

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	0D	0E	0F	Decoded text
0000A7C0	01	E2	23	00	00	00	0A	10	1F	01	00	00	50	80	F8	08	.ã#.....Pëø.
0000A7D0	00	00	80	02	C4	47	00	00	00	14	20	3E	02	00	00	A0	..ë.ÄG....>...
0000A7E0	00	F1	11	00	00	05	88	8F	00	00	00	28	40	7C	04		.ñ.....^.....(ë .
0000A7F0	00	00	40	01	E2	23	00	00	00	0A	10	1F	01	00	00	50	..@.ã#.....P
0000A800	80	F8	08	00	00	80	02	C4	47	00	00	00	14	20	3E	02	ëø...ë.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	@ ...@.ã#.....
0000A830	00	00	50	80	F8	08	00	00	80	02	C4	47	00	00	00	14	..Pëø...ë.ÄG....
0000A840	20	3E	02	00	00	A0	00	F1	11	00	00	00	D9	7E	7E	FE	>... .ñ.....Û~p
0000A850	7F	59	C3	0C	F1	A0	53	CF	51	00	00	00	00	49	45	4E	.YÄ.ñ siQ....IEN
0000A860	44	AE	42	60	82	4D	5A	90	00	03	00	00	00	04	00	00	DøB`MZ.....
0000A870	00	FF	FF	00	00	B8	00	00	00	00	00	00	00	00	40	00	.yy.....@.
0000A880	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000A890	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000A8A0	00	80	00	00	00	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	.ë.....°.....í!
0000A8B0	4C	CD	21	54	68	69	73	20	70	72	6F	67	72	61	6D	20	Li!This program
0000A8C0	63	61	6E	6E	6F	74	20	62	65	20	72	75	6E	20	69	6E	cannot be run in
0000A8D0	20	44	4F	53	20	6D	6F	64	65	2E	0D	0D	0A	24	00	00	DOS mode....\$..
0000A8E0	00	00	00	00	50	45	00	00	4C	01	0E	00	CF	DF	8E	PE..L...IBZ
0000A8F0	61	00	BC	00	00	49	02	00	00	E0	00	07	01	0B	01	02	a.4..I...ä.....
0000A900	1C	00	30	00	00	00	4E	00	00	00	02	00	00	E0	12	00	..0...N.....ä..
0000A910	00	00	10	00	00	00	40	00	00	00	00	40	00	00	10	00ë.....ë....
0000A920	00	00	02	00	00	04	00	00	00	01	00	00	00	04	00	00
0000A930	00	00	00	00	00	00	60	01	00	00	04	00	00	0D	29	01`.....).
0000A940	00	03	00	00	00	00	20	00	00	10	00	00	00	00	10	
0000A950	00	00	10	00	00	00	00	00	00	10	00	00	00	00	00	00
0000A960	00	00	00	00	00	00	80	00	00	D8	07	00	00	00	00	00ë...@.....
0000A970	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000A980	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000A990	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000A9A0	00	00	00	00	00	04	A0	00	00	18	00	00	00	00	00	00
0000A9B0	00	00	00	00	00	00	00	00	00	00	00	00	00	88	81	00^..
0000A9C0	00	10	01	00	00	00	00	00	00	00	00	00	00	00	00	00
0000A9D0	00	00	00	00	00	00	00	00	00	00	00	00	00	2E	74	65te
0000A9E0	78	74	00	00	00	18	2E	00	00	00	10	00	00	00	30	00	xt.....0.
0000A9F0	00	00	04	00	00	00	00	00	00	00	00	00	00	00	00	00
0000AA00	00	60	00	50	60	2E	64	61	74	61	00	00	00	1C	00	00	..`P`.data.....
0000AA10	00	00	40	00	00	00	02	00	00	00	34	00	00	00	00	00	..@.....4.....
0000AA20	00	00	00	00	00	00	00	00	00	00	40	00	30	C0	2E	72@.0Ä.rd
0000AA30	61	74	61	00	00	48	03	00	00	00	50	00	00	00	04	00	ata..H....P....
0000AA40	00	00	36	00	00	00	00	00	00	00	00	00	00	00	00	00	..6.....
0000AA50	00	40	00	30	40	2F	34	00	00	00	00	00	00	50	0A	00	..@.0@/4.....P..
0000AA60	00	00	60	00	00	00	0C	00	00	00	3A	00	00	00	00	00	..`.....
0000AA70	00	00	00	00	00	00	00	00	00	40	00	30	40	2E	62	73@.0@.bs
0000AA80	73	00	00	00	00	74	00	00	00	00	70	00	00	00	00	00	s....t....p....
0000AA90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000AAA0	00	80	00	30	C0	2E	69	64	61	74	61	00	00	D8	07	00	..ë.0Ä.idata..@..
0000AAB0	00	00	80	00	00	00	08	00	00	00	46	00	00	00	00	00	..ë.....F....
0000AAC0	00	00	00	00	00	00	00	00	00	40	00	30	C0	2E	43	52@.0Ä.CR
0000AAD0	54	00	00	00	18	00	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	C0	2E	74	6C	73	00	00	00	00	20	00	00	..@.0Ä.tls....
0000AB00	00	00	A0	00	00	00	02	00	00	00	50	00	00	00	00	00P....
0000AB10	00	00	00	00	00	00	00	00	00	40	00	30	C0	2F	31	34@.0Ä/14
0000AB20	00	00	00	00	00	58	00	00	00	00	B0	00	00	00	02	00X....°.....

malware.png

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000DE40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DE50	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000DE60	00	00	00	00	00	6C	69	62	67	63	63	5F	73	5F	64	77libgcc_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:... VirtualQu
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	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	00	2E	00	67	6C	6F	62	2D	e %d.....glob-
0000DFD0	31	2E	30	2D	6D	69	6E	67	77	33	32	00	00	00	00	2E	1.0-mingw32.....
0000DFE0	00	00	00	00	00	80	20	00	00	47	43	43	3A	20	28	47GCC: (G
0000DFF0	4E	55	29	20	36	2E	33	2E	30	00	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	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	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	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	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	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	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	00	6.3.0.....
0000E190	00	01	00	00	00	88	82	00	00	D2	15	00	00	20	00	00^,...ö....
0000E1A0	00	88	82	00	00	1F	16	00	00	20	00	00	00	00	00	00	^.....

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	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	3A	5C	fexceptions..C:\
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	3A	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\
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	03std.....
0000FD30	5F	5F	63	78	78	31	31	00	08	DF	04	08	DF	CA	00	00	__cxx11..\$..\$Ê..
0000FD40	00	05	04	40	90	1D	00	00	05	04	8B	DB	1B	00	00	05	...@.....<Û....
0000FD50	04	8D	A7	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	B.....\$.....'\$.
0000FD70	00	00	05	04	92	49	1E	00	00	05	04	93	66	1E	00	00'I....."f...
0000FD80	05	04	94	87	1E	00	00	05	04	95	A7	1E	00	00	05	04	.."+.....*\$.....
0000FD90	96	BF	1E	00	00	05	04	97	D0	1E	00	00	05	04	98	FF	-¿.....-Ð....."ÿ
0000FDA0	1E	00	00	05	04	99	28	1F	00	00	05	04	9A	48	1F	00"(.....\$H..
0000FDB0	00	05	04	9B	79	1F	00	00	05	04	9C	96	1F	00	00	05	...>y.....œ-....
0000FDC0	04	A0	B1	1F	00	00	05	04	A1	D1	1F	00	00	05	04	A2	. ±.....;ñ.....c
0000FDD0	F0	1F	00	00	05	04	A4	16	20	00	00	05	04	AA	3B	20	ð......";
0000FDE0	00	00	05	04	AC	60	20	00	00	05	04	AE	80	20	00	00-`.....@€..
0000FDF0	05	04	B0	9F	20	00	00	05	04	B1	C3	20	00	00	05	04	..°ÿ.....±Ã....
0000FE00	B2	E1	20	00	00	05	04	B3	FF	20	00	00	05	04	B4	1E	“á....."ÿ.....'
0000FE10	21	00	00	05	04	B5	3C	21	00	00	05	04	B6	5B	21	00	!.....µ<!.....[!]
0000FE20	00	05	04	B7	94	21	00	00	05	04	B8	AD	21	00	00	05".....!.....!
0000FE30	04	B9	D1	21	00	00	05	04	BA	F5	21	00	00	05	04	BB	..Ñ!.....°ð!.....»
0000FE40	19	22	00	00	05	04	BC	4A	22	00	00	05	04	BD	68	22	."...."4J"...."sh"
0000FE50	00	00	05	04	BF	96	22	00	00	05	04	C1	BD	22	00	00¿-"....Ã½"....
0000FE60	05	04	C2	DB	22	00	00	05	04	C3	FE	22	00	00	05	04	..ÃÛ"....Ãþ"....
0000FE70	C4	22	23	00	00	05	04	C5	46	23	00	00	05	04	C6	5E	Ã"#....ÃF#....Ã^
0000FE80	23	00	00	05	04	C7	82	23	00	00	05	04	C8	A6	23	00	#....Ç.#....È!#.
0000FE90	00	05	04	C9	CB	23	00	00	05	04	CA	EF	23	00	00	05	...ÉE#....Êi#....
0000FEA0	04	CB	0A	24	00	00	05	04	CC	24	24	00	00	05	04	CD	..Ë.\$.....î\$\$....Í
0000FEB0	42	24	00	00	05	04	CE	61	24	00	00	05	04	CF	80	24	B\$.....îa\$....îes
0000FEC0	00	00	05	04	D0	9E	24	00	00	06	04	08	01	C2	24	00Đž\$.....Ã\$.
0000FED0	00	06	04	09	01	F0	24	00	00	06	04	0A	01	14	25	00ð\$.....\$.
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	...\$.Ã\$....&.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_ptr.5l...
0000FF30	07	87	00	00	00	04	06	4D	24	07	00	00	08	5F	4D	5F	.+.....M\$...._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	ZNSt15_exceptio
0000FF70	6E	5F	70	74	72	31	33	65	78	63	65	70	74	69	6F	6E	n_ptr13exceptio
0000FF80	5F	70	74	72	43	34	45	50	76	00	2D	03	00	00	38	03	ptrC4EPv.-...8.
0000FF90	00	00	0A	55	25	00	00	0B	53	25	00	00	00	0C	5F	4D	...U\$....\$...._M
0000FFA0	5F	61	64	64	72	65	66	00	06	53	5F	5A	4E	53	74	31	_addrf...S_ZNSt1
0000FFB0	35	5F	5F	65	78	63	65	70	74	69	6F	6E	5F	70	74	72	5__exception_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_addrfEv.....

c) VirusTotal:



0 / 56

Community Score

✓ No security vendors flagged this file as malicious


dbd3b32b7327855cd335f14becb7f155e8fa166bf440f856752d87b7a44fdda6

malware.png

png

103.83 KB
Size

2021-11-17 23:07:06 UTC
4 days ago



DETECTION	DETAILS	COMMUNITY
Ad-Aware	✓ Undetected	AhnLab-V3
ALYac	✓ Undetected	Antiy-AVL
Arcabit	✓ Undetected	Avast
Avira (no cloud)	✓ Undetected	Baidu
BitDefender	✓ Undetected	BitDefenderTheta
Bkav Pro	✓ Undetected	CAT-QuickHeal
ClamAV	✓ Undetected	CMC
Comodo	✓ Undetected	Cynet
Cyren	✓ Undetected	DrWeb
Emsisoft	✓ Undetected	eScan
ESET-NOD32	✓ Undetected	F-Secure
FireEye	✓ Undetected	Fortinet
GData	✓ Undetected	Gridinsoft
Ikarus	✓ Undetected	Jiangmin
K7AntiVirus	✓ Undetected	K7GW
Kaspersky	✓ Undetected	Kingsoft
Lionic	✓ Undetected	Malwarebytes
MAX	✓ Undetected	MaxSecure
McAfee	✓ Undetected	McAfee-GW-Edition
Microsoft	✓ Undetected	NANO-Antivirus
Panda	✓ Undetected	Rising
Sangfor Engine Zero	✓ Undetected	Sophos

0

/ 56

?

Community Score

✓ No security vendors flagged this file as malicious

dbd3b32b7327855cd335f14becb7f155e8fa166bf440f856752d87b7a44fdda6

malware.png

png

103.83 KB

Size

2021-11-17 23:07:06 UTC

4 days ago

PNG

DETECTION

DETAILS

COMMUNITY

Basic Properties ⓘ

MD5

d322f42651cbd15190cff2854e449413

SHA-1

99c0388c13883c50ad01bb28db943b9b7ed4b039

SHA-256

dbd3b32b7327855cd335f14becb7f155e8fa166bf440f856752d87b7a44fdda6

SSDEEP

1536:kkUOEQC:Gi32wnlaOyDh7Bjaibgl/QGApVaxOPeDnalcJBhjNYLCHh9IHA7WtK1z7W:rTQlkBhL6uGzismnkkKNhGYL3l/P8Q

TLSH

T13DA38DA4FA568CF7DACA533DC4E7C7AC0728BE814E5147A3EB39B03C06A3B553586146

File type

PNG

Magic

PNG image, 874 x 1292, 8-bit/color RGB, non-interlaced

TrID

PNG Stereo bitmap (57.8%)

TrID

Portable Network Graphics (42.1%)

File size

103.83 KB (106321 bytes)

History ⓘ

First Submission

2021-11-12 21:45:03

Last Submission

2021-11-12 21:45:03

Last Analysis

2021-11-17 23:07:06

Names ⓘ

malware.png

d)

3

/ 67

?

Community Score

① 3 security vendors flagged this file as malicious

5ce6bc2c78ec45babbb393b2f8f1c30adce6e01a60fc23bfb22abc7e3496f50fa

malware.exe

overlay peexe

61.73 KB

Size

2021-11-19 21:45:14 UTC

2 days ago

EXE

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

AhnLab-V3

① Trojan.Win.Generic.C4775833

Jiangmin

① TrojanDownloader.Paph.gy

MaxSecure

① Trojan.Malware.300983.susgen

Acronis (Static ML)

✓ Undetected

3

167

?

Community Score

3 security vendors flagged this file as malicious

5ce6bc2c78ec45babb393b2f8f1c30adce6e01a60fc23bfb22abc7e3496f50fa

malware.exe

overlay peexe

61.73 KB

Size

2021-11-19 21:45:14 UTC

2 days ago

EXE

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Basic Properties

MD5	7b640307fe986f92cedb065f8d3beba0
SHA-1	77ad20a61557f60b7cb04efda301act1b791717fb
SHA-256	5ce6bc2c78ec45babb393b2f8f1c30adce6e01a60fc23bfb22abc7e3496f50fa
Vhash	0640e76d15151c0d5d1d1az1202=z
Authentihash	033e40006437d9848730e644cc18e0b742059b27f1acale3e466272f57ec2b97
Imphash	c66cd3467e79831ef3850115debaec25
SSDEEP	1536:68dvoTPTUh1YOTNMPP3ILuBZ7ho91P2LQ:6KNhGYL3J/jP8Q
TLSH	T1F4532995BA158CF7E592A33DD5EBC7A91738BE804E5207A3FB35B634072325634CA206
File type	Win32 EXE
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
TrID	Microsoft Visual C++ compiled executable (generic) (33.5%)
TrID	Win64 Executable (generic) (21.3%)
TrID	Win32 Dynamic Link Library (generic) (13.3%)
TrID	Win16 NE executable (generic) (10.2%)
TrID	Win32 Executable (generic) (9.1%)
File size	61.73 KB (63212 bytes)

History

Creation Time	2021-11-12 21:42:39
First Submission	2021-11-12 21:44:56
Last Submission	2021-11-12 21:44:56
Last Analysis	2021-11-19 21:45:14

Names

malware.exe

Portable Executable Info

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2021-11-12 21:42:39
Entry Point	4832
Contained Sections	14

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	11800	12288	6.04	d429ec636520b8d77c3ca17e61feb726	144032.78
.data	16384	28	512	0.22	3e20833b7ca3e1184fb7dc88928002c6	124017

e) Fişierele din DLLs.zip sunt de folos deoarece acestea sunt importate în codul sursă al executabilului, iar fără aceste DLL-uri am primi eroare când am încerca să rulăm executabilul.

f) Imaginea conţine un malware deoarece codul ascuns în interiorul acesteia şterge fişiere care ar putea fi importante pentru utilizator.

2.

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", valoarea lui *pass* ajunge sa fie "abcdef"

```
#include <iostream>
#include <string.h>

using namespace std;

int main()
{
    char pass[7] = "fmiSSI";
    char input[7];
    int passLen = strlen(pass);
    cout << "Introduceti parola: ";
    cin >> input;
    cout << endl << "input:" << input << endl;
    cout << endl << "pass:" << pass << endl;
    cout << endl;
    if (strcmp(input,pass,passLen) == 0) {
        cout<<"Parola introdusa este corecta!\n";
    } else {
        cout<<"Ati introdus o parola gresita :(\n";
    }
    return 0;
}
```

Introduceti parola: abcdef|abcdef

input:abcdef|abcdef

pass:abcdef

Parola introdusa este corecta!

Process returned 0 (0x0) execution time : 5.620 s

Press any key to continue.

4.

HxD:

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E8	00	00	00è....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°...!...Li!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$......
00000080	EC	96	DC	02	A8	F7	B2	51	A8	F7	B2	51	A8	F7	B2	51	l-Ü.."+Q"+Q"+Q
00000090	A3	98	B7	50	B0	F7	B2	51	A3	98	B6	50	A3	F7	B2	51	£~·P°+Q£~QPE+Q
000000A0	A3	98	B1	50	AA	F7	B2	51	A3	98	B3	50	AF	F7	B2	51	£~±P°+Q£~°P~+Q
000000B0	F3	9F	B3	50	AC	F7	B2	51	A8	F7	B3	51	FC	F7	B2	51	ôÿ°P~+Q~+Qü+Q
000000C0	6E	98	B7	50	A9	F7	B2	51	6E	98	4D	51	A9	F7	B2	51	n~·P@+Qn~MQ@+Q
000000D0	6E	98	B0	50	A9	F7	B2	51	52	69	63	68	A8	F7	B2	51	n~°P@+QRich~+Q
000000E0	00	00	00	00	00	00	00	00	50	45	00	00	64	86	0A	00PE...dt..
000000F0	4B	CC	9B	61	00	00	00	00	00	00	00	00	F0	00	22	00	KI>a.....8.."
00000100	0B	02	0E	19	00	88	00	00	00	7C	00	00	00	00	00	00^...
00000110	23	10	01	00	00	10	00	00	00	00	00	40	01	00	00	00	#.....@.....
00000120	00	10	00	00	00	02	00	00	06	00	00	00	00	00	00	00
00000130	06	00	00	00	00	00	00	00	00	70	02	00	00	04	00	00p.....
00000140	00	00	00	00	03	00	60	81	00	00	10	00	00	00	00	00`.....
00000150	00	10	00	00	00	00	00	00	00	00	10	00	00	00	00	00
00000160	00	10	00	00	00	00	00	00	00	00	00	10	00	00	00	00
00000170	00	00	00	00	00	00	00	00	D0	14	02	00	78	00	00	00ð...x...
00000180	00	50	02	00	3C	04	00	00	E0	01	00	4C	1D	00	00	00	..P.<...ä...L...
00000190	00	00	00	00	00	00	00	00	60	02	00	5C	00	00	00	00~...\\...
000001A0	88	B6	01	00	38	00	00	00	00	00	00	00	00	00	00	00	~g...8.....
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	C0	B6	01	00	30	01	00	00	00	00	00	00	00	00	00	00	Äg...0.....
000001D0	00	10	02	00	D0	04	00	00	00	00	00	00	00	00	00	00ð.....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	2E	74	65	78	74	62	73	73	00	00	01	00	00	10	00	00	..textbss.....

Data inspector

Binary (8 bit)	01001011
Int8	go to: 75
UInt8	go to: 75
Int16	go to: -13237
UInt16	go to: 52299
Int24	go to: -6566837
UInt24	go to: 10210379
Int32	go to: 1637600331
UInt32	go to: 1637600331
Int64	go to: Invalid
UInt64	go to: Invalid
LEB128	go to: -53
ULEB128	go to: 75
AnsiChar / char8_t	K
WideChar / char16_t	첼
UTF-8 code point	K (U+004B)
Single (float32)	3.59245773903996E20
Double (float64)	Invalid
OLETIME	Invalid
FILETIME	Invalid
DOS date	2/11/2082
DOS time	Invalid
DOS time & date	Invalid
time_t (32 bit)	11/22/2021 4:58:51 PM
time_t (64 bit)	Invalid

Pestudio:

d:\theo\info\fmi-labs\an 3 sem 1\securitatea sist	
indicators (38)	
virustotal (warning)	
> dos-header (64 bytes)	
dos-stub (168 bytes)	
> rich-header (9)	
> file-header (Nov.2021)	
> optional-header (console)	
directories (7)	
> sections (entry-point)	
libraries (5) *	
functions (84) *	
exports (n/a)	
tls-callbacks (n/a)	
.NET (n/a)	
resources (manifest) *	
abc strings (495)	
debug (Nov.2021)	
manifest (aslnvoker)	
version (n/a)	
certificate (n/a)	
overlay (n/a)	

property	value
md5	B908A14802A54F472B6ADCF30E018527
sha1	0ACA62FEC862028A566CA4237AF2DB56990B3835
sha256	9777A5CA59590DFDE6DD9B8E7A0926048EEB4BF37AA9575EF8AD148E0F7EF839
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00
first-bytes-text	M Z@
file-size	65536 (bytes)
entropy	3.702
imphash	23A885BB5C3FB9F399FD8E7150E0BFA4
signature	Microsoft Visual C++ 8.0 Debug
entry-point	E9 58 1C 00 00 E9 43 3B 00 00 E9 EE 10 00 00 E9 E9 11 00 00 E9 55 13 00 00 E9 6F 24 00 00 E9 00 4F
file-version	n/a
description	n/a
file-type	executable
cpu	64-bit
subsystem	console
compiler-stamp	0x619BCC4B (Mon Nov 22 18:58:51 2021)
debugger-stamp	0x619BCC4B (Mon Nov 22 18:58:51 2021)
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a