Novel Technique to Hide Identity of Alina Malware

Dhruv R. Gajjar

Abstract: Laptop infection's purpose billions of bucks of monetary each year. As to speak approximately this in current year is to make attention in humans approximately ongoing fraud approximately laptop malware and to save you them approximately it. Almost current assaults are finished the use of encrypted laptop malware form. Which maximum tough as it makes undetectable malware to be scanned through antivirus. Even it bypasses the firewalls after which does its effect on laptop or a laptop community system.

1. Introduction

1.1 What is Encryption?

In cryptography, encryption is the way toward encoding data. This cycle changes Over the primary portrayal of the data, known as plaintext, into an elective structure known as cipher text. In a perfect world, just approved gatherings can unravel a code textual content returned to plaintext and get to the first data. Encryption doesn't itself forestall impedance however denies a future interceptor's crystalline element.

For unique reasons, an encryption contrives normally makes use of a pseudo - sporadic encryption key made with the aid of using an estimation. It is doable to unscramble the message while not having the important thing but, for an all - round deliberate encryption conspire, massive computational property and competencies are required. An accredited beneficiary can absolutely unscramble the message with the important thing given with the aid of using the originator to beneficiaries but now no longer to unapproved clients.

1.2 What is Malware?

A laptop infection is any such laptop application that, while executed, copies itself through converting different laptop packages and embeddings its very own code. If this replication succeeds, the affected regions are then predicted to be "corrupted" with a laptop disease.

1.3 What is Alina malware?

Alina is a Point of Sales Malware or POS RAM Scraper this is utilized by cybercriminals to scrape credit card and debit card statistics from the factor of sale system. It first commenced to scrape statistics in past due 2012. It resembles JackPOS Malware.

1.4 How does Alina malware works?

Once executed, it receives set up at the user's laptop and assessments for updates. If an update is found, it removes the present Alina code and installs the trendy version. Then, for brand spanking new installations, it provides the report direction to an AutoStart run key to preserve persistence. Finally, it provides java. exe to the %APPDATA% listing and executes it the usage of the parameter alina=<path_to_executable> for new installations or, update=<orig_exe>; <new_exe> for upgrades.

Alina inspects the user's techniques with the assist of Windows API calls:

Create Tool help 32 Snapshot () takes an image of all walking techniques

Process32First () /Process32Next () retrieve the track 1 and track 2 records withinside the technique reminiscence

Alina continues a blacklist of techniques, if there's no technique records withinside the blacklist it makes use of OpenProcess () to study and technique the contents withinside the reminiscence dump. Once the information is scraped Alina sends it to C&C servers the usage of an HTTP POST command this is hardcoded in binary.

1.5 What is Encrypting Malware?

A scrambled contamination is a laptop contamination that encodes its payload with the aim of creating spotting the contamination greater troublesome. In any case, due to the fact something encoded desires a decryptor or a key an antivirus can make use of the decryptor because the method for discovery.

1.6 How does encrypting malware works?

Malware writers make use of a collection of bodily and digital intends to unfold malware that contaminate devices and organizations. For instance, vindictive tasks may be conveyed to a framework with a USB power or can unfold over the net via power - through downloads, which certainly malevolent tasks to frameworks without the client's endorsement or records. Phishing assaults are some other normal types of malware conveyance wherein messages masked as right messages includes pernicious connections or connections that can deliver the malware executable to clueless customers. Modern malware attacks often spotlight the usage of an order and - manipulate employee that lets in threat entertainers to talk with the contaminated frameworks, exfiltrate sensitive records or even distantly manipulate the undermined device or employee.

Arising traces of malware contain new avoidance and obscurity strategies which can be supposed to trick customers in addition to protection administrators and adverse to malware gadgets too. An element of those avoidance strategies relies upon simple strategies, for example, making use of net intermediaries to shroud malignant site visitors or supply IP addresses. More delicate risks contain polymorphic malware, which could again and again extrude its simple code to circumvent region instruments, adverse to sandbox strategies, which allow the malware to differentiate whilst it's miles being dissected and defer execution till after it leaves the sandbox, and report much less malware, which lives simply withinside the framework's RAM to strive now no longer to be found.

2. How to get prevented from malware?

Utilize a firewall to avoid all coming near institutions from the net to administrations that ought now no longer to be overtly accessible. As a count of course, strive now no longer to disclaim each unmarried coming near affiliation and simply allow administrations you expressly want to provide to the relaxation of the world.

Authorize a mystery key approach. Complex passwords make it difficult to interrupt mystery phrase facts on undermined LAPTOPs. This assists with forestalling or breaking factor damage whilst a LAPTOP is undermined.

Guarantee that tasks and customers of the LAPTOP make use of the maximum minimum diploma of blessings crucial to complete an errand. When incited for a root or UAC mystery phrase, assure that this system inquiring for organisation stage get admission to is a proper application.

Cripple AutoPlay to stop the programmed dispatching of executable facts on organisation and detachable drivers whilst now no longer wished. On the off hazard that compose get admission to is not wished, empower read simply mode is the opportunity is accessible.

Mood killer document sharing if now no longer required. On the off hazard that document sharing is required, use ACLs and mystery phrase coverage to limitation get admission to. Incapacitate mysterious admittance to shared organizers. Award get admission to simply to patron debts with strong passwords to envelopes that have to be shared.

Mood killer and put off superfluous administrations. Naturally, many running frameworks introduce assistant administrations that aren't basic. These administrations are roads of assault. On the off hazard that they may be taken out, risks have much less roads of assault.

In the occasion that a chance abuses at the least one organisation benefits, impair, or block admittance to, the ones administrations till a repair is applied.

Continuously live up with the latest, specifically on LAPTOPs which have public administrations and are to be had via the firewall, for example, HTTP, FTP, mail, and DNS administrations.

Arrange your e - mail employee to hinder or put off e - mail that includes record connections which might be usually used to unfold risks, for example, vbs, bat, exe, pif and. scr facts.

Seclude bargained LAPTOPs hastily to preserve risks from spreading further. Play out a systematic research and re - set up the LAPTOPs utilising relied on media.

Train representatives now no longer to open connections besides if they may be waiting for them. Likewise, do not execute programming this is downloaded from Internet besides if it's been tested for bargained Website can reason ailment if sure software weaknesses aren't fixed.

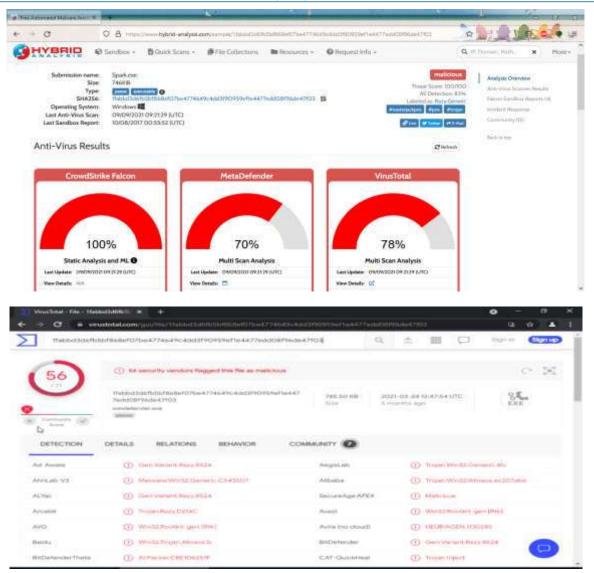
On the off hazard that Bluetooth is not wished for mobile caller phones, it must be killed. On the off hazard which you require its utilization, assure that the machine's perceivability is about to "Covered up" so it cannot be tested with the aid of using different Bluetooth devices. In the occasion that machine mixing has to be utilized, assure that each one device set to "Unapproved", requiring acclaim for each affiliation demand. Try now no longer to well - known programs which might be unsigned or despatched from difficult to understand sources.

Author name (s) and affiliation (s)

Dhruv Gajjar is a researcher in field of cyber security and cyber forensics. My google scholar link is: https: //scholar. google. com/citations?user=e - 2HIBYAAAAJ&hl=en. **Simulation**

Software's: https://github. com/ytisf/theZoo/tree/master/malware/Source/Original: -Alina Malware

Websites: https://www.virustotal.com: - Virus Total



Analysis Report of Original File of Hybrid Sandbox

and indication (SP)	encoding (2)	size (hytes)	file-offset	Interactions (49)	Print (283)	groving (19)	
	ancii	10	al-book-outers			windowing	
#3 vountular (36/71)	#1CH	11	8=10083209			synchronization	
	8101	9	0-000011111			synchronization	
- ich-hasder (9)	#8234	25	8-10081373			synchronication	
 file-beader (May 2014) 	ward	20	S-00081084			synchronization	
eptional-header (GUN)	494.04	20	Gw0006354.1			synchronization	
- m directories (f0	(0.0.0.0)	23	0x00081084			aynchronization	
- P sanfrorm (file)	00010	20	0+000811111			synchronization	
Alleranian (count)	01010	20	6400061778			synchronization	
and a service and a second sec	atcil	27	0+0001106			synchronization	
	ascil	19	0x000011764			synchronication	
- B annapitions (nd.s)	@82.04	37	0-000818018			synchronization	
	00001	25	D=00003A43			synchronization	
- D retocations (9706)	Mació .	10	4140000.11140			annvices.	
- in recourses (manifest) *	41114	14	0+000813-40			647/1046	
ate storage (4392)	8601	33	0400403568	. A.		services	
ZD debug (path)	micii	.13	0+000615010	X		107-1002	
- Jai manifest (astronker)	witti	3.2	Ex0008(1997).			INFVIENC	
	auti	11	Rentroperation 1			SPIVICES.	
	ancii	12	Dw000001002			services	
-T2 meeting (a) all	80(3)	24	0x0000.1563			security	
	apcil	20	SA000813578			telounity.	
	86616	7	(HONORI MP)			security	
	#101F	12	DHOODAUCAR			registry	
	ascil	15	DHOUA3CC1			registry	
	ascii	11	6x000A3CD5			registry	
	#9-CH	11	Gar000873508			registry	
	ascii	14	0.000083512			registry	
	-maziii	12	1 De1000811522			registry	
	4663	15	0=00083525			registry	
	031211	13	0+00001547			registry	
						100 M (100 M (10	

Volume 10 Issue 9, September 2021

<u>www.ijsr.net</u>

Licensed Under Creative Commons Attribution CC BY

DOI: 10.21275/SR21924073123

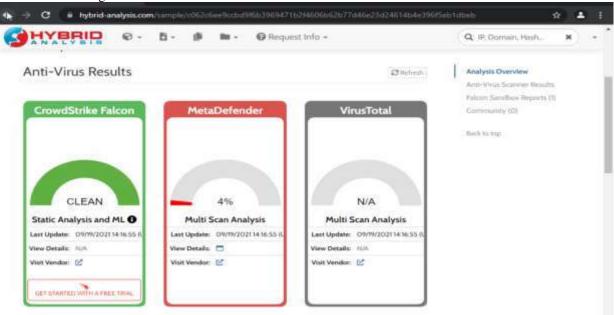
String used in original file to call functions

Address Disassembly	Text string
77D08D31 PUSH ntd11.77C86C70	ASCII "Locating procedure, "Xs" by name
77088038 PUSH ntd11.77C86C94	ASCII "LdrpGetProcedureAddress"
77088042 PUSH ntd11.77C86C54	ASCII "minkernel\ntdll\ldrsnap.c"
77008055 PUSH ntd11.77C86CRC	ASCII "Loading procedure 8xSix by ordinal"
7700805C PUSH ntd11.77C86C94	RSCI1 "Ldrp6etProcedureAddress"
77D88D66 PUSH ntd11.77C86C54	ASCII "minkernel\ntdll\ldrsnap.c"
77D08D8E PUSH ntd11.77C86CD0	ASCII "Procedure "Xs" could not be located in DLL at base 0xXp.
77D08D95 PUSH ntd11,77C86D0C	ASCII "LdrpMameToOrdinal"
77D88D9F PUSH ntd11.77C86C54	ASCII "minkernel\ntdll\ldrsnap.c"
7700955F PUSH ntd11.77C86870	ASCII "Found circular dependent DLL: "Xw2" that failed to load previously
77009566 PUSH ntd11.77C868C8	ASCII "LdrpFindOrPrepareLoadingModule"
77009570 PUSH ntd11.77C86850	ASCII "winkernel\ntdll\ldrwap.c"
770096F7 PUSH ntd11.77C91838	UNICODE "COMPLUS_Version"
7700977C PUSH ntd11.77C922F0	ASCII "Building shim engine DLL system32 filename failed with status 0x30
77009783 PUSH ntd11.77C92338	ASCII "LdrpInitShimEngine"
77009790 PUSH ntd11.77C92384	ASCII "Getting the shim engine exports failed with status 0xX081x0"
77D09796 PUSH ntd11.77C92338	ASCII "LdrpInitShimEngine"
77009700 PUSH ntd11.77C92044	ASCII "minkernel\ntdll\ldrinit.c"
77009789 PUSH ntd11.77C9234C	ASCII "Loading the shim engine DLL failed with status 0xX081x0"
770097BF PUSH ntd11.77C92338	ASCII "LdrpInitShimEngine"
770897C9 PUSH ntd11.77C92844	ASCII "minkernel\ntdll\ldrinit.c"
77009843 PUSH ntd11.77C92200	ASCII "Loading the shim DLL "Xw2" failed with status 0xX081x0"
77009848 PUSH ntd11.77C92238	ASCII "LdroLoadShinEngine"
77D89854 PUSH ntd11.77C92844	ASCII "minkernel\ntdll\ldrinit.c"
77089885 PUSH ntd11.77C9224C	ASCII "Initializing the shim DLL "Xw2" failed with status 0xX081x
77D09888 PUSH ntd11.77C92238	ASCII "LdrpLoadShinEngine"
77089895 PUSH ntd11_77C92844	ASCII "minkernel\ntdll\ldrinit.c"
77D098F7 PUSH ntd11.77C92288	ASCII "Initializing a shim dependency "Xw2" failed with status 0xX081s
770098FE PUSH ntd11.77C922CC	ASCII "LdrpInitializeShimOllDependencies"
77089988 PUSH ntd11,77C92844	ASCII "minkernel\ntdll\ldrinit.c"
77089942 PUSH ntd11.77C9218C	ASCII "Could not locate procedure "Xs" in the ship engine BLL
77089948 PUSH ntd11_77C921E4	ASCII "Ldrp6etShimEngineInterface"
77080059 0000 .1411 77009077	OSCII "minkagenellatellildeinit e"

System calls functions by original file

Boark exa	pFile	2.7.11						Flav	Date								Value	
MAGE DOS HEADER	000834120	00	00	00	00 0	0.0	00	00	00	00	00	00	00	00	00	00		
MS-DOS Stub Program	000634130	00	00	00	00 0	0.0	00	00	00	00	00	00	00	00	00	00		
BAAGE NT HEADERS	000634140	00	00	00	00 0	0.0	00	00	00	00	00	00	00	00	00	00		
MAGE SECTION DEAD	000694160	00	00	00	00 0	0.0	00 0	00	00	00	00	00	60	00	00	00		
MAGE SECTION HEAD	000834160	00	00	00	00 0	5.00	00	00	00	00	00	00	00	00	00	00		
MAGE BECTION HEAD	000054370	- 10	10	10	61.) fi	5 2	7.0	6.6	17	10	6.9	-	1.1	363	20	- 11	- Family and a constant of the	1
MAGE SECTION HEAD	000634180	26	30	27	20.6	5. 64	1.63	. 6F	64	69	68	67	30	27	6.6	54	0' secoling='UT	
-IMAGE SECTION HEAD	000694190	46	20	36	27 2	0.7.	1 74	61	-6E	64	61	6C	6E	6.62	6.5	3D	F-8' standalone=	
IMAGE_SECTION_HEAD	0.000EH41A0	27	79	66	73.2	7:34	31	00	OA.	30	61	73	73	66	6D	62	yes 7>. Hassents	
- MAGE_BECTION_HEAD	00004100	60	79	20	78 6	0 66	1 4 E	73	30	27	76	72	640	34	73	63	iy xmina="urn ac	
BECTION text	00084100	60	65	6D -	61 7	3 21	60	69	62	72	447	73	GE.	-646	74	20	hemaa microsoft -	
III SECTION rdata	00004100	63	67	6D :	3A 6	1 7	60	201	76	31	27	20	6D	61	683	69	com asm, v1' man i	
BECTION data	000B41E0	-66	46	73	74.6	6 61	1.72	77	69	GP'	485	30	27	31	26	30	featVersion= 1 B	
III BECTION Idata	0008541F0	27	385	00	0A 2	0 2	30	74	72	75	73	74	49	482	66	417	's «trustinfo	
# SECTION rec	00064200				6C 6			22	-76	72	-682	3A	73	63	68	65	xmins="urn sche	
in BECTION refee	000654210				20.6			72	- 147	73	6P	66		20			mas-microssft-co	
CONTRACTOR OF A	000654220				73.6			33			00						m sam v3">	
	00064230		23		63-7	$6, T_1$		74			005			50		20	~*************************************	
	00064240	1000			72.4	5 T		- 65		74					69		<**###################################	
	00064250			66	6Z 6	5 T.	36			20	20	20	50	20	20	-20	114345>	
	000694260		30	72	65.7	1.7		72	74	1000	-64	45	78	-66	63	76	《下会销销的演览 电接图共振电路	
	000694270		69	6F (6E.4	0.6		46		20	4C	65	76	46	80	-3D	tionLevel level=	
	000694280		6.1	73.	49.0	E. 71			-05	72	27	50	75	-99	41	1.1.2.	asinvoker' uIAc	
	00064290	1.00	-65	73	73.3	0,8		61	60	73	65	27	20	28		0D	cess, twise, '>	
	000E42A0			20	50.5			30	244	72	6.5	3.4	70	65	13		<td></td>	
	00084280				72.0			00		67	0.5	73	1.11				edPrivileges>	
	00084200		20	20	3C 3	1.2		63		72	69	74	79	381			necusity	
	00084208	20	50	3C :	28-7	4 77		73	74	49	-682	66	447	361	1.1.1	0A	witrustinfor	
	000B42E0	30	24	61	73 7	3 60		62	60	79	36	00	0A	00	100	00	/ as a sembliy>	
	000842F0	00	00	00	00 0	0.0		00	00	00	00	00	00	00	00			
	000654300	00	00	00	00 0	0.00		00	-		00	00	00	00	00	0.2		
	00064310	00	00	00	00 0	0.00		00	00			00	00	00	00	00		
	00004320	00	00	00	00 0	0 00		00		00		00	00	00	00			
P	00064330	00	00	00	00 0	0.00	00	00	00	00	0.0	00	00	00	00	00		

Got xml code of original file



Volume 10 Issue 9, September 2021

<u>www.ijsr.net</u>

Licensed Under Creative Commons Attribution CC BY

DOI: 10.21275/SR21924073123

Analysis Report after changes of Hybrid Sandbox

Views Toolal - File - 475	7409640% × +			• - •
-> C	nustofial.com/gov/file/24/17.df1%sc/6215aud0a.db/df12412/s22.dpa462.d	09433aa744676ce68c+	a503237640K	G (A) 🛋
4137/0179000	25ed8adbb07412c7)(5aec7d89d33ae7a487bccc66c10592237b	50f Q.	A 18 (C)	
43	43 security vendors flagged this file as maticious			C 36
0 - Contraction (10)	47374799ccn35ec88n480507412c270aaaA3899433aa7a482bc caalacta6922237a103 Spark atto 2986		zi on to grida zi unc normali aga	晋 王 72
DETECTION	DETAILS COMMUNITY			
Administration VA	() Matamaria West (arrange) constants	ALVIE	(D), George Vallant He	ary Altan
Army Avr.	(2) Trepus Genner: ASMetal9.85127C	Arcabit	(E) Trisier Beer Co	1045
Presently.	(3) Westantooden gewinnet	AVO	CD Write Problem	time (front)
Avios (no violad)	 Antonoscian concerne 	Baidu	D Werth Trouve A	front li
BitDeferschei	GerschriemBary #824	BitDefenderThate	() APPecker CBE	Da2D#
	Westinger Aster 8	Cottocko	D Maharender 24	continentworking (
ClamAV	CONTRACTOR AND A CONTRACT			

By Changing extension method

ViewsTintat - File - Allo	1ee325ar1) × +			• - ø
-> C	ustotal.com/gin/file/1661100225ci17708c6an6c0569025906a183	h#54c8-31054ab3367d64	6160e492a4	U 🕸 🚢
3fbf1ee325d	7708csde0c05b925905a183d94c8c3094ab1367db161s0e49	746 Q,	1 II	Says in Son up
42	() 42 security vendors flagged this file as malicious			e 23
0	3/httliwe225dt970/lice.detGc05h925905e183d94ctlic3094abit 36/httli64506492ab Sciences unese use		n oe w m na ozat uto caleert ego	0 Exe
DETECTION	DETAILS BEHAVIOR COMMUNITY			
Act Aware	Gen Triper Head #H triGhtsDPCorps	ALVec	() Gen Troum Em	of RP And Photo Photopa
SecureAge APEX	() Maticipa	Arcabit	Troper remaining RP	enG-fleOPDarps
Avant.	D Actual mounts that have	AVG	O Westamoth	genn (Rith)
Avita (no citou(i)	() TRABODERINAN	Thereiter	(1) wiegz.hupesie	Resource
BitDetoistor .	Genv Teppin General REFerreGROBE Cargol	BillDefenderTrista	() Athenas and	and the
Blav Pro	W32 Albotest manuarity	CharnAV	(). Whit Traper Alex	

By Packing method

	asterazzi e 🗇				• -	•
-> C = + ++	natota&com/gen/his/v/lia/is te (103790e) frz 1004b/be45007210	14657#7e70216ee64	dliafa2n9c539	810	G	10 A
cf0s3bte183	29be1f931804b3e450e2219fde52e7c1021ecee448afe2bdc53	ia(a. ±		sign is	(Sign up
27	(1) 27 security vendors flagged this file as malicidus					~ 14
Company (S)	crt2m3b/h18279baft#38804b3a45067719fdA57a7c10216cm 6448afs20dc5381 Spark.exe Softant counter serves	693.00 KB Siles	2021-09-161 7 hours ego	0.3130 U/IC	ext Ext	E)
DETECTION	DETAILS COMMUNITY					
Constanting of		ALYac.	٢	Gen Variers.MI	logy, 117135.	
let Aware		ALVac. SecureAge APEX	105	Cerry Martern Mit	May, 117135	
kd Aware Antiy AVL	Cleri Marced Milesy 19705		Ð			
Act Aware Antiy AVL Antiable	Cherri Vanweit Milwy 17115 Trajan Germena: ASMalweit 80127C.	SecureAge APEX	0	Melecious	e andi	
DETECTION Ad Avante Array AVL Avaable Avaable Clam,AV	Carri Variaret Milang (1713) Trajan Germeta: ASMalast: 00127C. Trajan Milang DIC 770	SecureAge APEX Avail	0	Małąckow Wiejsz Afrence (15 (Try) Reg, 117125	
Act Aveans Activy AVL Aveatulk	Open Variant, Milesy 17715 Traper-General: ASAMatu: 201727C Traper-General: ASAMatu: 201727C Traper-Milesy DSCV70 Winkiz Advance, C 17(1)	SecureAge APEX Avast BitDefender	000000000000000000000000000000000000000	Malisisus Wis32 Almass GentVation Mi	67 (TOJ) Reg 177 175 JL 48902	0

Volume 10 Issue 9, September 2021

www.ijsr.net

Licensed Under Creative Commons Attribution CC BY

DOI: 10.21275/SR21924073123

By Splitting and Joining method

City Westmanned	6046926740967419444444460078641004106410410979404739794044129731992	suel CL	t 181 (C)	Bilden an Calpin Lap
4	() A secondly version fragged the file as mellower			C* 245
	116799/konstreClass92,7409674154al/collass29bas300-tBa979 404752929400ba0 Reaction adva 09880	1444.19 HB2021-0 35560 7 filmark	9-16-12:36-48-07% -ages	1972 -
DETECTION	DETALS COMMUNITY			
C	C Hand Californi Party Information	SandinalCree (Statis ML)	C matter Ac - Martin	and the state
5-DEPHDE	CD NOTE +	fight of control and	CD WEEDOWNOUT	1911
And Assessed	Contractored	Adventionally 1472	Contraction to at	
AL TOC	(2) Undetected	Anthy Ant.	Chickelected	
for a matrix	Con Linearentent	(humo)	C thursday have	
	C Airchefeicheid	Mairie .	Chicklocted	
even too clouds				

By Hybrid method

53311 THFO: Executing 548400 THFO: Bootloade 548400 THFO: Bootloade 548100 THFO: Bootloade 548100 THFO: Checking 548100 ThFO: Checking 548100 ThFO: Checking 548100 ThFO: Checking 548100 ThFO: Copying 1 548100 THFO: Writing R 548100 THFO: Writing R 548100 THFO: Writing R 548100 THFO: Writing R 548100 THFO: Writing 548100 TH	HEG (CA PEG (CA PEG (CA PEG (CA EXE EFFO SXLEON T GROUP T ICON T ICON T ICON T ICON Marit fes Pesourt arthiv	om ['c:\\users\\ieuser\\appdats\	alocal/pyintaller/Hines cestfully algython/python30%10%14 %local/\programs/\python id/hello/run.ese.e00.5x35 %diat/hello.ese	ache01 te-pack	py30_64611\t) Ges\PyInsta	enet dll llertbootl	
30 Minus Torbal - File - Anti 12	ORE LUIT					• -	65 H
C = Autor	notational	فتعلمهم فالأراد فالمترا فتعاد والمعتدا الاستنا يبتهم	induction of Physics I Area (Control 1996)	and a first states	bie:	ita-	☆ ▲ 1
500 1000 1000 1000 1000 1000 1000 1000	04743100	Pochube&eteO1ecect??#c8113c103e827e0	stateartes (30	(田田 (広志)	10.0401	Citoria
	Autoritana Razburot Frankciana	anning the constitution of the providence of the second statements of t	East Min Scott		EXQ 64 UTC	9.4 250	* 981 0.
ENCTRICTION	DETAILS	RELATIONS BEHAVIOR	COMMUNITY				
Artis-5%	00	Treparationners: Addressed, Seatpriles	SecureAge APER	0	Automation and		
(Cption)	do.	General Second Sciences (Sciences)	Chryselinineraft	0			
Michhiel GIV Editors	CD	Birmenesista March Wernight March 197	100000	O	Trossertineyment	Cherce	
2939	cto	The second Disease We had also be	Annual Distance March	0	12meterian land		
AD mount	-	Gridestan, biol	Afen.mi 9/8	0	Undertexturist		
Althoughup	0	Comparison (sec.)	- And Street	0	and the local division of the local division		-
Advantation (2	Orientector	Part 100	60	Littlebalarchard		

By Exe method

Werestlated - File - 45							•		
		Contraction of the International Contractional Contr		Sales Pressil	10.4		Q.	* *	
48-017-00138	raumoonth	0.023-019356695546354657519576#7#5455775660		е ±	(#88)		21021-011	CSIUM LA	9
	0.6	move by conduct Reggest they be as multilistic						017.280	c.
0	49,0179	olos/4ettool4usedztanttabettec4e4u4tanttatee Plofeitee e	BubO MRB		00-01-24 U		75	0	
OFFECTION	DETAILS	COMMUNITY							
Anthy-Anti-		Property Sector Inc. A Description of the operation	Galidation		D Harmorth		and the state		
week all		Property Marcal Disease 1	Act America		S Linuster				
A.P		Carterine Internet	(*1.57mm)		> Linear	hand (
Performant and		Underholden?	A-1017	1	3 Livebertes	hed			
during trees cleaned.	0	Unideterment	Harristan	1	> thrushiles	total 1			
#Hillisteronder	0	Larscheidens Steel	Reconstruction Theory		> tarotates	1010		-	

Volume 10 Issue 9, September 2021 <u>www.ijsr.net</u> Licensed Under Creative Commons Attribution CC BY

The Party of the P	anne a contra			0 - 0
- C = 1810	Malacency with \$100.54000 hormatic 215-001625 the true	WHIN NUMBER	N472-08	10 (r 114
306754965360	9480.315x877x43577x47b2cx448c523bx42527b33x3x4x473c4	06 Q	本 第 四	Sann Gone
(8)	() 8 security ventions flagged this file as maktimes			0.2
	306/3-476 BHZ Medits 216 with Net30 Pile Mick of 485, 520 ex 125 2153 Marcol 475 (158) Normal Ann Anna Anna Anna Anna Anna Anna Anna		n on in 1924-30 (//C	2. Exc
There are a set of the				
ретестон	DETAILS COMMUNITY			
		Base Dro	WUADelector	
DETECTION		Base Pro CrossetElities Falcon		
DETECTION Semanalge APD	(C) Very tas		· ····································	entralescae, John (00)
DETECTION SecuritAge APD X Canoda Gyme	C Meneral Control Party Hast	Crower(Life International	· ····································	entense, son co entre
DETECTION SampleAgeAPEX Corresti	Versen Versen Versen Versen	CrowertSkillere Fallcon SamilinalOren (Starts: My	 ○ Minimum 2, 2 ○ Share A: Manual 	entense, son co entre

Packing and splitting and Joining methods

All above methods uses different tools for different things. Tools which are related to malware analysis.

3. Conclusion

The experimental process concludes that in order to encrypt laptop malware and to get prevented from its impact.

First process starts with Malware analysis to know more about malware working.

Second process started with using of different methods (Changing extension, Packing, Spitting and Joining, Hybrid, Exeand Extension and Exe) which can hide identity of Alina malware.

Third stage to protect laptop from this kind of malware which works related to update and other services usage of malware are solved by possible solution shown.

References

- [1] Encrypting Computer Virus: https://scholar.google. com/citations?user=e - 2HlBYAAAAJ&hl=en
- [2] Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali By: -OccupyThe Web
- [3] Cyber Forensics By: Dejey, Murugan
- [4] Laptop Forensics and Cyber Crime: An Introduction, 2e By: - Britz
- [5] https://www.wikipedia.org: Wikipedia
- [6] https://www.virustotal.com: Virus Total
- [7] Malware Analysing Tools

Volume 10 Issue 9, September 2021

www.ijsr.net

Licensed Under Creative Commons Attribution CC BY