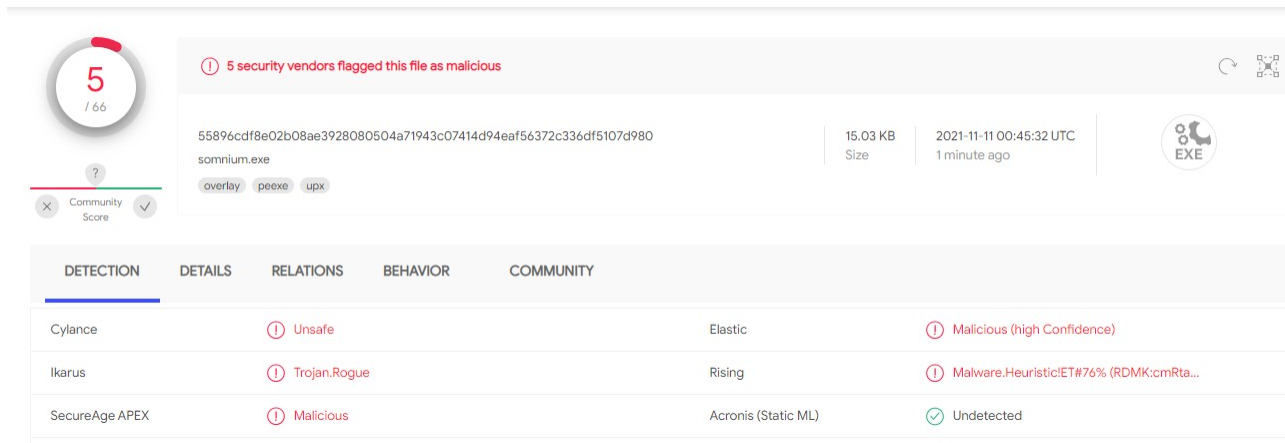


Cpsc 458 quiz 2

somnium.exe

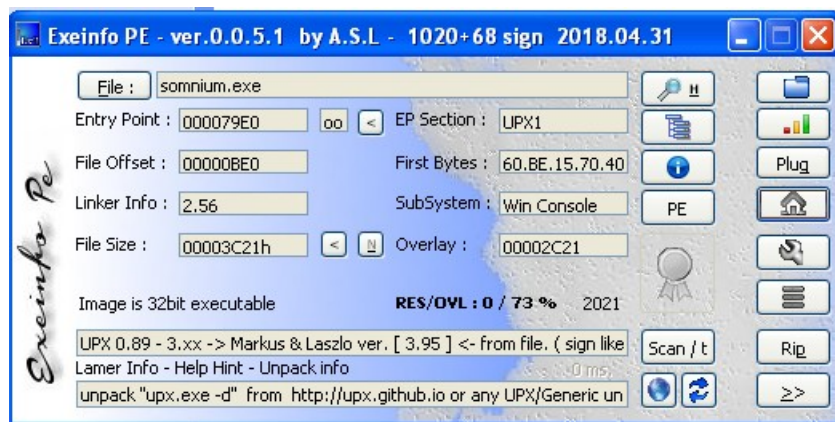
<https://www.virustotal.com/gui/file/55896cdf8e02b08ae3928080504a71943c07414d94eaf56372c336df5107d980/detection>



The image shows the VirusTotal detection results for the file `somnium.exe`. At the top, a circular badge indicates that 5 out of 66 security vendors have flagged the file as malicious. Below this, the file's SHA-256 hash is displayed: `55896cdf8e02b08ae3928080504a71943c07414d94eaf56372c336df5107d980`. The file size is 15.03 KB, and it was scanned on 2021-11-11 at 00:45:32 UTC, 1 minute ago. The file is identified as `somnium.exe` and is associated with the UPX packer. The detection results table shows the following:

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Cylance	Unsafe	Elastic	Malicious (high Confidence)	
Ikarus	Trojan.Rogue	Rising	Malware.Heuristic:ET#76% (RDMK:cmRta...	
SecureAge APEX	Malicious	Acronis (Static ML)	Undetected	

Ikarus says rogue trojan.



The program appears to be packed using UPX.

```
GA Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "C:\Documents and Settings\Administrator\Desktop\somnium-3\somnium"

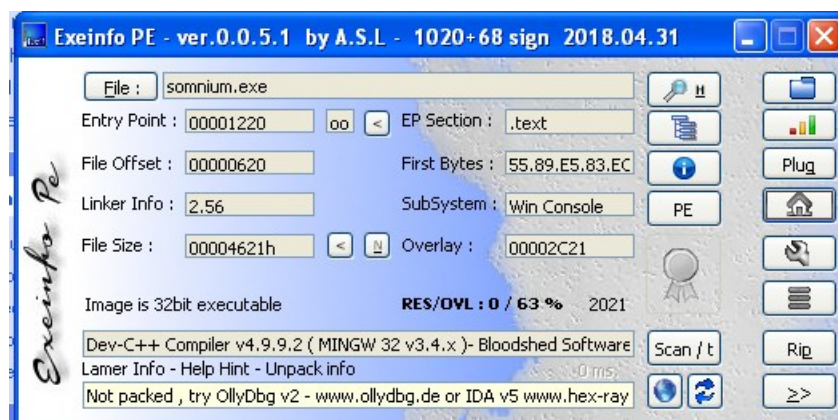
C:\Documents and Settings\Administrator\Desktop\somnium-3\somnium>upx -d somnium.exe

                          Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95d                Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

File size   Ratio   Format   Name
-----
17953 <-   15393   85.74%   win32/pe   somnium.exe

Unpacked 1 file.
C:\DOCUME~1\ADMINI~1\Desktop\SOMNIU~1\somnium>
```

The program has been unpacked successfully.



The program appears to be compiled using Dev-C++ compiler.

The program might use the command line.

compiler-stamp	0x6184E2FA (Thu Nov 04 23:53:30 2021 - UTC)
----------------	---

The program appears to have a compiler timestamp of Thursday November 4 23:53:30 2021 UTC.

type (1)	size (bytes)	file-offset	blacklist (6)	hint (21)	value (518)
ascii	28	0x000012B1	-	utility	Time for lunch crunch crunch
ascii	27	0x00001327	-	utility	Time to crunch munch munch!
ascii	25	0x000013C4	-	utility	start cmd %s -agnosthesia
ascii	37	0x000013E0	-	utility	Taskkill /IM procmon.exe /F >nul 2>&1
ascii	44	0x00001284	x	file	C:\Program Files\Mozilla Firefox\firefox.exe
ascii	34	0x00001304	x	file	C:\Program Files\IDA Free\idag.exe
ascii	42	0x00001480	-	file	../gcc/gcc/config/i386/w32-shared-ptr.c
ascii	12	0x000018BC	-	file	KERNEL32.DLL
ascii	10	0x00001928	-	file	msvcrt.dll
ascii	6	0x00001A12	-	file	crt1.c
ascii	10	0x00001B20	-	file	crtstuff.c
ascii	11	0x00001BD4	-	file	somnium.cpp
ascii	9	0x00001CBE	-	file	CRTglob.c
ascii	10	0x00001D4E	-	file	CRTfmode.c
ascii	9	0x00001DDE	-	file	txtmode.c
ascii	14	0x00001E6E	-	file	pseudo-reloc.c
ascii	10	0x00001F22	-	file	CRT_fp10.c
ascii	9	0x00001FE8	-	file	gccmain.c
ascii	10	0x00003632	-	file	crtstuff.c
ascii	19	0x00003F3B	-	file	pseudo-reloc-list.c
ascii	40	0x0000004D	-	dos-message	!This program cannot be run in DOS mode.

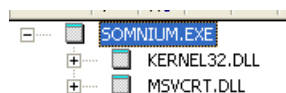
Possible Host based indicators:

- C:\Program Files\Mozilla Firefox\firefox.exe
- C:\Program Files\IDA Free\idag.exe
- somnium.cpp

There doesn't appear to be any network based indicators in the strings.

Other suspicious strings:

- Time for lunch crunch crunch
- Time to crunch munch munch!
- start cmd %s -agnosthesia
- Taskkill /IM procmon.exe /F >nul 2>&1
- Sorry, no memes here...
- I am a creature with many faces...
- What a bummer...
- This is dumb...
- -doit
- Bummer this is not...
- -doworse
- Are you frustrated yet? What a bummer!
- -actlikeafool
- -agnosthesia
- In my restless dreams I see that malware...altschmerz?
- In my restless dreams I see that malware...

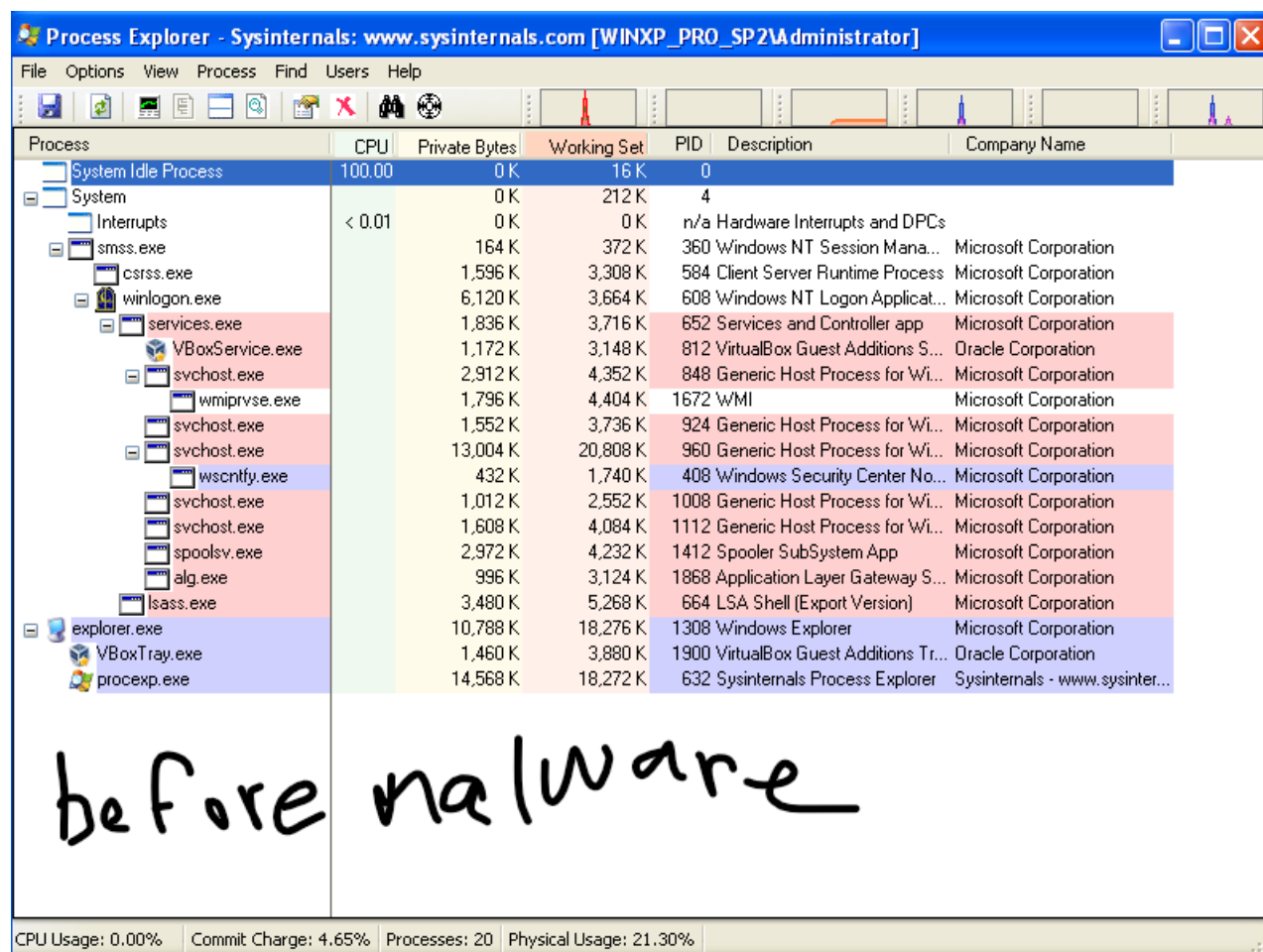


Imports:

- Kernel32.dll: might use kernel functions
- msvcrt.dll: might use c library functions

=

BASIC dynamic analysis

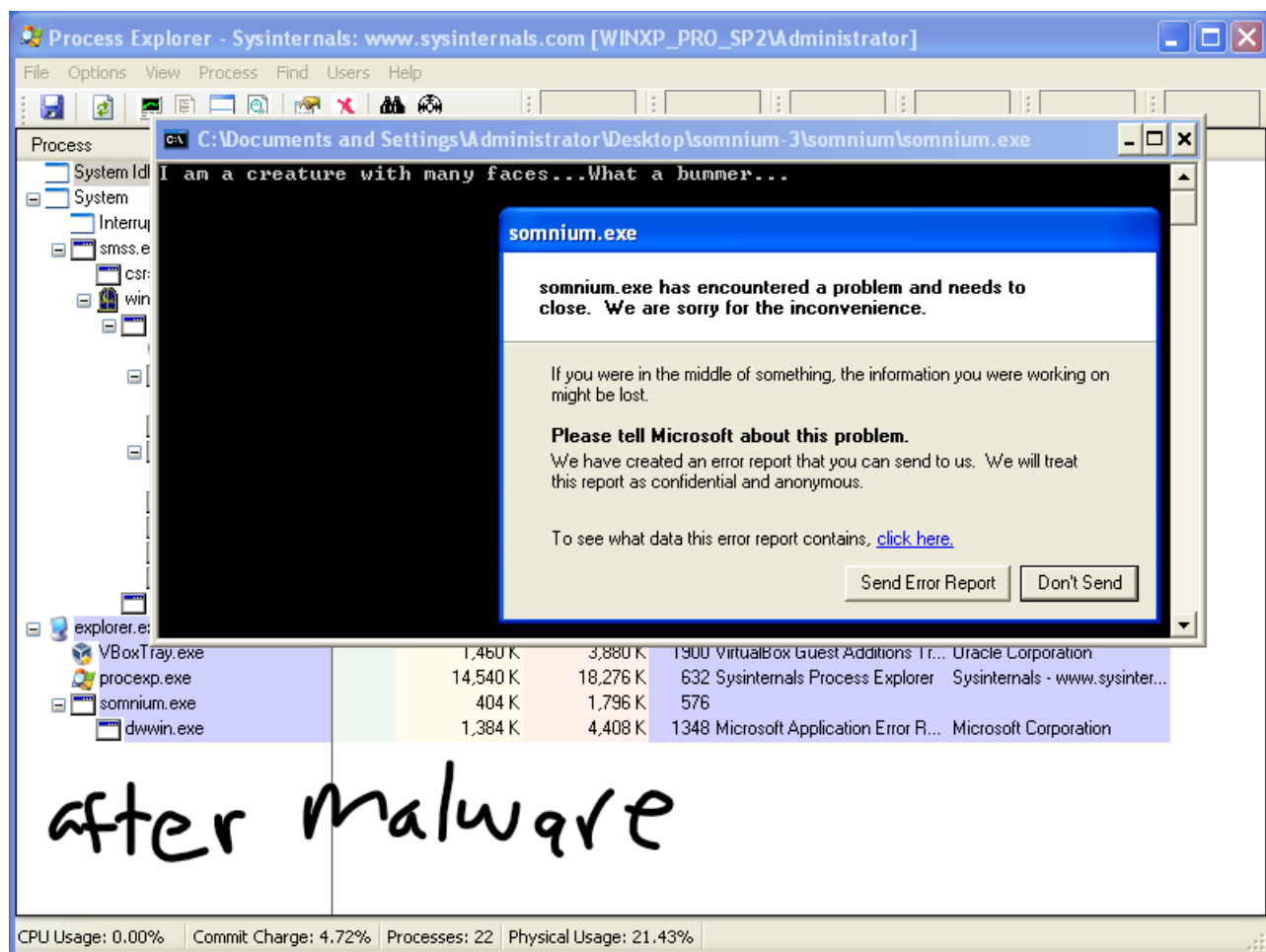


The screenshot shows the Process Explorer window from Sysinternals. The title bar reads "Process Explorer - Sysinternals: www.sysinternals.com [WINXP_PRO_SP2\AAdministrator]". The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains various icons for file operations and system functions. The main window displays a list of processes with columns for Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The processes are organized in a tree view on the left, starting with System Idle Process, System, Interrupts, and then user-level processes like explorer.exe, VBoxTray.exe, and procexp.exe. The status bar at the bottom shows CPU Usage: 0.00%, Commit Charge: 4.65%, Processes: 20, and Physical Usage: 21.30%.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	100.00	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	360	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,596 K	3,308 K	584	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,120 K	3,664 K	608	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,836 K	3,716 K	652	Services and Controller app	Microsoft Corporation
VBoxService.exe		1,172 K	3,148 K	812	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		2,912 K	4,352 K	848	Generic Host Process for Wi...	Microsoft Corporation
wmiprivse.exe		1,796 K	4,404 K	1672	WMI	Microsoft Corporation
svchost.exe		1,552 K	3,736 K	924	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,004 K	20,808 K	960	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		432 K	1,740 K	408	Windows Security Center No...	Microsoft Corporation
svchost.exe		1,012 K	2,552 K	1008	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,608 K	4,084 K	1112	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2,972 K	4,232 K	1412	Spooler SubSystem App	Microsoft Corporation
alg.exe		996 K	3,124 K	1868	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,480 K	5,268 K	664	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe		10,788 K	18,276 K	1308	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,460 K	3,880 K	1900	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe		14,568 K	18,272 K	632	Sysinternals Process Explorer	Sysinternals - www.sysinter...

before malware

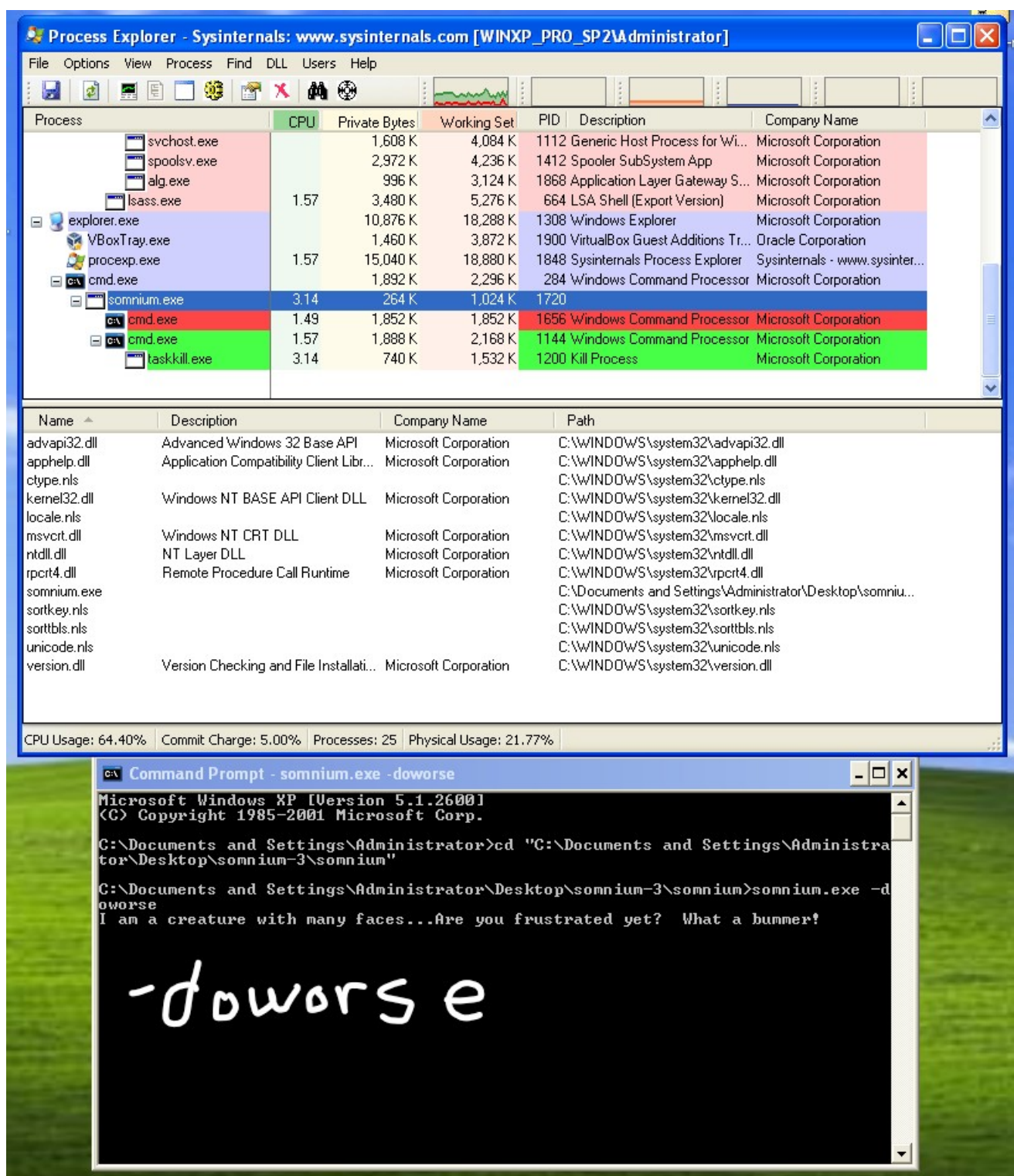
CPU Usage: 0.00% | Commit Charge: 4.65% | Processes: 20 | Physical Usage: 21.30%



Somnium.exe is visible in the process explorer and an error message has appeared. Perhaps this is a roadblock?

There appears to be command line arguments in the strings:

- -doit
- -doworse
- -actlikeafool
- -agnosthesia



With the argument -doworse, the malware appears to open up two child cmd.exe processes, and each cmd.exe process appears to be creating a child process taskkill.exe.

This seems to be similar to when the argument -doit was used, except a different message appears in the command line.

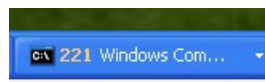
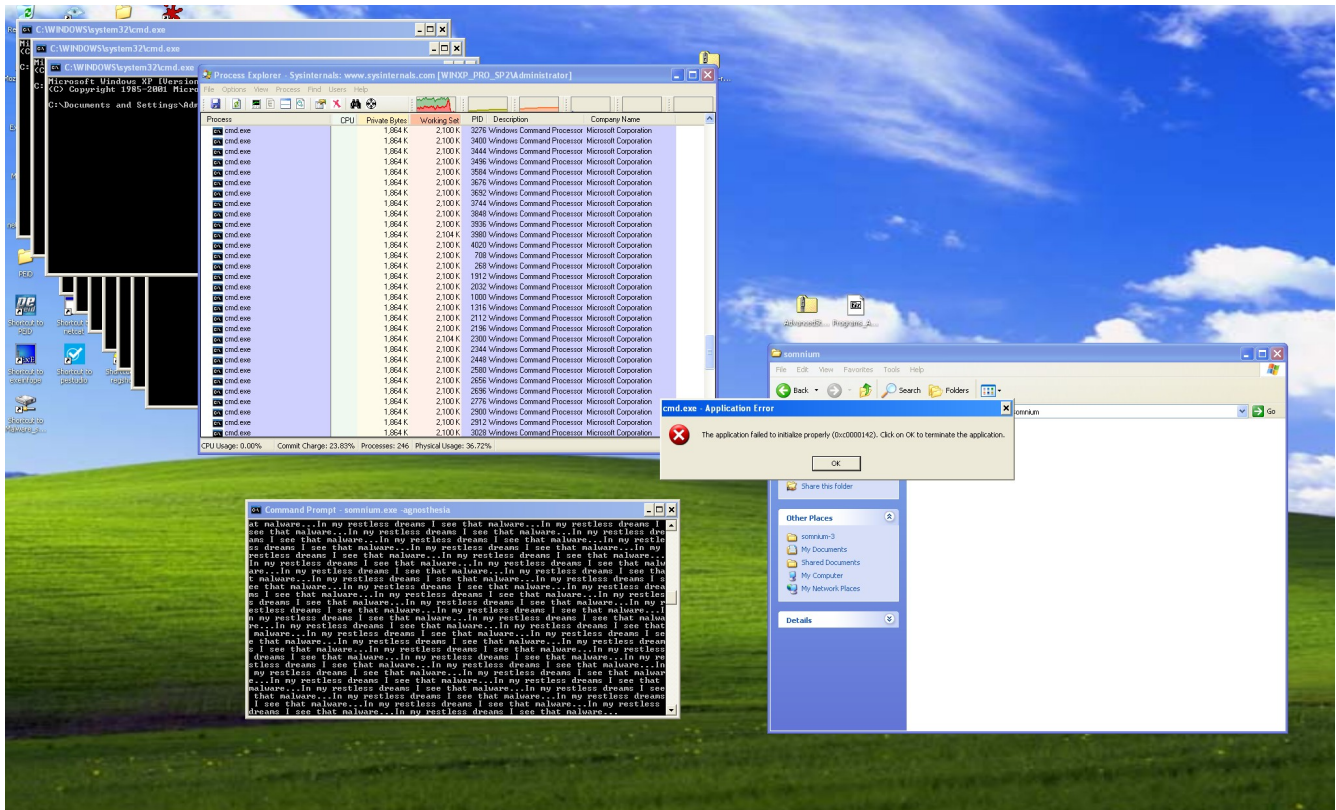
Type	Name
Directory	\BaseNamedObjects
Directory	\Windows
Directory	\KnownDlls
File	C:\Documents and Settings\Administrator\Desktop\somnium-3\somnium
Key	HKLM
Key	HKCU
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\ShimCacheMutex
Process	cmd.exe[452]
Process	<Non-existent Process>[1224]
Section	\BaseNamedObjects\ShimSharedMemory
Thread	<Non-existent Process>[1224]: 2032
Thread	cmd.exe[452]: 1248
WindowStation	\Windows\WindowStations\WinSta0

CPU Usage: 45.31% | Commit Charge: 5.07% | Processes: 25 | Physical Usage: 21.84%

Handles panel for -doworse.

[illegible]

This seems to be similar to when the arguments `-doit` and `-doworse` were used, except a different message appears in the command line.



With the argument -agnosthesia the malware appears to constantly create new instances of the command line, and on the original command line it constantly prints “In my restless dreams I see that malware...”

PROCMON

Regshot 1.8.2

Comments:

Datetime:2021/11/11 02:22:43 , 2021/11/11 02:27:31

Computer:WINXP_PRO_SP2 , WINXP_PRO_SP2

Username: ,

Values modified:9

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 5A F8 6C 61 7C FD 8C 83 F7 DE 95 B3 66 BB 35 CD 11 C0 0D 60 C4 A6 8F 87 0C C9 39 00 83 FD 86 36 F8 34 15 7C 7A 56 50 0D 18 4D CA 78 20 50 DA 43 86 1D DD F4 42 AC 52 4C 6D 84 68 A9 8A 04 58 EE 52 06 E7 5D 58 D1 6C 51 F1 77 08 98 CE B9 5F 59

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: AA 33 86 8C A5 43 4C DD AA 45 C9 BA 5A 6E 04 77 FA EF 90 90 63 53 C0 3F 8B 74 8E 37 CA BC FE A1 CD F7 99 B9 1D C6 4C 2B F2 1E

9D A9 FF 37 90 CB F5 4C 93 48 D1 5D C6 12 52 92 FE 52 43 72 1E 5D DD 3F 50 58 DA 43 E4 46
86 D0 24 57 40 1F 45 33

HKLM\SOFTWARE\Microsoft\DrWatson\NumberOfCrashes: 0x00000005

HKLM\SOFTWARE\Microsoft\DrWatson\NumberOfCrashes: 0x00000006

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\
HRZR_HVGBBYONE: 0B 00 00 00 26 00 00 00 D0 9F 8A 69 96 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\
HRZR_HVGBBYONE: 0B 00 00 00 27 00 00 00 90 B8 C9 08 A3 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\
HRZR_HVGBBYONE:0k1,130: 0B 00 00 00 21 00 00 00 D0 9F 8A 69 96 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{5E6AB780-7743-11CF-A12B-00AA004AE837}\Count\
HRZR_HVGBBYONE:0k1,130: 0B 00 00 00 22 00 00 00 90 B8 C9 08 A3 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACNGU: 08 00 00 00 8D 00 00 00 90 51 4F F9 A2 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACNGU: 08 00 00 00 8E 00 00 00 A0 FB 00 06 A3 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\pzq.rkr: 08 00 00 00 1C 00 00 00 10 F6 13 63 96 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\pzq.rkr: 08 00 00 00 1D 00 00 00 A0 FB 00 06 A3 D6 D7
01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACVQY: 08 00 00 00 18 00 00 00 10 F6 13 63 96 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACVQY: 08 00 00 00 19 00 00 00 A0 FB 00 06 A3 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACVQY:%pfvqy2%\Npprrffbevrf\Pbzznaq Cebzcg.yax: 08 00 00 00 13 00 00 00 10 F6 13
63 96 D6 D7 01

HKUS-1-5-21-682003330-2147343463-725345543-500\Software\Microsoft\Windows\
CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HRZR_EHACVQY:%pfvqy2%\Npprrffbevrf\Pbzznaq Cebzcg.yax: 08 00 00 00 14 00 00 00 A0 FB 00
06 A3 D6 D7 01

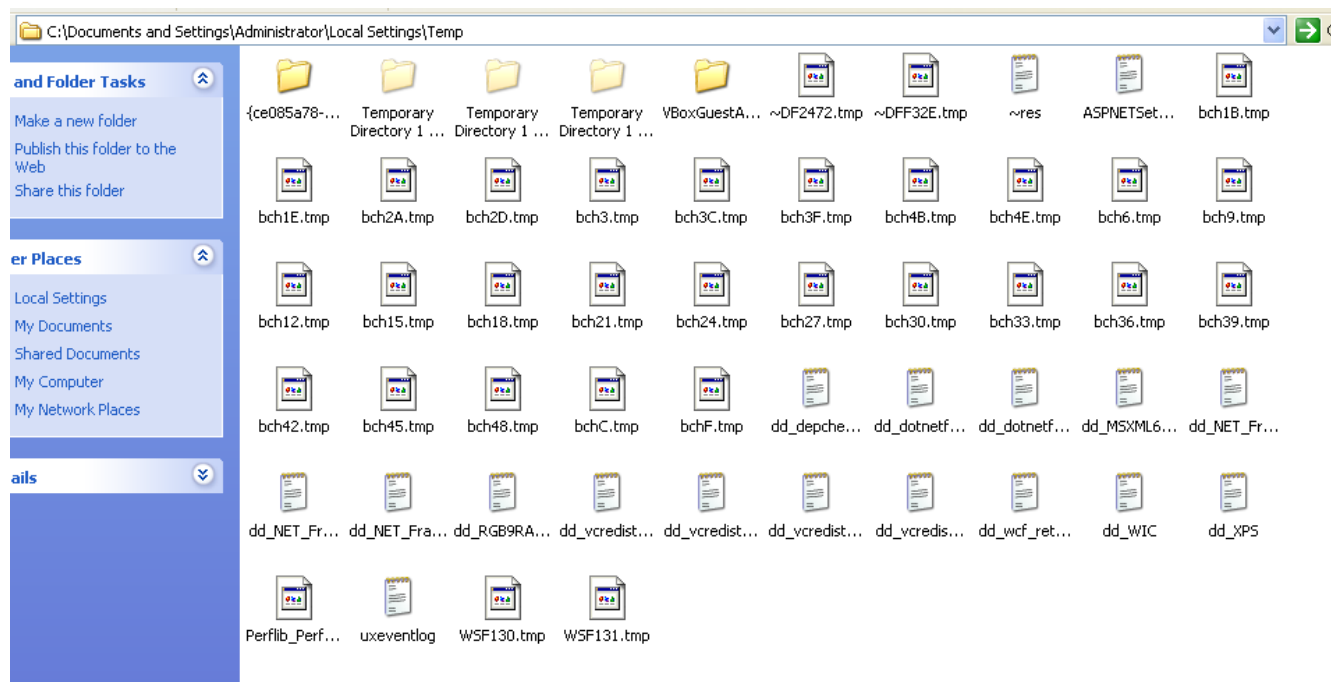
HKUS-1-5-21-682003330-2147343463-725345543-500\SessionInformation\ProgramCount:
0x00000003

HKUS-1-5-21-682003330-2147343463-725345543-500\SessionInformation\ProgramCount:
0x00000004

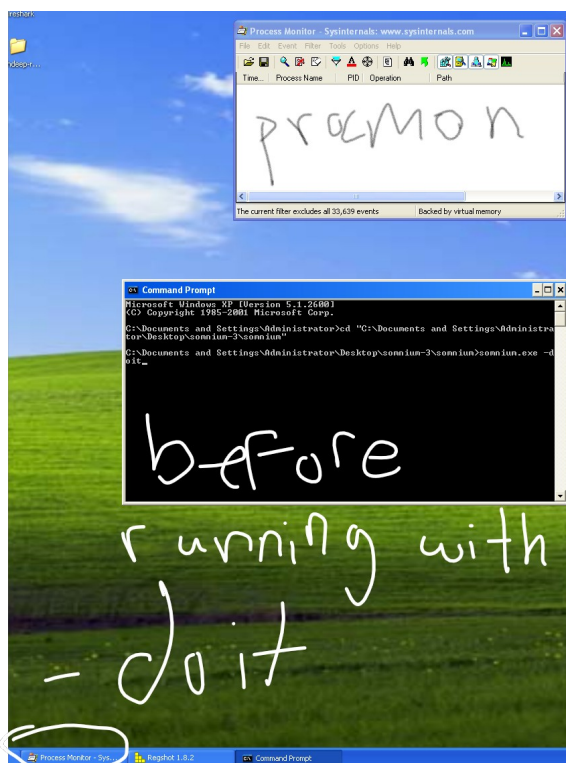
Regshot did not seem to catch any suspicious activity from the malware.

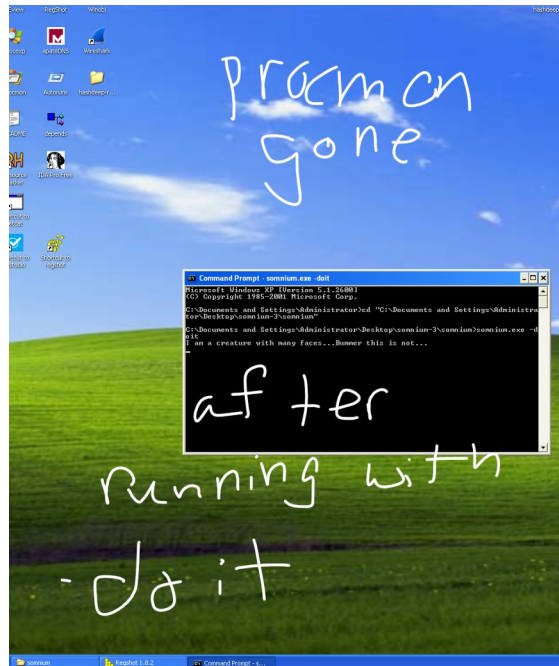
File path: \\fml-fs-02\pub\pub_data\pub_data\file\160401\COMMON\EXE\1D3DE5E5_6_1.GA

The malware appears to be accessing a file named `eb1e_appcompat.txt` located at `C:\Documents and Settings\Administrator\Local Settings\Temp\eb1e_appcompat.txt`.

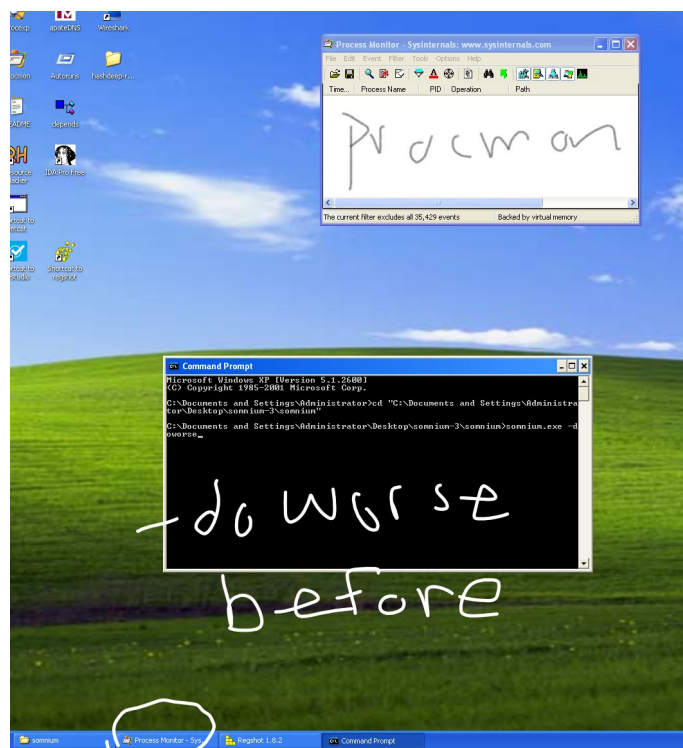


The mentioned file does not seem to be in this directory.





Running the malware with -doit seems to have resulted in the procmon program being closed.





Running the malware with -doworse seems to have resulted in the procmon program being closed.

This is similar to what seems to have happened with the argument -doit.