Laborator 8

Securitatea Sistemelor Informatice

1.

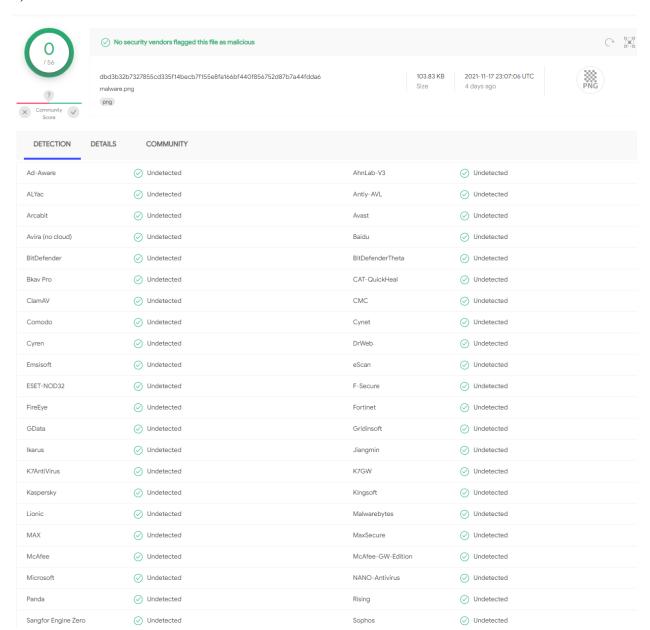
- a) Cand am deschis imaginea prin dublu click nu am putut observat nimic suspicios. Nu a aparut nicio eroare.
- b) Cand am deschis imaginea in HxD, am observat ca imaginea are ascunsa in ea un executabil.

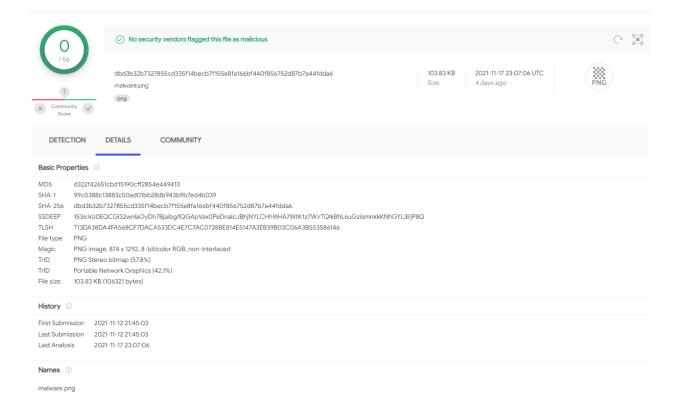
📓 malware.png																	
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	OD	0E	OF	Decoded text
0000A7C0	01	E2	23	00	00	00	0A	10	1F	01	00	00	50	80	F8	08	.â‡P€ø.
0000A7D0	00	00	80	02	C4	47	00	00	00	14	20	3E	02	00	00	A0	€.ÄG >
0000A7E0	00	F1	11	00	00	00	05	88	8F	00	00	00	28	40	7C	04	.ñ^(@ .
0000A7F0	00	00	40	01	E2	23	00	00	00	0A	10	1F	01	00	00	50	@.â#P
008A0000	80	F8	08	00	00	80	02	C4	47	00	00	00	14	20	3E	02	€ø€.ÄG >.
0000A810	00	00	A0	00	F1	11	00	00	00	05	88	8F	00	00	00	28	ñ^(
0000A820	40	7C	04	00	00	40	01	E2	23	00	00	00	0A	10	1F	01	@ @.â#
0000A830	00	00	50	80	F8	08	00	00	80	02	C4	47	00	00	00	14	P€ø€.ÄG
0000A840	20	3E	02	00	00	A0	00	Fl	11	00	00	00	D9	7E	7E	FE	>ñÙ~~þ
0000A850	7 F	59	C3	0C					51			00		49		4E	.YÃ.ñ_SÏQIEN
0000A860		ΑE		60			5A	90	00	03	00	00	00	04	00	0.0	D®B`,MZ
0000A870	00	FF	FF	00		В8			00		00		00	40	00	0.0	·ÿÿ,@
088A0000														00		0.0	
0000A890			00											00		0.0	
0000A8A0			00											21		01	.€°′.Í!,.
0000A8B0		CD			68	69	73			72	6F	67	72	61	6D	20	LÍ!This program
0000A8C0	63	61	6E	6E	6F	74	20	62	65	20	72	75	6E	20	69	6E	cannot be run in
0000A8D0														24		0.0	DOS mode\$
0000A8E0			00								01			CF		8E	PELÏߎ
0000A8F0	61	00	BC	00	00	49	02	00	00	E0	00	07	01	0B	01	02	a.4Ià
0000A900														ΕO			0Nà
0000A910														00			
0000A920														04			
0000A930			00											0D).
0000A940														00			
0000A950														00			
0000A960														00			€ø
0000A970			00											00			
0000A980														00			
0000A990														00			
0000A9A0			00											00			
0000A9B0														88			
0000A9C0 0000A9D0														2E			te
0000A9D0														00			xt
0000A9E0														00			xt
0000A9F0														1C			.`.P`.data
0000AA10														00			@4
0000AA10			00							40				2E			@.0À.rd
0000AA30														00			ataHP
0000AA40														00			6
0000AA10														50			.@.0@/4P
0000AA60														00			`
0000AA70														2E			
0000AA80			00											00			stp
0000AA90			00											00			
0000AAA0			00											D8			.€.0À.idataØ
0000AAB0			80											00			€
0000AAC0														2E			@.0À.CR
0000AAD0	54	00	00	00	00	18	00	00	00	00	90	00	00	00	02	00	T
0000AAE0	00	00	4E	00	00	00	00	00	00	00	00	00	00	00	00	00	N
0000AAF0	00	40	00	30	CO	2E	74	6C	73	00	00	00	00	20	00	00	.@.0À.tls
0000AB00	00	00	A0	00	00	00	02	00	00	00	50	00	00	00	00	00	
0000AB10	00	00	00	00	00	00	00	00	00	40	00	30	CO	2F	31	34	@.0À/14
0000AB20	00	00	00	00	00	58	00	00	00	00	во	00	00	00	02	00	X°
																	-

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
0000DE60 00 00 00 00 00 6C 69 62 67 63 63 5F 73 5F 64 77 .....libgcc s dw
0000DE70 32 2D 31 2E 64 6C 6C 00 5F 5F 72 65 67 69 73 74 2-1.dll. regist
0000DE80 65 72 5F 66 72 61 6D 65 5F 69 6E 66 6F 00 5F 5F er frame info.
0000DE90 64 65 72 65 67 69 73 74 65 72 5F 66 72 61 6D 65 deregister frame
0000DEA0 5F 69 6E 66 6F 00 6C 69 62 67 63 6A 2D 31 36 2E info.libgcj-16.
0000DEB0 64 6C 6C 00 5F 4A 76 5F 52 65 67 69 73 74 65 72 dll. Jv Register
0000DEC0 43 6C 61 73 73 65 73 00 00 00 2E 00 69 6D 70 46 Classes....impF
0000DED0 6F 6C 64 65 72 46 4D 49 5F 4D 41 4C 77 61 72 65 olderFMI MALware
0000DEE0 00 67 6F 74 48 61 63 6B 65 64 42 79 65 00 2E 70 .gotHackedBye..p
0000DEF0 64 66 00 45 72 72 6F 72 20 6F 70 65 6E 69 6E 67 df.Error opening
0000DF00 20 64 69 72 65 63 74 6F 72 79 00 48 65 6C 6C 6F directory.Hello
0000DF10 20 77 6F 72 6C 64 21 00 00 70 1C 40 00 4D 69 6E world!..p.@.Min
0000DF20 67 77 20 72 75 6E 74 69 6D 65 20 66 61 69 6C 75 gw runtime failu
0000DF30 72 65 3A 0A 00 20 20 56 69 72 74 75 61 6C 51 75 re:.. VirtualOu
0000DF40 65 72 79 20 66 61 69 6C 65 64 20 66 6F 72 20 25 ery failed for %
0000DF50 64 20 62 79 74 65 73 20 61 74 20 61 64 64 72 65 d bytes at addre
0000DF60 73 73 20 25 70 00 00 00 20 20 55 6E 6B 6E 6F ss %p.... Unkno
0000DF70 77 6E 20 70 73 65 75 64 6F 20 72 65 6C 6F 63 61 wn pseudo reloca
0000DF80 74 69 6F 6E 20 70 72 6F 74 6F 63 6F 6C 20 76 65 tion protocol ve
0000DF90 72 73 69 6F 6E 20 25 64 2E 0A 00 00 00 20 20 55 rsion %d..... U
0000DFA0 6E 6B 6E 6F 77 6E 20 70 73 65 75 64 6F 20 72 65 nknown pseudo re
0000DFB0 6C 6F 63 61 74 69 6F 6E 20 62 69 74 20 73 69 7A location bit siz
0000DFC0 65 20 25 64 2E 0A 00 00 02 E 00 67 6C 6F 62 2D e %d......glob-
0000DFD0 31 2E 30 2D 6D 69 6E 67 77 33 32 00 00 00 2E 1.0-mingw32.....
0000DFE0 00 00 00 00 00 80 20 00 00 47 43 43 3A 20 28 47
                                                       .....€ ..GCC: (G
0000DFF0 4E 55 29 20 36 2E 33 2E 30 00 00 00 47 43 43 NU) 6.3.0....GCC
0000E000 3A 20 28 47 4E 55 29 20 36 2E 33 2E 30 00 00 00 : (GNU) 6.3.0...
0000E010 00 47 43 43 3A 20 28 4D 69 6E 47 57 2E 6F 72 67
                                                      .GCC: (MinGW.org
0000E020 20 47 43 43 2D 36 2E 33 2E 30 2D 31 29 20 36 2E
                                                       GCC-6.3.0-1) 6.
0000E030 33 2E 30 00 00 47 43 43 3A 20 28 47 4E 55 29 20 3.0..GCC: (GNU)
0000E040 36 2E 33 2E 30 00 00 00 00 47 43 43 3A 20 28 47 6.3.0....GCC: (G
0000E050 4E 55 29 20 36 2E 33 2E 30 00 00 00 47 43 43 NU) 6.3.0....GCC
0000E060 3A 20 28 47 4E 55 29 20 36 2E 33 2E 30 00 00 00 : (GNU) 6.3.0...
0000E070 00 47 43 43 3A 20 28 47 4E 55 29 20 36 2E 33 2E .GCC: (GNU) 6.3.
0000E080 30 00 00 00 00 47 43 43 3A 20 28 47 4E 55 29 20 0....GCC: (GNU)
0000E090 36 2E 33 2E 30 00 00 00 47 43 43 3A 20 28 47 6.3.0....GCC: (G
0000E0A0 4E 55 29 20 36 2E 33 2E 30 00 00 00 47 43 43 NU) 6.3.0....GCC
0000E0B0 3A 20 28 47 4E 55 29 20 36 2E 33 2E 30 00 00 00 : (GNU) 6.3.0...
0000E0C0 00 47 43 43 3A 20 28 47 4E 55 29 20 36 2E 33 2E .GCC: (GNU) 6.3.
0000E0D0 30 00 00 00 00 47 43 43 3A 20 28 47 4E 55 29 20 0...GCC: (GNU)
0000E0E0 36 2E 33 2E 30 00 00 00 47 43 43 3A 20 28 47 6.3.0....GCC: (G
0000E0F0 4E 55 29 20 36 2E 33 2E 30 00 00 00 47 43 43 NU) 6.3.0....GCC
0000E100 3A 20 28 47 4E 55 29 20 36 2E 33 2E 30 00 00 00 : (GNU) 6.3.0...
0000E110 00 47 43 43 3A 20 28 47 4E 55 29 20 36 2E 33 2E .GCC: (GNU) 6.3.
0000E120 30 00 00 00 00 47 43 43 3A 20 28 47 4E 55 29 20 0....GCC: (GNU)
0000E130 36 2E 33 2E 30 00 00 00 00 47 43 43 3A 20 28 47 6.3.0....GCC: (G
0000E140 4E 55 29 20 36 2E 33 2E 30 00 00 00 47 43 43 NU) 6.3.0....GCC
0000E150 3A 20 28 47 4E 55 29 20 36 2E 33 2E 30 00 00 00 : (GNU) 6.3.0...
0000E160 00 47 43 43 3A 20 28 47 4E 55 29 20 36 2E 33 2E .GCC: (GNU) 6.3.
0000E170 30 00 00 00 00 47 43 43 3A 20 28 47 4E 55 29 20 0....GCC: (GNU)
0000E180 36 2E 33 2E 30 00 00 00 00 00 00 00 00 00 00 6.3.0.....
0000E190 00 01 00 00 08 82 00 00 D2 15 00 00 20 00 00 .....^,..ò... ..
0000E1A0 00 88 82 00 00 1E 16 00 00 20 00 00 00 00 00 .^.....
```

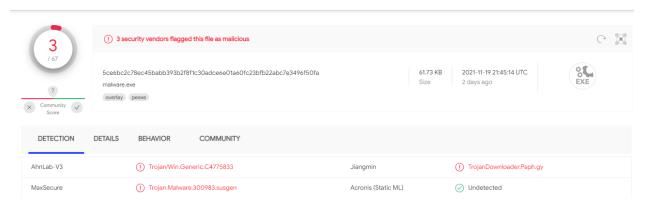
	_																
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	OF	Decoded text
0000FC70	01	47	4E	55	20	43	2B	2B	31	34	20	36	2E	33	2E	30	.GNU C++14 6.3.0
0000FC80	20	2D	6D	74	75	6E	65	3D	67	65	6E	65	72	69	63	20	-mtune=generic
0000FC90	2D	6D	61	72	63	68	3D	69	35	38	36	20	2D	67	20	2D	-march=i586 -g -
0000FCA0	66	65	78	63	65	70	74	69	6F	6E	73	00	04	43	ЗΑ	5C	fexceptionsC:\
0000FCB0	55	73	65	72	73	5C	4D	61	72	69	61	6E	5C	44	65	73	Users\Marian\Des
0000FCC0	6B	74	6F	70	5C	54	65	61	63	68	69	6E	67	20	53	53	ktop\Teaching SS
0000FCD0	49	5C	6D	61	6C	77	61	72	65	5C	77	6F	77	5C	6D	61	I\malware\wow\ma
0000FCE0	69	6E	2E	63	70	70	00	43	за	5C	55	73	65	72	73	5C	in.cpp.C:\Users\
0000FCF0	4D	61	72	69	61	6E	5C	44	65	73	6B	74	6F	70	5C	54	Marian\Desktop\T
0000FD00	65	61	63	68	69	6E	67	20	53	53	49	5C	6D	61	6C	77	eaching SSI\malw
0000FD10	61	72	65	5C	77	6F	77	00	60	14	40	00	41	02	00	00	are\wow.`.@.A
0000FD20	00	00	00	00	02	73	74	64	00	05	00	84	18	00	00	03	std"
0000FD30	5F	5F	63	78	78	31	31	00			04	08	DF	CA	00	00	cxx11ßßÊ
0000FD40	00	05	04	40	90	1D	00	00	05	04	8B	DB	1B	00	00	05	— @∢Û
0000FD50	04	8D	Α7	1D	00	00	05	04	8E	BF	1D	00	00	05	04	8F	§ž¿
0000FD60	DE	1D	00	00	05	04	90	07	1E	00	00	05	04	91	25	1E	Þ
0000FD70	00	00	05	04	92	49	1E	00	00	05		93	66	1E	00	00	'I"f
0000FD80	05	04	94	87	1E	00	00	05	04	95		1E	00	00	05	04	″‡•§
0000FD90	96	BF	1E	00	00			97			00			04	98	FF	-¿
0000FDA0	1E	00	00	05	04	99	28	1F	00	00	05	04	9A	48	1F	00	≝H
0000FDB0	00	05	04	9B	79		00	00	05	04		96			00	05	>yœ
0000FDC0	04	ΑO	В1	1F	00	00	05	04	A1	D1	1F	00	00	05	04	A2	. ±;Ñ¢
0000FDD0	FO	1F	00	00	05			16	20	00	00	05			3B		ð¤²;
0000FDE0	00					60			00				80				¬`®€
0000FDF0	05	04	ВО								C3	20	00		05		°Ÿ±Ã
0000FE00	В2	E1	20	00	00	05				20	00		05	04	В4	1E	²á';
0000FE10	21	00	00	05	04	В5	3C	21	00	00	05	04	В6	5B	21	00	!µ ¶[!.</td
0000FE20	00	05	04	В7	94	21	00	00	05	04	В8	AD	21	00	00	05	"!,.!
0000FE30	04	В9	D1	21	00	00	05	04	ва	F5	21	00	00	05	04	ВВ	.¹Ñ!°õ!»
0000FE40	19	22	00	00	05	04	вс	4A	22	00	00	05	04	BD	68	22	."¹₄J"³≤h"
0000FE50	00	00	05	04	BF	96	22	00	00	05	04	C1	BD	22	00	00	¿-"Á½"
0000FE60	05	04	C2	DB	22	00	00	05	04	C3	FE	22	00	00	05	04	ÂÛ"Ãþ"
0000FE70	C4	22	23	00	00	05	04	C5	46	23	00	00	05	04	C6	5E	Ä"#ÅF#Æ^
0000FE80	23	00	00	05	04	C7	82	23	00	00	05	04	C8	А6	23	00	#Ç,#Ȧ#.
0000FE90	00	05	04	C9	СВ	23	00	00	05	04	CA	EF	23	00	00	05	ÉË#Êï#
0000FEA0	04	СВ	0A	24	00	00	05	04	CC	24	24	00	00	05	04	CD	.Ë.şÌşşÍ
0000FEB0	42	24	00	00	05	04	CE	61	24	00	00	05	04	CF	80	24	B\$Îa\$Ï€\$
0000FEC0	00	00	05	04	D0	9E	24	00	00	06	04	08	01	C2	24	00	Đž\$Â\$.
0000FED0	00	06	04	09	01	FO	24	00	00	06	04	0A	01	14	25	00	ð\$%.
0000FEE0	00	06	04	18	01	96	22	00	00	06	04	1B	01	16	20	00	"
0000FEF0	00	06	04	1E	01	3B	20	00	00	06	04	21	01	80	20	00	;!.€ .
0000FF00	00	06	04	25	01	C2	24	00	00	06	04	26	01	F0	24	00	%.Â\$&.ð\$.
0000FF10	00	06	04	27	01	14	25	00	00	02	5F	5F	65	78	63	65	'% exce
0000FF20	70	74	69	6F	6E	5F	70	74	72	00	06	35	31	07	00	00	ption ptr51
0000FF30	07	87	00	00	00	04	06	4D	24	07	00	00	08	5F	4D	5F	.‡mş m
0000FF40	65	78	63	65	70	74	69	6F	6E	5F	6F	62	6A	65	63	74	exception object
0000FF50	00	06	4F	53	25	00	00	00	09	87	00	00	00	06	51	5F	OS%‡Q
0000FF60	5A	4E	53	74	31	35	5F	5F	65	78	63	65	70	74	69	6F	ZNSt15exceptio
0000FF70	6E	5F	70	74	72	31	33	65	78	63	65	70	74	69	6F	6E	n_ptrl3exception
0000FF80	5F	70	74	72	43	34	45	50	76	00	2D	03	00	00	38	03	_ptrC4EPv8.
0000FF90	00	00	0A	55	25	00	00	0B	53	25	00	00	00	0C	5F	4D	U%S%M
0000FFA0	5F	61	64	64	72	65	66	00	06	53	5F	5A	4E	53	74	31	_addrefS_ZNSt1
0000FFB0	35	5F	5F	65	78	63	65	70	74	69	6F	6E	5F	70	74	72	5exception_ptr
0000FFC0	31	33	65	78	63	65	70	74	69	6F	6E	5F	70	74	72	39	13exception_ptr9
0000FFD0	5F	4D	5F	61	64	64	72	65	66	45	76	00	7F	03	00	00	M_addrefEv

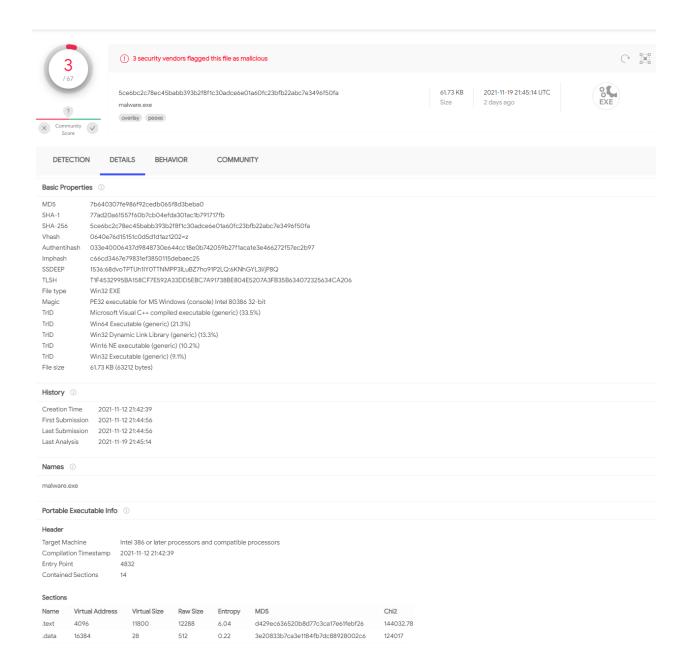
c) VirusTotal:





d)





- e) Fisierele din DLLs.zip sunt de folos deoarece acestea sunt importate in codul sursa al executabilului, iar fara aceste DLL-uri am primi eroare cand am incerca sa rulam executabilul.
- f) Imaginea contine un malware deoarece codul ascuns in interiorul acesteia sterge fisiere care ar putea fi importante pentru utilizator.

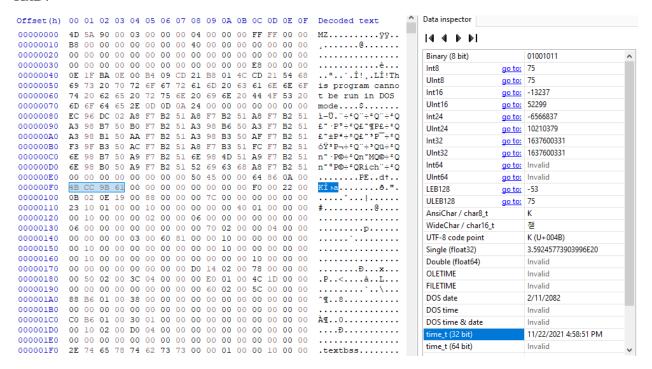
Exemplu de input pentru care se afiseaza mesajul "Parola introdusa este corecta!" este: "abcdef|abcdef".

Acest comportament se intampla deoarece suprascriem stiva din memorie, iar in loc de "fmiSSI", valorea lui *pass* ajunge sa fie "abcdef"

```
Introduceti parola: abcdef|abcdef
#include <iostream>
#include <string.h>
                                                          input:abcdef|abcdef
using namespace std;
                                                          pass:abcdef
int main()
                                                          Parola introdusa este corecta!
    char pass[7] = "fmiSSI";
                                                          Process returned 0 (0x0)
                                                                                       execution time : 5.620 s
    char input[7]:
                                                          Press any key to continue.
    int passLen = strlen(pass);
    cout << "Introduceti parola: ";</pre>
    cin >> input;
    cout << endl << "input:" << input << endl;</pre>
    cout << endl << "pass:" << pass << endl;
    cout << endl:
    if (strncmp(input,pass,passLen) == 0) {
        cout << "Parola introdusa este corecta! \n";
        cout<<"Ati introdus o parola gresita :(\n";</pre>
    return 0:
```

4.

HxD:



Pestudio:

