ID: 337281
Sample Name: BFSV-1F(N)_1B-8B_ANSI.exe
Cookbook: default.jbs
Time: 09:23:02
Date: 08/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

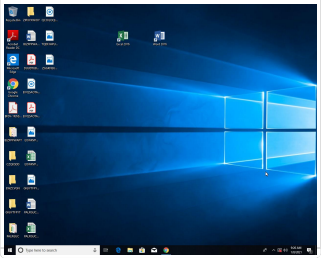
Analysis Report BFSV-1F(N)_1B-8B_ANSI.exe

Overview

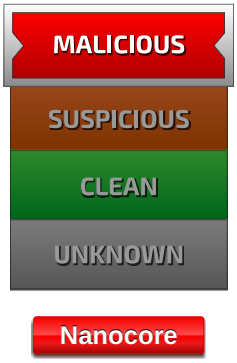
General Information

Sample Name:	BFSV-1F(N)_1B-8B_ANSI.exe
Analysis ID:	337281
MD5:	36f13aad903e851.
SHA1:	776d3d7e39a8b3..
SHA256:	41617ac4431c22..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

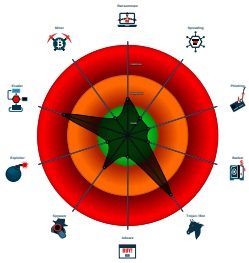


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Nanocore Rat
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Checks if Antivirus/Antispyware/Fire…
- Contains functionality to read the PEB
- Contains functionality which may be…

Classification



Startup

- **System is w10x64**
- BFSV-1F(N)_1B-8B_ANSI.exe (PID: 5932 cmdline: 'C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe' MD5: 36F13AAD903E851544FE137FECA3435B)
  - BFSV-1F(N)_1B-8B_ANSI.exe (PID: 4420 cmdline: 'C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe' MD5: 36F13AAD903E851544FE137FECA3435B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.242826392.0000000000D40000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.242826392.0000000000D40000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2135d:$x1: NanoCore Client.exe • 0x215e5:$x2: NanoCore.ClientPluginHost • 0x22c1e:$s1: PluginCommand • 0x22c12:$s2: FileCommand • 0x23ac3:$s3: PipeExists • 0x2987a:$s4: PipeCreated • 0x2160f:$s5: IClientLoggingHost
00000000.00000002.242826392.0000000000D40000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.242826392.0000000000D40000.00000004.00000001.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:$j: #=q
Process Memory Space: BFSV-1F(N)_1B-8B_ANSI.exe PID: 5932	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10dff2:$x1: NanoCore.ClientPluginHost • 0x10e053:$x2: IClientNetworkHost • 0x113458:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x1213ca:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 2 entries				

Unpacked PEs

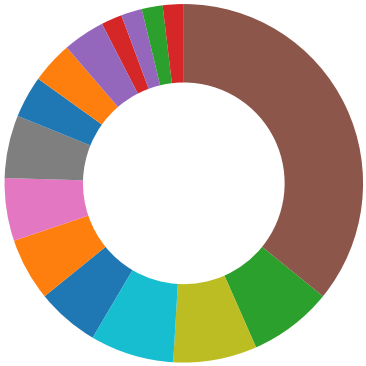
Source	Rule	Description	Author	Strings
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.d40000.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1d9e5:$x1: NanoCore.ClientPluginHost • 0x1da22:$x2: IClientNetworkHost • 0x21555:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.d40000.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1d75d:$x1: NanoCore Client.exe • 0x1d9e5:$x2: NanoCore.ClientPluginHost • 0x1f01e:$s1: PluginCommand • 0x1f012:$s2: FileCommand • 0x1fec3:$s3: PipeExists • 0x25c7a:$s4: PipeCreated • 0x1da0f:$s5: IClientLoggingHost
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.d40000.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.d40000.2.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:$j: #=q
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.d40000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x215e5:$x1: NanoCore.ClientPluginHost • 0x21622:$x2: IClientNetworkHost • 0x25155:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

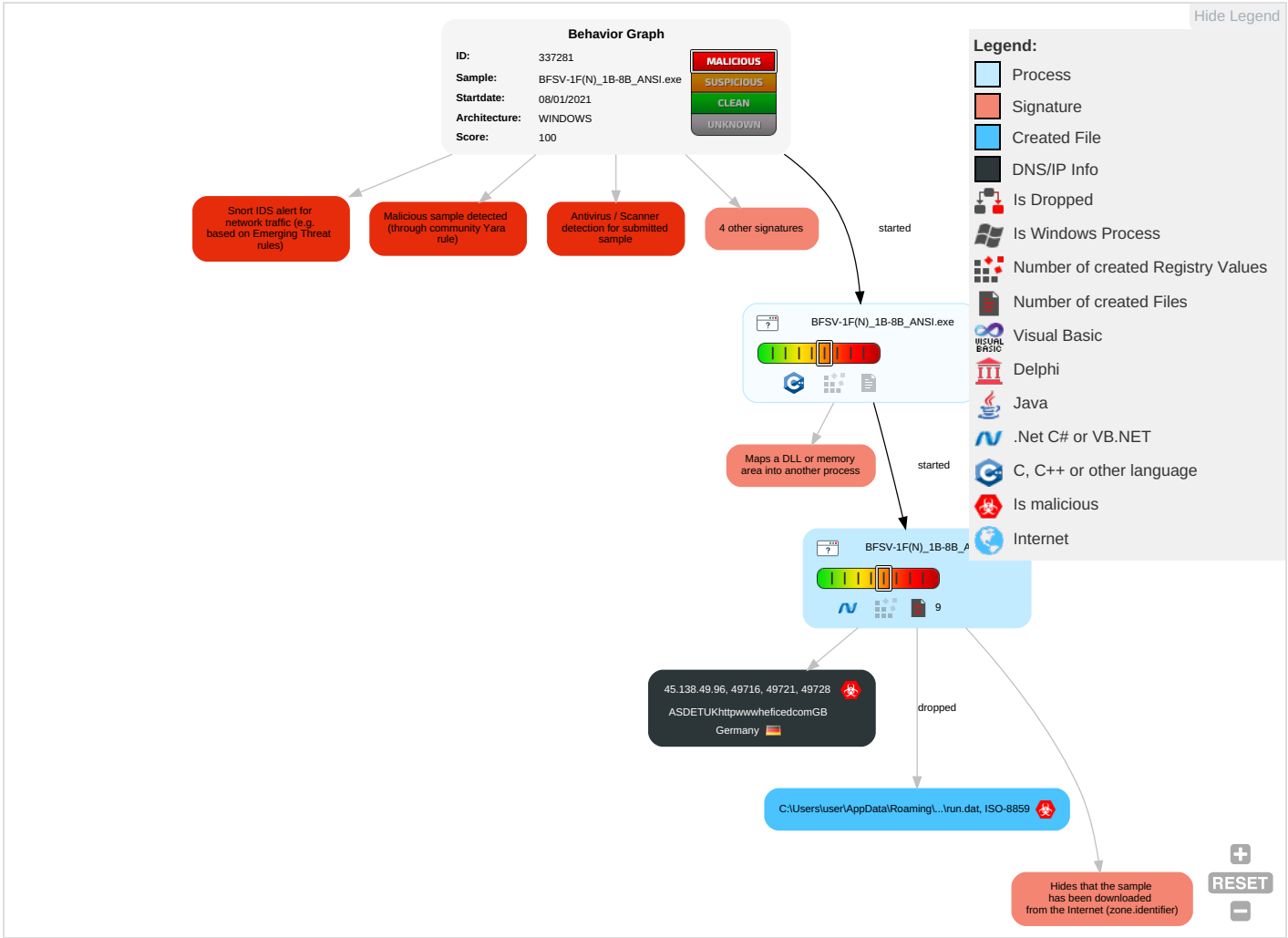
Remote Access Functionality:

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	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1 1	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service

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	100%	Avira	TR/Crypt.XPACK.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
0.2.BFSV-1F(N)_1B-8B_ANSI.exe.d20000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.BFSV-1F(N)_1B-8B_ANSI.exe.d20000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.BFSV-1F(N)_1B-8B_ANSI.exe.d20000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

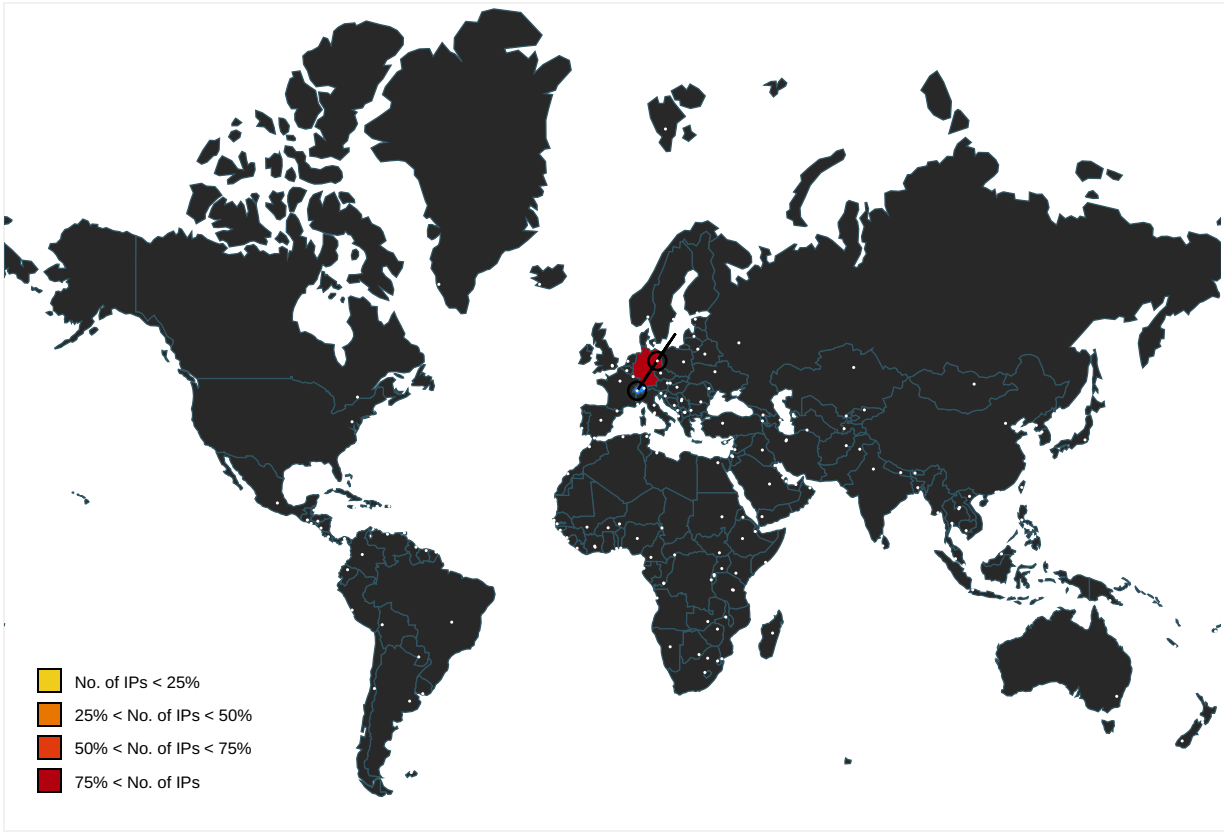
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.138.49.96	unknown	Germany		61317	ASDETUKhttpwwwheficedcomGB	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337281
Start date:	08.01.2021
Start time:	09:23:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 20s
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:	34
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:	mal100.troj.evad.winEXE@3/4@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, SgrmBroker.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:24:10	API Interceptor	1454x Sleep call for process: BFSV-1F(N)_1B-8B_ANSI.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.138.49.96	ts1593782194000000.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASDETUKhttpwwwheficedcomGB	ts1593782194000000.exe	Get hash	malicious	Browse	• 45.138.49.96
	http://https://mysp.ac/WJKWebxcAX/../4lj3C#fCfAXmrBDFsvHupFQHQULbmkQvY	Get hash	malicious	Browse	• 181.214.121.98
	http://https://storage.googleapis.com/hjjdkkejsdido/ar.html	Get hash	malicious	Browse	• 181.214.121.98
	SecuriteInfo.com.Variant.Bulz.286556.17709.exe	Get hash	malicious	Browse	• 191.96.184.151
	http://https://00000000.rdtk.io/5fea58f1588f49000120c69f?thru=thru2	Get hash	malicious	Browse	• 154.16.134.180
	http://p4fxv.info/D3c2Hp2HMI	Get hash	malicious	Browse	• 154.16.134.180
	http://p4fxv.info/D3c2Hp2HMI	Get hash	malicious	Browse	• 154.16.134.180
	http://https://uwvhagmjgz.objects-us-east-1.dream.io/1.html#qs=r-acacaegfhckeadkfkgjejaejcckababababadhadbfaccadieacjjkagggbcacb	Get hash	malicious	Browse	• 154.16.134.180
	Requestforprices..xlsx	Get hash	malicious	Browse	• 181.214.31.82
	SecuriteInfo.com.Trojan.BtcMine.3311.17146.exe	Get hash	malicious	Browse	• 181.214.59.30
	Shipping_Details.exe	Get hash	malicious	Browse	• 181.214.142.116
	zSPIyck1p9.exe	Get hash	malicious	Browse	• 181.214.142.116
	Shipping_Details.exe	Get hash	malicious	Browse	• 181.214.142.116
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 154.16.46.128
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 154.16.46.128
	rJz6SePuqu.dll	Get hash	malicious	Browse	• 191.96.108.132
	Inv_RM55024.exe	Get hash	malicious	Browse	• 181.214.142.131
	Receipt.exe	Get hash	malicious	Browse	• 181.214.142.131
	3yhnaDfaxn.exe	Get hash	malicious	Browse	• 154.16.46.128
	file 010.20.doc	Get hash	malicious	Browse	• 45.150.64.102

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
File Type:	data
Category:	dropped
Size (bytes):	1392
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUt4:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/f
MD5:	E78C6686C5A1A9CB0724F84DEA9A75F0
SHA1:	80E61D5BDC7AF293362024781DA66BEA9D370FF9
SHA-256:	FBE0B513511C00AC3B7169E1BCFB675CFD708B249365D724269C23FAC1184967
SHA-512:	FF3835238CAEA26D8800B56901AB962ACD2FA390F955C4A8A15B5817AAB7642D105538CF63938D218567501477FB4B23C2834F22CBC8BA0002C7BCACB2875637
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:nvt:n1
MD5:	3F3CD5C288B64A7072F09AC01296FBC4
SHA1:	E46242146BEBEFF9D2FF11B8C187518025E4E182
SHA-256:	35943387C3ACAE14B8EE9FA76521D176C82DEB8F1BA2EDDB1F3BDCFF2863236B
SHA-512:	A02091D483EB31B5590C522B6AD3192134BD1C3BED2D53ACAB699579EF4A6B882547006D443289B0CEDBEA6C0BC94CF2A596120F71E0C9FB7137C187F7F30CA C
Malicious:	**true**
Reputation:	low
Preview:	...5...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_....Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.860141249668034

General

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:	346624
MD5:	36f13aad903e851544fe137feca3435b
SHA1:	776d3d7e39a8b3e72e2e9b5c36a615e3157d05ad
SHA256:	41617ac4431c229ba27bf94617b465309e7f502ae5088cc12ee571a0428ea120
SHA512:	77a68e34a1bbf2360f8473368a0e3fd9c54567477a29561980851b82bd8ac1655919a109d6d4456a67bd633ef436ff4697fc77d17e03e701d36ee7b82f296e6
SSDEEP:	6144:cvnifsw4lp4UlclMNJO2OOZNYQjJntWar4u0PYlcf2ELdYyfHwgF2r2QQvipF:snL3lklmOkYstWa/7cfNLyR2kF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.3.g.]Ug.]Ug.]U..\Tv.]Ug.\UN.]U..SUf.]U..YTf.]U...Uf.]U..._Tf.]URichg.]U.....PE..L....._.....

File Icon

Icon Hash:	74f4c4ccccd4d0d4

Static PE Info

General

Entrypoint:	0x410000
Entrypoint Section:	.stub
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:	0x5FF7808C [Thu Jan 7 21:43:40 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:	6a01311f3b93e75b0932a2018ac2171e

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
mov eax, 00001A30h
call 00007FC2FCA2FBC8h
call 00007FC2FCA3DE33h
mov dword ptr [ebp-0Ch], eax
call 00007FC2FCA3DFABh
push 0000000Ah
push 004100D4h
push 00000000h
call dword ptr [00403024h]
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [ebp-04h]
push eax

Instruction
push 00000000h
call dword ptr [00403010h]
mov dword ptr [ebp-08h], eax
push 00001A05h
mov ecx, dword ptr [ebp-08h]
push ecx
lea edx, dword ptr [ebp-00001A30h]
push edx
call 00007FC2FCA3DF15h
mov ecx, 00000000h
mov al, byte ptr [ebp+ecx-00001A30h]
cmp ecx, 00001A05h
je 00007FC2FCA3EC02h
xor al, A3h
dec al
sub al, A3h
inc al
add al, A7h
dec al
add al, 40h
sub al, 8Bh
add al, 72h
xor al, ADh
sub al, E1h
add al, D6h
dec al
xor al, 99h
sub al, C3h
inc al
add al, 28h
add al, F0h
mov byte ptr [ebp+ecx-00001A30h], al
add ecx, 01h
jmp 00007FC2FCA3EB93h
mov al, 00h
mov ecx, 00000000h
lea eax, dword ptr [ebp-10h]
push eax
push 00000040h
push 00001A05h
lea ecx, dword ptr [ebp-00001A30h]
push ecx
call dword ptr [00403014h]
push 00000000h
push 00000000h
push 00000002h
lea edx, dword ptr [ebp-00001A30h]
push edx
call dword ptr [00403020h]
lea eax, dword ptr [ebp+00h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x30c4	0xb4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11000	0x4138	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x16000	0x80	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2000	0x1c	.data
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0xc4	.idata
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	0x15a	0x200	False	0.42578125	data	3.57394794431	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2000	0x150	0x200	False	0.37890625	data	2.5909148946	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x3000	0x576	0x600	False	0.486328125	data	4.62959328748	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.code	0x4000	0xb454	0xb600	False	0.499291723901	data	5.38349156704	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.stub	0x10000	0xe6	0x200	False	0.40625	data	3.07398255133	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x4138	0x4200	False	0.817412405303	data	7.56696464821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x16000	0x80	0x200	False	0.26953125	data	1.68689486927	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x11100	0x2615	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0x13730	0x1a05	data	English	United States
RT_GROUP_ICON	0x13718	0x14	data	English	United States

Imports

DLL	Import
KERNEL32.dll	LoadResource, VirtualProtect, GetProcessHeap, HeapAlloc, EnumLanguageGroupLocalesW, FindResourceW
wsnmp32.dll	
COMDLG32.dll	ChooseFontW, ReplaceTextA, PrintDlgA
SETUPAPI.dll	SetupOpenMasterInf, SetupDiCreateDeviceInfoListExA, SetupDiGetDeviceInfoListDetailW, SetupQueryDrivesInDiskSpaceListW, SetupDiCancelDriverInfoSearch, SetupQueryFileLogA
ole32.dll	OleCreateEmbeddingHelper, DllGetClassObjectWOW, OleGetIconOfFile, OleQueryLinkFromData, HWND_UserSize
WINSPOOL.DRV	FindNextPrinterChangeNotification, DeletePrinterDriverA, DeletePrinterDataW, DocumentPropertiesA, EnumPrinterDataExA, AddFormA
SHLWAPI.dll	SHRegGetBoolUSValueW, StrSpnA, StrRChrIA, SHDeleteEmptyKeyW, UrlEscapeW
loadperf.dll	UnloadPerfCounterTextStringsA, LoadPerfCounterTextStringsA

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/08/21-09:24:11.140705	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	9999	192.168.2.3	45.138.49.96
01/08/21-09:24:17.902668	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	9999	192.168.2.3	45.138.49.96
01/08/21-09:24:25.388192	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	9999	192.168.2.3	45.138.49.96
01/08/21-09:24:31.278859	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	9999	192.168.2.3	45.138.49.96
01/08/21-09:24:37.425775	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	9999	192.168.2.3	45.138.49.96
01/08/21-09:24:44.986569	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	9999	192.168.2.3	45.138.49.96
01/08/21-09:24:51.260108	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	9999	192.168.2.3	45.138.49.96
01/08/21-09:24:58.098409	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:03.147692	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:09.262215	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:15.224134	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:21.269898	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:27.242753	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:33.237074	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:39.241771	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:45.227980	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:51.238341	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	9999	192.168.2.3	45.138.49.96
01/08/21-09:25:57.259892	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:03.246907	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:09.229937	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:15.229234	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:21.249433	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:27.232176	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:34.829754	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:41.886345	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:47.983092	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	9999	192.168.2.3	45.138.49.96
01/08/21-09:26:54.327113	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	9999	192.168.2.3	45.138.49.96
01/08/21-09:27:02.343670	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	9999	192.168.2.3	45.138.49.96

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:24:11.053262949 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.093405008 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.095838070 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.140705109 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.185173035 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.194889069 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.235156059 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.257477999 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.317126989 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.340390921 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.340504885 CET	9999	49716	45.138.49.96	192.168.2.3

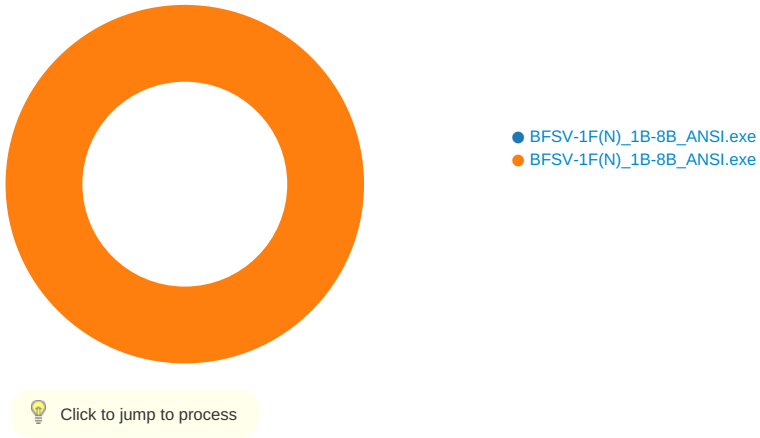
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:24:11.340545893 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.340631008 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.340713024 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.340735912 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.380659103 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.380758047 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.380801916 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.380870104 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.380924940 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.380947113 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.380964041 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.380986929 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.381031036 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.381095886 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.381148100 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.381150961 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.392416000 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421037912 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421087027 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421143055 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421180010 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421191931 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421211004 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421227932 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421267033 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421278000 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421282053 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421324015 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421365023 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421375990 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421380997 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421422005 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421456099 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421495914 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421541929 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421547890 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421546936 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421590090 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421642065 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421643972 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421648026 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421700954 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421741962 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421768904 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421817064 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.421868086 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.421875954 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.457406044 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.461874962 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.461918116 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.461977005 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462019920 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462064981 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462124109 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462148905 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462166071 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462213039 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462255001 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462316990 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462321043 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462332010 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462393999 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462450027 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462503910 CET	9999	49716	45.138.49.96	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 8, 2021 09:24:11.462569952 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462591887 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462598085 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462652922 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462696075 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462748051 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462784052 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462795019 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462800026 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462832928 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462871075 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462928057 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.462985039 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.462989092 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.463010073 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463052034 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463104010 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463151932 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463212013 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463274002 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.463273048 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463279009 CET	49716	9999	192.168.2.3	45.138.49.96
Jan 8, 2021 09:24:11.463323116 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463383913 CET	9999	49716	45.138.49.96	192.168.2.3
Jan 8, 2021 09:24:11.463416100 CET	49716	9999	192.168.2.3	45.138.49.96

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: BFSV-1F(N)_1B-8B_ANSI.exe PID: 5932 Parent PID: 5596

General

Start time:	09:24:03
Start date:	08/01/2021
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:	0xd20000
File size:	346624 bytes
MD5 hash:	36F13AAD903E851544FE137FECA3435B
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: 00000000.00000002.242826392.0000000000D40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.242826392.0000000000D40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.242826392.0000000000D40000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.242826392.0000000000D40000.00000004.00000001.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: 4420 Parent PID: 5932

General

Start time:	09:24:05
Start date:	08/01/2021
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:	0xd20000
File size:	346624 bytes
MD5 hash:	36F13AAD903E851544FE137FECA3435B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	24	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\BFSV-1F(N)_1B-8B_ANSI.exe:Zone.Identifier	success or wait	1	6CEC2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	a9 c2 f5 35 fa b3 d8 48	...5...H	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	6	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6CF41B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E0BD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E0BD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E0BD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E0BD72F	unknown

Disassembly

Code Analysis