Java Decompilers

written by Mert SARICA | 1 March 2016

I agree that working at byte code level is sometimes a bit challenging. If the mission is analyzing a Java malware, decompiling the class files into Java source code is the first step most analysts would take. However, like I mentioned in my post on July (Java Byte Code Debugging), if you are up against a malware that takes advantage of an obfuscator tool (like Allatori) Java decompilers (like JD) can most of the time let you fail.

Around December, a Java malware called siparisler.rar (siparisler.jar) took my attention which downloads additional payload from a website that I think was hacked with different password each time.



Siparişler		
	Dosya Hazır, İndirme İşlemine Başla	ayabilirsiniz
	Siparişleri İndir	

When I looked at the class files inside the JAR package that was made with the help of Allatori obfuscator tools' strongest features (long class and method names, reserved names like AUX e.t.c), I saw that file names were approximately 8000 digits long.

Because of the long file names, when I tried to extract the malware to the operating system with the use of tools like Winrar, 7zip, Unzip I realized that I got stuck at operating system limits and was not able to open the files. Also because of the long file and method names I noticed that most decompilers (except CFR) got an error during the decompilation process.

2	siparisler.jar - WinRAR (evaluation copy) – 🗖 🗙
File Commands Tools Favorites O	ptions Help
Add Extract To Test Vie	w Delete Find Wizard Info
🖆 🔬 siparisler.jar - ZIP archive, u	npacked size 846.630 bytes 🗸 🗸
Name	Size Packed Type Modified Obfuscation by Allatori Obfuscator http://www.allat ^
<u>)</u>	WinPAP: Diagnostic messages
a .	Winter Diagnostic messages
b c config META-INF O a.dat AAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAA	Message ^ C:\Users\Mert\Desktop\malware\siparisler.jar: Cannot create C:\Users\Mert\Desktop\AAA ^ C:\Users\Mert\Desktop\malware\siparisler.jar: Cannot create C:\Users\Mert\Desktop\AAA ^ C:\Users\Mert\Desktop\malware\siparisler.jar: Cannot create C:\Users\Mert\Desktop\AAA ^ C:\Users\Mert\Desktop\malware\siparisler.jar: Cannot create C:\Users\Mert\Desktop\AAA ^ C:\Users\Mert\Desktop\malware\siparisler.jar: Cannot create C:\Users\Mert\Desktop\AAA ^ The system cannot find the path specified. ^ C:\Users\Mert\Desktop\malware\siparisler.jar: Cannot create C:\Users\Mert\Desktop\AAA The system cannot find the path specified. C:\Users\Mert\Desktop\malware\siparisler.jar: Cannot create C:\Users\Mert\Desktop\AAA The system cannot find the path specified. The system ca
	00/22 1.70 < >
aUX.class	169 14 Close Break operation Copy to clipboard
Main.class	34.349 54
meeyg	10.381 10.03 Total errors: 5
<	
Selected 21.266 bytes in 1 fi	Total 6 folders and 418.927 bytes in 9 files
	sinarislar 1450150275 rat. WinPAP (evaluation conv)
File Commands Tools Favorites Options H	
Add Extract To Test View Del add Extract To Test View Del Signarister_1450159275.rar - RAR archir Name Size	Packed Type Modified Posya Sifresi: 7565
🔬 siparisler.jar * 366.786	131.248 Executable 14.12.2015 13:48
32	siparisler_1450159100.rar - WinRAR (evaluation copy) – 😐 🔀
File Commands Tools Fav	orites Options Help View Delete Find Wizard Info VirusScan Comment Protect SFX 00rar - RAB archive unpacked size 356 786 bytes
Name	Size Packed Type Modified Dosya Sifresi : 0432 A
📕 🔬 siparisler.jar *	File folder 366.786 131.248 Executable 14.12.2015 13:48
	🗃 siparisler_1450159284.rar - WinRAR (evaluation copy) 🗕 🗆 🗙
	File Commands Tools Favorites Options Help Add Extract To Test View Delete Find Wizard Info VirusScan Comment Protect SFX
	Size Decked Type Modified Dosva Sifresi : 5091
	Reference size Packed type Modified Posta Children Cost
<	isiparisler.jar * 366.786 131.248 Executable 14.12.2015 13:48 366.786 131.248 Executable 14.12.2015 13:48

As a person who witnessed that this malicious file was crashing a commercial product that does sandbox analysis while it is analyzing, I can state again that corporations whom only invest in and rely upon devices are on a thin ice.

Of course, with Python a simple tool like Allatori Zip Shortener, making this zip file openable was easy enough.

Applications - Places - S-T	erminal 🔻	Sun 11	:18			j≌ <u>1</u> <u>/</u> =0) U →
	root@kali: ~/Desktop/malware	• •	8			root@kali: ~/Desktop/malware/mal
File Edit View Search Terminal H	Help			File Edit V	iew Search Terminal	Help
root@kali:~/Desktop/malware	#			Allatori Z	ZIP Shortener v1.0	[http://www.mertsarica.com]
root@kali:~/Desktop/malware/ root@kali:~/Desktop/malware/ Archive: siparisler.jar Obfuscation by Allatori Obfu Length mat Date Time 0 2015-12-14 13:48	# # unzip -l siparisler.jar uscator http://www.allatori.com Name MFTA-INF/		0	[*] Shorte root@kali: allatori_z root@kali: Archive:	ened siparisler.ja ~/Desktop/malware zip_shortener.py ~/Desktop/malware siparisler-short. Date Time	r to siparisler-short.jar /mal# ls <mark>siparisler.jar siparisler-short.jar</mark> /mal# unzip -l siparisler-short.jar jar Name
195 2015-12-14 13:48 10381 2015-12-14 13:48 0 2015-12-14 13:48 0 2015-12-14 13:48 0 2015-12-14 13:48 107568 2015-12-14 13:48 GjBmMp4tRjVpjp6 0 2015-12-14 13:48 64 2015-12-14 13:48 64 2015-12-14 13:48 0 2015-12-14 13:48 4737 2015-12-14 13:48 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	META-INF/MANIFEST.MF meeyg 0/ 0/eAIuWf5mJJWp9bopZhbFDvFeL/ 0/eAIuWf5mJJWp9bopZhbFDvFeL/Tvjkyi2kzXIT 0/eAIuWf5mJJWp9bopZhbFDvFeL/Tvjkyi2kzXIT config/ config/config.pl a.dat a/ truncating. a/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	LinKjg/ LinKjg/L AAAAAAAA AAAAAAAA	-zdn AAAA AAAA	0 195 10381 0 0 107568 GjBmMp4tBj 306 64 64 4 0 14737 45305	2015-12-27 11:15 2015-12-27 11:15	META-INF/ META-INF/MANIFEST.MF meeyg O/ O/eAIuWf5mJJWp9bopZhbFDvFeL/ O/eAIuWf5mJJWp9bopZhbFDvFeL/Tvjkyi2kzX O/eAIuWf5mJJWp9bopZhbFDvFeL/Tvjkyi2kzX config/ config/config.pl a.dat a/ a/AVVNuL.class a/AVVcOn.class
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	MAAMAANAANAANAANAANAANAANAANAANAANAANAAN	4444444 444444 4444444 4444444 4444444 4444	AAA AAAA AAAA AAAA AAAA	0 79665 20739 14741	2015-12-27 11:15 2015-12-27 11:15 2015-12-27 11:15 2015-12-27 11:15 2015-12-27 11:15	D/ b/a/ b/a/AVVNuL.class b/a/AVVcOn.class b/a/AVVnUL.class
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	*****	AAAAAA	AAA			

To gain a more detailed information, I could have continued with a byte code level analysis, like in the article that I posted on July. If my purpose was to only find the type of this malware, I could have learned that it is a Jsocket RAT software by doing a quick search on the memory file without any trouble.

0					i de la composición de la composición de la composición de la composición de la composición de la composición d									Hex	Wor	ksho	p - [C:\Us	ers	Mert	Des	ktop	Java	∖java	aw.e>	ke.dr	np]			- 0	×
7() (1))	File Edit	Disk	Optio	ns To	ols F	lug-lr	ns Wi	ndow	Help	,																					e x
8	3830	* 5 6	8. B	26	88 4 8 6	69 (B		~ #	9 3	- 10																					
~	196 B B B 1	**	M	E Le	gacy /	ASC Y	100 4	P 101		×]																				Data Inspector	4 - 2
2			0	1	2	3	4	5	6	7	8	9	A	В	С	D	Е	F	10	11	12	13	14	15	16	17	18	0123456789ABCDEF012345678		Data at offset	t 0x0092EE
1	0092E	F87	В3	32	01	00	00	00	68	2A	B3	32	01	00	00	00	68	2A	B3	32	01	00	00	00	68	2A	B3	.2h*.2h*.2h*.	^	int8 10	1 ^
11	0092E	FA0	32	01	00	00	00	68	2A	В3	32	01	00	00	00	68	2A	В3	32	01	00	00	00	68	2A	В3	32	2h*.2h*.2h*.2		uint8 10	1
j	0092E	FB9	01	00	00	00	68	2A	В3	32	01	00	00	00	68	2A	В3	32	01	00	00	00	68	2A	B3	32	01	h*.2h*.2h*.2.		int16 25	
	0092E	FD2	00	00	00	68	2A	В3	32	01	00	00	00	C8	42	В3	37	44	01	00	00	7B	22	4E	45	54	57	h*.2B.7D{"NETW		uint 25	
	0092E	FEB	4F	52	4B	22	ЗA	5B	7B	22	50	4F	52	54	22	ЗA	31	34	37	35	36	2C	22	44	4E	53	22	ORK":[{"PORT":14756,"DNS"		int32 16	
	0092F	004	3A	22	65	62	65	64	69	79	61	7A	61	72	6C	61	72	2E	63	6F	6D	22	7D	5D	2C	22	49	:"ebediyazarlar.com"}],"I		uint 16	
	0092F	01D	4E	53	54	41	4C	4C	22	ЗA	. 74	72	75	65	2C	22	50	4C	55	47	49	4E	5F	46	4F	4C	44	NSTALL":true, "PLUGIN_FOLD		int64 88	
	0092F	036	45	52	22	3A	22	50	79	69	73	70	6B	22	2C	22	4A	52	45	5F	46	4F	4C	44	45	52	22	ER":"Pyispk","JRE_FOLDER"		uint 88	
	0092F	04F	3A	22	56	66	67	6C	71	6E	22	2C	22	4A	41	52	5F	46	$4 \mathrm{F}$	4C	44	45	52	22	3A	22	4D	:"Vfglqn","JAR_FOLDER":"M		halt 81	
	0092F	068	61	6C	72	70	79	22	2C	22	4A	41	52	5F	45	58	54	45	$4\mathrm{E}$	53	49	$4 \mathrm{F}$	$4\mathrm{E}$	22	3A	22	4B	alrpy", "JAR_EXTENSION": "K		float 1.6)
	0092F	081	78	72	71	6E	77	22	2C	22	44	45	4C	41	59	5F	49	4E	53	54	41	4C	4C	22	ЗA	31	2C	xrqnw", "DELAY_INSTALL":1,		dou 3.1	
	0092F	09A	22	4E	49	43	4B	4E	41	4D	45	22	3A	22	4E	43	5F	31	34	31	32	32	30	31	35	22	2C	"NICKNAME":"NC_14122015",		DATE SI	n
	0092F	0B3	22	56	4D	57	41	52	45	22	3A	66	61	6C	73	65	2C	22	50	4C	55	47	49	4E	5F	45	58	"VMWARE":false,"PLUGIN_EX		DOS 5.3	
	0092F	0CC	54	45	4 E	53	49	4 F	4E	22	3A	22	56	76	75	78	70	6D	22	2C	22	4A	41	52	5F	4E	41	TENSION": "Vvuxpm", "JAR_NA		FILE di	~
	0092F	0E5	4D	45	22	ЗA	22	4 D	77	72	6D	74	79	22	2C	22	4A	41	52	5F	52	45	47	49	53	54	52	ME":"Mwrmty","JAR_REGISTR		Expression Calc	
	0092F	OFE	59	22	3A	22	59	6A	76	79	77	63	22	2C	22	44	45	4C	41	59	5F	43	$4 \mathbb{F}$	4E	4E	45	43	Y": "Yjvywc", "DELAY_CONNEC		Signed V	/ 32 ∨
	0092F	117	54	22	3A	30	2C	22	56	42	4F	58	22	ЗA	66	61	6C	73	65	7D	01	00	00	00	68	2A	В3	T":0,"VBOX":false}h*.		1	
	0092F	130	32	01	00	00	00	68	2A	В3	32	01	00	00	00	68	2A	В3	32	01	00	00	00	68	2A	В3	32	2h*.2h*.2h*.2			
	0092F	149	01	00	00	00	68	2A	В3	32	01	00	00	00	F0	61	7A	37	10	00	00	00	01	00	00	00	00	h*.2az7			
	looom Biava	160	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	01	0.0	0.0	0.0	ΕO	012	01	00	ΕΩ	012	01	00	0.0	16	д Ц	•	Eval	
× 9	tructures														~	7 / B	nii 199 -	HAA	aa.		Eind	Rosulte								M 34	la al¥
-	dember 8							Malu	o (do 6				Mal	ue /h				Cine 8	2		Ado	iross P	0		lenat	h 19		Length N			1
2	viember •							valu	e (aec) "			va	ue (n	ex) 🖻			Size o			Auc	ness -			Lengt	10		Length 5			
ł.																															
dian Ve																												1.00.45			
																		👔 🗠 Compare 🖟 Checksum 🚊 Find 🗢 Bookmarks 🖾 Output													

Finding all instances...

Cursor: 0092F139 Caret: 0092EE5E 76991505 bytes OVR MOD READ

While I was analyzing this malware, I realized that most decompilers were not enough against Allatori thanks to a website

(http://www.javadecompilers.com/).Most decompilers were either unsuccessful to decompile this malware into a source code or the source code they decompiled was in a condition that could not be reorganized. If I wanted to move on with a byte code level static analysis, I could have seen that Allatori is hiding the strings and to be able to solve it I would have needed to find the method of hiding which would have made my work longer at byte code level. Because of this, I decided to evaluate existing decompilers against Allatori and try to find out which decompiler can reveal the algorithm that was used for hiding those strings. The criterion for success was that the class file which got decompiled to source code was reorganizable and executable.

First of all, in Java I wrote a simple code which prints "Hello World" to the command line and compiled it into a JAR package. Then with the Allatori, I create an obfuscated HelloWorld package. Finally, I started to decompile all the JAR files into the source code and then compile and run them by using this site http://www.javadecompilers.com/





C:\WINDOWS\system32\cmd.exe	- 🗆 ×
C:\Documents and Settings\Adm emo\tutorial\step01\files>Run	inistrator\Desktop\Allatori-5.6-Demo\Allatori-5.6-D Allatori.bat
C:\Documents and Settings\Adm emo\tutorial\step01\files>jav config.xml	inistrator\Desktop\Allatori-5.6-Demo\Allatori-5.6-D a -Xms128m -Xmx512m -jar\\lib\allatori.jar
<pre>####################################</pre>	<pre>####################################</pre>
🖉 Allatori Java Obfuscator - Do X) 🚡 Java decompler orline 🛛 X 🔲	
← → C f vww.javadecompilers.com	ය <u>ි</u>
Pecompilers online	
	.JAR and .Class to Java decompiler
Java decompilers	
APK decompiler	
Download Jad	
Decompile Java code in the cloud	
	Choose File obf helio jar Choose File obf helio
	Select a decompiler CFR (supports Java 8) Jadx, fast and with Android support DCCre (very fast) Procyon Fernflower (a) JAD (very fast. but outdated)
This site provides a user interface to extract sou	rce code from .class and .jar 'binary' files.
=	
Until recently, you needed to use a Java decompiler and all of them were eith bytecode.	r unstable, obsolete, unlinished, or in the best case all of the above. And, if not, then they were commercial. The obsoleteness was typically proved by the fact that they can only decomplie. JDK 1.3

As a result of the evaluation I found out that JadX and Procyon decompilers were able to successfully decompile the codes that were hidden by Allatori v5.6 Demo version to their original form.



C:\WINDOWS\system32\cmd.exe	
C:\Documents and Settings\Administrator\Desktop\Allatori-5.6-Demo\Allatori-5.6-D emo\tutorial\step01\files\obf-hello_source_from_jdcore\obf-hello_source_from_jdc ore>javac hello.java hello.java:38: error: not a statement 	I
hello.java:40: error: not a statement int ? = tmp68_67;	
hello.java:40: error: ';' expected int_? = tmp68_67;	
hello.java:40: error: not a statement int ? = tmp68_67;	
hello.java:43: error: not a statement tmp78_74;	
hello.java:45: error: not a statement ((0x3 ^ 0x5) << 3 ^ 0x2);	
hello.java:52: error: illegal start of expression ?[tmp102_99] = ((char)(k ^ a.charAt(tmp102_99) ^ n.charAt(j)));	
hello.java:52: error: illegal start of expression 💌 💌	1
C:\WINDOWS\system32\cmd.exe	1
emo\tutorial\step01\files\obf-hello_source_from_Procyon\obf-hello_source_from_Pr ocyon>javac hello.java	I
C:\Documents and Settings\Administrator\Desktop\Allatori-5.6-Demo\Allatori-5.6-D emo\tutorial\step01\files\obf-hello_source_from_Procyon\obf-hello_source_from_Pr ocyon>java hello	
* ** * ** *** *** *** ***	
	1
# # # Obfuscation bu Allatowi Obfuscatow u5 6 DFMO #	1
# http://www.allatori.com # # #	

Hello World!	
C:\Documents and Settings\Administrator\Desktop\Allatori-5.6-Demo\Allatori-5.6-D emo\tutorial\step01\files\obf-hello_source_from_Procyon\obf-hello_source_from_Pr	-



With the help of Procyon and JadX, the string obfuscation algorithm that is used by Allatori v5.6 came to light :)



Hope to see you on the next post, have a secure day.

Original Article: Java Kaynak Kodu Dönüştücüleri Translated to English by: Hüseyin Fatih Akar | Twitter: @thehakar)