

# BiBi Wiper: malware analysis

www.swascan.com



# Sommario

Introduction	3
Static analysis and malware assessment	4
Dynamic analysis and second malware assessment	15
Debugging	
IOCs:	
YARA Rule	
CONCLUSIONS:	50
References:	50



## Introduction

BiBi Wiper is a "destructive" malware used in the Israel-Hamas conflict by activists of the Sunni terrorist group. As of 30 October 2023, the threat has also been infecting Unix operating systems, although a more widely used variant is also Windows, which is analyzed in this article.

The artefact, similar to what happened during the Russian-Ukrainian war, was used as a hybrid warfare tool to carry out destructive actions against Israel's critical infrastructures, effectively contributing to Hamas's military and strategic offensive. The threat, by performing an overwriting and "locking" phase of the files (but without demanding a ransom), places BiBi Wiper in a different condition from a ransomware threat. The only objective of the wiper is to make the data of target systems inaccessible and unusable. [0]



### Static analysis and malware assessment

The analyzed sample has the hash **e26bba0304f14ef96beb60376791d32c** and was developed in C++.

Detect It Easy v3.04 [Windows 10 Version Detect It Easy v3.04 [Windows 10 Vers	on 1809](x86_64)		_	
File name C:/Users/IEUser/Desktop/New folder/40417e	e937cd244b2f928150cae6fa0eff55	51fdb401ea072f6ecdda67a	a747e17.exe	
File type Entry point		Base address		File info
PE64 <b>* 000000014000</b>	0ab10 > Disasm	00000014000000	0 Memory map	MIME
PE Export	Import Resources	.NET TLS	Overlay	Hash
Sections Time date stamp	Size of image	Resources		Strings
0007 > 2023-10-21 17	7:24:41 <b>00039000</b>	Manifes	t Version	Entropy
Scan	Endianness Mode	Architecture	Туре	Hex
Automatic 🔹	LE 64-bit	AMD64	Console	Signatures
<ul> <li>PE64 Compiler: Microsoft Visual C/C++ Linker: Microsoft Linker(14.29**)[C</li> </ul>			S ? S ?	Demangle
				Shortcuts
Signatures	Deep scan	cursive scan 🗌 All types		Options
			Scan	About
Directory 100%	> Log	260 msec		Exit

File name: C:/Users/IEUser/Desktop/New folder/40417e937cd244b2f928150cae6fa0eff5551fdb40lea072f6ecd Size: 207872(203.00 kB) MD5: e26bba0304f14ef96beb60376791d32c SHA1: 24f6785ca2e82dldld61f4cb01d5e753f80445cf Entropy: 6.19335(not packed) Operation system: Windows(Vista) Architecture: AMD64 Mode: 64-bit Type: Console Endianess: LE Entry point(Address): 000000014000ab10 Entry point(Offset): 9f10 Entry point (Relative address): ab10 Entry point (Bytes): 4883ec28e89f0600004883c428e972feffffcccc4883ec284d8b4138488bca498bdl Entry point (Signature): 4883ec..e8......4883c4..e9.....cccc4883ec..4d8b41..488bca498bd1 Entry point (Signature) (Rel): 4883ec..e8\$\$\$\$\$48895c24..55488bec4883ec..488b05......48bb.....



In the *.rsrc* section (which contains the details of the *manifest* metadata file and other resources) we can see an execution setting of *"asInvoker"*, so the threat is launched with the same privileges and security permissions as the parent process.

																	_		Save	×
Туре					M	lemory	r map													
PE64							Off					dress			Size			Name		
File offset		000000	0000	33331					800		0000 i 00001				00000000000000000000000000000000000000		Section(			
Virtual address						00000			000		D0001				000000000000000000000000000000000000000		Section(			
_		000000	01400	37120		rrrrr					00001				000000000000000000000000000000000000000		Section(			
Relative virtua	l address	000000	00000	37120		00000			000		00001				000000000000000020		Section(			
Mode	Endianness	,	Archited	ture		00000					00001				0000000000002		Section(			
64-bit	LE		AMD6	54		rrrrr		fff		0000	00001	4003	6200	00	000000000000e		Section(			
						00000	0000	0032	200	000	00001	4003	7000	00	0000000000002		Section(			
						fffffff	m	fff		0000	00001	4003	7200	00	00000000000e	00	Section(	[5)['.rs	rc']	
						00000	0000	00324	400	0000	00001	4003	8000	00	800000000000	00	Section(	(6)['.re	loc']	
										0000	00001	4003	8800	00	80000000000	00	Section(	(6)['.re	loc']	
										0000	00001									
lex											00001									
ex Address	Hex								••••					s	ymbols					
		65 63	75 7	2 69									20	L						
Address	3c 73	65 63 3c 72			9 74	79		Od	0a	20		20 2		L	ymbols	y>				
Address 0003:2320	3c 73 20 20		65 7	1 75	ə 74 5 65	79 73	3e 74	0d 65	0a 64	20 50	20 72	20 2	76		ymbols <securit< td=""><td>y&gt; st</td><td></td><td>L V</td><td></td><td></td></securit<>	y> st		L V		
Address 0003:2320 0003:2330	<mark>3c</mark> 73 20 20 69 6c	3c 72	65 7 65 7	1 75 3 3e	9 74 5 65 8 Oc	79 73 0a	3e 74 20	0d 65 20	0a 64 20	20 50 20	20 72	20 : 69 <sup>:</sup> 20 :	76 20		ymbols <securit <reque< td=""><td>y&gt; st</td><td>edPri</td><td></td><td></td><td></td></reque<></securit 	y> st	edPri			
Address 0003:2320 0003:2330 0003:2340	3c         73           20         20           69         6c           20         3c	3c 72 65 67	65 7 65 7 71 7	1 75 3 3e 5 65	9 74 5 65 9 00	79 73 0a	3e 74 20 65	0d 65 20 64	0a 64 20 45	20 50 20 78	20 72 20 65	20 2 69 <sup>-</sup> 20 2 63 <sup>-</sup>	76 20 75	l	ymbols <securit <reque ileges&gt;.</reque </securit 	y> st te	edPri dExec	u		
Address 0003:2320 0003:2330 0003:2340 0003:2350	3c         73           20         20           69         6c           20         3c           74         69	3c 72 65 67 72 65	65 7 65 7 71 7 4c 6	1 75 3 36 5 65 5 70	9 74 5 65 9 00 5 73 5 65	79 73 0a 74 6c	3e 74 20 65 20	0d 65 20 64 6c	0a 64 20 45 65	20 50 20 78 76	20 72 20 65 65	20 2 69 2 20 2 63 2 62 3	76 20 75 3d	-	ymbols <securit <reque ileges&gt;. <reques< td=""><td>y&gt; st te</td><td>edPri dExec level</td><td>su L=</td><td></td><td></td></reques<></reque </securit 	y> st te	edPri dExec level	su L=		
Address 0003:2320 0003:2330 0003:2340 0003:2350 0003:2360	3c         73           20         20           69         6c           20         3c           74         69           27         61	3c 72 65 67 72 65 6f 6e	65 7 65 7 71 7 4c 6 6e 7	1 75 3 36 5 65 5 76	9 74 5 65 9 00 5 73 5 65 5 61	79 73 0a 74 60 65	3e 74 20 65 20 72	0d 65 20 64 6c 27	0a 64 20 45 65 20	20 50 20 78 76 75	20 72 20 65 65 69	20 2 69 2 63 2 62 3 41 0	76 20 75 3d 63		ymbols <securit <reque ileges&gt;. <reques tionLeve</reques </reque </securit 	y> st te	edPri dExec level ' ui <i>l</i>	su L= Ac		
Address 0003:2320 0003:2330 0003:2340 0003:2350 0003:2360 0003:2370 0003:2380 0003:2390	3c         73           20         20           69         6c           20         3c           74         69           27         61           63         65           0a         20	3c 72 65 67 72 65 6f 6e 73 49 73 73 20 20	65 7 65 7 71 7 4c 6 6e 7 3d 2 20 2	1 75 3 3e 5 65 5 76 6 61 27 66 20 20	9 74 5 65 9 00 5 73 5 65 6 1 5 61 0 30	79 73 0a 74 60 65 60 21	3e 74 20 65 20 72 73 72	0d 65 20 64 6c 27 65 65	0a 64 20 45 65 20 27 71	20 50 20 78 76 75 20 75	20 72 20 65 65 69 2f 65	20 2 69 2 63 2 6c 3 41 0 3e 0	76 20 75 3d 63 0d 74	i i	ymbols <securit <reque ileges&gt;. <reques tionLeve 'asInvok cess='fa &lt;</reques </reque </securit 	y> st: te: l.er ls: /r:	edPri dExec level ' ui e' /: eques	cu L= Ac >.		
Address 0003:2320 0003:2330 0003:2340 0003:2350 0003:2360 0003:2370 0003:2380 0003:2390	3c         73           20         20           69         6c           20         3c           74         69           27         61           63         65           0a         20           65         64	3c 72 65 67 72 65 6f 6e 73 49 73 73 20 20 50 72	65 7 65 7 71 7 4c 6 6e 7 3d 2 20 2 69 7	1 7: 73 3e 75 6: 75 7: 76 6: 77 6: 70 20 76 6:	9 74 5 65 5 73 5 65 5 61 5 61 0 30 9 60	79 73 0a 74 6c 65 6c 2f 65	3e 74 20 65 20 72 73 72 67	0d 65 20 64 65 65 65 65	0a 64 20 45 65 20 27 71 73	20 50 20 78 76 75 20 75 3e	20 72 20 65 65 69 2f 65 0d	20 2 69 2 63 2 60 3 60 3 41 0 3e 0 73 2	76 20 75 3d 63 0d 74 20	i i	ymbols <securit <reque ileges&gt;. <reques tionLeve 'asInvok cess='fa <edprivil< td=""><td>y&gt; te l r ls /r</td><td>edPri dExec level ' ui/ e' /&gt; eques es&gt;</td><td>eu L= Ac &gt;. st</td><td></td><td></td></edprivil<></reques </reque </securit 	y> te l r ls /r	edPri dExec level ' ui/ e' /> eques es>	eu L= Ac >. st		
0003:2320 0003:2330 0003:2340 0003:2350 0003:2360 0003:2370 0003:2380 0003:2390	3c         73           20         20           69         6c           20         3c           74         69           27         61           63         65           0a         20           65         64           20         20	3c 72 65 67 72 65 6f 6e 73 49 73 73 20 20	65 7 65 7 71 7 4c 6 6e 7 3d 2 20 2 69 7 2f 7	1 75 3 36 5 65 5 76 6 61 27 66 20 20 76 65 73 65	<ul> <li>74</li> <li>5</li> <li>65</li> <li>73</li> <li>5</li> <li>65</li> <li>61</li> <li>3</li> <li>63</li> </ul>	79 73 0a 74 60 65 62 21 5 5 75	3e 74 20 65 20 72 73 72 67 72	0d 65 20 64 65 65 65 65	0a 64 20 45 65 20 27 71 73 74	20 50 20 78 75 20 75 3e 79	20 72 20 65 65 69 2f 65 0d 3e	20 2 69 2 63 2 63 2 66 2 66 2 66 2 66 2 73 2 73 2 73 2 73 2 73 2 73 2 73 2 73	76 20 75 3d 63 0d 74 20 0a	i i	ymbols <securit <reque ileges&gt;. <reques tionLeve 'asInvok cess='fa &lt;</reques </reque </securit 	y> te l er ls /r eg	edPri dExec level ' uiA e' /> eques es> ity>	u L= Ac ≻. st		

The functions imported via the *KERNEL32.dll* library refer to enumeration drives, creation and opening of processes, and calling up external libraries via *LoadLibraryA*:



Di PE							-		×
Reload		Hex	Disasm	Strings	Memory map	Entropy	Heuristic scan	📕 Rea	adonly
Info Hex Disasm	Hash 64 0000031		ash 32 <b>9aa5e843</b>						
Hash Strings Signatures	ginalFi 0 0002f9	irstThi neDateS c0 00000000	tan IrwarderCha	Name 0002fd80	FirstThunk 00022000	Hash 58dec74f	KERNEL32.dll	=	
Memory map Entropy Heuristic scan IMAGE DOS HEADER									
✓ IMAGE_NT_HEADERS IMAGE_FILE_HEADER ✓ IMAGE_OPTIONAL_HEADER IMAGE_DIRECTORY_ENTRIES	*								
RICH Signature Sections							,	_	
Import		Thunk	Ordinal	Hint			Nar	ne	•
<ul> <li>Resources</li> <li>Manifest</li> </ul>	0 000000	000002fce0		0271	GetLogicalDr	ives			
Exceptions		000002fcf4		0238	GetDriveType	A			
Relocs		000002fd04		026a	GetLastError				
Debug TLS		000002fd14		00e3	CreateProces				
Load config		000002fd26		059e	TerminatePro				
		000002fd3a		0412	OpenProcess				
		000002fd48		03c8	LoadLibraryA				
	7 000000	000002fd58		02b8	GetProcAddr	ess			•

De	Strings

\_

Filter			
		ANSI	👻 🔲 UTF8 📒 Unicode 📒 C Strings 5 💲 Save Search
	Offset 🔻	Size Typ	e String e
670	0002bd48	00000007 A	.data\$r
671	0002bd58	00000008 A	.data\$rs
672	0002bd7c	00000006 A	.pdata
673	0002bd8c	00000006 A	_RDATA
674	0002bd9c	00000008 A	.rsrc\$01
675	0002bdb0	00000008 A	.rsrc\$02
676	0002bdfc	00000006 A	060p00
677	0002e6e2	00000010 A	GetLogicalDrives
678	0002e6f6	A b0000000	GetDriveTypeA
679	0002e706	000000c A	GetLastError
680	0002e716	0000000e A	CreateProcessA
681	0002e728	00000010 A	TerminateProcess
682	0002e73c	000000ь А	OpenProcess
683	0002e74a	000000c A	LoadLibraryA
684	0002e75a	000000e A	GetProcAddress
685	0002e76c	0000013 A	GetCurrentProcessId
686	0002e780	000000c A	KERNEL32.dll
687	0002e790	000000ь А	CloseHandle
688	0002e79e	00000015 A	WaitForSingleObjectEx
689	0002e7b6	00000005 A	Sleep
690	0002e7be	000000e A	SwitchToThread
691	0002e7d0	00000012 A	GetCurrentThreadId
692	0002e7e6	00000011 A	GetExitCodeThread
			Close



Threads management functions are used to manage competitive executions:

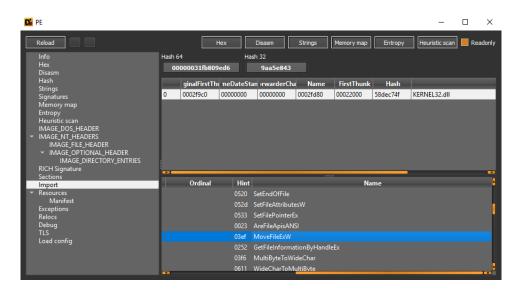
Di PE							-		×
Reload		Hex	Disasm	Strings	Memory map	Entropy	Heuristic scan	📕 Rea	adonly
Info Hex Disasm Hash	Hash 64 000000311	b809ed6	sh 32 9aa5e843						
Hash Strings Signatures Memory map	ginalFi 0 0002f9c	stThi neDateSt 0 00000000	an inwarderCha 00000000	Name 0002fd80	FirstThunk 00022000	Hash 58dec74f	KERNEL32.dll	=	
Entropy Heuristic scan IMAGE_DOS_HEADER									
<ul> <li>IMAGE_NT_HEADERS</li> <li>IMAGE_FILE_HEADER</li> <li>IMAGE_OPTIONAL_HEADER</li> </ul>									
IMAGE_DIRECTORY_ENTRIES RICH Signature Sections								_	
Import Resources	Ordi	nal Hint 058f			Na	me			
Manifest		0587	Sleep SwitchToThrea						
Exceptions			GetCurrentThr						
Relocs Debug		0225	GetExitCodeTh						
TLS		028e	GetNativeSyste						
Load config			LocalFree						
		01af	FormatMessag	еA					
	•	00ce	CreateFileW						•

Following are file enumerations loops and file attributes, as well as pointing using the *SetFilePointerEx* function. The latter is widely used by threats with external file referencing functionality as it allows more granular and specific management of the pointing location.

Di PE							-		×
Reload	Hex		Disasm	Strings	Memory map	Entropy	Heuristic scan	📕 📕 Rea	donly
Info Hex Disasm	Hash 64 00000031fb809ed6		sh 32 9aa5e843						
Hash Strings	ginalFirstThi me	DateSt	an )rwarderCha	Name	FirstThunk	Hash		_	
Signatures	0 0002f9c0 000	000000	00000000	0002fd80	00022000	58dec74f	KERNEL32.dll		
Memory map Entropy Heuristic scan IMAGE_DOS_HEADER * IMAGE_TILE_HEADER * IMAGE_FILE_HEADER IMAGE_DIRECTORY_ENTRIES RICH Signature Sections	T.						,		
Import	Ordinal	Hint			Na	me			•
✓ Resources		0184	FindFirstFileEx\						
Manifest Exceptions			FindNextFileW						
Relocs		024c	GetFileAttribut	esExW					
Debug TLS			SetEndOfFile						
Load config			SetFileAttribute						
			SetFilePointerE						
			AreFileApisAN						
	•	03ef	MoveFileExW	_					•



Files are renamed with the extension **.BiBi** after they have been made inaccessible through an overwriting process:



Details of the performance counter and execution frequency of CPU components are also obtained, and this information can allow a threat to identify a possible virtualized environment, such as virtual machines or sandboxes:

Di PE							-		×
Reload		Hex	Disasm	Strings	Memory map	Entropy	Heuristic scan	📕 Rea	adonly
Info Hex Disasm	Hash 64 00000031fb8		sh 32 9aa5e843						
Hash Strings	ginalFirst	Thi neDateSta	an )rwarderCh	a Name	FirstThunk	Hash			
Signatures	0 0002f9c0	00000000	00000000	0002fd80	00022000	58dec74f	KERNEL32.dll		
Memory map Entropy									
Heuristic scan									
IMAGE_DOS_HEADER VIMAGE NT HEADERS									
IMAGE FILE HEADER									
<ul> <li>IMAGE_OPTIONAL_HEADER</li> <li>IMAGE_DIRECTORY_ENTRIES</li> </ul>	-								
RICH Signature Sections								_	
Import	Ordina	l Hint			Na	me			-
<ul> <li>Resources</li> <li>Manifest</li> </ul>		03f6	MultiByteToW	ideChar					
Exceptions			WideCharToM						
Relocs			QueryPerform						
Debug TLS		0453 0370	QueryPerform InitializeSRWL						
Load config			ReleaseSRWLo						
			AcquireSRWLo						
	-		EnterCriticalSe						•

Note the debugger checking function *IsDebuggerPresent*, which avoids monitoring and tracking the execution of the process itself through breakpoints and code browsing tools:



De PE							-	n x
Reload		lex	Disasm	Strings	Memory map	Entropy	Heuristic scan	Readonly
	Hash 64	Has	h 32					
Hex Disasm	0000031fb809	ed6	9aa5e843					
Hash	ninalFirstTh	neDateSta	n •rwarderCha	Name	FirstThunk	Hash		
Strings Signatures		00000000	00000000	0002fd80	00022000	58dec74f	KERNEL32.dll	
Memory map								
Entropy								
Heuristic scan IMAGE DOS HEADER								
IMAGE_NT_HEADERS								
IMAGE_FILE_HEADER VIMAGE_OPTIONAL_HEADER								
IMAGE_DIRECTORY_ENTRIES								
RICH Signature Sections								
Import	Ordinal	Hint			Na	me		•
<ul> <li>Resources</li> </ul>			SetUnhandledE	exceptionFilte				
Manifest Exceptions			GetCurrentPro	cess				
Relocs		038c	sProcessorFeat	turePresent				
Debug TLS		036f	nitializeSListHe	ead				
Load config			sDebuggerPre					
			GetStartupInfo	W				
			RtlUnwindEx					
	•	04de	RtIPcToFileHea	der				°

The pointer values used are encoded by calling the *EncodePointer* function. Pointers make it possible to refer to further variables and objects within executed functions, in which case there is no precise knowledge of the values and attributes referred to as they are encoded.

De PE							_		×
Reload	н	ex	Disasm	Strings	Memory map	Entropy	Heuristic scan	📕 Re	adonly
Info Hex Disasm	Hash 64 00000031fb809e		h 32 9aa5e843						
Hash Strings Signatures		neDateSta 00000000	n FrwarderCha	Name 0002fd80	FirstThunk 00022000	Hash 58dec74f	KERNEL32.dll	-	=
signatures Memory map Entropy Heuristic scan IMAGE_DOS_HEADER									
<ul> <li>MAGE_UDS_HEADERS</li> <li>✓ IMAGE_NT_HEADERS</li> <li>IMAGE_FILE_HEADER</li> <li>✓ IMAGE_OPTIONAL_HEADER</li> <li>✓ IMAGE_DIRECTORY_ENTRIES</li> </ul>									
RICH Signature Sections							_	_	
Import	Ordinal	Hint			Na	me			•
<ul> <li>Resources</li> <li>Manifest</li> </ul>			SetLastError						
Exceptions			EncodePointer						
Relocs			nitializeCritica	ISectionAndS	pinCount				
Debug TLS			TIsAlloc						
Load config			TIsGetValue						
			TIsSetValue						
		05Ь1							
	•	01b4	FreeLibrary						•••••

In a concurrential context the files are read:



De PE							-		×
Reload		Hex Disa	ism S	trings	Memory map	Entropy	Heuristic scan	📕 Rea	donly
Info	Hash 64	Hash 32							
Hex Disasm	00000031fb809	ed6 9a	aa5e843						
Hash	ninalFirstTh	neDateStan III	warderCha	Name	FirstThunk	Hash			
Strings Signatures	0 0002f9c0			002fd80	00022000	58dec74f	KERNEL32.dll		
Memory map									
Entropy									
Heuristic scan IMAGE DOS HEADER									
IMAGE_NT_HEADERS									
IMAGE_FILE_HEADER VIMAGE_OPTIONAL_HEADER									
IMAGE_DIRECTORY_ENTRIES	:								
RICH Signature Sections									0
Import	Ordinal	Hint			Na	me			•
▼ Resources		05b1 TIsFr	ree						
Manifest Exceptions		01b4 Freel	Library						
Relocs		03ca Load							
Debug TLS		0479 Read							
Load config			iteThread						
			hread						
			LibraryAndEx						
	•	0280 GetN	AoduleHan <mark>dl</mark>	eexw					•

Here are the details of the sections of the Portable Executable in question. The main section appears to be *.text*, which contains the instructions directly executed by the CPU.

										1
Reload			Hex	Disa	sm St	rings Mei	mory map	Entropy	Heuristic scan	Readonly
Info										Save
Hex Disasm		2011		0(0 0		<b></b>	7.12	0.0		
Hash	Name	0002040c		00020600	a nteriokaw 00000400			0000	eloca erOfLinen	
Strings	0 .text		00001000			00000000	00000000		0000	6000020
Signatures	1 .rdata	0000e44e	00022000	0000e600	00020a00	00000000	00000000	0000		40000040
Memory map Entropy	2 .data	000027d0	00031000	00001000	0002f000	00000000	00000000	0000	0000	c0000040
Heuristic scan	3 .pdata	00001e60	00034000	00002000	00030000	00000000	00000000	0000	0000	40000040
IMAGE_DOS_HEADER	4 _RDATA	000000f4	00036000	00000200	00032000	00000000	00000000	0000	0000	40000040
<ul> <li>IMAGE_NT_HEADERS</li> <li>IMAGE FILE HEADER</li> </ul>	5 .rsrc	000001e0	00037000	00000200	00032200	00000000	00000000	0000	0000	40000040
<ul> <li>IMAGE_OPTIONAL_HEADER</li> </ul>	б.reloc	000007e0	00038000	00800000	00032400	00000000	00000000	0000	0000	42000040
IMAGE_DIRECTORY_ENTRIES										
RICH Signature Sections										
Import										
<ul> <li>Resources</li> </ul>										
Manifest										
Exceptions Relocs										
Debug	1									
TLS		-								
Load config	Hex Strings									
	Address	Hex					Symi	bols		
	0000:1000	48 83 ec	28 48 8d	0d 45 13	03 00 e8	64 96 00	00 Н.	. (HE	d	•
	0000:1010	48 8d 0d	e9 03 02	00 48 83	c4 28 e9	dc 9f 00	00 н.	н		
	0000:1020	48 8d 05	79 27 03	00 c3 cc	ce ce ce	cc cc cc	ee H.	.y'		
	0000:1030	48 89 4c	24 08 48	89 54 24	10 4c 89	44 24 18	4c H.	L\$.Н.Т	\$.L.D\$.L	
	0000:1040	89 4c 24	20 53 57	48 83 ec	38 b9 01	00 00 00	48 . L	\$ SWH.	. 8 н	
	0000:1050	8d 7c 24	58 e8 23	e6 00 00	48 8b d8	e8 bf ff	ff . 1	sx.#	. н	
	0000:1060					48 89 7c			.HH. \$	
	0000:1070					38 5f 5b			.н8 [.	
	0000:1080					48 8d 0d			.нн)	
	0000:1090					0b 48 8d			S.HH.H	
	0000.1050	10 02 00	01 04 00	10 00 33	00 20 05	010 10 Ou				
	0000:10a0	08 OF 11	02 e8 8b	ac 00 00	48 8b c3	48 83 c4	20		.нн	



Filter		ANSI		▼ UTF8 Unicode C Strings 5 \$ Save Search
	Offset 🔻	<b>C</b>	<b>T</b>	
22	00021930	Size 0000000b	Type ∆	String bad address
22	00021930	00000013		
23	00021940	00000013 0000000b		bad file descriptor
24				bad message
25	00021968	0000000b		broken pipe
26	00021978	00000012		connection aborted
27	00021990	0000001e		connection already in progress
28	000219Ь0	00000012		connection refused
29	000219c8	00000010		connection reset
30	000219e0	00000011		cross device link
31	000219f8	0000001c		destination address required
32	00021a18	00000013		directory not empty
33	00021a30	00000017	А	executable format error
34	00021a48	000000b		file exists
35	00021a58	0000000e		file too large
36	00021a68	00000011		filename too long
37	00021a80	00000016		function not supported
38	00021a98	00000010		host unreachable
39	00021ab0	00000012		identifier removed
40	00021ac8	00000015		illegal byte sequence
41	00021ae0	00000022		inappropriate io control operation
42	00021b08	0000000Ь		interrupted
43	00021b18	0000000c		invalid seek
44	00021b28	00000008	А	io error

Here the details of concurrential objects and resource management, specifically multithreading and *semaphores*. *Semaphores* objects allow the use of resources with exclusive access, thus preventing simultaneous access by several processes to the same resource:



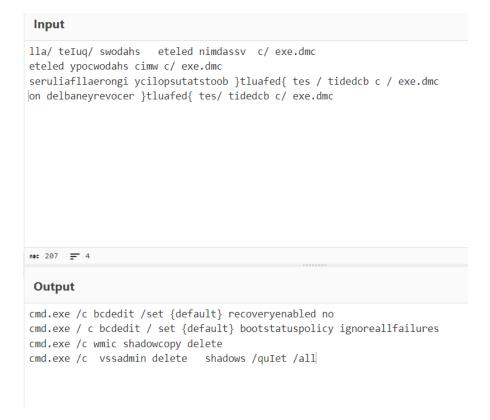
Filter				
		ANSI		🔻 📃 UTF8 📃 Unicode 📃 C Strings 5 💠 Save Search
	Offset 🔻	Size	Туре	String
91	00021f78	000000b		FlsGetValue
92	00021f88	0000000b		FlsSetValue
93	00021f98	0000001b		InitializeCriticalSectionEx
94	00021fb8	00000013		InitOnceExecuteOnce
95	00021fd0	0000000e		CreateEventExW
96	00021fe0	00000010		CreateSemaphoreW
97	00021ff8	00000012		CreateSemaphoreExW
98	00022010	00000015		CreateThreadpoolTimer
99	00022028	00000012		SetThreadpoolTimer
100	00022040	0000001f		WaitForThreadpoolTimerCallbacks
101	00022060	00000014		CloseThreadpoolTimer
102	00022078	00000014		CreateThreadpoolWait
103	00022090	00000011		SetThreadpoolWait
104	000220a8	00000013		CloseThreadpoolWait
105	000220c0	00000018		FlushProcessWriteBuffers
106	000220e0	0000001e		FreeLibraryWhenCallbackReturns
107	00022100	00000019		GetCurrentProcessorNumber
108	00022120	00000013		CreateSymbolicLinkW
109	00022138	00000013		GetCurrentPackageld
110	00022150	0000000e		GetTickCount64
111	00022160	0000001c		GetFileInformationByHandleEx
112	00022180	0000001a		SetFileInformationByHandle
113	000221a0	0000001e	А	GetSvstemTimePreciseAsFileTime

Below is evidence of the *directory iterator* phase, the .BiBi extension appended to files made inaccessible, the identification of booting settings CMD commands in order to disable the Windows Automatic Repair module and the checking of possible OS booting failures. The CMD commands in question are in *reversed* form (written backwards) in the extractable strings. Instances of Restart Manager are also used to manage the status and termination of the process, and shadow copies are removed in order not to allow files to be restored easily:



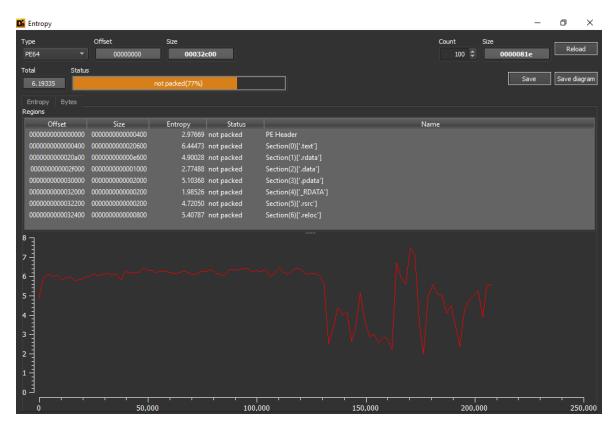
ilter		ANSI		👻 🔲 UTF8 📕 Unicode 📕 C Strings 5 🗣 Save Sea	rch
	Offset 🔻	Size	Туре	String	
604	0002a8e0	0000001f	A	directory_entry::symlink_status	
605	0002a908	00000026	A	directory_iterator::directory_iterator	
606	0002a930	0000001e /	A	directory_iterator::operator++	
607	0002a950	00000006	A	rename	
608	0002a958	00000015	A	invalid stoi argument	
609	0002a970	0000001a /	A	stoi argument out of range	
610	0002a9d8	00000005	U	.BiBi	
611	0002aa18	00000031	A	lla/ teluq/ swodahs eteled nimdassv c/ exe.dmc	
612	0002aa50	00000021	A	eteled ypocwodahs cimw c/ exe.dmc	
613	0002aa80	00000046	A	seruliafilaerongi ycilopsutatstoob }tluafed{ tes / tidedcb c / exe.dmc	
614	0002aac8	00000034	A	on delbaneyrevocer }tluafed{ tes/ tidedcb c/ exe.dmc	
615	0002ab00	0000008	A	C:\Users	
616	0002ab40	00000019	A	send attempt while closed	
517	0002ab60	00000017	A	invalid string position	
518	0002ab78	000000f	A	vector too long	
619	0002ab88	00000011	A	deque <t> too long</t>	
520	0002aba0	0000003e	U	0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz	
621	0002ac98	6000000 b	A	unknown error	
622	0002acc0	000000c /	Α	Rstrtmgr.dll	
523	0002acd0	0000000e /	A	RmStartSession	
524	0002ace0	00000013	A	RmRegisterResources	
625	0002acf8	0000009	A	RmGetList	
626	0002ad08	0000000a /	A	RmShutdown	

Through a text reversing process, we obtained the following commands executed:





Sections of the malware don't appear to possess packing peculiarities, so the threat actors did not arrange for bytes confusing in order to make any static analysis of the artefact more difficult. However, as we shall see later, some specific attributes of executed commands are in a "text reversed" or encoded form.





# **Dynamic analysis and second malware**

#### assessment

In the function *sub\_140005530*, a new process is created with the *booting modification* CMD commands (in text reversed form) as parameters:

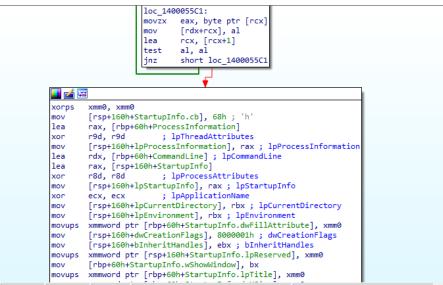
sub_140005530 proc near
bInheritHandles= dword ptr -140h
dwCreationFlags= dword ptr -138h
lpEnvironment= qword ptr -130h
lpCurrentDirectory= gword ptr -128h
lpStartupInfo= qword ptr -120h
lpProcessInformation= qword ptr -118h
var_110= qword ptr -110h
var_100= qword ptr -100h
var_F8= qword ptr -0F8h
StartupInfo= _STARTUPINFOA ptr -0F0h
ProcessInformation= _PROCESS_INFORMATION ptr -80h
CommandLine= byte ptr -60h
var_10= qword ptr -10h
arg_0= qword ptr 10h
mov [rsp-8+arg_0], rbx
push rbp
lea rbp, [rsp-60h]
sub rsp, 160h
mov rax, cs:security_cookie
xor rax, rsp
mov [rbp+60h+var_10], rax
xon ebx, ebx
mov [rsp+160h+var_F8], 0Fh
<pre>lea rdx, aLlaTeiuqSwodah ; "lla/ teIuq/ swodahs eteled nimdassv "</pre>
mov [rsp+160h+var 110]. rbx 100.00% (-95,78) (744,415) 00004955 000000140005558: sub 140005530+28 (Synchronized with Hex View-1)

mov	rax, cs:security_cookie
xor	rax, rsp
mov	[rbp+60h+var_10], rax
xor	ebx, ebx
mov	[rsp+160h+var_F8], 0Fh
lea	rdx, aLlaTeiuqSwodah ; "lla/ teIuq/ swodahs eteled nimdassv "
mov	[rsp+160h+var 110], rbx
lea	rcx, [rsp+160h+var 110] ; void *
mov	[rsp+160h+var_100], rbx
lea	r8d, [rbx+31h] ; Size
call	sub_140006990
cmp	[rsp+160h+var_F8], 10h
lea	rcx, [rsp+160h+var_110]
mov	rdx, [rsp+160h+var_100]
cmovnb	rcx, [rsp+160h+var 110]
add	rdx, rcx
lea	rcx, [rsp+160h+var_110]
cmp	[rsp+160h+var_F8], 10h
cmovnb	rcx, [rsp+160h+var_110]
call	std_reverse_trivially_swappable_1
cmp	[rsp+160h+var_F8], 10h
lea	rcx, [rsp+160h+var_110]
lea	rdx, [rbp+60h+CommandLine]
cmovnb	rcx, [rsp+160h+var 110]
CIIIOVIID	

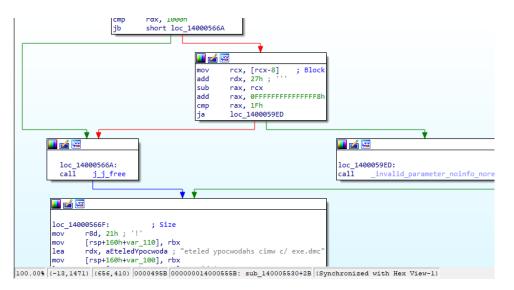
100.00% (-95,393) (732,400) 0000495B 00000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)

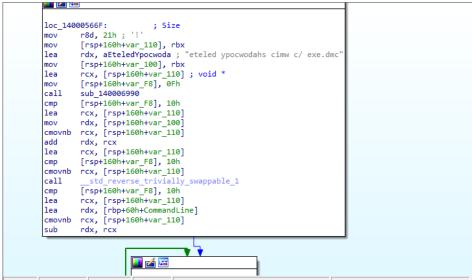
We highlight the details of setting up the threads and execution attributes of the process itself:





100.00% (-95,843) (788,413) 0000495B 00000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)





100.00% (-13,1786) (692,415) 0000495B 00000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)



Finally, the function *CreateProcessA* is called to create the process in question for executing the above-mentioned commands:

movups	xmmword ptr [rbp+60h+StartupInfo.lpTitle], xmm0							
movups	movups xmmword ptr [rbp+60h+StartupInfo.dwXSize], xmm0							
movups								
movups	movups xmmword ptr [rbp+60h+StartupInfo.hStdOutput], xmm0							
call	call cs:CreateProcessA							
mov								
cmp	rdx, 10h							
jb	short loc 14000578E							
5	-							
	mov rcx, [rsp+160h+var_110]							
	inc rdx							
	mov rax, rcx							
	cmp rdx, 1000h							
	jb short loc_140005789							
	mov rcx, [rcx-8] ; Block							
	add rdx, 27h; '''							
	sub rax, rcx							
	add rax, 0FFFFFFFFFFFFFFF							
	cmp rax, 1Fh							
	ja loc_1400059F3							

100.00% (-13,2617) (722,413) 0000495B 00000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)

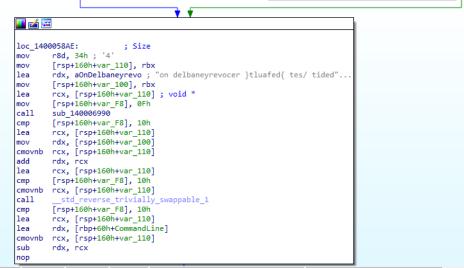
mov mov	r8d, 46h ; 'F' [rsp+160h+var 110], rbx	
lea	rdx, aSeruliafllaero ; "seruliafllaerongi ycilopsutatstoob }tlu"	
mov	[rsp+160h+var 100], rbx	
lea	rcx, [rsp+160h+var 110] ; void *	
mov	[rsp+160h+var F8], 0Fh	
call	sub 140006990	
cmp	[rsp+160h+var F8], 10h	
	rcx, [rsp+160h+var 110]	
mov	rdx, [rsp+160h+var 100]	
cmovnb	rcx, [rsp+160h+var 110]	
add	rdx, rcx	
lea	rcx, [rsp+160h+var 110]	
cmp	[rsp+160h+var F8], 10h	
cmovnb	rcx, [rsp+160h+var 110]	
call	std reverse trivially swappable 1	
cmp	[rsp+160h+var F8], 10h	
lea	rcx, [rsp+160h+var 110]	
lea	rdx, [rbp+60h+CommandLine]	
cmovnb	rcx, [rsp+160h+var_110]	
sub	rdx, rcx	
nop		
-		1

100.00% (-5,3182) (705,376) 0000495B 00000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)



xorps	xmm0, xmm0	
mov	<pre>[rsp+160h+StartupInfo.cb], 68h ; 'h'</pre>	
lea	<pre>rax, [rbp+60h+ProcessInformation]</pre>	
xor	r9d, r9d ; lpThreadAttributes	
nov	<pre>[rsp+160h+lpProcessInformation], rax ; lpProcessInformation</pre>	
lea	rdx, [rbp+60h+CommandLine] ; lpCommandLine	
lea	rax, [rsp+160h+StartupInfo]	
xor	r8d, r8d ; lpProcessAttributes	
nov	[rsp+160h+lpStartupInfo], rax ; lpStartupInfo	
xor	ecx, ecx ; lpApplicationName	
nov	<pre>[rsp+160h+lpCurrentDirectory], rbx ; lpCurrentDirectory</pre>	
nov	[rsp+160h+lpEnvironment], rbx ; lpEnvironment	
novups	<pre>xmmword ptr [rbp+60h+StartupInfo.dwFillAttribute], xmm0</pre>	
nov	[rsp+160h+dwCreationFlags], 8000001h ; dwCreationFlags	
mov	[rsp+160h+bInheritHandles], ebx ; bInheritHandles	
movups	xmmword ptr [rsp+160h+StartupInfo.lpReserved], xmm0	
mov .	[rbp+60h+StartupInfo.wShowWindow], bx	
movups	xmmword ptr [rbp+60h+StartupInfo.lpTitle], xmm0	
movups	xmmword ptr [rbp+60h+StartupInfo.dwXSize], xmm0	
movups	xmmword ptr [rbp+60h+StartupInfo.1pReserved2], xmm0	
movups	<pre>xmmword ptr [rbp+60h+StartupInfo.hStdOutput], xmm0</pre>	
call	cs:CreateProcessA	
nov	rdx, [rsp+160h+var F8]	
cmp	rdx, 10h	
jb	short loc 1400058AE	

100.00% (-6,3738) (689,411) 0000495B 00000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)



100.00% (17,4531) (805,398) 0000495B 00000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)



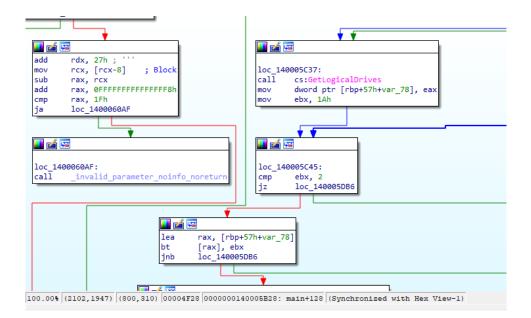


100.00% (16,5151) (734,403) 0000495B 000000014000555B: sub\_140005530+2B (Synchronized with Hex View-1)

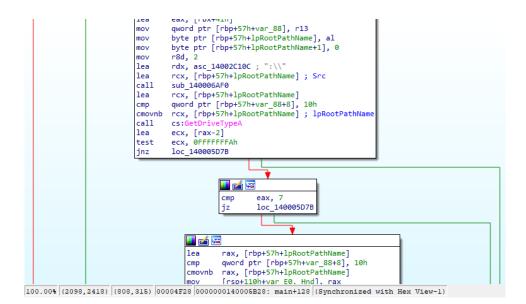
Files and data are taken from the root folder C:\\Users

<pre>loc_140005875: lea rax, aCUsers ; "C:\\Users" mov [rsp+110h+var_E0Hnd], rax mov qword ptr [rsp+110h+var_E0Id], 8 callstd_fs_code_page</pre>
<pre>lea rax, aCUsers ; "C:\\Users" mov [rsp+110h+var_E0Hnd], rax mov qword ptr [rsp+110h+var_E0Id], 8 callstd_fs_code_page</pre>
<pre>movaps xmm0, xmmword ptr [rsp+110h+var_E0Hnd] movdqa xmmword ptr [rsp+110h+var_E0Hnd], xmm0 lea r8, [rsp+110h+var_E0] mov edx, eax lea rcx, [rbp+57h+lpRootPathName]; Src call sub1400018E0 nop mov edi, 7 mov rdx, [rbp+57h+lpWideCharStr+8] cmp rdx, [rbp+57h+var_A0] iz short loc 140005BEA</pre>
jz short loc_140005BEA
Image: Second





Next, the various types of system disks are enumerated and classified:





.rdata:00000014002FCE0 word_14002F	
.rdata:000000014002FCE2	db 'GetLogicalDrives',0
.rdata:000000014002FCF3	align 4
.rdata:00000014002FCF4 word_14002F	
.rdata:00000014002FCF6	db 'GetDriveTypeA',0
.rdata:00000014002FD04 word_14002F	
.rdata:00000014002FD06	db 'GetLastError',0
.rdata:00000014002FD13	align 4
.rdata:00000014002FD14 word_14002F	
.rdata:00000014002FD16	db 'CreateProcessA',0
.rdata:00000014002FD25	align 2
.rdata:00000014002FD26 word_14002F	D26 dw 59Eh ; DATA XREF: .rdata:00000014002F9E
.rdata:000000014002FD28	db 'TerminateProcess',0
.rdata:000000014002FD39	align 2
.rdata:00000014002FD3A word_14002F	
.rdata:000000014002FD3C	db 'OpenProcess',0
.rdata:00000014002FD48 word_14002F	
.rdata:00000014002FD4A	db 'LoadLibraryA',0
.rdata:00000014002FD57	align 8
.rdata:00000014002FD58 word_14002F	
.rdata:000000014002FD5A	db 'GetProcAddress',0
.rdata:000000014002FD69	align 2
.rdata:00000014002FD6A word_14002F	D6A dw 221h ; DATA XREF: .rdata:00000014002FA0
.rdata:00000014002FD6C	db 'GetCurrentProcessId',0
.rdata:000000014002FD80 aKernel32D1	<pre>db 'KERNEL32.dll',0 ; DATA XREF: .rdata:00000014002F9A</pre>
.rdata:000000014002FD8D	align 2
.rdata:00000014002FD8E word 14002F	D8E dw 89h ; DATA XREF: .rdata:00000014002FA1

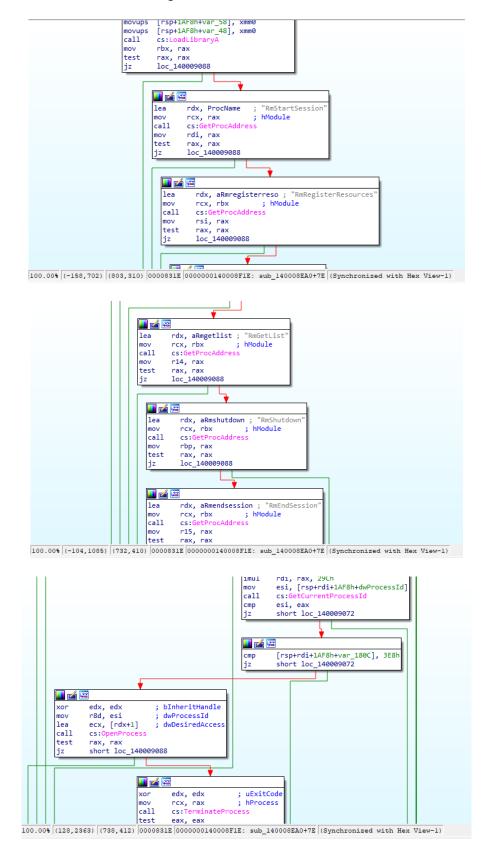
Attributes and parameters are collected to proceed with the infection chain phase, such as the number of threads, CPU cores, path and execution statistics:

				- · · · · · · · · · · · · · · · · · · ·
6	Ш́		🚺 🛃 😼	<u> </u>
	POEDCA		lea	rdx, [rbp+57h+Src] ; Src
	005DC4: ; Microsoft VisualC v14 64bit runtime		mov	rcx, rbx ; lpWideCharStr
L	unknown_libname_8		call	sub_140006B90
	r9d, eax		lea	rdx, [rbp+57h+Src]
	<pre>rcx, [rbp+57h+1pWideCharStr+8]</pre>		cmp	qword ptr [rbp+57h+var_C0+8], 10h
	<pre>rcx, [rbp+57h+1pWideCharStr]</pre>		cmovnb	rdx, qword ptr [rbp+57h+Src]
	rcx, 5		lea	<pre>rcx, aPathS ; "[+] Path: %s\n"</pre>
	eax, eax		call	sub_140001030
	edx, edx		mov	rdx, qword ptr [rbp+57h+var_C0+8]
	ncx		cmp	rdx, 10h
	eax, 1		jb	short loc_140005B6F
/1	eax, r13d			_
	r14d, [rax+rax*2]			
	r8d, r14d			
	edx, r9d			
	<pre>rcx, aCpuCoresDThrea ; "[+] CPU cores: %d, Threads: %d\n"</pre>			
L	sub 140001030			
	[rbp+57h+var 78], 1388h			
	rcx, [rbp+57h+var 78]			
L	sub 140007050			
	ecx, 8 ; Size			
L	??2@YAPEAX K@Z ; operator new(unsigned int64)			
	rcx, sub 140005530			
	[rax], rcx			
	gword ptr [rbp+57h+var 40], rax			
	rcx, [rbp+57h+var_50+8]			
100	00% (1860 4714) (803 312) 00004F28 000000140005B28; main+1	28 (Sum	hronized	with Hey View-1)

format-string	[+] Stats: %d   %d
format-string	[+] Path: %s
format-string	[+] CPU cores: %d, Threads: %d



We have evidence of *Restart Management* with the attributes of CurrentProcessID:





At the following addresses in the *.rdata* section identifiable by *00000014002FE48*, the file looping functions getting, for example *FindNextFileW*, *FindFirstFileExW* and *GetFileInformationByHandleEx*. The latter allows details of specific files to be obtained within an iterative phase:

.rdata:000000014002FE2E	db 'CreateFileW',0
.rdata:00000014002FE3A word 14002FE3A	
.rdata:00000014002FE3C	db 'FindClose',0
.rdata:000000014002FE46 word 14002FE46	
rdata:00000014002FF48	db 'FindFirstFileExW',0
rdata:00000014002EE59	align 2
.rdata:000000014002FE5A word 14002FE5A	
.rdata:00000014002FE5C	db 'FindNextFileW',0
.rdata:00000014002FE6A word 14002FE6A	
.rdata:00000014002FE6C	db 'GetFileAttributesExW',0
.rdata:00000014002FE81	align 2
.rdata:00000014002FE82 word 14002FE82	
.rdata:00000014002FE84	db 'SetEndOfFile',0
.rdata:00000014002FE91	align 2
.rdata:000000014002FE92 word 14002FE92	0
.rdata:00000014002FE94	db 'SetFileAttributesW',0
.rdata:00000014002FEA7	align 8
.rdata:00000014002FEA8 word 14002FEA8	dw 533h ; DATA XREF: .rdata:00000014002FA90
.rdata:00000014002FEAA	db 'SetFilePointerEx',0
.rdata:00000014002FEBB	align 4
.rdata:00000014002FEBC word_14002FEBC	dw 23h ; DATA XREF: .rdata:00000014002FA98
.rdata:00000014002FEBE	db 'AreFileApisANSI',0
.rdata:00000014002FECE word_14002FECE	dw 3EFh ; DATA XREF: .rdata:00000014002FAA0
.rdata:00000014002FED0	db 'MoveFileExW',0
.rdata:00000014002FEDC word_14002FEDC	dw 252h ; DATA XREF: .rdata:000000014002FAA8
.rdata:000000014002FEDE	<pre>db 'GetFileInformationByHandleEx',0</pre>
.rdata:00000014002FEFB	align 4
0002E85C 000000014002FE5C: .rdata:0000000	14002FE5C (Synchronized with Hex View-1)
	4

Further details within the .rdata section concerning performance counter querying, obtaining local timestamps for environment execution awareness are given below.

db 'MultiByteToWideChar',0
2 dw 611h ; DATA XREF: .rdata:00000014002FAB
db 'WideCharToMultiByte',0
8 dw 452h ; DATA XREF: .rdata:00000014002FAC
2 dw 453h ; DATA XREF: .rdata:00000014002FAC
db 'QueryPerformanceFrequency',0
E dw 370h ; DATA XREF: .rdata:00000014002FAD
db 'InitializeSRWLock',0
2 dw 4B8h ; DATA XREF: .rdata:00000014002FAD
db 'ReleaseSRWLockExclusive',0
C dw 0 ; DATA XREF: .rdata:00000014002FAE
db 'AcquireSRWLockExclusive',0
6 dw 138h ; DATA XREF: .rdata:00000014002FAE
db 'EnterCriticalSection',0
align 2
E dw 3C4h ; DATA XREF: .rdata:00000014002FAF
db 'LeaveCriticalSection',0
align 2
6 dw 36Ch ; DATA XREF: .rdata:00000014002FAF
<pre>db 'InitializeCriticalSectionEx',0</pre>
4 dw 5B9h ; DATA XREF: .rdata:00000014002FB00
db 'TryEnterCriticalSection',0
E dw 114h ; DATA XREF: .rdata:00000014002FB08
db 'DeleteCriticalSection',0
6 dw 2F3h ; DATA XREF: .rdata:00000014002FB10
db 'GetSystemTimeAsFileTime',0
0014002FF2A (Synchronized with Hex View-1)



.rdata:00000014002FFD5	align 2
.rdata:000000014002FFD6 word_14002FFD6	
.rdata:00000014002FFD8	db 'InitializeCriticalSectionEx',0
.rdata:00000014002FFF4 word_14002FFF4	dw 5B9h ; DATA XREF: .rdata:00000014002FB00
.rdata:00000014002FFF6	db 'TryEnterCriticalSection',0
.rdata:00000014003000E word_14003000E	dw 114h ; DATA XREF: .rdata:00000014002FB08
.rdata:000000140030010	db 'DeleteCriticalSection',0
.rdata:000000140030026 word 140030026	dw 2F3h ; DATA XREF: .rdata:00000014002FB10
.rdata:000000140030028	db 'GetSystemTimeAsFileTime',0
.rdata:000000140030040 word_140030040	dw 281h ; DATA XREF: .rdata:00000014002FB18
.rdata:000000140030042	db 'GetModuleHandleW',0
.rdata:000000140030053	align 4
.rdata:000000140030054 word_140030054	dw 4D5h ; DATA XREF: .rdata:00000014002FB20
.rdata:000000140030056	db 'RtlCaptureContext',0
.rdata:0000000140030068 word_140030068	dw 4DCh ; DATA XREF: .rdata:00000014002FB28
.rdata:00000014003006A	db 'RtlLookupFunctionEntry',0
.rdata:000000140030081	
.rdata:0000000140030082 word_140030082	dw 4E3h ; DATA XREF: .rdata:00000014002FB30
.rdata:000000140030084	db 'RtlVirtualUnwind',0
.rdata:000000140030095	align 2
.rdata:0000000140030096 word_140030096	dw 5C0h ; DATA XREF: .rdata:00000014002FB38
.rdata:000000140030098	db 'UnhandledExceptionFilter',0
.rdata:0000001400300B1	align 2
.rdata:00000001400300B2 word_1400300B2	
.rdata:0000001400300B4	db 'SetUnhandledExceptionFilter',0
.rdata:00000001400300D0 word_1400300D0	dw 220h ; DATA XREF: .rdata:000000014002FB48
.rdata:0000001400300D2	db 'GetCurrentProcess',0
0002E9F6 00000014002FFF6: .rdata:0000000	14002FFF6 (Synchronized with Hex View-1)
41	

#### Here are further references to the *IsDebuggerPresent* and *EncodePointer* functions:

.rdata:000000140030098	db 'UnhandledExceptionFilter',0
.rdata:0000001400300B1	align 2
.rdata:0000001400300B2 word 1400300B	32 dw 57Fh ; DATA XREF: .rdata:00000014002
.rdata:0000001400300B4	db 'SetUnhandledExceptionFilter',0
.rdata:0000001400300D0 word_1400300D	00 dw 220h ; DATA XREF: .rdata:00000014002
.rdata:0000001400300D2	db 'GetCurrentProcess',0
.rdata:0000001400300E4 word_14003008	E4 dw 38Ch ; DATA XREF: .rdata:00000014002
.rdata:0000001400300E6	<pre>db 'IsProcessorFeaturePresent',0</pre>
.rdata:0000000140030100 word_14003010	00 dw 36Fh ; DATA XREF: .rdata:00000014002
.rdata:000000140030102	db 'InitializeSListHead',0
.rdata:0000000140030116 word_14003011	L6 dw 385h ; DATA XREF: .rdata:00000014002
.rdata:000000140030118	db 'IsDebuggerPresent',0
.rdata:000000014003012A word_14003012	
.rdata:00000014003012C	db 'GetStartupInfoW',0
.rdata:000000014003013C word_14003013	3C dw 4E2h ; DATA XREF: .rdata:00000014002
.rdata:000000014003013E	db 'RtlUnwindEx',0
.rdata:00000014003013E .rdata:000000014003014A word_14003014	A dw 4DEh ; DATA XREF: .rdata:00000014002
.rdata:00000014003014C	db 'RtlPcToFileHeader',0
.rdata:000000014003015E word_14003019	5E dw 468h ; DATA XREF: .rdata:00000014002
.rdata:0000000140030160	db 'RaiseException',0
.rdata:000000014003016F	align 10h
.rdata:0000000140030170 word_14003017	70 dw 541h ; DATA XREF: .rdata:00000014002
.rdata:000000140030172	db 'SetLastError',0
.rdata:00000014003017F	align 20h
.rdata:0000000140030180 word_14003018	30 dw 134h ; DATA XREF: .rdata:00000014002
.rdata:000000140030182	db 'EncodePointer',0
.rdata:0000000140030190 word 14003019	90 dw 36Bh ; DATA XREF: .rdata:00000014002
0002EAD0 00000001400300D0: .rdata:word	1400300D0 (Synchronized with Hex View-1)



#### The executable was compiled on **21 October 2023:**

property	value
md5	E26BBA0304F14EF96BEB60376791D32C
sha1	
sha256	24F6785CA2E82D1D1D61F4CB01D5E753F80445CF
	40417E937CD244B2F928150CAE6FA0EFF5551FDB401EA072F6ECDDA67A747E17
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
first-bytes-text	M Z
file-size	207872 (bytes)
entropy	6.193
imphash	7339438F1FA3FBACA1E35B75D7395E40
signature	n/a
entry-point	48 83 EC 28 E8 9F 06 00 00 48 83 C4 28 E9 72 FE FF FF CC CC 48 83 EC 28 4D 8B 41 38 48 8B CA 49 8B
file-version	n/a
description	n/a
file-type	executable
сри	64-bit
subsystem	console
compiler-stamp	0x65346BC9 (Sat Oct 21 17:24:41 2023)
debugger-stamp	0x65346BC9 (Sat Oct 21 17:24:41 2023)
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

The most interesting indicators inherent in the sample refer mostly to file management, environment and hardware information discovery, services management and execution, and external function calling:

indicator (37)	detail	level
The file references string(s)	type: blacklist, count: 36	1
The count of libraries is suspicious	count: 1	1
The file imports symbol(s)	type: blacklist, count: 21	1
The file contains a blacklist section	section: _RDATA	1
The time-stamp of the compiler is suspicious	year: 2023	2
The time-stamp of a directory is suspicious	directory: debug, stamp: Sat Oct 21 17:24:41 2023	2
The file checksum is invalid	checksum: 0x00000000	3
The file references a group of API	type: synchronization, count: 38	3
The file references a group of API	type: execution, count: 68	3
The file references a group of API	type: file, count: 38	3
The file references a group of API	type: reckoning, count: 14	3
The file references a group of API	type: services, count: 13	3
The file references a group of API	type: storage, count: 4	3
The file references a group of API	type: diagnostic, count: 10	3
The file references a group of API	type: dynamic-library, count: 16	3
The file references a group of API	type: memory, count: 16	3
The file references a group of API	type: exception, count: 8	3
The file references a group of API	type: console, count: 12	3
The file references a group of hint	type: file, count: 8	3
The file references a group of hint	type: format-string, count: 3	3
The file references a group of hint	type: utility, count: 1	3
The file references a group of hint	type: rtti, count: 22	3
The file references a group of hint	type: function, count: 1	3



Additional attributes regarding the Portable Executable are listed here, including the file signature:

property	value	detail
compiler-stamp	0x65346BC9	Sat Oct 21 17:24:41 2023
size-of-optional-header	0x00F0	240 bytes
signature	0x00004550	PE00
machine	0x8664	Amd64
sections	0x0007	7
pointer-symbol-table	0x00000000	0x0000000
number-of-symbols	0x00000000	0x0000000
processor-32bit	0x0000000	false
system-image	0x0000000	false
executable	0x0000002	true
dynamic-link-library	0x0000000	false
debug-stripped	0x00000000	false
line-stripped-from-file	0x0000000	false
local-symbols-stripped-from-file	0x0000000	false
relocation-stripped	0x0000000	false
large-address-aware	0x0000020	true
uniprocessor	0x0000000	false
bytes-of-machine-words-reversed-Low	0x0000000	false
bytes-of-machine-words-reversed-Hi	0x0000000	false
media-run-from-swap	0x0000000	false
network-run-from-swap	0x00000000	false

In the sections of the artifact, the entropy coefficient values and the entrypoint (the initial address of execution) of the *.text* section (CPU instructions) at address *0x0000AB10* are shown:



property	value	value	value
name	.text	.rdata	.data
md5	47086F913C767FB79FF63FEA	FC9155991D99E81FAA884AE	F4D28948DD21F61F2911F50
entropy	6.445	4.900	2.775
file-ratio (99.51%)	63.79 %	28.33 %	1.97 %
raw-address	0x00000400	0x00020A00	0x0002F000
raw-size (206848 bytes)	0x00020600 (132608 bytes)	0x0000E600 (58880 bytes)	0x00001000 (4096 bytes)
virtual-address	0x0000000040001000	0x0000000040022000	0x000000040031000
virtual-size (211262 bytes)	0x0002040C (132108 bytes)	0x0000E44E (58446 bytes)	0x000027D0 (10192 bytes)
entry-point	0x0000AB10	-	-
characteristics	0x6000020	0x40000040	0xC0000040
writable	-	-	x
executable	x	-	-
shareable	-	-	-
discardable	-	-	-
initialized-data	-	x	х
uninitialized-data	-	-	-
unreadable	-	-	-
self-modifying	-	-	-
virtualized	-	-	-
file	n/a	n/a	n/a

value	value	value	value
.pdata	_RDATA	rsrc	.reloc
E969B76C781BFBAFF75A595	91DDDA35C6D0A6CCD1D39	2D5EB1E7989B77F5C38C725	CC5B904DECA074980130772
5.104	1.982	4.718	5.407
3.94 %	0.25 %	0.25 %	0.99 %
0x00030000	0x00032000	0x00032200	0x00032400
0x00002000 (8192 bytes)	0x00000200 (512 bytes)	0x00000200 (512 bytes)	0x00000800 (2048 bytes)
0x0000000040034000	0x000000040036000	0x000000040037000	0x000000040038000
0x00001E60 (7776 bytes)	0x000000F4 (244 bytes)	0x000001E0 (480 bytes)	0x000007E0 (2016 bytes)
-	-	-	-
0x40000040	0x40000040	0x40000040	0x42000040
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	х
Х	х	х	х
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-
n/a	n/a	n/a	n/a

There are several functions that can be classified as attentionable: *CreateProcessA*, *OpenProcess, SwitchToThread, GetCurrentThreadId, GetNativeSystemInfo, FindFirstFileExW, FindNextFileW, MoveFileExW* and *SetFileAttributesW*.



functions (99)	blacklist (21)	type (1)	ordinal (0)	library (1)
CreateProcessA	x	implicit	-	kernel32.dll
TerminateProcess	x	implicit	-	kernel32.dll
OpenProcess	x	implicit	-	kernel32.dll
GetCurrentProcessId	x	implicit	-	kernel32.dll
SwitchToThread	x	implicit	-	kernel32.dll
GetCurrentThreadId	x	implicit	-	kernel32.dll
GetNativeSystemInfo	x	implicit	-	kernel32.dll
FindFirstFileExW	x	implicit	-	kernel32.dll
FindNextFileW	x	implicit	-	kernel32.dll
<u>SetFileAttributesW</u>	x	implicit	-	kernel32.dll
MoveFileExW	x	implicit	-	kernel32.dll
GetFileInformationByHandleEx	x	implicit	-	kernel32.dll
QueryPerformanceFrequency	x	implicit	-	kernel32.dll
RtlLookupFunctionEntry	x	implicit	-	kernel32.dll
RtIPcToFileHeader	x	implicit	-	kernel32.dll
RaiseException	x	implicit	-	kernel32.dll
FreeLibraryAndExitThread	x	implicit	-	kernel32.dll
GetModuleHandleExW	x	implicit	-	kernel32.dll
WriteFile	x	implicit	-	kernel32.dll
<u>GetEnvironmentStringsW</u>	x	implicit	-	kernel32.dll
SetEnvironmentVariableW	x	implicit	-	kernel32.dll

Here are some strings of information and attributes gathering, as well as the extension appended to the .BiBi files.

format-string	[+] Stats: %d   %d
format-string	[+] Path: %s
format-string	[+] CPU cores: %d, Threads: %d
file	<u>dj.H</u>
file	<u>Rstrtmgr.dll</u>
file	KERNEL32.dll
file	kernel32.dll
file	mscoree.dll
file	<u>.exe</u>
file	<u>.dll</u>
file	<u>-SVS</u>
dos-message	!This program cannot be run in DOS mode.
-	oBYwo
-	oRich

<u>zu-za</u>
<u>\r\n</u>
<u>CONOUT\$</u>
. <u>BiBi</u>
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
<u>\r\n</u>
<u>\r\n</u>
<u>\r\n</u>
<u>\r\n5</u>



property	value
md5	7AD0B3E52BDC0524CC523484FD471772
sha1	107DE9369E5B8D11496BA77ED21CBC8AD9908FA0
sha256	302217B570AC70A8BD2D75279D478D731FF02BD211514B77A0ED5FB2C7EF644D
size	968 (bytes)
format	PGO
debugger-stamp	0x65346BC9 (Sat Oct 21 17:24:41 2023)
path	n/a

The debugger timestamp is also dated **21 October 2023**:

Note the following evidence related to the PE assessment phase and the included sections, including *VirtualSizes* (the size of the sections as they are mapped in memory):

👔 Stud_PE editing : "40417e937cd24	4b2f928150cae6fa0eff555 — 🗆 🗙								
File Edit Tools Help									
c:\users\ieuser\desktop\new folder\40	417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6e								
🦻 Headers 🌗 Dos 📔 🗳 Sections 🕴 💷 Functions 🛛 🕫 Resources 🛛 🏶 Signature 📄 🖷 F 💶 🕨									
HEADERS (Coff+Optional)	DATA DIRECTORY								
0000AB10 EntryPoint (rva)	RVA Size Raw								
	Import Table 0002F994 00000028 0002E394								
00009F10 EntryPoint (raw)									
0000000140000000 ImageBase	Export Table 00000000 00000000 00000000								
00039000 Size of Image									
00001000 Sections Alignment	Data Dir : IMAGE_DIR_ENTRY_RESOURCE								
	GoHex ++ 00037000 000001E0 00032200								
00000200 File Alignment									
0007 Number of sections									
0022 Characteristics+	Basic HEADERS tree view in hexeditor SAVE to file								
Visit Stud PE Forum <- News Here	Test'it Rva<=>Raw File Compare OK								



c:\users	:\users\ieuser\desktop\new folder\40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6										
> Head	• Headers 🕽 Þ Dos 🎴 Sections 🛛 🕫 Functions 🛛 🕫 Resources 🛛 🏶 Signature 🕅 🕅 F ┥										
No	Name	VirtualSize	VirtualOffset	RawSize	RawOffset	Characteri					
ep 01	.text	0002040C	00001000	00020600	00000400	60000020					
02	.rdata	0000E44E	00022000	0000E600	00020A00	40000040					
03	.data	000027D0	00031000	00001000	0002F000	C0000040					
04	.pdata	00001E60	00034000	00002000	00030000	40000040					
05	_RDATA	000000F4	00036000	00000200	00032000	40000040					
06	.rsrc	000001E0	00037000	00000200	00032200	40000040					
07	.reloc	000007E0	00038000	0080000	00032400	42000040					

Reference is made to the import of several main functions of drive enumeration, performance counter information gathering and file pointing:

- m.	liting : "40417e937cd244b ools Help	o2f928150cae6fa0e	ff555 —	• ×
c:\users\ieuser	\desktop\new folder\4041	7e937cd244b2f9281	150cae6fa0eff55	i51fdb401ea072f6ε
▶ Headers   ■ □Imported Functi	Dos 🕒 Sections 👎	Functions Rs Res		nature   R F 🕢 🕨 Exported Functions
	AreFileApisANSI ord:35 m MoveFileExW ord:1007 m GetFileInformationByHand MultiByteToWideChar ord WideCharToMultiByte ord QueryPerformanceFrequer InitializeSRWLock ord:88 ReleaseSRWLockExclusiv AcquireSRWLockExclusiv	va2iat: 000220E0 lleEx ord:594 rvai t:1014 rva2iat: 00 t:1553 rva2iat: 00 r ord:1106 rva2ia ncy ord:1107 rva i0 rva2iat: 000221 ve ord:1208 rva2	Found N	lo Exports !
Show Imp	O OriginalFirstThunk 🖲	FirstThunk		Show Exp 🔽
Visit Stud PE F	Forum <- News Here	Test'it Rva<=>	Raw File Com	pare OK



c:\users\ieuser\desktop\new folder\40417e937cd244b2f928150caef	δfa0eff5551fdb401ea072f6ε
▶ Headers ▶ Dos ► Sections fx Functions Rs Resources Imported Functions	Signature   R F   I
<ul> <li>▲ ● f(*) FormatMessageA ord:431 rva2iat: 0002209</li> <li>● f(*) CreateFileW ord:206 rva2iat: 00022098</li> <li>● f(*) FindClose ord:382 rva2iat: 000220A0</li> <li>● f(*) FindFirstFileExW ord:388 rva2iat: 000220A</li> <li>● f(*) FindNextFileW ord:405 rva2iat: 000220B0</li> <li>● f(*) GetFileAttributesExW ord:588 rva2iat: 0002</li> <li>E f(*) SetEndOfFile ord:1312 rva2iat: 000220C0</li> <li>● f(*) SetFileAttributesW ord:1325 rva2iat: 000220C0</li> <li>● f(*) SetFileAttributesW ord:1325 rva2iat: 000220C0</li> <li>● f(*) SetFilePointerEx ord:1331 rva2iat: 0002200</li> <li>● f(*) AreFileApisANS1 ord:35 rva2iat: 0002200</li> </ul>	Found No Exports !
Show Imp C OriginalFirstThunk 💿 FirstThunk	Show Exp 🔽
Stud_PE editing : "40417e937cd244b2f928150cae6fa0eff555 File Edit Tools Help	– 🗆 X
c:\users\ieuser\desktop\new folder\40417e937cd244b2f928150cael	
c:\users\ieuser\desktop\new folder\40417e937cd244b2f928150cael	9 Signature   R F.∢
c:\users\ieuser\desktop\new folder\40417e937cd244b2f928150cael	9 Signature   R F.∢
c:\users\ieuser\desktop\new folder\40417e937cd244b2f928150cael         Headers       > Dos       ⊆ Sections       fx       Functions         Imported Functions       fx       Functions       Rs       Resources         Imported Functions       fx       GetLogicalDrives       ord:625 rva2iat: 0002200       fx         fx       GetLogicalDrives       ord:568 rva2iat: 0002200       fx       GetLogicalDrives       ord:568 rva2iat: 0002200         fx       GetLastError       ord:618 rva2iat: 00022010       fx       TerminateProcess       ord:1438 rva2iat: 00022018         fx       TerminateProcess       ord:1042 rva2iat: 00022028       fx       OpenProcess       ord:1042 rva2iat: 00022030	Signature   ■ F Exported Functions

In the *.text* section, the use of the *OR* operator can be seen with the attribute **QWORD PTR** [*RIP* + **0x263A7**]. The logical *OR* operation is performed with the hexadecimal element **0xFFFFFFFFFFFFFFFFFF**, which represents a **read access violation error**.



Settings View Compare Info																												
40417e937cd244b2f928150cae ^	× :	<b>-</b>	•	-	5	ß		Þ	- 😭																			
<ul> <li>DOS Header</li> <li>DOS stub</li> </ul>			0	1	2 3	4	5	6	7	8	9	A J	вс	D	Е	F	0 1	2 3	4	56	78	9 2	AВ	ср	EF	F	^	
NT Headers	9	FOF	90	48	83 E	C 28	3 E8	91	7 06	00	00 4	18 8	3 C4	28	E9	72	н								ér			
Signature	9	F1F	FE	FF	FF C	c co	2 48	8 83	B EC	28	4D 8	в 4	1 38				þÿ	ÿÌ		н.		Μ.		8 H		ŝ		
File Header	9	F2F	49	8B	D1 E	8 OI	0 00	0 00	0 00	BS	01 0	00 0	0 00	48	83	C4	п.	Ñè						. н	. Ä	i.		
Optional Header	9	F3F	28	СЗ	cc c	c co	2 40	53	3 4 5	8B	18 4	18 8	B DA	41	83	E3	( Ã	ìì	î	@ S	Е.	. 1	Η.	ÚΑ	. a	ĩ		
Section Headers	9	F4F	FS	4C	8B C	9 4:	L FG	5 00	0 0 4	4C	8B I	01 7	4 13	41	8B	40	ø L	. É	A		. L	. i	Ĭτ	. A	. 0	3		
Sections	9	F5F	08	4D	63 5	0 04	1 F7	DE DE	3 4C	03	D1 4	18 6	зса	4C	23	D1	. M	c I		÷ø		ÑI	łc	ÈЦ	# Ñ	ñ		
🗸 👬 .text	9	F6F	49	63	C3 42	A 81	3 14	110	48	8B	43 1	.0 8	B 48	8 08	48	8B	Ιc	à J			н.			н.	н.			
⇒ EP = 9F10	9	F7F	43	08	F6 4	4 03	L 03	8 01	74	0B	OF E	36 4	4 01	03	83	EO	с.	öΙ				. 9	[ D		. á	i	~	
📫 .rdata		D:			~											_											40.	
🙀 .data		Disasm	: .tex		Gene	ral	D	oos	Hdr	H	Rich	Hdr	ŀ	ile H	dr	OF	otiona	al Hdr		Section	on H	drs		Imp	orts		<r s<="" td=""><td></td></r>	
🙀 .pdata						Hex			Disasm								^											
💑 _RDATA	9 2	C69			895C2404			MOV DWORD PTR [RSP + 4], EBX																				
📫 .rsrc	e. 2	CGD			88	F9							10V I	EDI,														
📫 .reloc	10 I	C6F			89	4C2							10V I	DWOF	RD P		RSP	+ 81	, E									
	a74	C73			89	542	40C					1	10V I	DWOF	RD P	TR	RSP	+ 02	(C],	EDX								
	a67	C77			75	50				1	V		JNE :	SHO	RT O	X14(	000A	CC9										
	g a	C79					DA7		2001			<b>~</b> 9	DR QI	WORI	) PT	R []	RIP -	⊦ ox2	263A	7],	OXFI	FFF	FFFF	FFFI	FFFF	'/ '		
	2 Lee	C81				F03	FFF					2	AND 1	EAX,		FFF	BFFO											
	20 <sup>2</sup>	C86			ЗD	C00							IMP I	EAX,		1060												
	0 <sup>6</sup>	C8B			74	28					v		JE SI	HORT	r ox	1400	OACE	35										
	db4	CSD			ЗD	600							MP I	EAX,		2066	50											
	21E	C92			74	21					v		JE SI	HORT	r ox	1400	OACE	35										
	122 J	C94			зD	700	602	00					MP I	EAX.	ox	2061	70											
	a0e	C99			74	1A					<b>T</b>						OACE	35										
	ae6	C9B					9FC	चच									(F9B)											
	ž,	CAO				F82						-	MP 1															
	èo –	CA3				24					•						OAC	-0										
	b2f5	CA5							0001.									.0001										
	54																											
		CAF			48	0036	3C1						BT R	UA.	KAX													

In the last page of the Portable Executable there are 90 bytes:

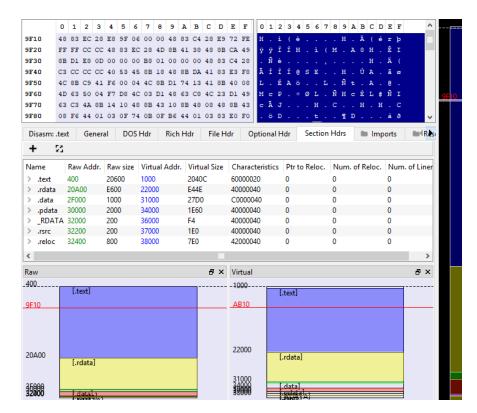
Offset	Name	Value
0	Magic number	5A4D
2	Bytes on last page of file	90
4	Pages in file	3
6	Relocations	0
8	Size of header in paragraphs	4
Α	Minimum extra paragraphs needed	0
C	Maximum extra paragraphs needed	FFFF
E	Initial (relative) SS value	0
10	Initial SP value	B8
12	Checksum	0
14	Initial IP value	0
16	Initial (relative) CS value	0
18	File address of relocation table	40
1A	Overlay number	0
1C	Reserved words[4]	0, 0, 0, 0
24	OEM identifier (for OEM information)	0
26	OEM information; OEM identifier specific	0
28	Reserved words[10]	0, 0, 0, 0, 0, 0, 0, 0, 0, 0
3C	File address of new exe header	100



The *Import Address Table* (an element containing the addresses of imported external DLL libraries) has a size of **320**:

Offset	Name	Value	Value
		8000	TerminalServer aware
160	Size of Stack Reserve	100000	
168	Size of Stack Commit	1000	
170	Size of Heap Reserve	100000	
178	Size of Heap Commit	1000	
180	Loader Flags	0	
184	Number of RVAs and Sizes	10	
~	Data Directory	Address	Size
188	Export Directory	0	0
190	Import Directory	2F994	28
198	Resource Directory	37000	1E0
1A0	Exception Directory	34000	1E60
1A8	Security Directory	0	0
1B0	Base Relocation Table	38000	7E0
1B8	Debug Directory	2C340	38
1C0	Architecture Specific Data	0	0
1C8	RVA of GlobalPtr	0	0
1D0	TLS Directory	2C500	28
1D8	Load Configuration Directory	2C380	138
1E0	Bound Import Directory in headers	0	0
1E8	Import Address Table	22000	320
1F0	Delay Load Import Descriptors	0	0
1F8	.NET header	0	0

Here are the sizes of the sections:





Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	
2E394	KERNEL32.dll	99	FALSE	2F9C0	0	0	
< KERNEL32.0	dll [99 entries]						
	dll [99 entries] Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint	
KERNEL32.0		Ordinal	Original Thunk 2FCE0	Thunk 2FCE0	Forwarder	Hint 271	
KERNEL32.4 Call via 22000	Name	Ordinal -	2		Forwarder - -		
KERNEL32.4 Call via 22000 22008	Name GetLogicalDrives	Ordinal - -	2FCE0	2FCE0	Forwarder - -	271	
KERNEL32.1 Call via 22000 22008 22010	Name GetLogicalDrives GetDriveTypeA	Ordinal - - -	2FCE0 2FCF4	2FCE0 2FCF4	Forwarder - - -	271 238	
KERNEL32.0 Call via 22000 22008 22010 22018	Name GetLogicalDrives GetDriveTypeA GetLastError	-	2FCE0 2FCF4 2FD04	2FCE0 2FCF4 2FD04	Forwarder - - -	271 238 26A	
KERNEL32. Call via	Name GetLogicalDrives GetDriveTypeA GetLastError CreateProcessA	-	2FCE0 2FCF4 2FD04 2FD14	2FCE0 2FCF4 2FD04 2FD14	Forwarder - - - -	271 238 26A E3	
KERNEL32. Call via 22000 22008 22010 22018 22020	Name GetLogicalDrives GetDriveTypeA GetLastError CreateProcessA TerminateProcess	-	2FCE0 2FCF4 2FD04 2FD14 2FD26	2FCE0 2FCF4 2FD04 2FD14 2FD26	Forwarder - - - - - - -	271 238 26A E3 59E	

#### The debugging timestamp is **22 October 2023:**

)ffset	Name	Value	Meaning
2AD40	Characteristics	0	
2AD44	TimeDateStamp	65346BC9	Sunday, 22.10.2023 00:24:41 UTC
2AD48	MajorVersion	0	
2AD4A	MinorVersion	0	
2AD4C	Туре	D	POGO
2AD50	SizeOfData	3C8	
2AD54	AddressOfRaw	2CFF4	
2AD58	PointerToRawD	2B9F4	
Offset	Name	Value	

The executable was compiled in *DllCharacteristics* **8160** (relating to the application of ASLR and high entropy of the PE for the purpose of protection against exploits by making the addresses of the called functions and fundamental memory portions used by the process itself de facto random).



er CFF Explorer VIII - [40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17.exe]	
File Settings 2	

File Settings ?							
🔌 🤳 🔊	40417e937c	40417e937cd244b2f928150cae6fa					
	Property	Valu	e				
File: 40417e937cd244b2f9281 cae6fa0eff5551fdb401ea072f6	Eile Name	C:\U	sers\IEUser\Desktop\New folder\40417e937cd244b2f928150cae6f				
dda67a747e17.exe      B Dos Header      B Nt Headers      B Dis Header      B Optional Header      B Data Directories [x]      B Section Headers [x]      Call Resource Directory      Call Re	File Type	Port	Portable Executable 64				
	File Info	Microsoft Visual C++ 8.0 (DLL)					
	File Size	203.00 KB (207872 bytes)					
	PE Size	203.00 KB (207872 bytes)					
	Created	eated Tuesday 14 November 2023, 03.19.28					
	Modified	dified Tuesday 14 November 2023, 03.19.29					
	Accessed	d Monday 27 November 2023, 02.51.29					
	MD5	E26BBA0304F14EF96BEB60376791D32C					
	SHA-1	24F6785CA2E82D1D1D61F4CB01D5E753F80445CF					
	Property		Value				
- Mildentifier	Empty		No additional info available				
— 🐁 Import Adder							

40417e937cd244b2f928150	cae6fa			
Member	Offset	Size	Value	Meaning
SizeOfInitializedData	00000120	Dword	00013A00	
SizeOfUninitializedData	00000124	Dword	0000000	
AddressOfEntryPoint	00000128	Dword	0000AB10	.text
BaseOfCode	0000012C	Dword	00001000	
ImageBase	00000130	Qword	00000014000000	
SectionAlignment	00000138	Dword	00001000	
FileAlignment	0000013C	Dword	00000200	
MajorOperatingSystemVers	00000140	Word	0006	
MinorOperatingSystemVers	00000142	Word	0000	
MajorImageVersion	00000144	Word	0000	
MinorImageVersion	00000146	Word	0000	
MajorSubsystemVersion	00000148	Word	0006	
MinorSubsystemVersion	0000014A	Word	0000	
Win32VersionValue	0000014C	Dword	0000000	
SizeOfImage	00000150	Dword	00039000	
SizeOfHeaders	00000154	Dword	00000400	
CheckSum	00000158	Dword	0000000	
Subsystem	0000015C	Word	0003	Windows Console
DIICharacteristics	0000015E	Word	8160	Click here
SizeOfStackReserve	00000160	Qword	000000000100000	
SizeOfStackCommit	00000168	Qword	0000000000001000	
SizeOfHeapReserve	00000170	Qword	000000000100000	
SizeOfHeapCommit	00000178	Qword	000000000001000	
LoaderFlags	00000180	Dword	00000000	
NumberOfRvaAndSizes	00000184	Dword	00000010	



Various file management and external library import functions are contained in the hexadecimal dump (*WriteFile, LoadLibraryExW* and *GetFileType*) of the Portable Executable:

Here is the resource of the manifest file, where execution privileges and security permissions are revealed:

40417e937cd244b2f928150cae6fa						
Configuration Files	<pre><?xml version ='1.0' encoding ='UTF-8' standalone ='yes'?> <assembly manifestversion="1.0" xmlns="urn:schemas-microsoft-com:asm.v1"> <trustinfo urn:schemas-microsoft-com:asm.v3"="" xmlns=""> <security> <requestedfrivileges> <requestedexecutionlevel level="asInvoker" uiaccess="false"></requestedexecutionlevel>   </requestedfrivileges>  </security></trustinfo></assembly></pre>					



In the function *fun\_14000f4a4* we note the call of *QueryPerformanceCounter* in order to monitor the utilization of the Performance Counter and detect a possible execution within a virtualized environment:

asm('movups [rdx], xmm0"); fur_14000bd34(&rdx->f8, &rcx->f8, r8, r9b); return rcx; }	^
<pre>int64_t fun_14000f4a4() {     void*rsp1;     uint64_trax2;     uint64_t v3;     uint64_t v3;     uint64_t v5; </pre>	
<pre>rsp1 = reinterpret_cast<void*>(reinterpret_cast<int64_t>(_zero_stad、offset()) - 40); rax2 = reinterpret_cast<uint64_t>(QueryPerformanceFrequency(reinterpret_cast<int64_t>(rsp1) + 48)); if (!*reinterpret_cast<uint64_t>(QueryPerformanceCounter(reinterpret_cast<int64_t>(QueryPerformanceCounter(reinterpret_cast<int64_t> rax4 = 0.5 g140032c00 = 0.5 g140032c00 = rax4; return 0; }</int64_t></int64_t></uint64_t></int64_t></uint64_t></int64_t></void*></pre>	~(r
void fun_140003bbc() { }	
void fun_1400041d4() { }	
struct s276 { int64_tf0; void*** f8; };	
<pre>struct s277 {     signed char[8] pad8;     void*** f8; };</pre>	
<pre>struct s276* fun_1400066e0(struct s276* rcx, struct s277* rdx, void*** r8, unsigned char r9b) {    asm("xorps xmm0, xmm0");     rcx-&gt;f0 = 0x140022610;    asm("movups [rdx], xmm0");     fun_14000bd34(%rdx-&gt;f8, %rcx-&gt;f8, r8, r9b);</pre>	



# Debugging

By making a debugging session, we can see the .BiBi extension added to files made inaccessible and logging strings of multithreaded executions and Windows boot setting commands:

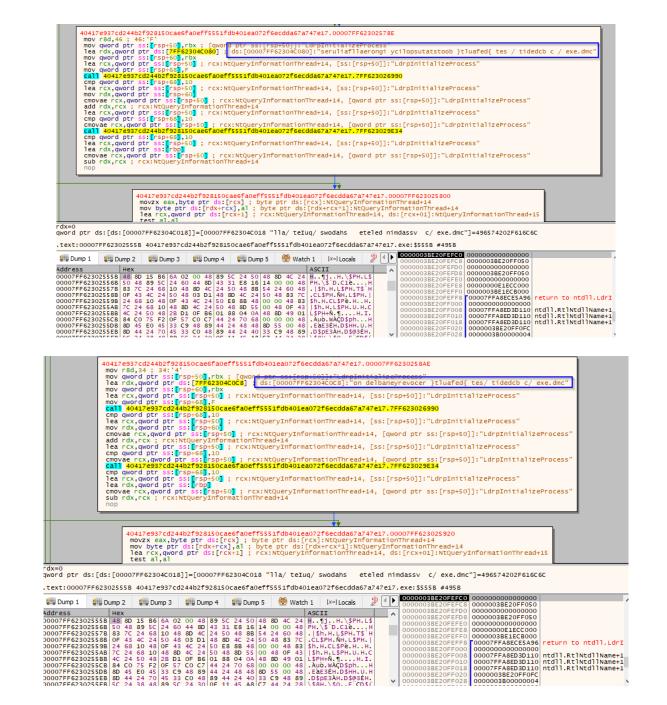
	l. [ds: [ds: [oo		448 48 48 445 48 445 48 445 48 445 48 445 9 48 445 9 48 445 14 445 14 44	: 33F 8 05 39 2877 9 05 2877 224 48 2805 24 48 280 26 47302 280 47506 280 47506 280 47506 280 47506 280 47506 280 4	) 200 200 200 2000 2000 2000 2000 20000 20000 20000 20000 20000 20000 20000 20000 20000 20000 2000 2000 2000 2000 2000 200 200 2000 2000 2000 2000 2000 2000000	[qwor [ss:[ [qwor rcx:N 0A:'\ ds:[0 cs:[ ds:[0 rcx:N rsi:" rcx:N	d ptr ss:[ rsp+38]]:L d ptr ss:[ TueryInfo 0007FF6230 rsp+38]]:L 0007FF6230 tQueryInfo LdrpInitia tQueryInfo 000590042002	rsp+48 drInit (rsp+38 rmatic (4BFD8] (drInit (4BFD8] ormatic (1izePr (1izePr	]]:" Shim ]]:L nThr :L". Shim :L". nThr occes	B1B1" EngineDynamic+37E6 B1B1" ead+14, [ss:[rsp+: s" ead+14	s /namic+37E6	gineDynamic+37E6
.text:00007	FF6230240	6D 40417e93	cd244b2f928	150cae6fa0ef	f5551fd	lb401ea	072f6ecdda	a67 a7 47	'e17.	exe:\$4C6D #406D		
00007FF6230 00007FF6230 00007FF6230 00007FF6230	4BFF8 69 4C008 5B 4C018 6C 4C028 61	00 42 00 69 00 28 00 62 6E 67 20 46 2B 5D 20 52 6C 61 2F 20 68 73 20 20 61 73 20 20	00 42 00 69 00 00 00 58 6F 72 20 51 6F 75 6E 64 74 65 49 75 20 65 74 65 20 20 63 26	000 00 00 00 21 5D 20 55 75 65 75 65 20 25 64 0/ 71 2F 20 7 6C 65 64 2/	0 00 00 7 61 69 5 20 0A A 00 00 3 77 6F 0 6E 69	00 in 00 [+ 64 11 6D ah	II 3.i.B.i F.b[!] N For Queu For Queu Round %d a/ teIuq/ s s eteled	wait e swod nim e.dm ed y mw c	<b>^</b>	0000038E20FFC3 0000038E20FFC3 0000038E20FFC9 0000038E20FFF0 0000038E20FFF0 0000038E20FFF0 0000038E20FF08 0000038E20FF00 0000038E20FF00 0000038E20FF01 0000038E20FF01 0000038E20FF028	00000000000000000000000000000000000000	Ý
Image: Decision of the second secon	4C078 00 4C088 6C 4C098 73 4C0A8 66 4C0B8 63 4C0C8 6F 4C0D8 65 4C0D8 2F 4C0F8 2E	20 65 78 65 00 00 00 00 6C 61 65 72 75 74 61 74 65 64 78 20 62 20 63 20 62 20 64 65 72 20 7D 74 20 74 69 63 46 65 30	2E 64 6D 63 00 00 00 73 6F 6E 67 69 73 74 6F 67 3 20 2F 20 65 78 6C 62 61 6E 6C 75 61 6E 6C 75 61 6E	00 00 00 00 65 72 75 60 62 20 79 63 69 62 20 70 74 2F 20 74 65 65 2E 64 60 65 79 72 65 65 64 78 20 20 63 2F 20 3A 5C 57 73	0 00 00 69 61 9 6C 6F 4 6C 75 9 64 65 9 63 00 5 76 6F 0 74 65 0 65 78 8 65 72	66 70 11a 61 sut 64 fec 00 cb 63 on	<pre>[x=]Locals III exe.dmc seru aerongi yc: tatstoob } i{ tes / t c / exe.dr delbaneyr. }tluafed{ idedcb c/ ncC:\U: .:\[+]]</pre>	liaf ilop tlua ided mc evoc tes exe sers Path		COCOURSIDATION CONTRACTOR CONTRAC	00000000000000000000000000000000000000	return to ntdll.LdrI
Address 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C	118 3A 20 128 63 68 138 64 73	25 73 0A 0 72 65 73 3 3A 20 25 6	0 00 00 58 A 20 25 64 A 0A 00 73	Dump 5 20 63 2F 20 3A 5C 55 73 2B 5D 20 50 2B 5D 20 50 2B 5D 20 43 2C 20 43 2C 20 43 2C 20 44 68 56 6E 64 20 6E 76 61 6C 6E 76 61 6C 73 69 74 69 6F 20 6C 6F 74 6F 6F 20	65 78 65 72 61 74 50 55 72 65 61 74 65 72	73 .dn 68 20 : 9 61 cor 74 ds:	:idedcb c/ icC:\U .:\[+] (s[+] 'es: %d, T %dsend	exe sers Path CPU hrea att	<	0000003820FEC0 0000003820FEC0 000003820FED0 000003820FED0 000003820FEF0 000003820FEF0 000003820FEF0 000003820FF00 000003820FF00 000003820FF00 000003820FF00	0000003BE20FF05 0000000000000000 00000008E1ECE000 000007FFA8ECE5A9 00007FFA8ED3D11 00007FFA8ED3D11 00007FFA8ED3D11 00007FFA8ED3D11 00007FFA8ED3D11	0 0 0 0 0 1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1
Address 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C 00007FF62304C	2F8 52 60 308 52 60 318 52 60 328 00 00	Dump 3 68 6E 6F 7 04 23 F6 7 02 23 F6 7 6C 6C 00 0 73 69 6F 6 52 65 73 6 47 65 74 4 53 68 75 7 45 66 64 5 80 68 6D 8	C 69 73 74 4 64 6F 77 3 65 73 73 E 08 43 00	10         02         23         F6           73         74         72         74           GD         53         74         61           GD         52         65         67           GD         00         00         00           00         00         00         00           65         73         00         00           66         00         00         00           69         6F         6E         00           00         00         00         00	00 00 7F 00 6D 67 72 74 69 73 00 00 00 00 00 00 00 00 00 00	00 hI. 72 A. 53 .dI 74 ess 00 erm 00 RmS 00 RmS 00 RmB 00 RmB	known erro #öRstr 11RmSt Sion.RmRe Resources. SetList. Shutdown. IndSession	ö tmgr arts gist	•	0000003BE20FEFC0 0000003BE20FEFC8 0000003BE20FEFC8 0000003BE20FEFC8 000003BE20FEFC8 000003BE20FFFC8 000003BE20FFFC8 000003BE20FFC8 000003BE20FF08 000003BE20FF08 000003BE20FF08	000003BE20FF05           000000000000000000000000000000000000	0 0 0 0 0 0 0 1 0 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1



Here is an example of a *lea* instruction that copies the hexadecimal value of the attribute containing the shadow copy deletion command within the *rdx* register:

40417e937cd244b2f928150cae6fa0eff5551fdb401ee072f6ecdda67e747e17.00007FF622025558 lea rdx,qword ptr ds:[7FF62304C018] ; ds:[00007FF62304C018]:"lla/ teIuq/ swodahs eteled nimdassv c/ exe.dmc"
<pre>4041/53/CU24402/5230Cd66 ade1355 ds:[00007FF62304C018]:"11a/ teIuq/ swodahs eteled nimdassv c/ exe.dmc" iea rdx.qword ptr ds:[FF62304C018] ds:[00007FF62304C018]:"11a/ teIuq/ swodahs eteled nimdassv c/ exe.dmc" mov qword ptr ds:[F59+50]; rtx: [qw0rd ptr sst[r59750]]: "LdrpIntitalizeProcess" iea rcx.qword ptr sst[r59760]; rtx: NtQueryInformationThread+14, [ss:[r59+50]]:"LdrpIntitalizeProcess" mov qword ptr ds:[F59+60],rbx lea r63,qword ptr ds:[F59+60],rbx</pre>
mov gword ptr ss:[rsp=60], bx lea rsd gword ptr ds:[fbres1]
call 40417e937cd24492f928150Cae6fa0eff5551fdb401ea072f6ecdda67a747e17.7FF623026990 con. gword str. sci.fsca.e63_100
<pre>lea rcx,qword ptr ss:[rsp+50] ; rcx:NtQueryInformationThread+14, [ss:[rsp+50]]:"LdrpInitializeProcess"</pre>
mov rdx, dovid ptr ss.[rsprso] : rcx:NtgueryInformationThread+14, [qword ptr ss:[rsp+50]]:"LdrpInitializeProcess"
<pre>add rox,rcx ; rcx:ntoqueryInformationThread+14 lea rcx,qword ptr_ssi[rsp+50] ; rcx:ntoqueryInformationThread+14, [ss:[rsp+50]]:"LdrpInitializeProcess"</pre>
<pre>cmp qword ptr ss:[rsp+68],10 cmovae rcx,qword ptr ss:[rsp+60]; rcx:NtQueryInformationThread+14, [qword ptr ss:[rsp+50]]:"LdrpInitializeProcess"</pre>
<pre>call a0i1resiz/d24402fs28is0cae6fa0eff5551fdb401ea072f6ecdda67a747e17.7FF623026990 cmp qword ptr ss:[rsp+60]; rcx:htQueryInformationThread+14, [ss:[rsp+50]]:"LdrpInitializeProcess"</pre>
<pre>lea rcx,qword ptr ss: rsp+50]; rcx:NtQueryInformationThread+14, [ss:[rsp+50]]:"LdrpInitializeProcess" lea rdx,qword ptr ss: rbpl</pre>
<pre>cmovae rcx,qword ptr ss:[rsp+50] ; rcx:NtQueryInformationThread+14, [qword ptr ss:[rsp+50]]:"LdrpInitializeProcess" sub rdx.rcx : rcx:NtQueryInformationThread+14</pre>
THE CONTRACT OF A CONTRACT OF
40417e937cd24402f928150cae6faoeff5551fdb401ea072f5ecdda67a74re17.00007FF6230255C1 movzx eax, byte ptr ds:[rcx]; byte ptr ds:[rcx]:htQueryInformationThread+14
<pre>movzx eax,byte ptr ds:[rcx]; byte ptr ds:[rcx]:httpueryInformationThread+14 mov byte ptr ds:[rdx+rcx],al; byte ptr ds:[rdx+rcx+]:httpueryInformationThread+14 lea rcx,qword ptr ds:[rcx+1]; rcx:httpueryInformationThread+14 ds:[rcx+1]:httpueryInformationThread+14</pre>
test al, al <u>ine 40417e937cd244b2f928150cae6fa0eff5551fdb40lea072f6ecdda67a747e17.7FF6230255C1</u>
rdx=0 word ptr ds:[ds:[00007FF62304C018]]=[00007FF62304C018 "]]a/ teIuq/ swodahs eteled nimdassv c/ exe.dmc"]=496574202F616C6C
.text:00007FF62302555B 40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17.exe:\$555B #495B
Dump 1 Jump 2 Jump 3 Jump 4 Jump 5 Hours 2 Watch 1 Ix=l Locals 2 1 00000033E20FEFC8 000000000000000000000000000000000000
Address Hex ASCII 0000038E20FER5 00000038E20FER5 00000038E20FER5
20007FF62302555B 48 8D 15 B6 6A 02 00 48 89 5C 24 50 48 8D 4C 24 H. 1i. H. PH.LS
00007FF62302557B 83 7C 24 68 10 48 80 4C 24 50 48 88 54 24 60 48   \$h. H. L\$PH.T\$" H 0000003BE20FFFF0 0000003BE20FFFF0 0000003BE20FFF0 0000003BE20FFFF0 0000003BE20FFF0 0000003BE20FFF0 0000003BE20FFF0 0000003BE20FFF0 0000003BE20FFF0 0000003BE20FFF0 0000003BE20FFF0 0000003BE20FFF0 000003BE20FFF0 0000003BE20FFF0 000000000BE20FFF0 0000003BE20FFF0 000000000BE20FFF0 0000003BE20FFF0 00000000BE20FFF0 0000000000000BE20FFF0 00000000BE20FFF0 00000000BE20FFF0 00000000BE20FFF0 00000000BE20FFF0 0000000BE20FFF0 00000000BE20FFF0 000000000BE20FFF0 00000000BE20FFF0 00000000BE20FFF0 00000000BE20FFF0 00000000BE20FF0 000000BE20FF0 0000000BE20FFF0 0000000BE20FFF0 00000000BE20FFF0 00000000BE20FFF0 0000000BE20FFF0 0000000BE20FFF0 0000000BE20FFF0 0000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 0000000BE20FFF0 0000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 000000BE20FFF0 00000BE20FFF0 00000BE20FFF0 00000BE20FFF0 00000BE20FF0 00000BE20FFF0 00000BE20FFF0 00000BE20FFF0 00000BE20FFF0 00000BE20FFF0 00000BE20FFF0 00000BE20FF0 0000BE20FF0 00000BE20FF0 0000BE20FF0 0000BE20FF0 00000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 00000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 00000BE20FF0 0000BE20FF0 00000BE20FF0 0000BE20FF0 00000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 0000BE20FF0 00000BE20FF0 0000BE20FF0 00000BE20FF0 00000BE20FF0 00000BE20FF0 00000BE
20007FF623025598 24 68 10 48 0F 43 4C 24 50 E8 88 48 00 00 48 83 \$h.H.C.\$Pè.H.H.
00007FF6230255A8 7C 24 68 10 48 80 4C 24 50 48 80 55 00 48 0F 43 [\$h+h_\$PH.U.H.C 00007FF6230255B8 4C 24 50 48 28 D1 0F B6 01 88 04 0A 48 80 49 01 [\$PH+\$,H.I. 00007FF6230255B8 4C 24 50 48 28 D1 0F B6 01 88 04 0A 48 80 49 01 [\$PH+\$,H.I. 000003E20FF001 00007FFA8ED3D110 ntdll.Rt]NtdlName+1 0000003E20FF001 00007FFA8ED3D110 ntdll.Rt]NtdlName+1 0000003E20FF001 00007FFA8ED3D110 ntdll.Rt]NtdlName+1
D0007FF6230255DB 8D 45 E0 45 33 C9 48 89 44 24 48 48 8D 55 00 48 EaE3ÉH.D\$HH.U.H
20007FF5230255EB 80 44 24 70 5 33 C0 48 89 44 24 40 33 C9 48 89 05 12 12 12 12 12 12 12 12 12 12 12 12 12
<pre>uti//es/tu2+tu2/selsutes aver isssi aver utilises aver isssi aver utilizer of the self of the sel</pre>
40417e937cd244b2f92815Ocae6fa0eff5551fdb401ea072f6ecdda67a747e17.00007FF6230256E0 movz eax,byte ptr ds:[rcx]; byte ptr ds:[rcx]:NtQueryInformationThread+14 mov byte ptr ds:[rcx+rcx],a]; byte ptr ds:[rdx+rcx1]:NtQueryInformationThread+14 lea rcx,qword ptr ds:[rcx+1]; rcx:NtQueryInformationThread+14, ds:[rcx+01]:NtQueryInformationThread+15
<pre>lea rcx,qword ptr ds:[rcx+1]; rcx:NtQueryInformationThread+14, ds:[rcx+0]:NtQueryInformationThread+15 test al.al</pre>
014 10127037cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17.7FF6230256E0
rdx=0 gword ptr ds:[ds:[00007FF62304C018]]=[00007FF62304C018 "]]a/ teIug/ swodahs eteled nimdassv c/ exe.dmc"]=496574202F616C6C
<pre>uword pir ds:[us:[u000/FF62304C018]]=[0000/FF62304C018 11a/ LE1ud/ Sw0uans Elefed InmudsSv C/ Exe.umc ]=+3%5/4202F616C6C .text:00007FF623025558 40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17.exe:\$5558 #4958</pre>
web ump 1         web ump 2         web ump 3         web ump 4         web ump 5         web ump 1         web ump 4         web ump 5         web ump 4         web ump 4         web ump 5         web ump 4         web ump 4 <thweb 4<="" th="" ump=""> <thweb 4<="" th="" ump=""> <thw< td=""></thw<></thweb></thweb>
A0072FF623025558 48 80 15 86 6A 02 00 48 89 5C 24 50 48 80 4C 24 H. 1], H. \\$PH.L\$ 00007FF623025558 [50 48 80 5C 24 60 44 80 43 31 E8 16 14 00 00 48 PH.\\$ D.C1èH
00007FF623025588 0F 43 4C 24 50 48 03 D1 48 8D 4C 24 50 48 83 7C . CLSPH. NH.LSPH. 000003BE20FEFF8 00007FFA8ECESA96 return to ntdll.LdrI
00007FF6230255AB 7C 24 68 10 48 8D 4C 24 50 48 8D 55 00 48 0F 43 [\$h.H.L\$PH.U.H.C 00007FF6230255BB 4C 24 50 48 22 D1 0F B6 01 88 04 0A 48 8D 49 01 L\$PH.U.H.L 000007FF6230255BB 4C 24 50 48 22 D1 0F B6 01 88 04 0A 48 8D 49 01 L\$PH.U.H.L 00000038E20FF010 00007FFA8ED3D110 ntdll.RtlNtdllName+1
00007FF623025558 84 C0 75 F2 0F 57 C0 C7 44 24 70 68 00 00 00 48 LAUG.WACD55hH 00007FF623025558 80 45 E0 45 33 C9 48 89 44 24 48 48 80 50 00 48 LAUG.WACD55hH
00007FF62303305 00 45 26 45 33 C0 48 89 44 24 40 33 C9 48 89 .05pt3Ah.05mt0.1 v 0000003BE20FF020 0000003BE20FF02C 00000000000000000000000000000000





The OSINT classifications of the examined artefact refer to the signature **"Trojan/Win.BiBiWiper.C5541532":** 



57	① 57 security vendors and 2 sandboxes flagged this file as malicious	$\bigcirc$ Reanalyze $\implies$ Similar - More -									
/72	40417e937cd244b2f92815Ocae6fa0eff5551fdb401ea072f6ecdda67a747e1 bibiexe pewe 64bits checks-cpu-name	7	Size Last Analysis Date 203.00 KB a moment ago								
Community Score	heave anore cherve cho renie										
DETECTION DETA	DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 16+										
Join the VT Community	and enjoy additional community insights and crowdsourced detections, plus an	API key to automate checks.									
Popular threat label 🕧	trojan.stealer/bibi Threat categories trojan rar	nsomware	Family labels stealer bibi wiper								
Security vendors' analys	is ①		Do you want to automate checks?								
AhnLab-V3	() Trojan/Win.BiBiWiper.C5541532	Alibaba	TrojanPSW:Win32/Stealer.174fc9b9								
ALYac	Trojan.Agent.Wiper	Antiy-AVL	Trojan/Win64.Filecoder								
Aciac	() Irojan.Agenc.wiper										
Arcabit	① Trojan.Generic.D42E85A7	Avast	() Win32:Bibi-B [Wpr]								
	-	Avast Avira (no cloud)	-								

Here are the identifications of some IDS rules referring to ICMP and Ping operations:



Here is an example of malicious detonation that takes files and makes them accessible by adding the .BiBi extension and a numeric reference attribute.



### Activity Summary

F:\lxcsvwuz7h.bibi1

— 🛞 F:\dashBorder\_192.bmp

F:\nu4nrybhld.bibi1

— 😻 F:\delete.avi

F:\kkesj8mktm.bibi1

— 😻 F:\toolbar.bmp

F:\lbjn9ahsxk.bibi1

#### **Files Dropped**

- + C:\Users\Default User\Application Data\Microsoft\Windows\SendTo\CVticrMb7U.BiBi3 (copy)
- + C:\Users\Default User\Application Data\Microsoft\Windows\SendTo\mji6rELaVg.BiBi3 (copy)
- + C:\Users\Default User\ItfVcM7kEH.BiBi2 (copy)
- + C:\Users\Default User\Local Settings\Microsoft\Windows\Shell\j8RbPMfTmV.BiBi4 (copy)
- + C:\Users\Default User\M9k5iX5yCh.BiBi2 (copy)
- + C:\Users\Default User\SendTo\UMGBLwzpGG.BiBi4 (copy)
- + C:\Users\Default User\guKHsGa1zb.BiBi2 (copy)
- + C:\Users\Default User\lbl7Y4cu5z.BiBi2 (copy)
- + C:\Users\Default User\vs2Werllgv.BiBi2 (copy)
- + C:\Users\Default\5f915EmUbN.BiBi1

The screenshot below shows the handling of system attributes while obtaining the files to be overwritten detected by the execution of a *while* loop:



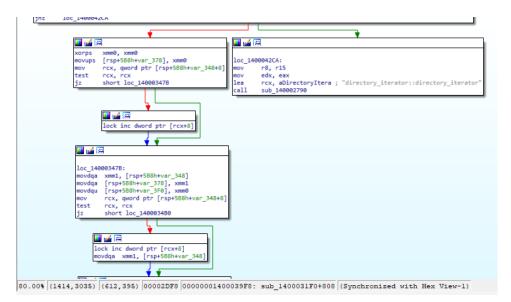


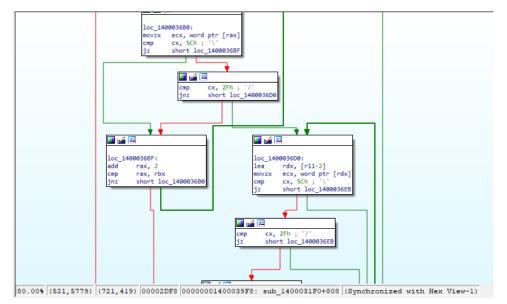
The following file types are "skipped" during malware execution: .exe, .dll and .sys.

	- -	9			-		~~~		A	~		halfs in a	
🕮 CPU 🛛		Notes	<ul> <li>Breakp</li> </ul>	oints 📖	Memory Map	Call Stack	SEH 🧐	Script	ٵ Symbols	Source	References	🛸 Threads	
			DDC93280 DDC93283										
			DDC93283 DDC93285										
			DDC 93280										
			DDC 932 95	Faword	ptr ss:[rsp	+16011:Term	srvGetWindo	wsDirecto	r v/w				
			DDC9329D	L'duoi a	per bortrop		Strucchinde						
			DDC932A5										
	• 0	0007FF7	DDC932B1										
	• 0	0007FF7	DDC932BA										
			DDC932BF		D07FF7DDCBBF								
			DDC932C6	rcx:Nt(	QueryInforma	tionThread+	14, [ss:[rs	p+160]]:T	ermsrvGetWind	lowsDirector	УW		
			DDC932CE										
			DDC932D3										
			DDC 932D 4										
			DDC932DC DDC932E4	Faword	ptr ss:[rsp		KnownD11c"						
			DDC932F0	[ [qwor u	bri ssifist	HI20]].C //	KHOWHDTTS						
			DDC932F9										
			DDC932FE	ds: Foo	007FF7DDCBBF	881:0 ". d11"							
			DDC93305		QueryInforma								
			DDC9330D										
	• 0	0007FF7	DDC93312										
	• 0	0007FF7	DDC93313										
			DDC9331B										
			DDC93323										
			DDC9332F										
			DDC 93338	Lan Food									
			DDC9333D DDC93344		D07FF7DDCBBF QueryInforma		14						
			DDC 9334C	The contract of the second	quel y in orma	cronni eau+	14						
			DDC93351										
			DDC93352										
			DDC 93355										
=0				-									
rd ptr d	ls:[ds:[00	007FF7DD	CBBFA8]]=	=[00007FF	7DDCBBFA8 L	'.exe"]=6500	780065002E						
t:00007	FF7DDC 9321	BF 40417	e937cd244	b2f92815	0cae6fa0eff	551fdb401ea	072f6ecdda	57a747e17.	exe:\$32BF #2	SBF			
	Dump 2	D D	ump 3 🔋	Dump 4	💷 Dump 5	🧶 Watch 1	[x=] Locals	2 🔹	00000011814F		00000000000 011814FEEC0		
Dump 1	B Dump 2												
ress	Hex					ASC		<u>^</u>		EE40 000000			
ess 07FF7DDCI	Hex BBF48 61	74 GF 72			5 6E 61 6D	65 00 00 ato	or++renam	e	00000011814F	EE48 000000	11814FEEC0		
ress 07FF7DDCI	Hex BBF48 61 BBF58 69	74 GF 72 GE 76 G1	L 6C 69 64	\$ 20 73 7	4 GF 69 20	65 00 00 ato 61 72 67 inv	or++renam /alid stoi	e arg		EE48 000000 EE50 000000	011814FEEC0		
ress 07FF7DDCI 07FF7DDCI 07FF7DDCI	Hex BBF48 61 BBF58 69 BBF68 75	74 6F 72 6E 76 61 6D 65 6E	L 6C 69 64	4 20 73 7 0 00 73 7	4 6F 69 20 4 6F 69 20	55 00 00 ato 51 72 67 inv 51 72 67 umo	or++renam /alid stoi entstoi	e arg arg	00000011814F 00000011814F	EE48 000000 EE50 000000 EE58 000000	11814FEEC0		
ress 07FF7DDC 07FF7DDC 07FF7DDC 07FF7DDC	Hex BBF48 61 BBF58 69 BBF68 75 BBF78 75	74 GF 72 GE 76 G1 GD 65 GE GD 65 GE	L 6C 69 64 74 00 00 74 20 6	4 20 73 7 0 00 73 7 5 75 74 2	4 6F 69 20 4 6F 69 20 0 6F 66 20	65 00 00 ato 61 72 67 inv 51 72 67 umo 72 61 6E umo	or++renam /alid stoi entstoi ent out of	e arg arg ran	00000011814F 00000011814F 00000011814F 00000011814F	EE48 000000 EE50 000000 EE58 000000 EE60 000000	011814FEEC0 00000000000 000812C5000 011812C4000	eturn to ntdl'	1.Ld
ress 07FF7DDC 07FF7DDC 07FF7DDC 07FF7DDC 07FF7DDC	Hex BBF48 61 BBF58 69 BBF68 75 BBF78 75 BBF78 67	74 GF 72 GE 76 G1 GD G5 GE GD G5 GE GD G5 GE	L 6C 69 64 74 00 00 74 20 68 0 00 00 00	4 20 73 7 0 00 73 7 75 74 2 0 00 5B 2	4 6F 69 20 4 6F 69 20 0 6F 66 20 8 5D 20 53	65 00 00 ato 51 72 67 inv 51 72 67 ume 72 61 6E ume 74 61 74 ge	or++renam valid stoi entstoi ent out of [+] S	e arg arg ran	00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F	EE48 00000 EE50 00000 EE58 00000 EE60 00000 EE68 00007 EE70 00000	011814FEEC0 0000000000 000812C5000 011812C4000 FFD83C25A96 00000000000		
ress 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1	Hex BBF48 61 BBF58 69 BBF68 75 BBF78 75 BBF78 75 BBF78 73	74 6F 72 6E 76 61 6D 65 6E 6D 65 6E 65 00 00 3A 20 25	L 6C 69 64 74 00 00 74 20 66 0 00 00 00 6 64 20 70	4 20 73 7 0 00 73 7 5 75 74 2 0 00 5B 2 2 20 25 6	4 6F 69 20 4 6F 69 20 0 6F 66 20 8 5D 20 53 4 0A 00 00	55 00 00 ato 51 72 67 inv 51 72 67 ume 72 61 6E ume 74 61 74 ge 50 00 00 s:	or++renam valid stoi entstoi ent out of [+] S %d   %d	e arg arg ran	00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F	EE48 000000 EE50 000000 EE58 000000 EE60 000000 EE68 00007 EE70 00000 EE78 00007	011814FEEC0 0000000000 000812C5000 011812C4000 FFD83C25A96 r0000000000 FFD83C7D110 n	tdll.RtlNtdll	Name
r ess 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1	Hex BBF48 61 BBF58 69 BBF68 75 BBF78 75 BBF88 67 BBF88 67 BBF98 73 BBFA8 2E	74 6F 72 6E 76 61 6D 65 6E 6D 65 6E 65 00 00 3A 20 25 00 65 00	L 6C 69 64 74 00 00 74 20 66 0 00 00 00 64 20 70 78 00 65	4 20 73 7 0 00 73 7 7 75 74 2 0 00 5B 2 2 20 25 6 5 00 00 0	4 6F 69 20 4 6F 69 20 0 6F 66 20 8 5D 20 53 4 0A 00 00 0 00 00 00	55         00         00         atc           51         72         67         inv           51         72         67         ume           72         61         6E         ume           74         61         74         ge           00         00         00         s:           00         00         00         s:	or++renam /alid stoi entstoi ent out of [+] S %d   %d e.x.e	e arg arg ran	00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F	EE48 000000 EE50 000000 EE58 000000 EE60 000000 EE70 00000 EE78 00007 EE78 00007	011814FEEC0 0000000000 000812C5000 011812C4000 FFD83C25A96 r 00000000000 FFD83C7D110 n FFD83C7D110 n	tdll.RtlNtdll tdll.RtlNtdll	Name Name
r ess 07FF7DDC0 07FF7DDC0 07FF7DDC0 07FF7DDC0 07FF7DDC0 07FF7DDC0 07FF7DDC0 07FF7DDC0	Hex BBF48 61 BBF58 69 BBF68 75 BBF78 75 BBF78 75 BBF88 67 BBF98 73 BBFA8 2E BBF88 2E	74 GF 72 GE 76 G1 GD G5 GE GD G5 GE G5 00 00 GA 20 25 D0 G5 00 D0 G4 00	L 6C 69 64 74 00 00 74 20 66 0 00 00 00 64 20 70 78 00 65 0 6C 00 60	4 20 73 7 0 00 73 7 7 75 74 2 0 00 58 2 2 20 25 6 5 00 00 0 0 00 0	4 6F 69 20 4 6F 69 20 0 6F 66 20 8 5D 20 53 4 0A 00 00 0 00 00 00 0 00 00 00	55         00         00         atc           51         72         67         inv           51         72         67         ume           72         61         6E         ume           74         61         74         ge           00         00         00         s:           00         00         00         s:           00         00         00         s:	or++renam /alid stoi entstoi ent out of [+] S %d   %d e.x.e. 	e arg arg ran	00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F	EE48 000000 EE50 000000 EE50 000000 EE60 000000 EE68 00007 EE70 00000 EE78 00007 EE88 00007	011814FEEC0 0000000000 000812C5000 011812C4000 FFD83C25A96 r 00000000000 FFD83C7D110 n FFD83C7D110 n FFD83C7D110 n	tdll.RtlNtdll	Name Name
ress 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1 07FF7DDC1	Hex BBF48 61 BBF58 69 BBF68 75 BBF78 75 BBF88 67 BBF98 73 BBF48 22 BBF88 22 BBF88 22 BBF88 22	74 6F 72 6E 76 61 6D 65 6E 6D 65 6E 65 00 00 3A 20 25 00 65 00 00 64 00 00 73 00	L 6C 69 64 74 00 00 74 20 66 0 00 00 00 64 20 70 78 00 65 0 6C 00 60 79 00 73	4         20         73         7           0         00         73         7           7         75         74         2           0         00         58         2           20         00         58         2           20         00         00         0           5         00         00         0           0         00         00         0           0         00         00         0	4 6F 69 20 4 6F 69 20 0 6F 66 20 8 5D 20 53 4 0A 00 00 0 00 00 00 0 00 00 00 0 00 00 00	55         00         00         atc           51         72         67         inv           51         72         67         dm           72         61         62         um           74         61         74         ge.           00         00         00         s:         00           00         00         00          00           00         00         00          00	or++renam /alid stoi entstoi ent out of [+] S %d   %d e.x.e. 1.1.1	e arg arg ran tat	00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F	EE48         000000           EE50         000000           EE58         000000           EE68         000000           EE70         00000           EE78         00007           EE88         00007           EE88         00007           EE88         00007           EE88         00007           EE88         00007	011814FEEC0 0000000000 000812C5000 011812C4000 FFD83C25A96 r 00000000000 FFD83C7D110 n FFD83C7D110 n FFD83C7D110 n 011814FEF6C	tdll.RtlNtdll tdll.RtlNtdll	Name Name
07FF7DDCI 07FF7DDCI 07FF7DDCI 07FF7DDCI 07FF7DDCI 07FF7DDCI 07FF7DDCI 07FF7DDCI 07FF7DDCI	Hex           BBF48         61           BBF58         69           BBF68         75           BBF88         67           BBF98         73           BBF88         2E           BBF28         2E           BBF28         2E           BBF28         2E           BBF28         2E           BBF28         2E           BBF28         2E	74 6F 72 6E 76 61 6D 65 6E 6D 65 6E 65 00 00 3A 20 25 00 65 00 00 64 00 00 73 00 00 42 00	L 6C 69 64 74 00 00 74 20 66 0 00 00 00 5 64 20 70 0 78 00 65 0 6C 00 66 0 79 00 73 0 69 00 43	4         20         73         7           0         00         73         7           7         75         74         2           0         00         58         2           20         20         25         6           000         00         00         0           0         00         00         0           0         00         00         0           0         00         00         0           0         00         00         0           0         00         00         0           0         00         00         0	4 6F 69 20 4 6F 69 20 0 6F 66 20 8 5D 20 53 4 0A 00 00 0 00 00 00 0 00 00 00	55         00         00         atc           51         72         67         inv           51         72         67         uma           72         61         62         uma           72         61         74         ge.           00         00         00         s:         00           00         00         00          00           00         00         00             00         00         00             00         00         00             00         00         00	<pre>pr++renam valid stoi entstoi ent out of[+] S %d   %d e.x.e d.l.l s.y.s i.i.B.i</pre>	e arg arg ran tat	00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F 00000011814F	EE48         000000           EE50         000000           EE58         000000           EE68         000000           EE70         00000           EE78         00007           EE88         00007           EE88         00007           EE88         00007           EE88         00007           EE88         00007	011814FEEC0 0000000000 000812C5000 011812C4000 FFD83C25A96 r 00000000000 FFD83C7D110 n FFD83C7D110 n FFD83C7D110 n	tdll.RtlNtdll tdll.RtlNtdll	Name Name

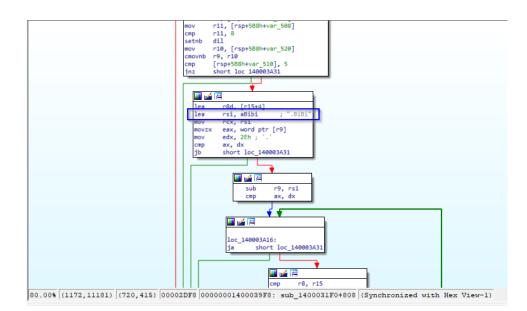


In the function *sub\_1400031F0* the iteration of the system directories is carried out, once the files to be made inaccessible have been identified, they are partially overwritten with a random pattern generated and inserted within the stream that can be highlighted in function *sub\_1400048D0*. After the overwriting action has been performed, the files taken in consideration are renamed with the extension **.BiBi** and a specific digit.







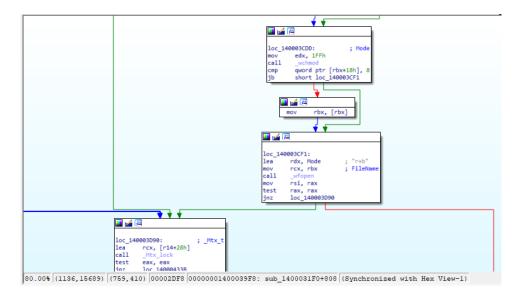


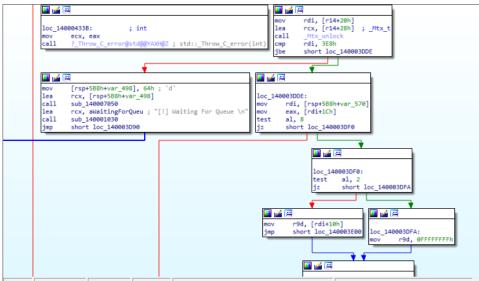
### Files are opened with the *r+b configuration (read or write mode)*

cmp qword ptr [rbx+18h], 8 jb short loc_1400038FE
loc_140003BFE: lea rdx, Node ; "r+b" callwfopen mov rsi, rax test rax, rax jnz loc_140003D90
call _errmo cap dword ptr [rax], 00h jnz loc_140003F6A
call cs:GetLastError cmp eax, 20h; '' jnz loc_140003CD0
80.00% (1089,14265) (728,403) 00002DF8 0000001400039F8: sub_1400031F0+808 (Synchronized with Hex View-1)

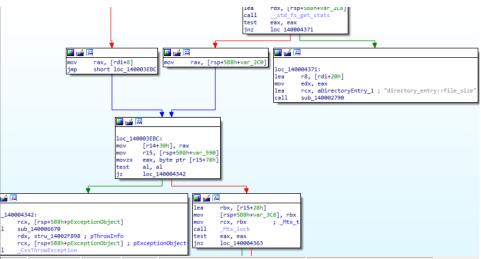
The *mutex* objects for the files in question are then put in *lock* status in order to allow exclusive access to them, without interference from any external processes:





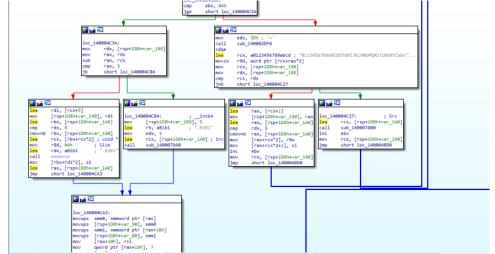


80.00% (973,16252) (737,411) 00002DF8 0000001400039F8: sub\_1400031F0+808 (Synchronized with Hex View-1)

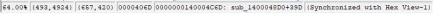


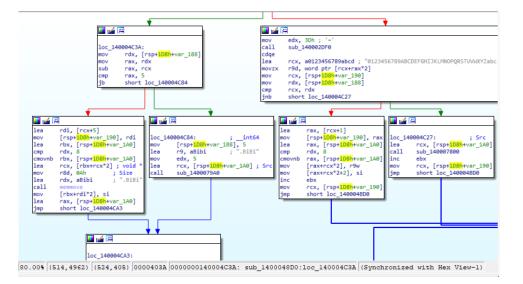
80.00% (1068,18149) (717,389) 00002DF8 0000001400039F8: sub\_1400031F0+808 (Synchronized with Hex View-1)

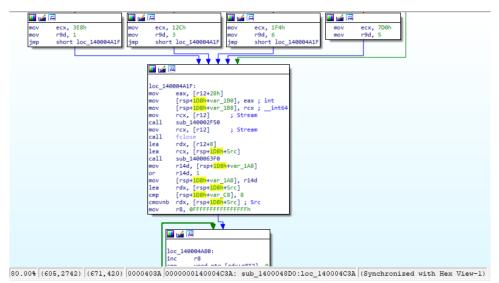




### Here the handling of the random pattern contextual to the overwriting of enumerated files:

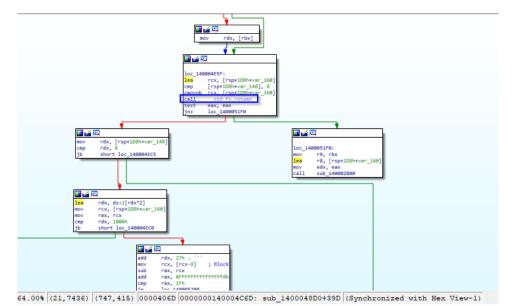








### Note the action of renaming overwritten files:



<sup>🖾 (</sup>PII) 🕼 I on 👘 Notes • Breakmoints 🗰 Memory Man 🦳 Call Stady 📨 SEH 💿 Scrint 💽 Symbols 🗘 Sympose 🖓 Deferences 👒 Threads 🚚 🌗

	Z LOG		otes	Brea	акроіп	ts	ann b	iemor	у мар			aii St	аск	SEH	1	Scription	pt	Symbols	- X2	Source	≥ Reference	es 🛥	Inreads		Ľ
			cdqe lea rc movzx mov rc mov rd cmp rc	x,qword r9d,wor x,qword x,qword x,rdx	ptrd d ptr ptrs ptrs	s: (7FF ds: (no s: (nspi s: (nspi s: (nspi	00CBC (+rax*) 48 50	[10]; []	ds: (00	007FF7	7 DDC BC	1A0]:	L "012	7 e17.7FF700C 23456789ABCDE 7e17.7FF700C9	FGHIJK	MNO PQR S	stuw	wxvZabcdefghijklmoj	oqrstuvi	wxyz*					
		- 17											-it								-1				
37cd244b2f925150c x,quord ptr 5:5 fal7e937cd244b2f9 x,quord ptr 5:5 \$17e937cd244b2f92	rsp+38] 28150cae6fa0 rsp+48]	eff 5 55 1	fdb401ea072	f 6e cd da	a 67a 747	e17.7F	F 700 C9	7800									lea nov lea cmp cmo mov nov nov	170937cd244b2f92815 a rax, qword ptr ds: v qword ptr ss:[ray a rax, qword ptr ss:] ordx,8 ordx,8 v word ptr ds:[rax+ v word ptr ds:[rax+ v cebx v rcx,qword ptr ss:] a 40417e937cd244b2f	[rcx+1] 48], rax rsp+38 ss:rsp rcx+2], rcx+2+2]	* -38] -9w ],si					
																_					1.				
																	4041 cmp 198	17e937cd244b2f928150 ebx,A ; 0A:'\n' 40417e937cd244b2f							
																	_							_	
																	mov sub	17e937cd244b2f92815 v rdx.qword ptr ss: v rax.rdx p rax.rcx p rax.5 40417e937cd244b2f9.	rsp+50	1					
													<u> </u>												
						lea nov	quord r9,quo edx,5	nd ptr	: [n sp +2	F700C	BBFDS			a 07 2f 6e c dd a6 7 0 07 FF 70 D CB BF 0			¥ F 70	00094084						0417e937c lea rd1,c nov quoro lea rbx,c rmn rdx S	d pt dwor
edx=0 3D '=' .text:00007	FF7DDC94	BD 5	40417e9	37cd2	244b2	f928	1500	ae6f	a0ef	f555	i1fd	b401	Lead	)72f6ecdd	la67a	747e1	17.	exe:\$4BD5 #3F	D5						
Ump 1										-	🐌 w			Inc. I to a set	-	<b>9</b> 1		00000011814F	EE30	00000	00000000000				~
	Ump 🕹		Ump Dump	5	0-0 L	ump 4	•	- Du	mp 5	5	VV VV	_	_	[x=] Locals	5 A	g ()	빅	00000011814F 00000011814F			011814FEEC0				
Address 00007FF7DDC	He 190110 58		5D 2015	0.61	74.5	0 2 *	20	25.2	2 0 1	00	00		ASCI				^	00000011814F			011814FEEC0				
00007FF7DDC 00007FF7DDC	BC120 58 BC130 64	2B 2C	5D 20 4 20 54 6	3 50 8 72	55 2 65 6	0 63	6F 73	72 G 3A 2	5 73 0 25	3A 64	20 0A	25 00	(+) d, 1	Path: %s CPU core Threads:	es: 9 %d			00000011814F 00000011814F 00000011814F	EE58	00000	00000000000 000812C5000 011812C4000				
00007FF7DDC 00007FF7DDC 00007FF7DDC	BC150 60	65	6E 64 2 20 63 6 76 61 6		73 G		00	00 0	0 00	00	00	00	leo	d attempt closed alid stri				00000011814F 00000011814F 00000011814F	EE68 EE70	00007 00000	FFD83C25A96 00000000000 FFD83C7D110		to ntdll		
00007FF7DDC 00007FF7DDC 00007FF7DDC	BC180 6F	6F	20 GC 6	9 6F F 6E 0 6C	67 0	0 64	65	71 7	5 65	ЗC	54	3E (	DO 1	tion.vect long.dequ o long	ie <t></t>			00000011814F 00000011814F	EE80 EE88	00007 00007	FFD83C7D110 FFD83C7D110	ntdll.F	tlntdllntdlln	Name+1	
00007FF7DDC	BC1A0 30	00	31 00 3	2 00	33 0	0 34	00	35 0	0 36	00	37	00	0.1.	.2.3.4.5.	6.7.		~	00000011814F 00000011814F			011814FEF6C 01100000004				¥
<																>		<						>	



## **IOCs:**

- e26bba0304f14ef96beb60376791d32c
- 24f6785ca2e82d1d1d61f4cb01d5e753f80445cf
- 40417e937cd244b2f928150cae6fa0eff5551fdb401ea072f6ecdda67a747e17
- .BiBi
- 2e 42 69 42 69

# **YARA Rule**

rule	e BiBiRu	ıle		
{				
S	trings:			

\$strBiBi = ".BiBi"

\$hexBiBi = { 2e 42 69 42 69 }

condition:

\$strBiBi or \$hexBiBi

}



## **CONCLUSIONS:**

BiBi Wiper is a threat that follows the pattern of the wipers used in the context of the Russian-Ukrainian conflict, such as HermeticWiper or IsaacWiper (developed and disseminated immediately before Russia's de facto invasion on 24 February 2022).

In this specific case, however, there are some differentiating elements compared to the abovementioned threats: the data and files taken in consideration in the enumeration phase are rendered inaccessible and overwritten by means of a random pattern. However, the analyzed behaviour doesn't belong to a ransomware classification, as no ransom is demanded for the recovery of files by means of a ransom note created on infected machines. The threat's only objective is to perpetrate its destructive action against the adversary's main critical infrastructures, and it can be associated with the ever-present concept of hybrid warfare that we have become familiar with due to the current delicate geopolitical situation.

A key feature of this concept is the fact that, even without military belligerence, devastating results can still be achieved. Attention was also paid to managing resources and files potentially in use by other external processes and to modifying Windows start-up settings, as well as to eliminating shadow copies in order to maximize the threat's impact.

The growing and constant risk of an increasingly compromised and deteriorating geopolitical situation leads one to assume that the development and distribution of such malware will increase. These threats will be increasingly sophisticated, evasive and destructive.

References:

[0] (introduction to BiBi Wiper): <u>BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows</u> (blackberry.com)