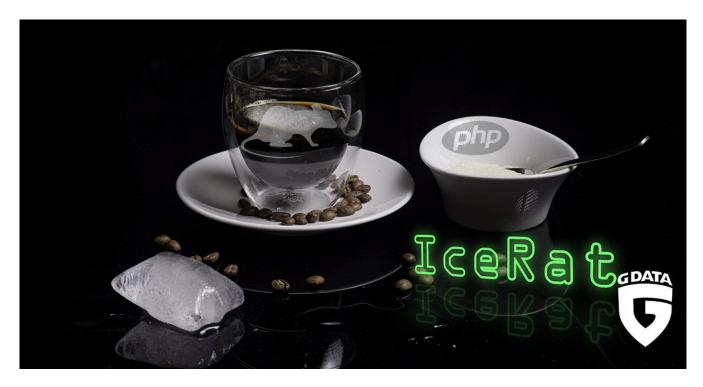
IceRat evades antivirus by running PHP on Java VM

G gdatasoftware.com/blog/icerat-evades-antivirus-by-using-jphp



IceRat keeps low detections rates for weeks by using an unusual language implementation: JPHP. But there are more reasons than the choice of the compiler. This article explores IceRat and explains a way to analyze JPHP malware.

Discovery of IceRat

User <u>McMcbrad</u> of the <u>Malwaretips.com</u> forums discovered the first IceRat samples^{[5][7]}. The malware caught his interest due to the low detection rates on VirusTotal for most related samples. At the time of discovery only 2 to 3 engines showed a detection despite the samples being a month old.

Static analysis reveals that most components of IceRat are written in **JPHP**. This is a PHP implementation that runs on the Java VM. This implementation uses .phb files instead of Java .class files -- a file type that, as I suspect, is not commonly supported by antivirus products. So far I haven't heard or found any other malware that uses JPHP which partially explains the low detection rates on VirusTotal.

The name **IceRat** is based on the module name of an older sample^[11] that McMcbrad found.

Decompiling JPHP

There don't seem to be any tools to decompile JPHP code yet. But JPHP has to produce Java Bytecode in order to run in the Java VM. So decompilation to Java code is possible.

Unpacking the executable^[5] with 7zip reveals the following structure.

Name	Änderungsdatum	Тур	Größe
data	04.11.2020 15:49	Dateiordner	
📊 .packages	05.11.2020 22:28	Dateiordner	
, system	26.11.2020 15:02	Dateiordner	
, theme	04.11.2020 15:49	Dateiordner	
action	05.11.2020 22:28	Dateiordner	
hehaviour	05.11.2020 22:28	Dateiordner	
📊 com	14.06.2016 17:55	Dateiordner	
📊 facade	05.11.2020 22:28	Dateiordner	
JPHP-INF	04.11.2020 15:53	Dateiordner	
META-INF	05.11.2020 22:28	Dateiordner	
📊 mio	05.11.2020 22:28	Dateiordner	
ng org	23.12.2016 10:34	Dateiordner	
📙 php	05.11.2020 22:28	Dateiordner	
script	19.11.2020 08:26	Dateiordner	
📊 timer	05.11.2020 22:28	Dateiordner	
📊 tray	28.10.2017 23:49	Dateiordner	
App.phb	05.11.2020 22:28	PHB-Datei	7 KB
Async.phb	05.11.2020 22:28	PHB-Datei	4 KB
📄 Dialog.phb	05.11.2020 22:28	PHB-Datei	8 KB
📄 Files.phb	05.11.2020 22:28	PHB-Datei	12 KB

As I noticed after looking at several JPHP samples, the entrypoint for the main JPHP code is under **.system**application.conf (see picture below). So for our klient.exe sample^[5] the main code resides in app\forms\rqfdeqwf.phb.

1	# MAIN CONFIGURATION
2	
3	app.name = klient
4	app.uuid = ab8ac8be-fddc-4300-aeaf-a97b213ec143
5	app.version = 1
6	
7	
8	app.namespace = app
9	app.mainForm = rqfdeqwf
10	app.showMainForm = 1
11	
12	app.fx.splash.autoHide = 0
-	

The **.phb** files contain the **0xCAFEBABE** magic bytes for Java .class files somewhere down below. Removing the first part of the file excluding the magic bytes makes it possible to decompile these files into Java code with, e.g., Fernflower. The right side of the picture below shows how the file should look like after modification.

Startup		Main	Forn	n.ph	bх															
	0	1	2	3	4	Š	6	7	8	9	A	В	с	D	E	F	0	1	2	0123456789ABCDEF012
0000h:		9A	<u>4</u> A																	.šJ'.3SÓG.GC
0013h:																				:\Users\Pk\DevelNex
0026h:																				tProjects\mine\src_
0039h:																				generated\mio\forms
004Ch:																				\MainForm.php
005Fh:																				<pre>\$php_module_md06491</pre>
0072h:	39	36	66	37	66	65	34	33	65	30	61	63	35	62	65	31	63	66	39	96f7fe43e0ac5be1cf9
0085h:	38	33	35	37	65	30	34	00	01	FF	FF	FF	FF	FF	FF	FF	FF	00	07	8357e04ÿÿÿÿÿÿÿÿ
0098h:	55	6E	6B	6E	6F	77	6E	00	00	00	00	00	00	00	01	00	00	00	36	Unknown6
00ABh:																				.6\$php_module_md064
00BEh:																				9196f7fe43e0ac5be1c
00D1h:																			00	f98357e04_closure0.
00E4h:																				·····ÿÿÿÿ··ÿÿÿÿÿÿ
00F7h:																				ÿÿinv
010Ah:	61	6B	65	00	00	00	08	00	80	51	51	69	6E	76	61	6B	65	01	00	okeinvoke
011Dh:																				GC:\Users\P
0130h: 0143h:																				k\DevelNextProjects
0143h: 0156h:																				\mine\src_generated \mio\forms\MainForm
0169h:																				.php
017Ch:																				ÉÊþº¾26\$
018Fh:																				php_module_md064919
01A2h:																				6f7fe43e0ac5be1cf98
01B5h:	33	35	37	65	30	34	5F	63	6C	6F	73	75	72	65	30	07	00	01	01	357e04 closure0
01C8h:																				php/runtime/lang/
01DBh:																				ClosureGC:\Use
			<u> </u>			14		~ ~							2.1					C10501 C11110C1 (05C
Startup			nFor												577					<
Startup	ð	Mai 1	nFor 2	m.ph 3	1 b* > 4	د 5	6	7	8	9	A	В	С	D	E	F	0	1	2	0123456789ABCDEF012
Startup 0000h :	0 CA	Mai 1 FE	nFor 2 BA	m .ph 3 BE	1 b* > 4 00	< 5 00	6 00	7 32	8 01	9 03	A 01	B 00	C 36	D 24	E 70	F 68	0 70	1 5F	2 6D	<pre></pre> <pre></pre>
Startup 0000h : 0013h :	0 [CA 6F	Mai 1 FE 64	nFor 2 BA 75	m.ph 3 BE 6C	4 4 00 65	5 00 5F	6 00 6D	7 32 64	8 01 30	9 03 36	A 01 34	B 00 39	C 36 31	D 24 39	E 70 36	F 68 66	0 70 37	1 5F 66	2 6D 65	<pre>< 0123456789ABCDEF012 Êpº%26\$php_m odule_md0649196f7fe</pre>
Startup 0000h: 0013h: 0026h:	0 CA 6F 34	Mai 1 FE 64 33	2 BA 75 65	m.ph 3 BE 6C 30	4 4 00 65 61	5 00 5F 63	6 00 6D 35	7 32 64 62	8 01 30 65	9 03 36 31	A 01 34 63	B 00 39 66	C 36 31 39	D 24 39 38	E 70 36 33	F 68 66 35	0 70 37 37	1 5F 66 65	2 6D 65 30	<pre></pre> <pre></pre>
Startup 0000h: 0013h: 0026h: 0039h:	0 6F 34 34	Mai FE 64 33 5F	2 BA 75 65 63	m.ph 3 BE 6C 30	4 00 65 61 6F	5 00 5F 63 73	6 00 6D 35 75	7 32 64 62 72	8 01 30 65 65	9 03 36 31 30	A 01 34 63 07	B 00 39 66 00	C 36 31 39 01	D 24 39 38 01	E 70 36 33 00	F 68 66 35 18	0 70 37 37 70	1 5F 66 65 68	2 6D 65 30 70	<pre></pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch:	0 CA 6F 34 34 2F	Mai 1 64 33 5F 72	2 BA 75 65 63 75	m.ph 3 BE 6C 30 6C 6E	4 00 65 61 6F 74	5 00 5F 63 73 69	6 00 6D 35 75 6D	7 32 64 62 72 65	8 01 30 65 65 2F	9 03 36 31 30 6C	A 01 34 63 07 61	B 00 39 66 00 6E	C 36 31 39 01 67	D 24 39 38 01 2F	E 70 36 33 00 43	F 68 66 35 18 6C	0 70 37 37 70 6F	1 5F 66 65 68 73	2 6D 65 30 70 75	<pre></pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh:	0 6F 34 34 2F 72	Mai 1 64 33 5F 72 65	2 BA 75 65 63 75 07	m.ph 3 8E 6C 30 6C 6E 00	4 00 65 61 6F 74 03	5 00 5F 63 73 69 01	6 00 6D 35 75 6D 00	7 32 64 62 72 65 47	8 01 30 65 65 2F 43	9 03 36 31 30 6C 3A	A 01 34 63 07 61 5C	B 00 39 66 00 6E 55	C 36 31 39 01 67 73	D 24 39 38 01 2F 65	E 70 36 33 00 43 72	F 68 66 35 18 6C 73	0 70 37 37 70 6F 5C	1 5F 66 65 68 73 50	2 6D 65 30 70 75 6B	<pre></pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h:	0 6F 34 34 2F 72 50	Mai 1 64 33 5F 72 65 44	2 BA 75 65 63 75 07 07	m.ph 3 6C 30 6C 6E 00 76	4 00 65 61 6F 74 03 65	5 00 5F 63 73 69 01 6C	6 6D 35 75 6D 00 4E	7 64 62 72 65 47 65	8 01 30 65 65 2F 43 78	9 36 31 30 6C 3A 74	A 01 34 63 07 61 50	B 00 39 66 00 6E 55 72	C 36 31 39 01 67 73 6F	D 24 39 38 01 2F 65 6A	E 36 33 00 43 72 65	F 68 66 35 18 6C 73 63	0 37 37 70 6F 5C 74	1 5F 66 65 68 73 50 73	2 6D 30 70 75 6B 5C	<pre></pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h:	0 6F 34 2F 72 5C 6D	Mai 1 64 33 5F 72 65 44 69	2 BA 75 65 63 75 07 65 65	m.ph 3 6C 30 6C 6E 00 76 65	4 00 65 61 6F 74 03 65 5C	5 00 5F 63 73 69 01 6C 73	6 6D 35 75 6D 00 4E 72	7 64 62 72 65 47 65 63	8 01 30 65 2F 43 78 5F	9 36 31 30 6C 3A 74 67	A 01 34 63 07 61 5C 50 65	B 00 39 66 00 6E 55 72 6E	C 36 31 39 01 67 73 6F 65	D 24 39 38 01 2F 65 6A 72	E 70 36 33 00 43 72 65 61	F 68 35 18 6C 73 63 74	0 37 37 70 6F 5C 74 65	1 5F 66 65 68 73 50 73 64	2 6D 30 70 75 6B 5C 5C	<pre> Õ123456789ABCDEF012 Êp%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0098h:	0 6F 34 34 2F 72 50 6D	Mai FE 64 33 5F 72 65 44 69 69	2 BA 75 63 75 63 75 07 65 6E 6F	m.ph 3 6C 30 6C 6E 00 76 5C	4 00 65 61 6F 74 03 65 5C 66	5 00 5F 63 73 69 01 6C 73 6F	6 00 35 75 6D 00 4E 72 72	7 64 62 72 65 47 65 63 60	8 01 65 65 2F 43 78 5F 73	9 36 31 30 6C 3A 74 67 5C	A 01 34 63 07 61 50 65 4D	B 00 39 66 00 6E 55 72 6E 61	C 36 31 39 01 67 73 6F 65 69	D 24 39 38 01 2F 65 6A 72 6E	E 70 36 33 00 43 72 65 61 46	F 68 35 18 6C 73 63 74 6F	0 37 37 70 6F 5C 74 65 72	1 5F 66 65 68 73 50 73 64 6D	2 6D 65 30 70 75 6B 5C 5C 2E	<pre> Õ123456789ABCDEF012 Êþ%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0098h: 00ABh:	0 6F 34 34 2F 72 5C 6D 6D 70	Mai FE 64 33 5F 72 65 44 69 69 68	2 BA 75 65 63 75 07 65 65 6E 6F 70	m.ph 3 6C 30 6C 6E 00 76 65 5C 01	4 00 65 61 6F 74 03 65 5C 66 00	5 00 5F 63 73 69 01 6C 73 6F 03	6 00 35 75 6D 00 4E 72 72 24	7 64 62 72 65 47 65 63 60 46	8 01 30 65 65 2F 43 78 5F 73 4E	9 36 31 30 6C 3A 74 67 5C	A 01 34 63 07 61 50 50 65 4D 00	B 00 39 66 00 6E 55 72 6E 61 12	C 36 31 39 01 67 73 6F 65 69 4C	D 24 39 38 01 2F 65 6A 72 6E 6A	E 70 36 33 00 43 72 65 61 46 61	F 68 66 35 18 6C 73 63 74 6F 76	0 37 37 70 6F 5C 74 65 72 61	1 5F 66 65 68 73 50 73 64 6D 2F	2 6D 30 70 75 6B 5C 5C 2E 6C	<pre></pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0098h:	0 6F 34 2F 72 6D 6D 70 61	Mai FE 64 33 5F 72 65 44 69 69 68 68	2 BA 75 63 75 07 65 65 6E 6F 70 67	m.ph 3 6C 30 6C 6E 00 76 65 5C 01 2F	4 00 65 61 74 03 65 50 66 00 53	5 00 5F 63 73 69 01 6C 73 6F 03 74	6 6D 35 75 6D 00 4E 72 72 24 72	7 64 62 72 65 47 65 63 63 60 46 69	8 01 30 65 2F 43 78 5F 73 4E 6E	9 36 31 30 6C 3A 74 67 5C 01 67	A 01 34 63 07 61 50 65 4D 00 3B	B 00 39 66 00 6E 55 72 6E 61 12 08	C 36 31 39 01 67 73 6F 65 69 4C 00	D 24 39 38 01 2F 65 6A 72 6E 6A 05	E 70 36 33 00 43 72 65 61 46 61 01	F 68 66 35 18 60 73 63 74 6F 76 00	0 37 37 70 6F 5C 74 65 72 61 04	1 5F 66 65 73 50 73 64 6D 2F 24	2 6D 30 70 75 6B 5C 5C 2E 6C 54	<pre> Õ123456789ABCDEF012 Êpº%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0085h: 008Bh: 00ABh: 00BEh:	0 6F 34 2F 72 5C 6D 6D 6D 70 61 52	Mai 1 64 33 5F 72 65 44 69 69 69 68 68 68 68	2 BA 75 65 63 75 65 65 65 65 65 67 07	3 BE 6C 30 6C 6E 00 76 65 5C 01 2F 00	4 00 65 61 6F 74 03 65 5C 66 00 53 1C	5 00 5F 63 73 69 01 6C 73 6F 03 74 5B	6 00 35 75 6D 00 4E 72 72 24 72 24 72 4C	7 32 64 62 72 65 47 65 63 63 60 46 69 70	8 01 30 65 2F 43 78 5F 73 4E 6E 68	9 36 31 30 6C 3A 74 67 5C 01 67 70	A 01 34 63 07 61 50 65 4D 00 3B 2F	B 00 39 66 00 6E 55 72 6E 61 12 08 72	C 36 31 39 01 67 73 6F 65 69 4C 00 75	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E	E 70 36 33 00 43 72 65 61 46 61 01 74	F 68 66 35 18 62 73 63 74 6F 76 00 69	0 37 37 70 6F 5C 74 65 72 61 04 6D	1 5F 66 65 68 73 50 73 64 6D 2F 24 65	2 6D 65 30 70 75 6B 5C 5C 2E 6C 54 2F	<pre> Õ123456789ABCDEF012 Êpº%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String:\$T RC[Lphp/runtime/</pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 0072h: 0072h: 0085h: 0098h: 00ABh: 00BEh:	0 6F 34 2F 72 5C 6D 6D 70 6D 70 61 52 65	Mai 1 64 33 5F 72 65 44 69 69 69 68 68 68 68	2 BA 75 65 63 75 65 67 65 65 65 67 70 67 01 76	BE 6C 30 6C 6C 6C 6C 6C 6C 6C 6C 6C 6C 00 76 65 5C 01 2F 00 2F	4 00 65 61 6F 74 03 65 5C 66 66 00 53 1C 54	5 00 5F 63 73 69 01 60 73 6F 03 74 5B 72	6 00 35 75 6D 00 4E 72 72 24 72 24 72 61	7 32 64 62 72 65 47 65 63 60 46 69 70 63	8 01 30 65 65 2F 43 78 5F 73 4E 6E 68 65	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 49	A 01 34 63 07 61 50 50 65 4D 00 3B 2F 6E	B 00 39 66 00 6E 55 72 6E 61 12 08 72 66	C 36 31 39 01 67 73 65 65 69 4C 00 75 6F	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B	E 70 36 33 00 43 72 65 61 46 61 01 74 01	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00	0 37 37 70 6F 5C 74 65 72 61 04 6D 04	1 5F 66 65 68 73 50 73 64 6D 2F 24 65 24	2 6D 30 70 75 6B 5C 5C 2E 6C 54 2F 4D	<pre> Õ123456789ABCDEF012 Êpº%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mio\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String:\$T RC[Lphp/runtime/ env/TraceInfo;\$M </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0085h: 008Bh: 00ABh: 00BEh: 00D1h: 00E4h:	0 6F 34 34 2F 72 6D 6D 6D 70 61 52 65 45	Mai 1 644 33 5F 722 65 64 69 69 68 68 68 68 68 68 68 68 68 68 68 68 68	2 BA 75 65 63 75 65 63 75 67 67 67 67 67 01 76 70	m.ph 3 6C 30 6C 6C 6C 6C 6C 6C 6C 6C 00 65 5C 01 2F 00 2F 00	4 00 65 61 6F 74 03 65 5C 5C 66 00 53 1C 54 15	5 5 63 73 69 01 60 73 67 03 6F 03 74 5B 72 5B	6 00 6D 35 75 6D 00 4E 72 72 24 72 4C 61 4C	7 32 64 62 72 65 63 60 46 69 70 63 70	8 01 30 65 65 2F 43 78 5F 73 4E 68 65 68 65 68	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 49 70	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F	B 00 39 66 00 6E 55 72 6E 61 12 08 72 66 72	C 36 31 39 01 67 73 65 65 69 4C 00 75 6F 75	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E	E 70 36 33 00 43 72 65 61 46 61 01 74 01 74	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00 69	0 37 37 70 6F 5C 74 65 72 61 04 6D 04 6D	1 5F 66 65 68 73 50 73 64 6D 2F 24 65 24 65	2 6D 65 30 70 75 6B 5C 2E 6C 54 2F 4D 2F	<pre> Õ123456789ABCDEF012 Êpº%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String:\$T RC[Lphp/runtime/</pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 008Bh: 00BEh: 00BEh: 00D1h: 00E4h: 00F7h: 010Ah: 011Dh:	0 6F 34 2F 72 5C 6D 70 6D 70 61 52 65 45 45 5B	Maii 1 FE 64 33 5F 72 65 44 69 69 69 69 69 68 68 68 68 68 68 68 68 68 68 68 68 68	2 BA 755 65 63 75 65 65 65 65 65 67 07 01 76 01 76 01 6D 70	BE 6C 30 6C 6C 6E 00 76 65 5C 01 2F 00 2F 00 6F 68	4 000 65 61 6F 74 03 65 5C 66 60 53 1C 54 15 72 70	 5 00 5F 63 73 69 01 62 73 67 03 74 58 72 58 79 2F 	6 00 35 75 6D 00 4E 72 24 72 4C 61 4C 3B 72	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 01 75	8 01 30 65 65 2F 43 78 5F 73 4E 6E 68 65 68 65 68 00 6E	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 49 70 05 74	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 2F 24 69	B 00 39 66 00 6E 55 72 6E 61 12 08 72 66 72 41 6D	C 36 31 39 01 67 73 6F 65 69 4C 00 75 6F 75 4D 65	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 45 2F	E 70 36 33 00 43 72 65 61 46 61 01 74 01 74 40 40	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00 69 01 65	0 70 37 70 6F 5C 74 65 72 61 04 6D 04 6D 00 6D	1 5F 66 55 68 73 50 73 64 6D 2F 24 65 24 65 16 6F	2 6D 65 30 70 75 6B 5C 5C 5C 5C 5C 5C 5C 54 2F 4D 2F 5B 72	<pre> Ô123456789ABCDEF012 Êp%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ EM.</pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0098h: 008Bh: 008Eh: 0001h: 00E4h: 0007h: 010Ah: 010Ah: 0110h:	0 6F 34 2F 72 5C 6D 6D 70 61 52 65 45 45 45 79	Maii 1 644 333 5F 722 655 444 699 699 688 682 699 699 688 682 642 400 655 440 400 655 440 38	2 BA 755 655 633 755 655 670 670 670 670 670 01 766 01 700 600 700 01	BE 6C 30 6C 6C 6C 00 76 5C 01 2F 00 2F 00 6F 68 00	4 00 65 61 6F 74 03 65 5C 66 00 53 1C 54 15 72 70 10	 5 63 73 69 01 67 73 6F 03 74 5B 72 5B 79 2F 24 	6 00 35 75 6D 00 4E 72 24 72 4C 61 4C 3B 72 43	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 63 70 01 75 41	8 01 30 65 2F 43 78 5F 73 4E 6E 68 65 68 00 6E 4C	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 70 9 70 05 74 40	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 24 69 5F	B 00 39 66 00 6E 55 72 6E 61 12 08 72 66 72 66 72 41 6D 46	C 36 31 39 01 67 73 65 65 69 4C 00 75 67 75 4D 65 55	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 45 2F 4E	E 70 363 33 72 65 61 46 61 01 74 01 74 4D 4D 43	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00 69 00 69 01 65 5F	0 37 37 70 6F 5C 74 65 72 61 04 6D 04 6D 00 6D	1 5F 66 65 68 73 50 73 64 6D 2F 24 65 24 65 16 6F 41	2 6D 65 30 70 55 5C 5C 2E 6C 54 2F 5B 72 43	<pre> Õ123456789ABCDEF012 Ép%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[Lphp/runtime/ Memory;\$AMEM[Lphp/runtime/ Y;\$CALL_FUNC_CAC </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0088h: 0088h: 0088h: 0088h: 0088h: 0084h: 0007h: 010Ah: 010Ah: 0110h: 0130h:	0 6F 34 34 2F 72 5C 6D 6D 70 61 52 65 45 45 45 45 45 45 45 45 45 45 45 45 45	Maii 1 5 644 333 5 722 655 444 699 689 688 688 688 689 640 699 639 640 640 640 640 640 640 640 640	2 BA 75 65 63 75 65 63 75 65 67 67 67 01 76 67 01 76 01 70 60 70 01 01	BE 6C 30 6C 6C 6C 00 76 5C 00 2F 00 2F 00 6F 68 00 00 00	4 00 65 61 6F 74 03 65 5C 66 00 53 1C 54 15 72 70 10 2C	 5 00 5F 63 73 69 01 6C 73 6F 03 74 5B 72 5B 79 2F 24 4C 	6 00 6D 35 75 6D 00 4E 72 24 72 4C 61 4C 3B 72 43 70	7 32 64 62 72 65 63 60 46 69 70 63 70 01 75 41 68	8 01 30 65 2F 43 78 5F 73 4E 68 65 68 65 68 00 6E 4C 70	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 49 70 05 74 4C 2F	A 01 34 63 07 61 50 50 65 4D 00 3B 2F 6E 2F 2F 24 69 5F 72	B 00 39 66 00 6E 55 72 6E 61 12 72 66 72 41 6D 46 75	C 36 31 39 01 67 73 65 69 40 75 6F 75 4D 65 55 6E	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 45 2F 4E 74	E 70 36 33 00 43 72 65 61 46 61 74 01 74 4D 4D 40 43 69	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00 69 01 65 5F 6D	0 37 37 70 6F 5C 74 65 72 61 04 6D 04 6D 00 6D 43 65	1 5F 66 65 68 73 50 73 64 6D 2F 24 65 24 65 16 6F 41 2F	2 6D 65 30 70 75 6B 5C 5C 2E 6C 54 2F 4D 2F 5B 72 43 69	<pre> Õ123456789ABCDEF012 Êpº¾26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[Lphp/runtime/ y;\$CALL_FUNC_CAC HE,Lphp/runtime/i </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0085h: 008Bh: 008Bh: 00BEh: 0001h: 00E4h: 00F7h: 010Ah: 011Dh: 0130h: 0143h:	0 6F 34 34 2F 72 5C 6D 6D 70 61 52 65 45 45 45 45 45 45 45 45 45 45 45 45 45	Maii 1 5 6 6 6 7 6 5 7 7 6 5 7 6 6 6 6 6 6 6 6 6 6 6 6 6	2 BA 75 65 63 75 65 65 67 65 67 67 67 01 76 60 70 60 70 01 60 70 60 70 60	BE 6C 30 6C 6E 00 76 65 5C 01 2F 00 2F 00 6F 68 00 6F 68 00 00 6B	4 00 65 61 67 74 03 65 50 50 50 50 50 50 50 50 50 5	5 00 5F 63 73 69 01 6C 73 6F 73 6F 73 6F 73 5B 72 5B 79 2F 24 4C 2F	6 00 6D 35 75 6D 00 4E 72 24 72 4C 61 4C 3B 72 43 70 63	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 01 75 41 68 61	8 01 30 65 65 2F 43 78 5F 73 4E 68 65 68 65 68 00 6E 4C 70 63	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 05 74 9 70 05 74 4C 2F 68	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 24 69 5F 72 65	B 00 39 66 00 6E 55 72 6E 61 12 08 72 66 72 66 72 41 6D 46 75 2F	C 36 31 39 01 67 73 65 69 40 75 67 75 4D 65 55 6E 46	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 45 2F 4E 74 74 75	E 70 36 33 00 43 72 65 61 46 61 74 61 74 4D 40 40 43 69 6E	F 68 66 35 18 67 73 63 74 6F 76 00 69 00 69 01 65 5F 6D 63	0 37 37 70 6F 5C 74 65 72 61 6D 04 6D 00 6D 6D 6D 3 65 74	1 5F 66 65 68 73 50 73 64 65 24 65 24 65 16 6F 41 2F 69	2 6D 30 70 5C 5C 2E 6C 5C 2F 4D 2F 5B 72 43 69 6F	<pre> Õ123456789ABCDEF012 Êp°%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String:\$T RC[Lphp/runtime/ env/TraceInfo:\$M EM[Lphp/runtime/ Memory:\$AMEM[Lphp/runtime/ Memory:\$AMEM[Lphp/runtime/ movke/cache/Functio </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0098h: 00ABh: 00ABh: 00BEh: 0001h: 00E4h: 010Ah: 011Dh: 0110h: 0143h: 0156h: 0169h:	0 6F 34 2F 72 6D 6D 70 61 52 65 4D 58 79 48 6E 6E	Maii 1 5 5 5 7 2 5 7 2 5 7 2 5 5 7 2 5 7 2 5 7 2 5 7 2 5 7 2 5 5 7 2 5 5 7 2 5 5 5 6 5 6 5 6 5 6 5 6 5 6 6 6 6 6 6 6 6 6 6 6 6 6	2 BA 75 65 63 75 65 65 67 65 67 67 67 01 76 67 01 76 01 60 70 01 60 61 61	BE 6C 30 6C 6E 00 76 65 5C 01 2F 00 2F 00 6F 68 00 00 6F 68 00 00 6B	4 00 65 61 6F 74 03 65 5C 66 00 53 1C 54 15 72 70 10 2C 65 6C	5 00 5F 63 73 69 01 6C 73 6F 73 6F 73 6F 73 5B 72 5B 79 2F 24 4C 2F 43	6 00 35 75 6D 00 4E 72 24 72 24 4C 61 4C 3B 72 43 70 63 61	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 01 75 41 68 61 63	8 01 30 65 65 2F 43 78 78 78 78 78 78 78 65 68 65 68 65 68 00 6E 40 70 63 68	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 49 70 05 74 4C 2F 68 65	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 24 69 5F 72 65 3B	B 00 39 66 55 72 6E 61 12 08 72 66 72 66 72 41 6D 46 75 2F 01	C 36 31 39 01 67 73 65 65 69 4C 00 75 6F 75 6F 75 65 55 6E 46 00	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 45 2F 4E 74 75 10	E 70 36 33 00 43 72 65 61 46 61 01 74 01 74 4D 40 43 69 6E 24	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00 69 01 65 5F 6D 63 43	0 37 37 70 6F 5C 74 65 72 61 04 6D 04 6D 00 6D 43 65 74 41	1 5F 66 65 68 73 50 73 64 65 24 65 24 65 16 65 16 67 41 2F 69 40	2 6D 65 30 75 6B 5C 5C 2E 6C 54 2F 4D 2F 5B 72 43 69 6F 4C	<pre> Õ123456789ABCDEF012 Êp°%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String:\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory:\$AMEM[[Lphp/runtime/Memor y;\$CALL_FUNC_CAC HELphp/runtime/i nvoke/cache/Functio nCallCache;\$CALL </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0085h: 008Bh: 008Bh: 008Bh: 001h: 0057h: 010Ah: 011Dh: 0120h: 0156h: 0169h: 017Ch:	0 6F 34 2F 72 6D 6D 70 61 52 65 4D 5B 79 48 6E 5F	Maii 1 FE 64 333 5F 722 65 44 69 69 69 68 68 68 68 68 68 68 68 68 68	For 2 BA 75 65 63 75 65 67 65 67 65 67 65 67	3 BE 6C 30 6C 6E 00 76 65 5C 01 2F 00 2F 00 6F 68 00 6F 68 00 6F 68 54	4 00 65 61 6F 74 03 65 5C 66 00 53 1C 54 15 72 70 10 2C 65 6C 48	5 000 5F 63 73 69 01 6C 73 6F 03 74 5B 79 2F 24 5B 79 2F 24 4C 2F 43 5F	6 00 35 75 6D 00 4E 72 24 72 24 4C 61 4C 3B 72 43 70 63 61 43	7 32 64 62 72 65 63 60 69 70 63 70 63 70 01 75 41 68 61 63 41	8 01 30 65 65 2F 43 78 5F 73 4E 68 68 65 68 00 6E 40 70 63 68 43	9 03 36 31 30 6C 3A 74 67 5C 01 67 70 49 70 05 74 4C 2F 68 65 48	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 2F 24 69 5F 72 65 3B 45	B 00 39 66 55 72 6E 61 12 08 72 66 72 66 72 41 6D 46 75 2F 01 01	C 36 31 39 01 67 73 65 69 4C 00 75 65 65 55 6E 40 00 00	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 45 2F 4E 74 75 10 2A	E 70 36 33 00 43 72 65 61 46 61 01 74 01 74 4D 40 43 69 6E 24 4C	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00 69 01 65 5F 6D 63 43 70	0 37 37 70 6F 5C 74 65 72 61 04 6D 04 6D 00 6D 43 65 74 41 68	1 5F 66 65 68 73 50 73 64 65 24 65 24 65 16 65 16 67 41 2F 69 4C 70	2 6D 65 30 70 75 6B 5C 2E 6C 54 2F 4D 2F 5B 72 43 69 6F 4C 2F	<pre> Õ123456789ABCDEF012 Êp°%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[[Lphp/runtime/Memor y;\$CALL_FUNC_CAC HELphp/runtime/i nvoke/cache/Functio nCallCache;\$CALL _METH_CACHE*Lphp/ </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0085h: 0084h: 0084h: 00024h: 0057h: 010Ah: 0120h: 0143h: 0143h: 0156h: 0169h: 017Ch: 018Fh:	0 6F 344 2F 72 6D 6D 70 61 52 45 45 45 45 45 45 6E 5F 72	Mai FE 64 33 5F 72 65 65 69 69 69 69 69 69 68 68 68 68 68 68 68 68 68 68	For 2 BA 75 65 63 75 65 67 66 701 67	BE 6C 300 6C 6E 00 765 5C 01 2F 00 2F 00 00 6F 68 00 6F 68 00 6F 68 00 6F 74	4 000 65 61 6F 74 03 65 50 66 66 00 53 10 54 15 72 70 10 20 65 60 48 69	5 000 5F 633 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 69 01 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 60 73 74 55 74 55 74 72 74 72 74 72 74 72 74 72 74 72 74 74 75 79 74 79 74 79 74 79 74 79 74 79 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 79 25 65 79 25 79 25 65 79 25 65 79 24 40 25 75 75 75 75 75 75 75 75 75 7	6 00 6D 35 75 6D 00 4E 72 24 47 22 4 72 24 47 72 40 61 40 3B 70 63 61 43 65	7 32 64 62 72 65 47 65 63 60 70 63 70 01 75 41 68 61 63 41 2F	8 01 30 65 2F 43 73 4E 68 65 68 00 6E 4C 70 63 68 43 69	9 36 31 30 6C 3A 67 5C 01 67 70 49 70 05 74 4C 2F 68 65 48 65	A 01 34 63 07 65 50 65 40 00 38 2F 6E 2F 24 69 5F 72 65 38 45 76	B 00 39 66 55 72 6E 61 12 08 72 66 72 41 6D 46 75 2F 01 01 6F	C 36 31 39 01 67 65 65 69 4C 00 75 65 65 55 6E 40 00 65 6E 46 00 00 68	D 24 39 38 01 2F 6A 72 6E 6A 05 6E 3B 6E 45 2F 4E 74 75 10 2A 65	E 70 36 33 72 65 61 01 74 01 74 01 74 40 40 40 43 69 6E 24 4C 2F	F 688 666 355 188 673 63 74 67 76 000 69 001 659 60 63 63 433 70 63	0 37 37 50 6F 52 61 04 6D 00 6D 6D 6D 6D 6D 6D 6D 6D 6D 6D 6D 6D 6D	1 5F 666 65 68 73 50 73 64 27 24 65 24 65 24 65 16 6F 41 2F 69 4C 70 63	2 6D 65 30 70 75 6B 5C 5C 2E 6C 2F 4D 2F 5B 72 43 69 6F 4C 2F 68	<pre> Ô123456789ABCDEF012 Êp%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[[Lphp/runtime/Memor y;\$CALL_FUNC_CAC HE,Lphp/runtime/i nvoke/cache/Functio nCallCache;\$CALL METH_CACHE*Lphp/ runtime/invoke/cach </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0088h: 008H: 000Eh: 000Eh: 00E4h: 00F7h: 010Ah: 0143h: 0143h: 0143h: 0143h: 0143h: 0143h: 0143h: 0143h: 0143h:	0 6F 344 2F 72 6D 70 6D 70 61 52 65 45 45 45 45 6E 5F 72 65	Main FE 64 33 5F 722 65 44 69 69 69 69 69 69 69 69 69 69	For 2 BA 755 655 633 755 657 670 671 670 671 760 671 670 671 670 671 671 670 671 671 670 761 670 671 671 672 673 674 675 675 677 670 701 670 701 670 701 675 676 701 676 671 671 672 673 674 674	BE 6C 300 6C 6E 000 76 65 5C 01 2F 000 2F 000 6F 68 000 6F 68 000 6F 68 000 6F 68 000 6F 68 000 6F 64 74	4 000 65 61 67 74 03 65 50 66 00 53 10 54 15 72 70 10 20 65 60 10 20 65 60 10 54 15 72 70 10 20 65 61 10 10 10 10 10 10 10 10 10 1	5 00 5F 63 73 69 01 6C 73 6F 03 74 5B 79 2F 24 5B 79 2F 24 4C 2F 43 5F 6D 68	6 00 6D 35 75 6D 00 4E 72 24 72 24 72 24 72 40 61 40 3B 70 63 61 43 65 6F	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 01 75 41 68 61 63 41 2F 64	8 01 30 65 65 2F 43 78 78 78 78 65 68 65 68 65 68 65 68 65 68 65 68 65 68 65 68 65 68 65 68 65 68 69 43 69 43	9 36 31 30 6C 3A 67 5C 01 67 70 49 70 05 74 4C 2F 68 65 48 65 48 65	A 01 34 63 07 65 50 65 25 65 2F 24 69 5F 72 65 3B 45 76 62	B 00 39 66 55 72 6E 61 12 08 72 66 72 41 6D 46 75 2F 01 01 6F 6C	C 36 31 39 01 67 73 6F 65 65 6F 75 40 55 55 6E 46 00 00 6B 43	D 24 39 38 01 2F 6A 72 6E 6A 05 6E 3B 6E 45 2F 4E 74 75 10 2A 65 61	E 70 36 33 72 65 61 01 74 01 74 01 74 40 40 40 40 43 69 6E 24 40 2F 63	F 68 66 35 18 6C 73 63 67 67 69 00 69 00 69 00 69 01 55 55 60 63 43 70 63 68	0 70 37 70 6F 5C 74 65 72 61 04 6D 04 6D 00 6D 04 35 74 41 68 61 65	1 5F 66 55 73 50 73 64 6D 2F 24 65 24 65 16 6F 41 2F 69 4C 70 63 3B	2 6D 65 30 70 75 6B 5C 2E 6C 2F 4D 2F 5B 72 43 69 6F 4C 2F 68 01	<pre> Ô123456789ABCDEF012 Êp%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[[Lphp/runtime/Memor y;\$CALL_FUNC_CAC HE,Lphp/runtime/i nvoke/cache/Functio nCallCache;\$CALL METH_CACHE*Lphp/ runtime/invoke/cach e/MethodCallCache;. </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0088h: 008Eh: 008Eh: 00624h: 00624h: 010Ah: 0143h: 0156h: 0143h: 0156h: 017Ch: 018Fh: 01A2h: 0185h:	0 6F 344 2F 722 50 6D 6D 70 6D 70 6D 70 61 52 65 45 45 45 45 45 65 79 8 6E 5F 72 65 00	Main 1 FE 644 333 5F 722 655 444 699 699 688 688 688 688 433 688 433 688 433 649 435 649 435 649 649 649 649 649 649 649 649	Provide a constraint of the second se	BE 6C 300 6C 65 5C 01 2F 000 2F 000 6F 688 000 6F 688 000 6F 688 000 6F 684 000 6F 688 000 665 676 676 676 676 676 676 676 676 676	4 000 65 61 67 74 03 65 50 66 00 53 10 54 15 72 70 10 20 65 66 00 53 10 54 15 72 70 10 20 65 64 65 66 66 66 66 67 67 67 67 67 67	5 00 5F 63 73 69 01 60 73 67 03 74 5B 79 2F 24 43 5F 6D 68 40 68 40	6 60 60 35 75 60 4E 72 24 72 4C 3B 72 43 72 43 70 63 61 43 65 6F 4C	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 01 75 41 63 61 63 41 2F 64 5F	8 01 30 65 65 2F 43 78 5F 73 4E 68 65 68 65 68 65 68 65 68 00 6E 40 70 63 68 9 43 50	9 36 31 30 6C 3A 74 67 5C 01 67 70 49 70 05 74 4C 2F 68 65 48 65 48 65 48 65 52	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 24 69 5F 72 65 3B 45 76 6C 4F	B 00 39 66 55 72 6E 61 12 08 72 66 72 66 72 41 6D 46 75 2F 01 01 6F 6C 50	C 36 31 39 01 67 73 6F 65 65 6F 75 4D 65 55 6E 46 00 00 6B 43 5F	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 2F 4E 75 10 2A 65 61 43	E 70 365 33 72 65 61 46 61 01 74 01 74 40 40 43 69 6E 24 4C 2F 63 41	F 68 66 35 18 6C 73 63 74 6F 76 00 69 00 69 00 69 00 69 01 65 5F 6D 63 43 70 63 88 43	0 70 37 70 6F 5C 74 65 72 61 04 6D 00 04 6D 00 6D 43 65 74 61 65 43 65 43 65 74 65 74 65 72 61 65 72 61 65 72 74 70 70 70 70 70 70 70 70 70 70	1 5F 66 50 73 64 6D 2F 24 65 24 65 24 65 16 6F 41 2F 69 4C 70 63 3B 45	2 6D 65 30 70 75 6B 5C 2E 6C 2F 4D 2F 5B 72 43 69 6F 4C 2F 68 01 01	<pre> O123456789ABCDEF012 Êp%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[[Lphp/runtime/Memor y;\$CALL_FUNC_CAC HELphp/runtime/i nvoke/cache/Functio nCallCache;\$CALL _METH_CACHE*Lphp/ runtime/invoke/cach e/MethodCallCache;. \$CALL_PROP_CACHE. </pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 010Ah: 0126h: 0130h: 0130h: 0130h: 0136h: 0136h: 017Ch: 0185h: 0185h: 0188h:	0 6F 344 34 72 50 6D 70 8D 70 8D 70 6D 70 8D 70 6D 70 6D 70 8D 70 8D 70 6D 70 8D 70 8D 70 6D 70 8D 70 8D 70 8D 70 8D 70 8D 70 8D 70 8D 70 8D 70 6D 70 8D 70 70 70 8D 70 70 70 70 70 70 70 70 70 70 70 70 70	Mai 1 5FE 644 333 5F 722 65 444 69 69 68 68 68 68 68 68 68 68 68 68 68 68 68	For 2 BA 755 655 633 755 655 633 755 655 633 755 656 677 657 670 670 011 600 701 011 616 701 617 618 610 701 611 612 613 614 615 616 617 618 619 620 621 621 621 6224 420	BE 6C 30 6C 6C 6E 00 76 65 5C 01 2F 00 2F 00 00 6F 68 00 00 6F 68 00 00 6F 68 00 00 6F 68 00 00 6F 68 00 00 76 67 00 76 76 76 76 76 76 76 76 76 76 76 76 76	4 000 655 611 6F 744 033 655 502 666 000 533 102 544 155 722 700 100 202 655 665 665 665 674 408 744 155 742 740 100 100 100 100 100 100 100 1	5 5 63 73 69 01 6C 73 6F 73 6F 73 6F 73 6F 5B 79 2F 24 4C 2F 24 4C 2F 5B 6D 68 84C 70	6 60 35 75 6D 00 4E 72 24 72 24 72 4C 3B 72 43 70 63 61 43 65 6F 4C 2F	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 01 75 41 63 70 01 75 41 63 41 25 64 55 72	8 01 30 65 65 2F 43 78 5F 73 4E 68 68 65 68 68 65 68 68 00 6E 40 70 63 68 3 69 43 50 75	9 36 31 30 6C 3A 74 67 5C 01 67 70 49 70 05 74 40 2F 68 65 48 65 48 65 48 65 48 65 48 65 48 65	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 24 69 5F 72 65 3B 45 76 6C 4F 74	B 00 39 66 55 72 6E 61 12 8 8 8 72 66 72 41 6D 46 75 2F 01 01 6F 6C 50 69	C 36 31 39 01 67 73 6F 65 69 40 075 6F 75 6F 75 65 55 6E 46 00 00 6B 43 5F 6D	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 3B 6E 2F 4E 75 10 2A 65 61 43 65	E 70 363 33 72 65 61 46 61 01 74 01 74 40 40 43 69 6E 24 4C 2F 63 41 2F	F 68 66 35 18 60 73 63 73 63 74 67 60 69 00 69 00 69 01 65 5 F 6D 63 43 70 63 843 68 843 69	0 70 37 37 70 6F 5C 74 65 72 61 60 40 6D 60 60 60 60 60 60 74 41 68 61 65 74 41 65 74 65 74 65 74 65 74 65 74 65 72 65 72 74 70 70 70 70 70 70 70 70 70 70 70 70 70	1 5F 66 65 68 73 50 73 64 65 24 65 24 65 16 6F 41 2F 69 4C 70 63 3B 45 76	2 6D 65 30 70 55 2E 6C 54 2F 4D 2F 4D 2F 5B 72 43 69 6F 4C 2F 68 01 01 6F	<pre> Õ123456789ABCDEF012 Ép%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[[Lphp/runtime/Memor y;\$CALL_FUNC_CAC HE,Lphp/runtime/i nvoke/cache/Functio nCallCache;\$CALL _METH_CACHE*Lphp/ runtime/invoke/cache \$CALL_PROP_CACHE. \$CALL_</pre>
Startup 0000h: 0013h: 0026h: 0039h: 004Ch: 005Fh: 0072h: 0085h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 0088h: 010Ah: 0126h: 0130h: 0130h: 0143h: 0156h: 0169h: 018Fh: 0185h: 0188h:	0 6F 344 34 72 50 6D 70 8D 70 70 70 70 70 70 70 70 70 70 70 70 70	Mai 1 5FE 644 333 5F 722 65 444 69 69 68 68 68 68 68 68 68 68 68 68 68 68 68	For 2 BA 755 655 633 755 655 633 755 655 633 755 656 677 657 670 670 011 600 701 011 616 701 617 618 610 701 611 612 613 614 615 616 617 618 619 620 621 621 621 6224 420	BE 6C 30 6C 6C 6E 00 76 65 5C 01 2F 00 2F 00 00 6F 68 00 00 6F 68 00 00 6F 68 00 00 6F 68 00 00 6F 68 00 00 76 67 00 76 76 76 76 76 76 76 76 76 76 76 76 76	4 000 655 611 6F 744 033 655 502 666 000 533 102 544 155 722 700 100 202 655 665 665 665 674 408 744 155 742 740 100 100 100 100 100 100 100 1	5 5 63 73 69 01 6C 73 6F 73 6F 73 6F 73 6F 5B 79 2F 24 4C 2F 24 4C 2F 5B 6D 68 84C 70	6 60 35 75 6D 00 4E 72 24 72 24 72 4C 3B 72 43 70 63 61 43 65 6F 4C 2F	7 32 64 62 72 65 47 65 63 60 46 69 70 63 70 01 75 41 63 70 01 75 41 63 41 25 64 55 72	8 01 30 65 65 2F 43 78 5F 73 4E 68 68 65 68 68 65 68 68 00 6E 40 70 63 68 3 69 43 50 75	9 36 31 30 6C 3A 74 67 5C 01 67 70 49 70 05 74 40 2F 68 65 48 65 48 65 48 65 48 65 48 65 48 65	A 01 34 63 07 61 50 65 4D 00 3B 2F 6E 2F 24 69 5F 72 65 3B 45 76 6C 4F 74	B 00 39 66 55 72 6E 61 12 8 8 8 72 66 72 41 6D 46 75 2F 01 6F 6C 50 69	C 36 31 39 01 67 73 6F 65 69 40 075 6F 75 6F 75 65 55 6E 46 00 00 6B 43 5F 6D	D 24 39 38 01 2F 65 6A 72 6E 6A 05 6E 3B 6E 3B 6E 2F 4E 75 10 2A 65 61 43 65	E 70 363 33 72 65 61 46 61 01 74 01 74 40 40 43 69 6E 24 4C 2F 63 41 2F	F 68 66 35 18 62 73 63 63 74 65 60 69 00 69 01 65 5 F 6D 63 43 70 63 88 43 68 843 69	0 70 37 37 70 6F 5C 74 65 72 61 60 40 6D 6D 6D 6D 6D 6D 65 74 41 68 61 65 548 66	1 5F 66 65 68 73 50 73 64 65 24 65 24 65 16 6F 41 2F 69 4C 70 63 3B 45 76	2 6D 65 30 70 55 2E 6C 54 2F 4D 2F 4D 2F 5B 72 43 69 6F 4C 2F 68 01 01 6F	<pre> O123456789ABCDEF012 Êp%26\$php_m odule_md0649196f7fe 43e0ac5be1cf98357e0 4_closure0php /runtime/lang/Closu reGC:\Users\Pk \DevelNextProjects\ mine\src_generated\ mio\forms\MainForm. php\$FNLjava/l ang/String;\$T RC[Lphp/runtime/ env/TraceInfo;\$M EM[Lphp/runtime/ Memory;\$AMEM[[Lphp/runtime/Memor y;\$CALL_FUNC_CAC HELphp/runtime/i nvoke/cache/Functio nCallCache;\$CALL _METH_CACHE*Lphp/ runtime/invoke/cach e/MethodCallCache;. \$CALL_PROP_CACHE. </pre>

The decompiled code is still hard to read. As a first step I restored the strings. All of them are in an array called **\$MEM**. Replacing the array access **\$MEM[X]** with the actual value in the array will improve readability of the code. I achieved this with a python snippet.

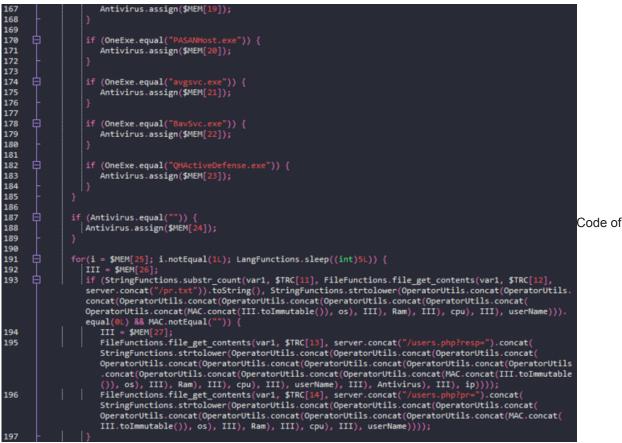
As a second step I replaced methods like assign and concat with operators. E.g., this can be done using regex and capture groups. See table below for replacements. The replacement for one operator must be done several times until all nested calls are replaced. The order must be preserved.

All analysed JPHP samples in this article can be decompiled to Java in the same fashion.

Find	Replace
$\label{eq:operatorUtils} OperatorUtils (([^,]+),([^)]+)) \\$	\1 + \2
\.assign\(([^\)]+)\)	= \1

Find	Replace
Memory\.assignRight\((.+),([^)]+)\);	\2 = \1
\.equal\(([^\)]+)\)	== \1
\.notEqual\(([^\)]+)\)	!= \1
\.concat\(([^\)]+)\)	+ \1
StringMemory\.valueOf\(([^)]+)\)	\1
\.toImmutable\(\)	
StringFunctions\.strtolower\(([^\)]+)\)	\1
LongMemory\.valueOf\(([^\)]+)\)	\1

There is still room for improvement but after the replacements the resulting code is readable without pain.



klient.exe[5] before deobfuscation

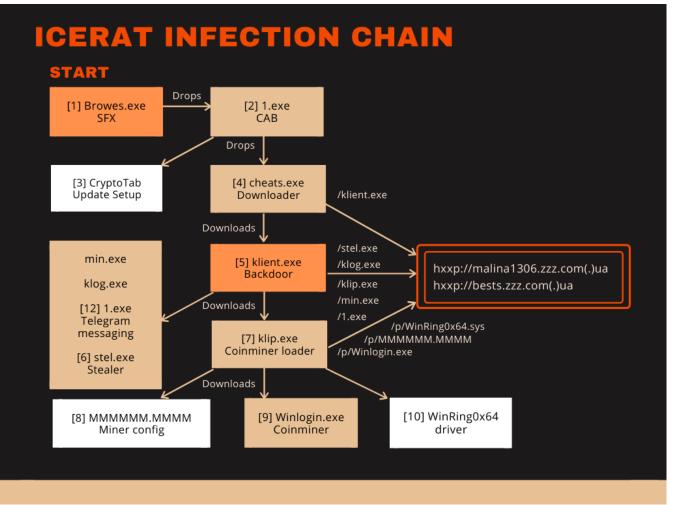


klient.exe[5] after deobfuscation

Infection chain and components

IceRat consists of several small components instead of putting all functionality into one file. As a result most of these files may not attract any attention if their context is missing. E.g., a downloader is only malicious if the downloaded file is malware. If information about the downloaded file is missing and cannot be inferred, there is no reason to detect the downloader as malware.

The chain of infection and related files is in the graphic below. White boxes show non-malicious files. At least four of these files are JPHP EXE files, namely **cheats.exe**^[4], **1.exe**^[12], **klient.exe**^[5] and **klip.exe**^[7]. The main component of IceRat is **klient.exe**^[5].



Infection chain and components of IceRat

According to McMcbrad the first IceRat sample came from a malicious document for which he didn't keep a hash or file. The first part of the chain that I could find is **Browes.exe**^[1] which may have been distributed as trojanized software download for CryptoTab. **Browes.exe** is a selfextracting WinRAR archive that drops and executes the Windows Cabinet file **1.exe**^[2].

The Windows Cabinet file is also a dropper for two more files, namely a non-malicious setup^[3] for CryptoTab software, and a malware downloader named **cheats.exe**^[4]. CryptoTab is a browser with mining features, but its installation is not silent. The affected user will see the browser setup window (see image below) which is why I assume CryptoTab is provided as a lure. To summarize: The infection chain starts with a downloader in a trojanized dropper in a dropper.

Connecting to the Internet...



The JPHP file **cheats.exe**^[4] has the project name **droper** (sic). It accesses IceRat's main server to download the backdoor **klient.exe**^[5]. It chooses randomly one of the following names from a list:

- System
- Jawas
- WindowsShell
- exploler
- antiDrw
- antiSsl
- ADB
- Microsoft
- system

Then it will write the file into the following locations:

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\.<name>.exe
- c:\Windows\Temp\.<name>.exe
- d:\Windows\Temp\<name>.exe

This file, klient.exe, is the main component that will be controlled by the server.

Command and Control

Although the name IceRat indicates a remote access trojan, the current malware is better described as a backdoor. Features for actual remote control, e.g., moving the mouse or typing the keyboard, are missing.

The command and control happens by periodically checking the contents of certain files on the malware server. E.g. **klient.exe**^[5] will check the content of the file hxxp://malina1306.zzz.com.ua/**dow_stil.txt**. If that file contains a line that matches the string **<MAC>:<OS>:<RAM>:rocessor>:<username> for the infected system (see image below), klient.exe** will download the stealer^[6] from hxxp://malina1306.zzz.com.ua/**stel.exe** and save it to **c:\Windows\Temp\.Browser.exe**.

Similarly, a coinminer downloader^[7] will be obtained if hxxp://malina1306.zzz.com.ua/**dow_klip.txt** has a corresponding line for the infected system. It will be downloaded from hxxp://malina1306.zzz.com.ua/**klip.exe** to **c:\Windows\Temp\.Chrome.exe.**

The file 1.exe^[12] is downloaded from hxxp://malina1306.zzz.com.ua/**1.exe** or hxxp://bests.zzz.com.ua/**1.exe** and saved under a randomly generated name by creating a random number between 10000 and 1000000. The resulting file location is **c:\Windows\Temp\.<10000-1000000>.exe**. This component communicates via Telegram to the malware operator.

Two more files are referenced in klient.exe but don't exist anymore: hxxp://malina1306.zzz.com.ua/min.exe would be downloaded to c:\Windows\Temp\.Jawaw Se binar.exe. hxxp://malina1306.zzz.com.ua/klog.exe would be downloaded to c:\Windows\Temp\.Windows Push.exe. Based on the filenames one would assume that min.exe should be the coinminer whereas klip.exe rather sounds like a clipbanker. But that was not provided by the server. klog.exe might have been a keylogger.

	/-ь.1:3.82:intei(r) core(tm) 15-3210m cpu @ 2.50gnz:андреи	
	10-10.0:7.45:amd a6-9225 radeon r4, 5 compute cores 2с 3g:домашний 8.1-6.3:7.98:intel(r) core(tm) i5-2310 сри @ 2.90ghz:admin	
	10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:	
	10-10.0:3.86:intel(r) core(tm) i5-2430m cpu @ 2.40ghz:user	
	10-10.0:3.48:amd a8-3820 apu with radeon(tm) hd graphics:001-pc	
	10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:0	
	10-10.0:5.9:intel(r) pentium(r) cpu 2020m @ 2.40ghz:hp	
	7-6.1:4:amd athlon(tm) ii x3 450 processor:пользователь	
	10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:	
	7-6.1:3.91:intel(r) pentium(r) cpu b940 @ 2.00ghz:админ	
	10-10.0:7.96:amd phenom(tm) ii x4 965 processor:neo-4	
	10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:ф 10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:ф	
	8.1-6.3:7.88:intel(r) core(tm) i3-7020u cpu @ 2.30ghz:nik p	
	10-10.0:3.22:amd a8-6410 apu with amd radeon r5 graphics:nExa	
	7-6.1:5.98:amd a8-3820 apu with radeon(tm) hd graphics:user	
	8.1-6.3:7.91:intel(r) core(tm) i5-2450m cpu @ 2.50ghz:home 7-6.1:5.99:intel(r) core(tm) i5 cpu 750 @ 2.67ghz:администратор jetin	
		ng
	7-6.1:4:pentium(r) dual-core cpu e5400 @ 2.70ghz:user 10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:ф	
	10-10.0:0.91:amd a8-7410 apu with amd radeon r5 graphics:ф 8.1-6.3:7.89:intel(r) pentium(r) сри g4400 @ 3.30ghz:алексей	
	10-10.0:15.95:intel(r) core(tm) i3-9100f cpu @ 3.60ghz:galactic lol	
	10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:	
	10-10.0:0.91:amu a8-7410 apu with amu radeon r5 graphics:ф 8.1-6.3:7.81:intel(r) celeron(r) n4120 сри @ 1.10ghz:руслан	
	10-10.0:5.98:intel(r) cereron(r) h4120 cpu @ 1.10ghz:pychaH 10-10.0:5.98:intel(r) core(tm) i3-2100 cpu @ 3.10ghz:user2	
	10-10.0:7.94:amd a10-6700 apu with radeon(tm) hd graphics:user	
	8.1-6.3:7.88:intel(r) core(tm) i7-3537u cpu @ 2.00ghz:wesel	
	10-10.0:3.91:intel(r) core(tm) 17-35370 cpu @ 2.60ghz:wese1	
	7-6.1:2:pentium(r) dual-core сри е5700 @ 3.00ghz:камила	
	8.1-6.3:7.92:intel(r) pentium(r) gold g5400 cpu @ 3.70ghz:RaMu/A	
	10-10.0:5.59:intel(r) pentium(r) cpu 2020m @ 2.40ghz:владелец	
	10-10.0:3.91:intel(r) core(tm) i5-4300m cpu @ 2.60ghz:egort	
	8.1-6.3:7.97:intel(r) core(tm) i5-2380p cpu @ 3.10ghz:dbrnj	
windows	8.1-6.3:3.96:intel(r) core(tm) i3-3220 сри @ 3.30ghz:ринат	
	8.1-6.3:6:amd athlon(tm) 64 x2 dual core processor 3600 :илья	
	8.1-8.5:8:amd atrion(tm) 64 x2 dual core processor 5000 :илья 10-10.0:6.91:amd a8-7410 apu with amd radeon r5 graphics:ф	
	MACS: SPAM: and above and and radeon regraphics of	_

of infected clients, format: <MAC>:<OS>:<RAM>:<processor>:<username>. The MAC address is obfuscated by us.

Stealer and coinminer

Unlike other IceRat components the stealer^[6] is written in Python 3 and was compiled with PyInstaller to an EXE file. It steals credentials from the following browsers:

- Firefox
- Yandex
- Filezilla
- Chrome
- Amigo
- kometa
- Orbitum
- Chromium
- K-Melon

The coinminer downloader obtains the configuration file **MMMMMM.MMMM**^[8], the driver **WinRing0x64.sys**^[10] by OpenLibSys.org, as well as the coinminer **Winlogin.exe**^[9] from hxxp://malina1306.zzz.com.ua/p/. The configuration shows the user **dimargo2003@gmail.com**.

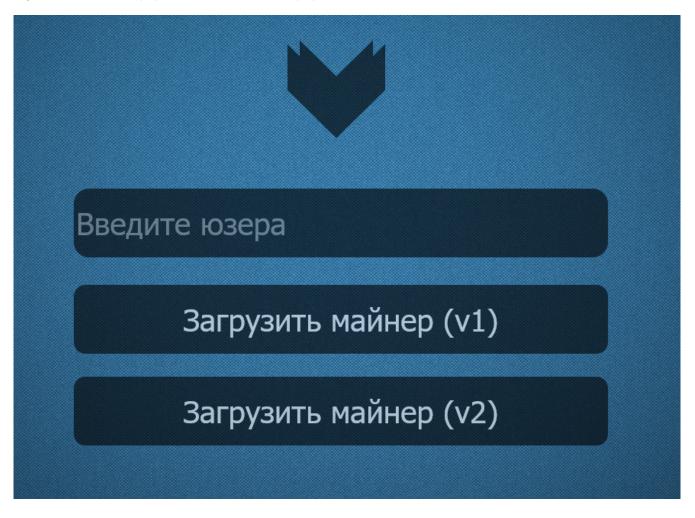
At the time of writing this article the stealer and the coinminer are well-detected with more than 40 detections on Virustotal. This is a remarkable contrast to the low detection rates of the JPHP components.

2	① 2 engines detected this file		$C \approx \pm 3$
7 68 2 X Community Score	8a3dd23d0d47114c06ace407b93a3403e33b8cb2e243a548f4c7158b4d340165 checks-network-adapters checks-user-input direct-cpu-clock-access ftp-communication overlay peexe	3.48 MB 2020-11-27 15:05:38 UTC Size 1 minute ago runtime-modules	e exe
41	① 41 engines detected this file		$C \approx \overline{7}$
/72		5.12 MB 2020-11-18 11:41:29 UT	c SL EXE

Detection rate of Telegram communicator[12] (top) is much lower than the coinminer[9] (bottom), although the coinminer was scanned 1.5 weeks ago

Hosting domain

The malware host and CnC server hxxp://malina1306.zzz(.)com.ua also provides a Russian website with two buttons and a text field. The field seems to require a username because the text is translated to "Enter User". The buttons say "Download miner (v1)" and "Download miner (v2)".



Severity and targeted regions

IceRat has gone unnoticed for longer than usual. I attribute this mainly to the choice of using JPHP as well as the fragmentation of the malware's features into many small files. "Small" does not mean the size of the files here. These are comparably large because they carry the JPHP runtime with them. "Small" rather refers to the amount of features they have or capability of the code. If one file does only little on its own, it won't show malicious behaviour to an automated analysis system. That way it stays undetected.

The log files that are used to communicate with the server contain more than 200 entries with different systems. Many usernames of the infected systems are kyrillic which indicates that mostly East European and Russian regions are affected.

Antivirus engines may have to upgrade their engines to support .phb files as well as take a holistic approach for automated analysis systems to detect fragmented malware.

Indicators of compromise

Description	Filename	SHA256
[1] PE SFX containing [2]	Browes.exe	6a7cc0ab2cfaa9457f47d5e21ef41e56800b37d7e5bfe69b296545bff95fdf96
[2] Windows Cabinet file, containing [3] [4]	1.exe	592c60435099477a2656784f28dd31523a91ebf9dd348827d9120a4b411ab6c9
[3] CryptoTab setup file	BrowserSetup.exe	3c63d911e4f911f2ba6f411e93ba850091aac9c6c4c962eee914358ac1ac8e0c
[4] Backdoor downloader, JPHP	cheats.exe	0161540edfceb643389a28ebe7d1092639596325e8f40defe52192ab999d3d36
[5] IceRat backdoor, JPHP	klient.exe	cebee34d5f0292befca058537bf2320dd1492afa26fb9af471155c9332046320
[6] Stealer, Python	stel.exe	fdff65ae03fab7bfd6f943833bf7aa16f6ada9219786995df9ef7127ab9aa93d
[7] Coinminer downloader, JPHP	klip.exe	06a10cf99cc7c2d2ebc3e41300404e8f5816eb31a869d22835ade3a381199c0b
[8] Miner config, JSON file	MMMMMM.MMMM	c0a3b67b4056aeefd086edbe0c6ccb5fa7835505ef4ebe6220e5f914012e9e32
[9] Coinminer	Winlogin.exe	e656c75017a557ad342dfa95d76e1b36b54a004825615f721a5dd51431899e90
[10] WinRing0x64 driver	WinRing.sys	11bd2c9f9e2397c9a16e0990e4ed2cf0679498fe0fd418a3dfdac60b5c160ee5
[11] IceRat backdoor, older sample	lceRat.exe	29c63169ffc5dfacef9245c0f3afae987525f9b164a17133e51f598d3b75120d
[12] Telegram communicator, JPHP	1.exe	8a3dd23d0d47114c06ace407b93a3403e33b8cb2e243a548f4c7158b4d340165

