thread ID: 9336, ...
1:33:1...	5.exe	8912	Thread Exit		SUCCESS	Thread ID: 7468, ...
1:33:1...	5.exe	8912	Process Exit		SUCCESS	Exit Status: 0, User...

As we can see it opens up two processes mentioned above.
Let's explore them.

The first terminal that popped up seems to further enumerate the registry and read more files.

1:32:4...	Conhost.exe	7524	Process Start		SUCCESS	Parent PID: 8912, ...
1:32:4...	Conhost.exe	7524	Thread Create		SUCCESS	Thread ID: 3660
1:32:4...	Conhost.exe	7524	Load Image	C:\Windows\System32\conhost.exe	SUCCESS	Image Base: 0x7ff7...
1:32:4...	Conhost.exe	7524	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc...
1:32:4...	Conhost.exe	7524	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
1:32:4...	Conhost.exe	7524	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
1:32:4...	Conhost.exe	7524	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
1:32:4...	Conhost.exe	7524	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
1:32:4...	Conhost.exe	7524	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
1:32:4...	Conhost.exe	7524	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
1:32:4...	Conhost.exe	7524	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
1:32:4...	Conhost.exe	7524	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
1:32:4...	Conhost.exe	7524	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
1:32:4...	Conhost.exe	7524	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
1:32:4...	Conhost.exe	7524	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
1:32:4...	Conhost.exe	7524	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...

Now let's see what the second 5.exe does, presumably the unpacked version of the first.

Time ...	Process Name	PID	Operation	Path	Result	Detail
1:32:5...	5.exe	4116	Process Start		SUCCESS	Parent PID: 8912, ...
1:32:5...	5.exe	4116	Thread Create		SUCCESS	Thread ID: 6796
1:32:5...	5.exe	4116	Load Image	C:\Users\user\Desktop\dynamic\5.exe	SUCCESS	Image Base: 0x7ff7...
1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
1:32:5...	5.exe	4116	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
1:32:5...	5.exe	4116	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
1:32:5...	5.exe	4116	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
1:32:5...	5.exe	4116	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	

This process again continues to query the registry and to use a lot of files.

1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\version.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	Load Image	C:\Users\user\AppData\Local\Temp_...	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\cryptsp.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\rsaenh.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\cryptbase.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\bcryptprimitives.dll	SUCCESS	Image Base: 0x7ffc...

Apparently it also loads crypt libraries…

1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\rasadhlp.dll	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	Load Image	C:\Windows\System32\FWPUCLNT.DLL	SUCCESS	Image Base: 0x7ffc...
1:32:5...	5.exe	4116	TCP Reconnect	Windows11PC:50502 -> tlv03s02-in-f14....	SUCCESS	Length: 0, seqnum:...
1:33:0...	5.exe	4116	TCP Reconnect	Windows11PC:50502 -> tlv03s02-in-f14....	SUCCESS	Length: 0, seqnum:...
1:33:0...	5.exe	4116	TCP Reconnect	Windows11PC:50502 -> tlv03s02-in-f14....	SUCCESS	Length: 0, seqnum:...
1:33:1...	5.exe	4116	TCP Reconnect	Windows11PC:50502 -> tlv03s02-in-f14....	SUCCESS	Length: 0, seqnum:...
1:33:1...	5.exe	4116	TCP Disconnect	Windows11PC:50502 -> tlv03s02-in-f14....	SUCCESS	Length: 0, seqnum:...
1:33:1...	5.exe	4116	Load Image	C:\Windows\System32\kernel.appcore.dll	SUCCESS	Image Base: 0x7ffc...
1:33:1	5.exe	4116	Thread Exit		SUCCESS	Thread ID: 5024

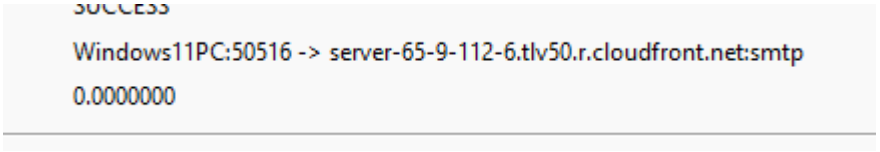
And here we can see it try to connect to a remote server.

Windows11PC:50502 -> tlv03s02-in-f14.1e100.net:smtp

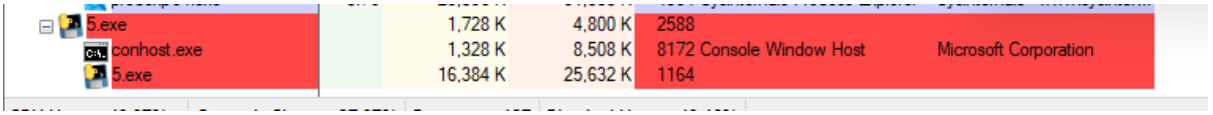
it tries to use SMTP, mail protocol.

On second run it tries to connect to another server

1:48:5...	5.exe	9472	TCP Reconnect	Windows11PC:50515 -> server-65-9-11...	SUCCESS	Length: 0, seqnum:...
1:49:0...	5.exe	9472	TCP Reconnect	Windows11PC:50515 -> server-65-9-11...	SUCCESS	Length: 0, seqnum:...
1:49:1...	5.exe	9472	TCP Disconnect	Windows11PC:50515 -> server-65-9-11...	SUCCESS	Length: 0, seqnum:...
1:49:1...	5.exe	9472	TCP Reconnect	Windows11PC:50516 -> server-65-9-11...	SUCCESS	Length: 0, seqnum:...
1:49:1...	5.exe	9472	TCP Reconnect	Windows11PC:50516 -> server-65-9-11...	SUCCESS	Length: 0, seqnum:...
1:49:1...	5.exe	9472	TCP Reconnect	Windows11PC:50516 -> server-65-9-11...	SUCCESS	Length: 0, seqnum:...
1:49:2...	5.exe	9472	TCP Reconnect	Windows11PC:50516 -> server-65-9-11...	SUCCESS	Length: 0, seqnum:...
1:49:5...	5.exe	9472	Thread Create		SUCCESS	Thread ID: 1676
1:49:5...	5.exe	9472	Thread Create		SUCCESS	Thread ID: 3808

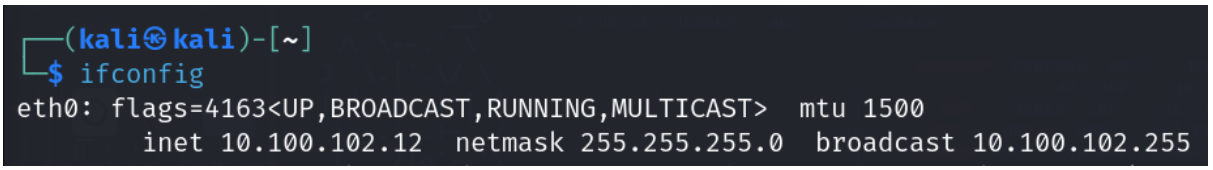


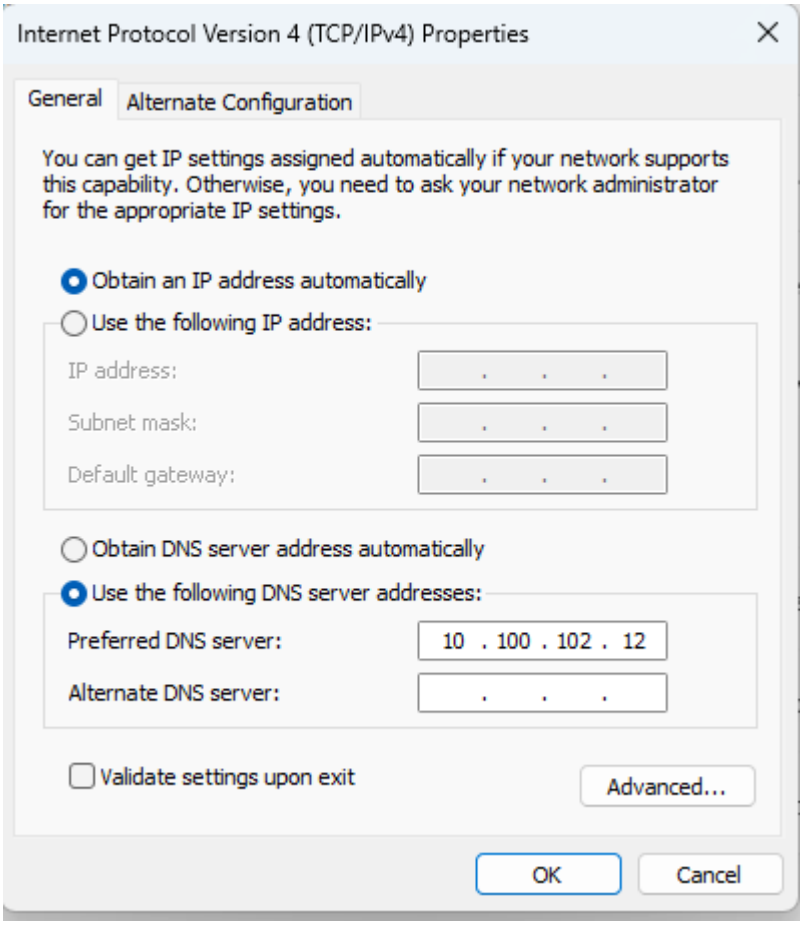
again with SMTP.



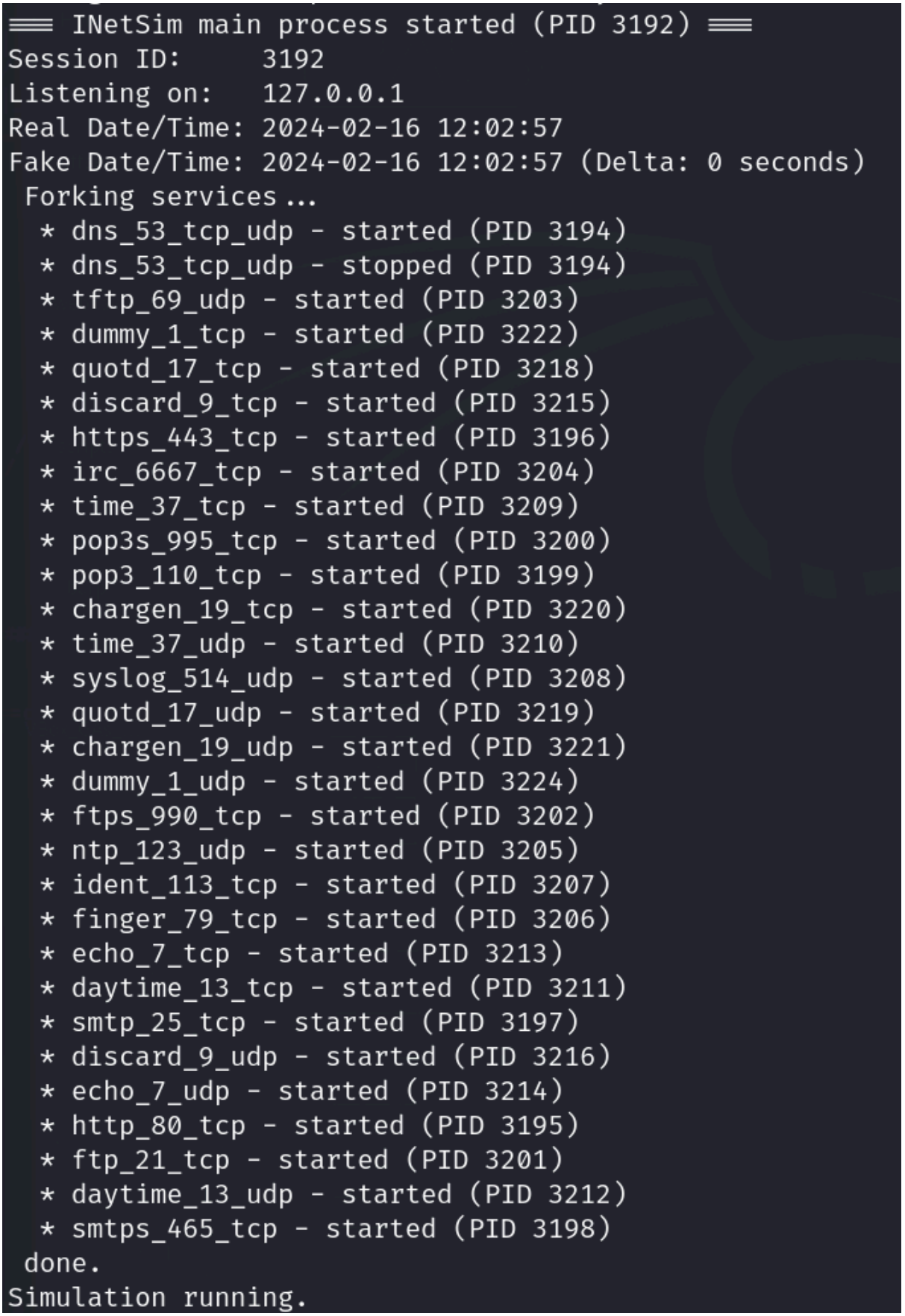
Before exiting it writes that it failed to connect to the SMTP server.

Let's set up Inetsim and Apatedns:





*** We also setted up Apatedns and it changed the DNS server to 127.0.0.1.



Here we run Inetsim, (needed to change from 127.0.0.1 to the current adapter…)

procexp64.exe	< 0.01	23,820 K	46,920 K	4364 Sysinternals Process Explorer	Sysinternals - www.sysinter...
5.exe	4.40	1,340 K	4,784 K	3520	
conhost.exe	< 0.01	6,348 K	20,924 K	9152 Console Window Host	Microsoft Corporation
5.exe	2.93	8,224 K	15,412 K	7644	

Now the process seems to find the SMTP server that previously it didn't find.

After that it connects as well to ftp server and prints:
"Infected computer"

3:38:1...	5.exe	6524	TCP Send	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 28, startim...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 14, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 14, seqnu...
3:38:1...	5.exe	6524	TCP Send	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 17, startim...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 14, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 14, seqnu...
3:38:1...	5.exe	6524	TCP Send	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 6, startime:...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 37, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 37, seqnu...
3:38:1...	5.exe	6524	TCP Send	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 161, starti...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 34, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 34, seqnu...
3:38:1...	5.exe	6524	TCP Send	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 6, startime:...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 31, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 31, seqnu...
3:38:1...	5.exe	6524	TCP Disconnect	Windows11PC:50200 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:38:1...	5.exe	6524	TCP Connect	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 0, mss: 14...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 32, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 32, seqnu...
3:38:1...	5.exe	6524	TCP Send	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 16, startim...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 34, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 34, seqnu...
3:38:1...	5.exe	6524	TCP Send	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 17, startim...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 23, seqnu...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 23, seqnu...
3:38:1...	5.exe	6524	TCP Disconnect	Windows11PC:50201 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...
3:38:1...	5.exe	6524	TCP Connect	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 0, mss: 14...
3:38:1...	5.exe	6524	TCP Send	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 153, starti...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 151, seqn...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 151, seqn...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 1460, seq...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 1460, seq...
3:38:1...	5.exe	6524	TCP TCPCopy	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 956, seqn...
3:38:1...	5.exe	6524	TCP Receive	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 956, seqn...
3:38:1...	5.exe	6524	TCP Disconnect	Windows11PC:50202 -> 16.102.100.10....	SUCCESS	Length: 0, seqnum:...

We see the TCP connection going out.

In Inetsim log file we see the FTP and SMTP

```
2024-02-16 13:37:34  First simulated date in log file
2024-02-16 13:37:34  HTTP connection, method: POST, URL: http://fomfotiqo.in/main.php, file name: /var/l
ib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:37:34  HTTP connection, method: POST, URL: http://wbofelmd.nl/main.php, file name: /var/li
b/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:37:35  HTTP connection, method: POST, URL: http://kqovdubeptl.fr/main.php, file name: /var
/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:37:35  HTTP connection, method: POST, URL: http://xgliacigulmjum.nl/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:37:40  SMTP connection, mails sent: 1, number of recipients: 1, authentication: , authenti
cation data: , bytes: 158 tls=0 cipher=
2024-02-16 13:37:40  FTP connection, created: 0, deleted: 0, retrieved: 0, authentication data: anonymou
s:anonymous@
2024-02-16 13:37:40  HTTP connection, method: GET, URL: http://i.imgur.com/Xig1JQE.gif, file name: /var/
lib/inetsim/http/fakefiles/sample.gif
2024-02-16 13:37:51  SMTP connection, mails sent: 1, number of recipients: 1, authentication: , authenti
cation data: , bytes: 158 tls=0 cipher=
2024-02-16 13:37:51  FTP connection, created: 0, deleted: 0, retrieved: 0, authentication data: anonymou
s:anonymous@
2024-02-16 13:37:51  HTTP connection, method: GET, URL: http://i.imgur.com/Xig1JQE.gif, file name: /var/
lib/inetsim/http/fakefiles/sample.gif
2024-02-16 13:38:01  SMTP connection, mails sent: 1, number of recipients: 1, authentication: , authenti
cation data: , bytes: 158 tls=0 cipher=
2024-02-16 13:38:01  FTP connection, created: 0, deleted: 0, retrieved: 0, authentication data: anonymou
s:anonymous@
2024-02-16 13:38:01  HTTP connection, method: GET, URL: http://i.imgur.com/Xig1JQE.gif, file name: /var/
lib/inetsim/http/fakefiles/sample.gif
2024-02-16 13:38:07  SMTP connection, mails sent: 1, number of recipients: 1, authentication: , authenti
cation data: , bytes: 158 tls=0 cipher=
2024-02-16 13:38:07  FTP connection, created: 0, deleted: 0, retrieved: 0, authentication data: anonymou
s:anonymous@
2024-02-16 13:38:07  HTTP connection, method: GET, URL: http://i.imgur.com/Xig1JQE.gif, file name: /var/
lib/inetsim/http/fakefiles/sample.gif
2024-02-16 13:38:13  SMTP connection, mails sent: 1, number of recipients: 1, authentication: , authenti
cation data: , bytes: 158 tls=0 cipher=
2024-02-16 13:38:13  FTP connection, created: 0, deleted: 0, retrieved: 0, authentication data: anonymou
s:anonymous@
2024-02-16 13:38:13  HTTP connection, method: GET, URL: http://i.imgur.com/Xig1JQE.gif, file name: /var/
lib/inetsim/http/fakefiles/sample.gif
2024-02-16 13:38:17  HTTP connection, method: POST, URL: http://ejpcvdmkrjsjvn.in/main.php, file name: /
var/lib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:38:17  HTTP connection, method: POST, URL: http://rypsrq.eu/main.php, file name: /var/lib/
inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:38:17  HTTP connection, method: POST, URL: http://fomfotiqo.in/main.php, file name: /var/l
ib/inetsim/http/postdata/97aa9d2b9f72917664553ed4dba45571199cb58693d17e47186d7afd7c7a11fd
2024-02-16 13:38:18  SMTP connection, mails sent: 1, number of recipients: 1, authentication: , authenti
cation data: , bytes: 158 tls=0 cipher=
```

It send some mails.

Conclusion 5

This is a malware that reports to a remote C2 server that it has infected a computer. Could have installed a backdoor for connection later. Would catalog it as a virus.