A Trojan infected my Laptop on 20 Feb 2024. I received this warning from Windows 10 Defender / Security.

A screenshot of a computer

Description automatically generated

My Microsoft Visual Studio 2019 had stopped working. A Windows 10 Defender / Security was unable to remove the Trojan (I think the Trojan is in the Registry).

I eventually found an Anti-Virus progam that was able to fix it, I thought, as I could use Visual Studio 2019 again. However, other problems occurred.

I noticed an abnormal folder named “!-” .

A screenshot of a computer

Description automatically generated

I “renamed” the “!-” folder to “~!-” → The abnormal folder named “!-” reappeared.

I also noticed a new folder $RECYCLE.BIN which contains the Recycle Bin folder and other folders.

A screenshot of a computer

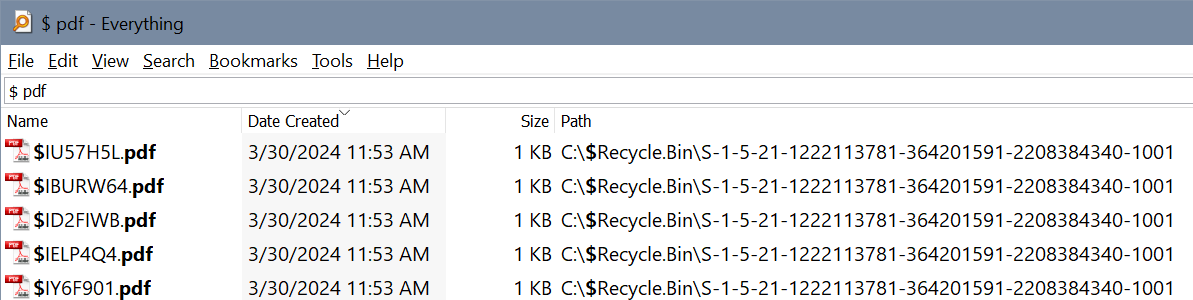
Description automatically generated

I am unable to access those other folders.

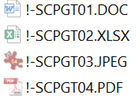
A screenshot of a computer

Description automatically generated

An “Everything” search for pdf files finds strange names: $l9R38K.pdf, etc. … in the $RECYCLE.BIN. Those are not my names.



I also noticed abnormal file names.



These files include the words “Scape Goat”.

--------------------------------------------------

Recently, these files below were the contents of the “!-” . folder.

A screenshot of a computer

Description automatically generated

Compiling Visual Studio 2019 resulted in these messages.

A screenshot of a computer error message

Description automatically generated

A close-up of a computer screen

Description automatically generated

The contents of the “!-” . folder changed after attempting to recompile Visual Studio.

A screenshot of a computer

Description automatically generated

Note that the “**Date created**” changes. The “**Date modified**” does not change. Also note that every “**Date created**" has “**identical**” dates and times.

Recompiling Visual Studio 2019 a second time (F5) works. The failure occurs every other time.

--------------------------------------------------

I did an “Everything” search for “Data01.exe”

A screenshot of a computer

Description automatically generated

These exact identical file names are on two drives, and in different folders. The Trojan is in many locations.

--------------------------------------------------

I zipped the “!-” folder → “!-.zip”. When I attach “!-.zip” to an email message (Firefox - Gmail) I get this message:

A screenshot of a computer screen

Description automatically generated

Firefox and / or Gmail is detecting the Trojan inside the zip file. This means there is a Trojan in one, or more, of the files in the “!-“ folder. Mozilla or Google knows what to detect.

This “!-.zip” file has been uploaded to my website <https://aaa.foxping.com/> so others can analyze.

--------------------------------------------------

This Trojan also affects opening pdf files, and accessing folders with File Explorer. It takes multiple attempts for for them to work.

This Trojan has also infected my wife’s laptop. It takes mulitiple attempts for her to open a pdf file. She uses Acrobat Reader. I use Acrobat Adobe Pro.

I suspect that the Trojan is inside some pdf files. Don’t know it there is a way to remove a Trojan inside of pdf files?

--------------------------------------------------

I noticed that an abnormal file name appears in some folders. See the file named “aam84824”. This is a Trojan file.

A white background with black text

Description automatically generated

This type of file name appears when I attempt to open a pdf file and compile. The name changes to other names such as “aak28764”.

--------------------------------------------------

I have a program that displays the contents of the “aam84824” file (hex numbers):

25 50 44 46 2D 31 2E 37 0D 25

% P D F - 1 . 7 cr %

E2 E3 CF D3 0D 0A 36 30 30 20

. . . . cr lf 6 0 0

30 20 6F 62 6A 0D 3C 3C 2F 4C

0 o b j cr < < / L

69 6E 65 61 72 69 7A 65 64 20

i n e a r i z e d

31 2F 4C 20 35 39 34 33 34 2F

1 / L 5 9 4 3 4 /

4F 20 36 30 35 2F 45 20 32 35

O 6 0 5 / E 2 5

34 31 35 2F 4E 20 32 2F 54 20

4 1 5 / N 2 / T

35 39 30 33 37 2F 48 20 5B 20

5 9 0 3 7 / H [

35 31 30 20 32 32 34 5D 3E 3E

5 1 0 2 2 4 ] > >

0D 65 6E 64 6F 62 6A 0D 20 20

cr e n d o b j cr

20 20 20 20 20 20 20 20 20 20

20 20 20 20 0D 0A 36 32 32 20

cr lf 6 2 2

30 20 6F 62 6A 0D 3C 3C 2F 44

0 o b j cr < < / D

65 63 6F 64 65 50 61 72 6D 73

e c o d e P a r m s

3C 3C 2F 43 6F 6C 75 6D 6E 73

< < / C o l u m n s

20 34 2F 50 72 65 64 69 63 74

4 / P r e d i c t

6F 72 20 31 32 3E 3E 2F 46 69

o r 1 2 > > / F i

6C 74 65 72 2F 46 6C 61 74 65

l t e r / F l a t e

44 65 63 6F 64 65 2F 49 44 5B

D e c o d e / I D [

3C 32 38 38 30 43 39 32 45 42

< 2 8 8 0 C 9 2 E B

255044462D312E370D25

%PDF-1.7cr%

E2E3CFD30D0A36303020

....crlf600

30206F626A0D3C3C2F4C

0 objcr<</L

696E656172697A656420

inearized

312F4C2035393433342F

1/L 59434/

4F203630352F45203235

O 605/E 25

3431352F4E20322F5420

415/N 2/T

35393033372F48205B20

59037/H [

353130203232345D3E3E

510 224]>>

0D656E646F626A0D2020

crendobjcr

20202020202020202020

202020200D0A36323220

crlf622

30206F626A0D3C3C2F44

0 objcr<</D

65636F64655061726D73

ecodeParms

3C3C2F436F6C756D6E73

<</Columns

20342F50726564696374

4/Predict

6F722031323E3E2F4669

or 12>>/Fi

6C7465722F466C617465

lter/Flate

4465636F64652F49445B

Decode/ID[

3C323838304339324542

<2880C92EB