

JOeSandbox Cloud BASIC



ID: 452735

Sample Name: FCL

ABONOF2201.exe

Cookbook: default.jbs

Time: 19:11:29

Date: 22/07/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report FCL ABONOF2201.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	5
Stealing of Sensitive Information:	5
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
Contacted IPs	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
Static File Info	12
General	12
File Icon	12
Static PE Info	12
General	13
Entrypoint Preview	13
Data Directories	13
Sections	13
Resources	13
Imports	13
Version Infos	13
Network Behavior	13
Code Manipulations	13
Statistics	13
Behavior	13
System Behavior	13
Analysis Process: FCL ABONOF2201.exe PID: 5492 Parent PID: 5644	14
General	14
File Activities	14
File Created	14
File Written	14
File Read	14
Analysis Process: FCL ABONOF2201.exe PID: 3596 Parent PID: 5492	14
General	14
Analysis Process: FCL ABONOF2201.exe PID: 4608 Parent PID: 5492	14
General	14
Analysis Process: FCL ABONOF2201.exe PID: 5992 Parent PID: 5492	15
General	15
File Activities	15
File Created	15
File Read	15

Disassembly	15
Code Analysis	15

Windows Analysis Report FCL ABONOF2201.exe

Overview

General Information

Sample Name:	FCL ABONOF2201.exe
Analysis ID:	452735
MD5:	8df4b43e11c352b.
SHA1:	e8e6745a74fec6d.
SHA256:	86324507b99ead..
Tags:	exe
Infos:	
Most interesting Screenshot:	

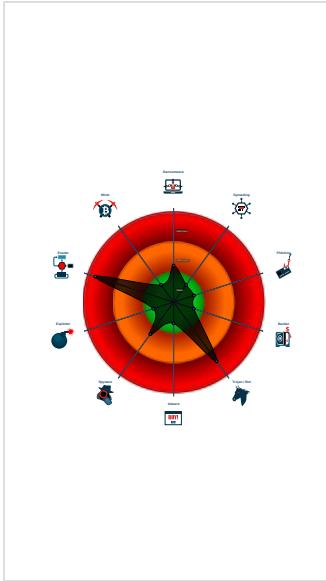
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN AgentTesla	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Yara detected AgentTesla
Yara detected AgentTesla
Yara detected AntiVM3
.NET source code contains potentia...
Injects a PE file into a foreign proce...
Machine Learning detection for samp...
Queries sensitive BIOS Information ...
Queries sensitive network adapter in...
Tries to detect sandboxes and other...
Antivirus or Machine Learning detec...
Contains long sleeps (>= 3 min)
Creates a DirectInput object (often fo...

Classification



Process Tree

System is w10x64
- FCL ABONOF2201.exe (PID: 5492 cmdline: 'C:\Users\user\Desktop\FCL ABONOF2201.exe' MD5: 8DF4B43E11C352B502CEA6A13E220468) - FCL ABONOF2201.exe (PID: 3596 cmdline: {path} MD5: 8DF4B43E11C352B502CEA6A13E220468) - FCL ABONOF2201.exe (PID: 4608 cmdline: {path} MD5: 8DF4B43E11C352B502CEA6A13E220468) - FCL ABONOF2201.exe (PID: 5992 cmdline: {path} MD5: 8DF4B43E11C352B502CEA6A13E220468)
cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "info@aereks.si",
  "Password": "10Jure03",
  "Host": "mail.aereks.si"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.520080449.0000000002CA1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000011.00000002.520080449.0000000002CA1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000011.00000002.517483655.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000011.00000002.517483655.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.346788150.0000000003C3 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.FCL ABONOF2201.exe.3d4eb98.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.FCL ABONOF2201.exe.3d4eb98.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.FCL ABONOF2201.exe.3d4eb98.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.FCL ABONOF2201.exe.3d4eb98.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
17.2.FCL ABONOF2201.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:



.NET source code contains potential unpacker

Malware Analysis System Evasion:



Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:



Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected AgentTesla

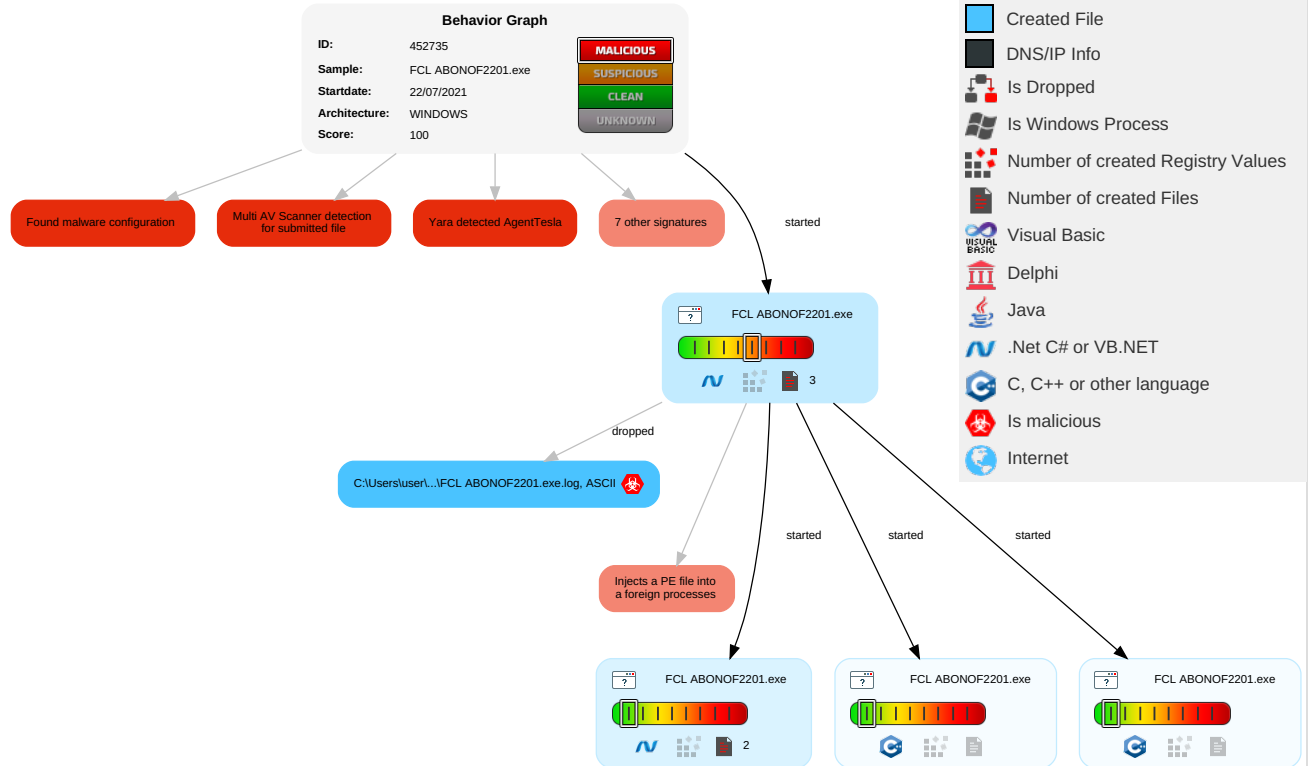
Remote Access Functionality:



Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 1 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	

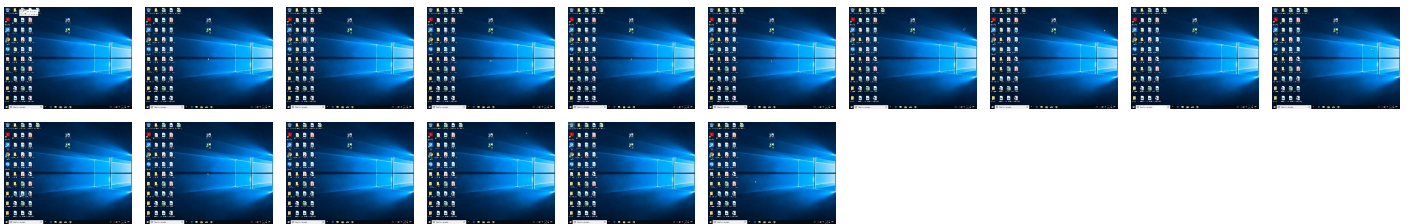
Behavior Graph



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
FCL ABONOF2201.exe	24%	ReversingLabs	Win32.Trojan.AgentTesla	
FCL ABONOF2201.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.FCL ABONOF2201.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/norm	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comAm	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/BnT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Dh	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/m	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/d	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ww.m	0%	Avira URL Cloud	safe	
http://www.fontbureau.commn	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.fontbureau.comeff	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/DhT	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	

Overall analysis duration:	0h 10m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FCL ABONOF2201.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:	29
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@7/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3% (good quality ratio 1.8%) • Quality average: 36.3% • Quality standard deviation: 36.5%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:13:14	API Interceptor	511x Sleep call for process: FCL ABONOF2201.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FCL ABONOF2201.exe.log	
Process:	C:\Users\user\Desktop\FCL ABONOF2201.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DC8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6
Malicious:	true
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd18480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.063301597004948
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.83% - Win32 Executable (generic) a (10002005/4) 49.78% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Generic Win/DOS Executable (2004/3) 0.01% - DOS Executable Generic (2002/1) 0.01%
File name:	FCL ABONOF2201.exe
File size:	874496
MD5:	8df4b43e11c352b502cea6a13e220468
SHA1:	e8e6745a74fec6d5ea7c0ae5fce8e775689cacef
SHA256:	86324507b99eadd23e1c94340269fc33d8a9cf64c6df71822d4b0cf59078535
SHA512:	f16112e048be6466692e52f08eef0326f5eb27b12510017914e74c04c9dba2ce381bad9bc7045524be90b5a58de67b0b51b8cb25a9b9f2e592d94a3b069c1382
SSDEEP:	12288:DZCZiWqRwvYwkt+YASFPE3pRPjutfLRlRiIqkPtOllecN5SvZ+f6q:NCZ2qtrz83nPjYfLRlRiIqkPtolJ
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......PE!..b0..... ..@.. @.....

File Icon

	
Icon Hash:	e8b8ec44cce8e2e8

Static PE Info

General	
Entrypoint:	0x47b89e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F8D662 [Thu Jul 22 02:22:26 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x798a4	0x79a00	False	0.847688367163	data	7.7080390285	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x5b870	0x5ba00	False	0.0554842044679	data	2.3211907839	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: FCL ABONOF2201.exe PID: 5492 Parent PID: 5644**General**

Start time:	19:12:32
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\FCL ABONOF2201.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\FCL ABONOF2201.exe'
Imagebase:	0x820000
File size:	874496 bytes
MD5 hash:	8DF4B43E11C352B502CEA6A13E220468
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.346788150.0000000003C31000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.346788150.0000000003C31000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.344995346.0000000002C98000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created**File Written****File Read****Analysis Process: FCL ABONOF2201.exe PID: 3596 Parent PID: 5492****General**

Start time:	19:13:15
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\FCL ABONOF2201.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x10000
File size:	874496 bytes
MD5 hash:	8DF4B43E11C352B502CEA6A13E220468
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: FCL ABONOF2201.exe PID: 4608 Parent PID: 5492**General**

Start time:	19:13:15
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\FCL ABONOF2201.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x7ff72bb0000

File size:	874496 bytes
MD5 hash:	8DF4B43E11C352B502CEA6A13E220468
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: FCL ABONOF2201.exe PID: 5992 Parent PID: 5492

General

Start time:	19:13:16
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\FCL ABONOF2201.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x770000
File size:	874496 bytes
MD5 hash:	8DF4B43E11C352B502CEA6A13E220468
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.520080449.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.520080449.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.517483655.000000000402000.00000040.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000002.517483655.000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis