

pehash brbbot.exe

```
remnux@remnux:~/Malware/day1$ pehash brbbot.exe
file
  filepath:          brbbot.exe
  md5:              1c7243c8f3586b799a5f9a2e4200aa92
  sha1:             4db5a8e237937b6d7b435a8506b8584121a7e9e3
  sha256:           f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e
  ssdeep:           1536:b6sMD3H8V3jsUnHLiREsTbDV/48004vh47483gLi9+LSG:b6srVzJiRrTHV0Re75g4+LS
  imphash:          475b069fec5e5868caeb7d4d89236c89
```

[https://www.virustotal.com/gui/file/\[Hash File\]](https://www.virustotal.com/gui/file/[Hash File])

58
/ 72

?

Community Score

58 security vendors and 1 sandbox flagged this file as malicious

f47060d0f7de5ee651878eb18dd2d24b5003bdb03ef4f49879f448f05034a21e

brbbot.exe

peexe assembly runtime-modules direct-cpu-clock-access 64bits persistence

74.00 KB

Size

2022-11-24 18:39:41 UTC

1 month ago

Q1
EX

b5003bdb03ef4f49879f448f05034a21e

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Gen.Variant.Fugrafa.10989
AhnLab-V3	Trojan.Win.Blocker.R448988	Alibaba	Ransom.Win32/Blocker.863e972d
ALYac	Trojan.Ransom.Blocker.gen	Antiy-AVL	Trojan[Ransom]/Win32.Blocker
Arcabit	Trojan.Fugrafa.D2AED	Avast	Win32:Agent-BCKN [Trj]
AVG	Win32:Agent-BCKN [Trj]	Avira (no cloud)	TR/Blocker.srvdv
BitDefender	Gen.Variant.Fugrafa.10989	Comodo	Malware.@#27qzfujyxzofk
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.8f3586
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.Encoder.27924	Elastic	Malicious (high Confidence)
Emsisoft	Gen.Variant.Fugrafa.10989 (B)	eScan	Gen.Variant.Fugrafa.10989
ESET-NOD32	Win64/Agent.HQ	F-Secure	Trojan.TR/Blocker.srvdv
Fortinet	W64/Agent.HQltr	GData	Gen.Variant.Fugrafa.10989
Google	Detected	Gridinsoft (no cloud)	Ransom.Win64.Blocker.vbls1
Ikarus	Trojan.Win64.Agent	Jiangmin	Trojan.Blocker.ivu
K7AntiVirus	Trojan (005141831)	K7GW	Trojan (005141831)
Kaspersky	Trojan-Ransom.Win32.Blocker.kdyo	Kingsoft	Win32.Troj.Undef(kcloud)
Lionic	Trojan.Win32.Blocker.trtV	Malwarebytes	Malware.AI.4197897917
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.11730447.susgen

File Section

property	value	value	value	value	value	value
name	.text	.rdata	.data	.pdata	.rsrc	.reloc
md5	BBD3AF727B760F43F799...	17F740269D4D7B5A4DB...	2E35BBDF7154182A2211...	41D59B361C2388908534...	60DBB5E97FAB0B443417...	839270E9B89F3DE10367...
file-ratio (98.65 %)	66.22 %	19.59 %	6.76 %	4.05 %	0.68 %	1.35 %
virtual-size (83651 bytes)	49823 bytes	14426 bytes	15616 bytes	2820 bytes	192 bytes	774 bytes
virtual-address	0x00001000	0x0000E000	0x00012000	0x00016000	0x00017000	0x00018000
raw-size (74752 bytes)	50176 bytes	14848 bytes	5120 bytes	3072 bytes	512 bytes	1024 bytes
raw-address	0x00000400	0x0000C800	0x00010200	0x00011600	0x00012200	0x00012400
cave (1597 bytes)	353 bytes	422 bytes	0 bytes	252 bytes	320 bytes	250 bytes
entropy	6.349	4.760	1.973	4.505	1.868	2.555

peframe brbbot.exe

```
-----
File Information (time: 0:00:15.376038)
-----
filename      brbbot.exe
filetype      PE32+ executable (GUI) x86-64, for MS Windows
filesize      75776
hash sha256   f47060d0f7de5ee651878eb18dd2d24b5003bdbb03ef4f49879f448f05034a21e
virustotal    /
imagebase     0x140000000 *
entrypoint    0x3f94
imphash       475b069fec5e5868caeb7d4d89236c89
datetime      2015-02-25 06:12:18
dll           False
directories    import, tls, resources, relocations
sections      .rdata, .data, .pdata, .rsrc, .reloc, .text *
features      mutex, antidebg, packer, crypto

-----
Yara Plugins
-----
IsPE64
IsWindowsGUI
HasRichSignature
Advapi Hash API

-----
Behavior
-----
anti dbg
Xor
network http
screenshot
win registry
win files operation

-----
Crypto
-----
Advapi Hash API
```

```
-----  
Sections Suspicious  
-----
```

```
.text          6.34
```

pestr brbbot.exe

```
CONFIG  
brbconfig.tmp  
YnJlYm90  
exec  
file  
conf  
exit  
sleep  
encode  
%02x  
%s?i=%s&c=%s&p=%s  
APPDATA  
Software\Microsoft\Windows\CurrentVersion\Run  
brbbot  
Microsoft Enhanced Cryptographic Provider v1.0  
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)  
HTTP/1.1  
Connection: close  
ZwQuerySystemInformation  
ntdll.dll  
Idle  
regSetValueExA  
RegOpenKeyExA  
RegDeleteValueA  
RegFlushKey  
RegCloseKey  
CryptAcquireContextW  
CryptDeriveKey  
CryptReleaseContext  
CryptEncrypt  
CryptCreateHash  
CryptDestroyKey
```

Access Malware Windows Flare

```
remnux@remnux:~/Malware/day1$ python3 -m http.server 9001
Serving HTTP on 0.0.0.0 port 9001 (http://0.0.0.0:9001/) ...
192.168.153.1 - - [03/Jan/2023 11:10:35] "GET / HTTP/1.1" 200 -
192.168.153.1 - - [03/Jan/2023 11:10:35] code 404, message File not found
192.168.153.1 - - [03/Jan/2023 11:10:35] "GET /favicon.ico HTTP/1.1" 404 -
192.168.153.1 - - [03/Jan/2023 11:10:43] "GET /brbbot.zip HTTP/1.1" 200 -
```

Pestudio

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

File Help

c:\users\rem\desktop\malwar

- indicators (2/11)
- virustotal (network error)
- dos-stub (!This program c
- file-header (Feb.2015)
- optional-header (GUI)
- directories (5)
- sections (98.65%)
- libraries (2/5)

type	size	blacklist (55)	hint (7)	whitelist (96)	group (15)	value (1050)
ascii	40	-	x	-	-	!This program cannot be run in DOS mode.
ascii	6	-	x	-	-	@.rsr
ascii	13	-	x	-	-	brbconfig.tmp
ascii	45	-	x	-	-	Software\Microsoft\Windows\CurrentVersion\Run
ascii	63	-	x	-	-	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
ascii	9	-	x	-	-	ntdll.dll
unicode	10	-	x	-	-	USER32.DLL

Libraries Used

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000F948	N/A	0000F414	0000F418	0000F41C	0000F420	0000F424
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	14	00010C90	00000000	00000000	00011148	0000E000
WININET.dll	9	00010FD0	00000000	00000000	00011212	0000E340
WS2_32.dll	5	00011020	00000000	00000000	0001121E	0000E390
KERNEL32.dll	86	00010D08	00000000	00000000	0001144C	0000E078
USER32.dll	1	00010FC0	00000000	00000000	00011462	0000E330

OFTs	FTs (IAT)	Hint	Name
Qword	Qword	Word	szAnsi
00000000000011050	00000000000011050	027D	RegSetValueExA
00000000000011062	00000000000011062	0260	RegOpenKeyExA
00000000000011072	00000000000011072	0247	RegDeleteValueA
00000000000011084	00000000000011084	0253	RegFlushKey
00000000000011092	00000000000011092	0230	RegCloseKey
000000000000110A0	000000000000110A0	00B1	CryptAcquireContextW
000000000000110B8	000000000000110B8	00B5	CryptDeriveKey

Ke Registry

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\brbbot: "C:\Users\REM\AppData\Roaming\brbbot.exe"

HKLM\SYSTEM\ControlSet001\Control\Session Manager\PendingFileRenameOperations: 5C 3F 3F 5C 43 3A 5C 55 73 65 72 73 5C 52 45 4D 5C 44 65 73 6B 74 6F 70 5C 4D 61 6C 77 61 72 65 5C 44 61 79 31 5C 6F 74 5C 62 72 62 62 6F 74 2E 65 78 65 00 00 5C 3F 3F 5C 43 3A 5C 55 73 65 72 73 5C 52 45 4D 5C 44 65 73 6B 74 6F 70 5C 4D 61 6C 77 61 72 65 5C 44 61 79 31 5C 62 72 62 62 6F 74 5C 62 72 62 63 6F 67 2E 74 6D 70 00 00 00

HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations: 5C 3F 3F 5C 43 3A 5C 55 73 65 72 73 5C 52 45 4D 5C 44 65 73 6B 74 6F 70 5C 4D 61 6C 77 61 72 65 5C 44 61 79 31 62 62 6F 74 5C 62 72 62 62 6F 74 2E 65 78 65 00 00 5C 3F 3F 5C 43 3A 5C 55 73 65 72 73 5C 52 45 4D 5C 44 65 73 6B 74 6F 70 5C 4D 61 6C 77 61 72 65 5C 44 61 79 31 5C 62 72 62 62 6F 74 5C 62 72 62 66 69 67 2E 74 6D 70 00 00 00

HKU\S-1-5-21-1866265027-1870850910-1579135973-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\REM\Desktop\Malware\Day1\brbbot\brbbot.exe: 50 01 00 00 00 00 00 00 07 00 00 00 28 00 00 00 00 28 01 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 0A 73 20 00 00 DB 80 FD AC 28 39 D3 01 00 00 00 00 00 00 00 00