ID: 336687
Sample Name: BFSV-1F(N)_1B-8B_ANSI.exe
Cookbook: default.jbs
Time: 17:30:37
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

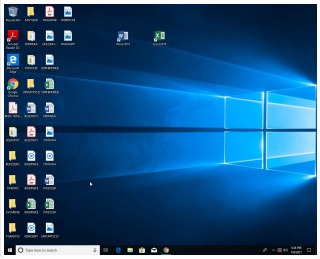
Analysis Report BFSV-1F(N)_1B-8B_ANSI.exe

Overview

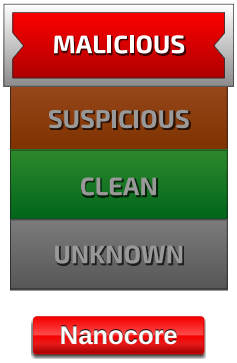
General Information

Sample Name:	BFSV-1F(N)_1B-8B_ANSI.exe
Analysis ID:	336687
MD5:	157d3320cafb979.
SHA1:	b8dc9d3720b846..
SHA256:	5b474ca6fc8158b..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

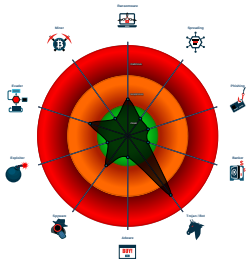


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Nanocore RAT
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- Program does not show much activi…
- Sample file is different than original

Classification



Startup

- **System is w10x64**
- BFSV-1F(N)_1B-8B_ANSI.exe (PID: 5812 cmdline: 'C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe' MD5: 157D3320CAFB9799ED5D996692E8BEA7)
  - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 6560 cmdline: 'C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe' MD5: 157D3320CAFB9799ED5D996692E8BEA7)
  - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 5748 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
    - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 5728 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
    - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 4544 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
      - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 2228 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
      - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 6592 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
        - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 6584 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
        - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 4944 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
          - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 6980 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
          - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 6648 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
            - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 6884 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
            - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 6644 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
              - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 7140 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
              - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 7100 cmdline: C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe MD5: 157D3320CAFB9799ED5D996692E8BEA7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0000000A.00000002.691981291.0000000000D0 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000002.691981291.0000000000D0 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2135d:$x1: NanoCore Client.exe • 0x215e5:$x2: NanoCore.ClientPluginHost • 0x22c1e:$s1: PluginCommand • 0x22c12:$s2: FileCommand • 0x23ac3:$s3: PipeExists • 0x2987a:$s4: PipeCreated • 0x2160f:$s5: IClientLoggingHost
0000000A.00000002.691981291.0000000000D0 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000002.691981291.0000000000D0 0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2134d:$a: NanoCore • 0x2135d:$a: NanoCore • 0x21591:$a: NanoCore • 0x215a5:$a: NanoCore • 0x215e5:$a: NanoCore • 0x213ac:$b: ClientPlugin • 0x215ae:$b: ClientPlugin • 0x215ee:$b: ClientPlugin • 0x214d3:$c: ProjectData • 0x21eda:$d: DESCrypto • 0x298a6:$e: KeepAlive • 0x27894:$g: LogClientMessage • 0x23a8f:$i: get_Connected • 0x22210:$j: #=q • 0x22240:$j: #=q • 0x2225c:$j: #=q • 0x2228c:$j: #=q • 0x222a8:$j: #=q • 0x222c4:$j: #=q • 0x222f4:$j: #=q • 0x22310:$j: #=q
00000008.00000002.686570986.000000000287 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 38 entries				

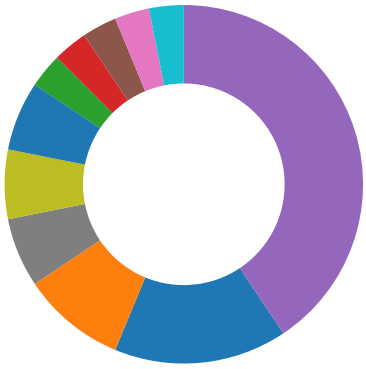
Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.BFSV-1F(N)_1B-8B_ANSI.exe.2870000.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1d9e5:$x1: NanoCore.ClientPluginHost • 0x1da22:$x2: IClientNetworkHost • 0x21555:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
8.2.BFSV-1F(N)_1B-8B_ANSI.exe.2870000.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1d75d:$x1: NanoCore Client.exe • 0x1d9e5:$x2: NanoCore.ClientPluginHost • 0x1f01e:$s1: PluginCommand • 0x1f012:$s2: FileCommand • 0x1fec3:$s3: PipeExists • 0x25c7a:$s4: PipeCreated • 0x1da0f:$s5: IClientLoggingHost
8.2.BFSV-1F(N)_1B-8B_ANSI.exe.2870000.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8.2.BFSV-1F(N)_1B-8B_ANSI.exe.2870000.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1d74d:$a: NanoCore • 0x1d75d:$a: NanoCore • 0x1d991:$a: NanoCore • 0x1d9a5:$a: NanoCore • 0x1d9e5:$a: NanoCore • 0x1d7ac:$b: ClientPlugin • 0x1d9ae:$b: ClientPlugin • 0x1d9ee:$b: ClientPlugin • 0x1d8d3:$c: ProjectData • 0x1e2da:$d: DESCrypto • 0x25ca6:$e: KeepAlive • 0x23c94:$g: LogClientMessage • 0x1fe8f:$i: get_Connected • 0x1e610:$j: #=q • 0x1e640:$j: #=q • 0x1e65c:$j: #=q • 0x1e68c:$j: #=q • 0x1e6a8:$j: #=q • 0x1e6c4:$j: #=q • 0x1e6f4:$j: #=q • 0x1e710:$j: #=q
13.2.BFSV-1F(N)_1B-8B_ANSI.exe.a10000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1d9e5:$x1: NanoCore.ClientPluginHost • 0x1da22:$x2: IClientNetworkHost • 0x21555:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 51 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

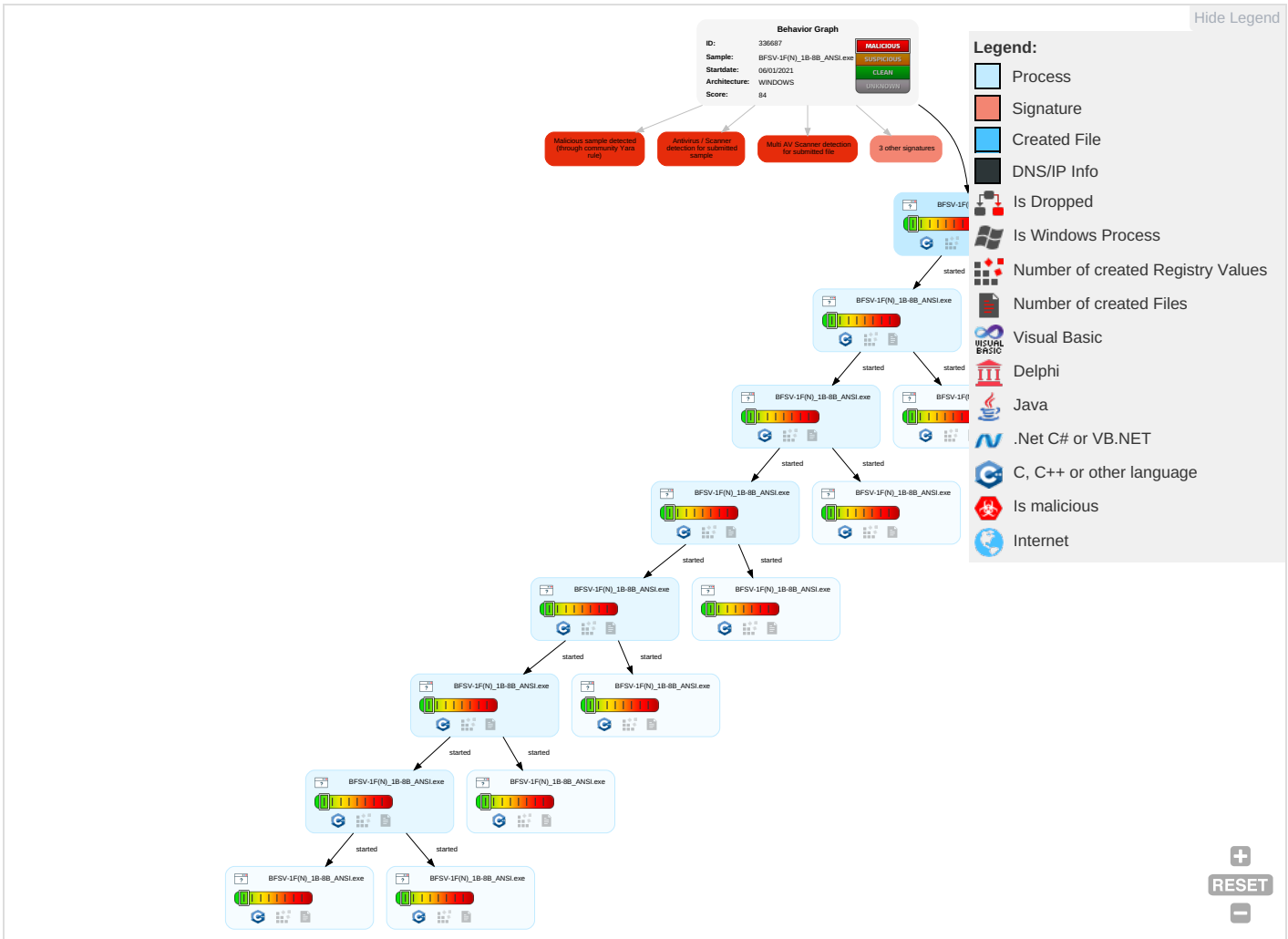
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Software Packing 1	Input Capture 1	Process Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
BFSV-1F(N)_1B-8B_ANSI.exe	43%	ReversingLabs	Win32.Trojan.Generic	
BFSV-1F(N)_1B-8B_ANSI.exe	100%	Avira	TR/Dropper.Gen	
BFSV-1F(N)_1B-8B_ANSI.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.BFSV-1F(N)_1B-8B_ANSI.exe.c90000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
10.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.2.BFSV-1F(N)_1B-8B_ANSI.exe.1430000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.2910000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.BFSV-1F(N)_1B-8B_ANSI.exe.14c0000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.2.BFSV-1F(N)_1B-8B_ANSI.exe.d60000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.BFSV-1F(N)_1B-8B_ANSI.exe.d60000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.2.BFSV-1F(N)_1B-8B_ANSI.exe.2c40000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.2.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
3.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
1.0.BFSV-1F(N)_1B-8B_ANSI.exe.3e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336687
Start date:	06.01.2021
Start time:	17:30:37

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BFSV-1F(N)_1B-8B_ANSI.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.winEXE@29/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.5209083744680925
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	BFSV-1F(N)_1B-8B_ANSI.exe
File size:	451584
MD5:	157d3320cafb9799ed5d996692e8bea7
SHA1:	b8dc9d3720b84695bc18a4310a5f34e2603fc829
SHA256:	5b474ca6fc8158bd6f14d53bca8962f25db3392dfe324f49ddf376610bd785e4
SHA512:	aafe5ef3c4e7f0f24eb41da724b6a518bf18f5226e00e3318a888ab0b69de6724ee3da4fa210080f29f254f6a043ecfaa4753a841a21ef6f3f39c338feed8983
SSDEEP:	12288:aVZsUDYE0ewlQyiKIRhyIAI6vFxxBEEmfVfXeVKl:aV7XGQyjl2IAJxxA52Kl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&+..bJ..bJ..bJ...=K.nJ..bJ..MJ...U..aJ...V..`J...U..iJ..E.<.cJ..E.;.cJ..E.>.cJ..RichbJ.....PE..L...>t._.....R.

File Icon

Icon Hash:	74f4c4ccccd4d0d4

Static PE Info

General

Entrypoint:	0x425eef
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FF5743E [Wed Jan 6 08:26:38 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	31c815897a3b55d8d8afcee958fa181c

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 004270D0h
push 00426070h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 68h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
xor ebx, ebx
mov dword ptr [ebp-04h], ebx
push 00000002h
call dword ptr [00427044h]
pop ecx
or dword ptr [00428054h], FFFFFFFFh
or dword ptr [00428058h], FFFFFFFFh
call dword ptr [00427048h]
mov ecx, dword ptr [00428050h]
mov dword ptr [eax], ecx
call dword ptr [0042704Ch]
mov ecx, dword ptr [0042804Ch]
mov dword ptr [eax], ecx
mov eax, dword ptr [00427050h]
mov eax, dword ptr [eax]
mov dword ptr [0042805Ch], eax
call 00007F8C60F8ED06h
cmp dword ptr [00428030h], ebx
jne 00007F8C60F8EBFEh
push 0042606Ch
call dword ptr [00427054h]
pop ecx
call 00007F8C60F8ECD8h
push 0042800Ch
push 00428008h
call 00007F8C60F8ECC3h
mov eax, dword ptr [00428048h]
mov dword ptr [ebp-6Ch], eax
lea eax, dword ptr [ebp-6Ch]
push eax
push dword ptr [00428044h]
lea eax, dword ptr [ebp-64h]
push eax
lea eax, dword ptr [ebp-70h]
push eax
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [0042705Ch]
push 00428004h
push 00428000h
call 00007F8C60F8EC90h

Rich Headers

Programming Language:	• [C] VS98 (6.0) build 8168 • [LNK] VS2012 build 50727 • [C] VS2012 build 50727 • [LNK] VS98 (6.0) imp/exp build 8168 • [RES] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x270dc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x29000	0x4138	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2e000	0xa4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x27000	0xd0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x25124	0x25200	False	0.416831071128	data	5.57014558903	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0x5ac	0x600	False	0.51171875	data	4.78880407178	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x28000	0x60	0x200	False	0.056640625	data	0.195201267787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x29000	0x4138	0x4200	False	0.816761363636	data	7.55093870165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2e000	0x264	0x400	False	0.1689453125	data	1.22391765681	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x29100	0x2615	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x2b730	0x1a05	data	English	United States
RT_GROUP_ICON	0x2b718	0x14	data	English	United States

Imports

DLL	Import
MSVCRT.dll	_controlfp, _except_handler3, __set_app_type, __p__fmode, __p__commode, _adjust_fdiv, __setusermatherr, _initterm, __getmainargs, _acmdln, free, exit, _XcptFilter, _exit, malloc
KERNEL32.dll	GetStartupInfoA, GetModuleHandleA
MSACM32.dll	acmDriverMessage, acmDriverPriority, acmFilterChooseW, acmFilterDetailsA, acmFilterEnumW, acmFormatTagEnumW
mscms.dll	UnregisterCMMA, CloseColorProfile, UninstallColorProfileW, CheckBitmapBits
WINSPOOL.DRV	DeleteMonitorA, EnumMonitorsA, EnumPrintProcessorDatatypesW, PrinterMessageBoxA, ResetPrinterW, GetPrinterA, AddPrinterConnectionW
COMDLG32.dll	GetFileTitleW, ChooseColorW, ReplaceTextA, PageSetupDlgA
SHLWAPI.dll	GetMenuPosFromID, StrCmpNW, StrToIntW, SHQueryValueExA, PathGetDriveNumberA, PathFindNextComponentW, SHRegEnumUSKeyW

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

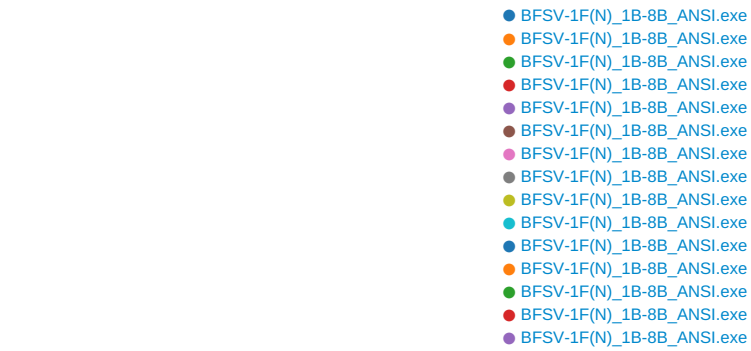
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 5812 Parent PID: 6084

General

Start time:	17:31:25
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe'
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.658023980.0000000000D70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.658023980.0000000000D70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.658023980.0000000000D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.658023980.0000000000D70000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 6560 Parent PID: 5812

General

Start time:	17:31:28
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe'
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 5748 Parent PID: 5812

General

Start time:	17:31:29
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.664101566.0000000001430000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.664101566.0000000001430000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.664101566.0000000001430000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.664101566.0000000001430000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 5728 Parent PID: 5748

General

Start time:	17:31:31

Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 4544 Parent PID: 5748

General

Start time:	17:31:31
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.670372139.0000000001530000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.670372139.0000000001530000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.670372139.0000000001530000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.670372139.0000000001530000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 2228 Parent PID: 4544

General

Start time:	17:31:33
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 6592 Parent PID: 4544

General

Start time:	17:31:34
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.675497262.0000000002F40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.675497262.0000000002F40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.675497262.0000000002F40000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.675497262.0000000002F40000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 6584 Parent PID: 6592

General

Start time:	17:31:36
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 4944 Parent PID: 6592

General

Start time:	17:31:37
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000

File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.686570986.0000000002870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.686570986.0000000002870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.686570986.0000000002870000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.686570986.0000000002870000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 6980 Parent PID: 4944

General

Start time:	17:31:38
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 6648 Parent PID: 4944

General

Start time:	17:31:39
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.691981291.0000000000D00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.691981291.0000000000D00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.691981291.0000000000D00000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.691981291.0000000000D00000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 6884 Parent PID: 6648

General

Start time:	17:31:43
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 6644 Parent PID: 6648

General

Start time:	17:31:44
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.1018854481.0000000000A10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.1018854481.0000000000A10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.1018854481.0000000000A10000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.1018854481.0000000000A10000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 7140 Parent PID: 6644

General

Start time:	17:31:46
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x3e0000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 7100 Parent PID: 6644

General

Start time:	17:31:47
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
Imagebase:	0x360000
File size:	451584 bytes
MD5 hash:	157D3320CAFB9799ED5D996692E8BEA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis