JoeSandbox Cloud BASIC

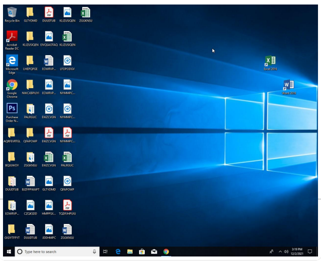
ID: 532633
Sample Name: Purchase Order No. XIV21623..exe
Cookbook: default.jbs
Time: 15:18:35
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report Purchase Order No. XIV21623…

Overview

General Information

Sample Name:	Purchase Order No. XIV21623..exe
Analysis ID:	532633
MD5:	5e5c83d04f20a03.
SHA1:	840248f52491715.
SHA256:	62c4b3a0c36572..
Tags:	agenttesla exe
Infos:	
Most interesting Screenshot: 	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

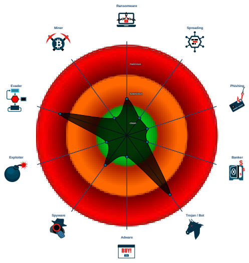
AgentTesla

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected AgentTesla
- Initial sample is a PE file and has a …
- Executable has a suspicious name (…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…

Classification



Process Tree

- **System is w10x64**
- Purchase Order No. XIV21623..exe (PID: 496 cmdline: "C:\Users\user\Desktop\Purchase Order No. XIV21623..exe" MD5: 5E5C83D04F20A03826B8CD80D2C4A0B5)
  - aspnet_compiler.exe (PID: 1552 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "anjay@peoplesource.in",
  "Password": "Admin@12345",
  "Host": "mail.peoplesource.in"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.250031063.0000000013189000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.250031063.0000000013189000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Process Memory Space: Purchase Order No. XIV21623..exe PID: 496	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.Purchase Order No. XIV21623..exe.13454660.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order No. XIV21623..exe.13454660.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order No. XIV21623..exe.13454660.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase Order No. XIV21623..exe.13454660.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious aspnet_compiler.exe Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

System Summary:

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

Stealing of Sensitive Information:

Yara detected AgentTesla

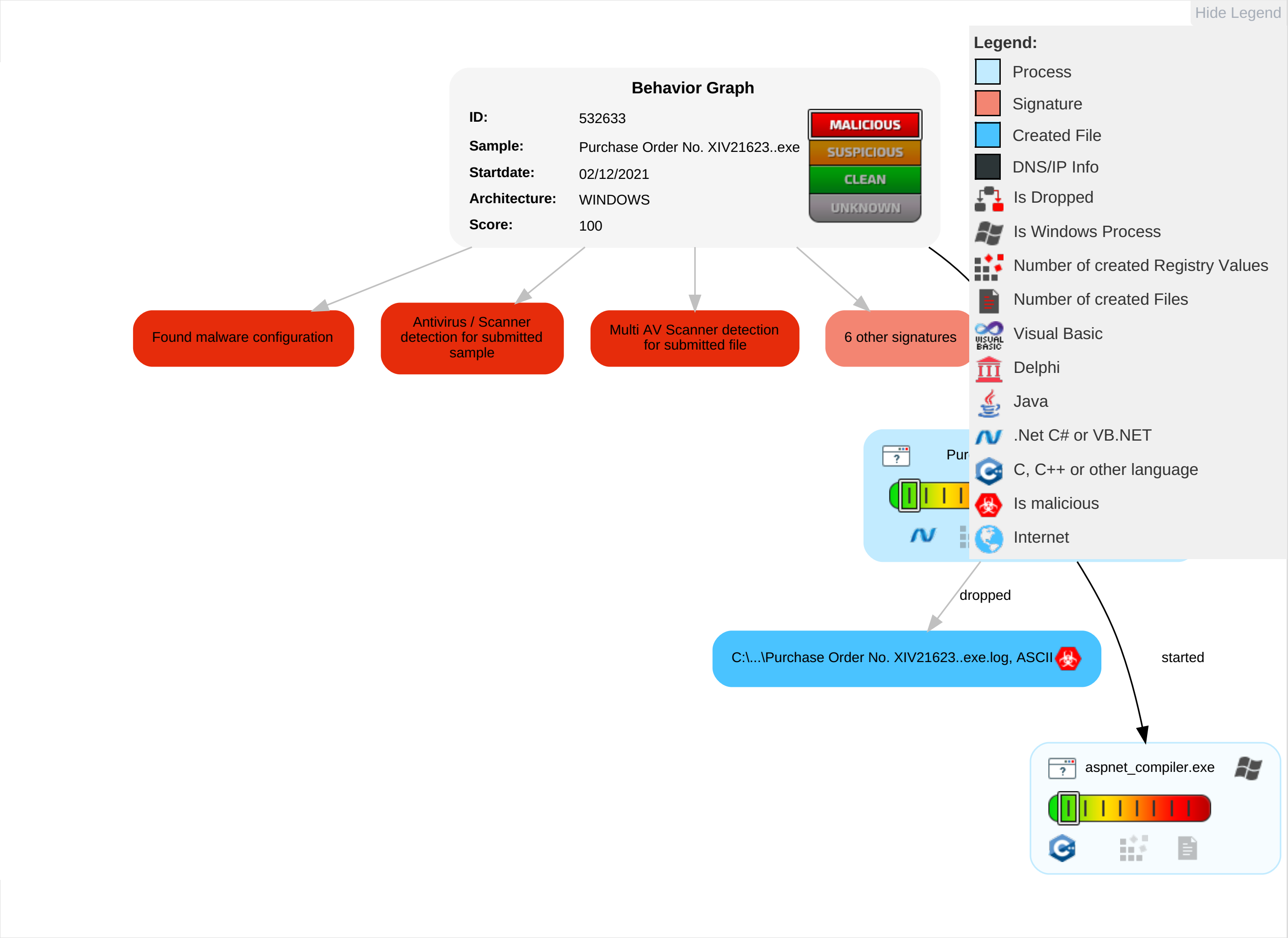
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



Behavior Graph

ID: 532633

Sample: Purchase Order No. XIV21623..exe

Startdate: 02/12/2021

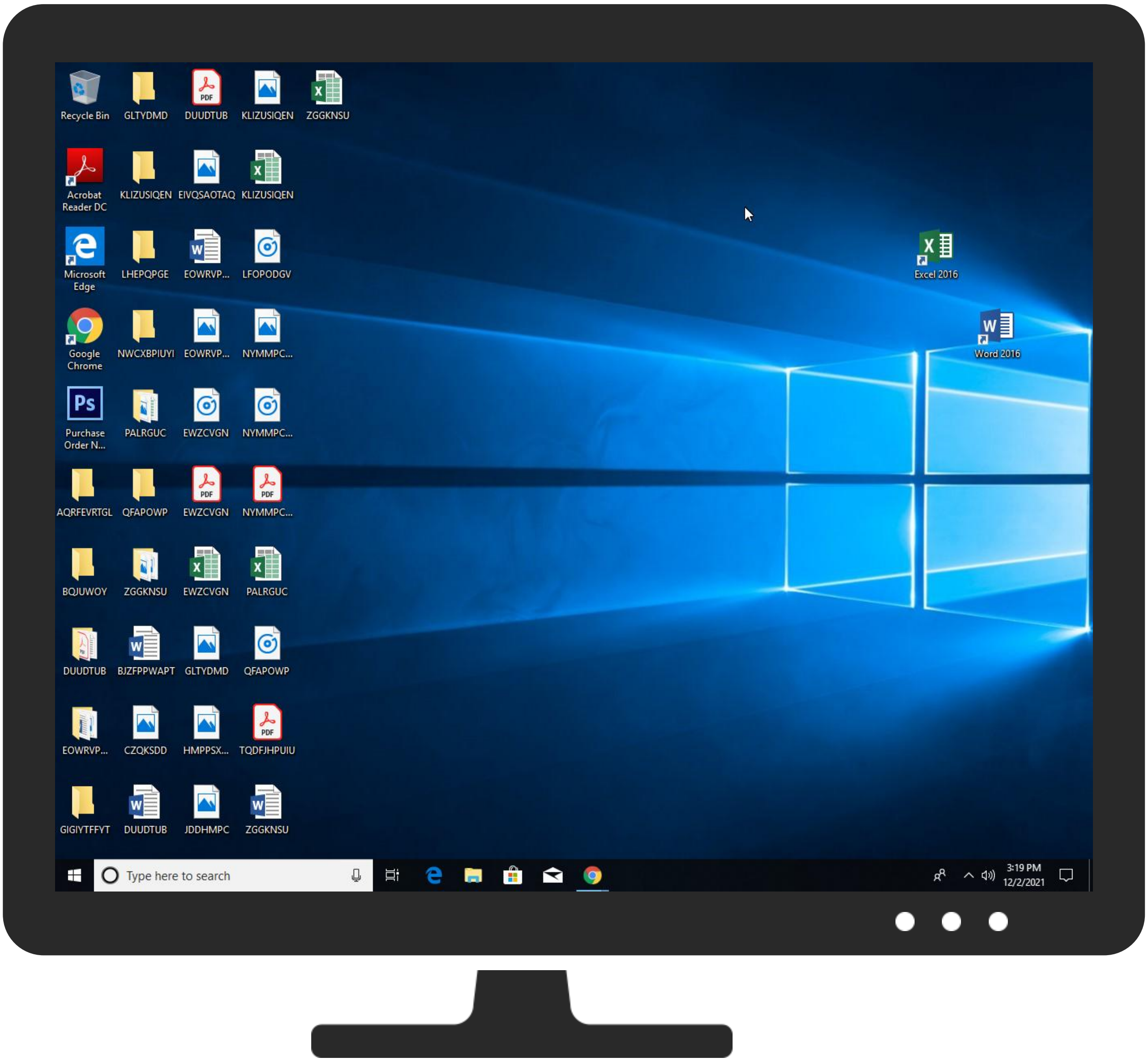
Architecture: WINDOWS

Score: 100

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
Purchase Order No. XIV21623..exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Purchase Order No. XIV21623..exe	100%	Avira	TR/Dropper.MSIL.Gen	
Purchase Order No. XIV21623..exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Purchase Order No. XIV21623..exe.810000.0.unpack	100%	Avira	HEUR/AGEN.1105850		Download File
0.0.Purchase Order No. XIV21623..exe.810000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532633
Start date:	02.12.2021
Start time:	15:18:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order No. XIV21623..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:	3
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@3/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.2% (good quality ratio 1.3%) • Quality average: 40.6% • Quality standard deviation: 37.2%
HCA Information:	• Successful, ratio: 87% • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Purchase Order No. XIV21623..exe.log	
Process:	C:\Users\user\Desktop\Purchase Order No. XIV21623..exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.374391981354885
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIOKbbDLI4MWuPOKN08JOKhap+92n4MNQpN9tv:ML9E4KrgKDE4KGKN08AKh6+84xpNT
MD5:	C8A62E39DE7A3F805D39384E8BABB1E0
SHA1:	B32B1257401F17A2D1D5D3CC1D8C1E072E3FEE31
SHA-256:	A7BC127854C5327ABD50C86000BF10586B556A5E085BB23523B07A15DD4C5383
SHA-512:	7DB2825131F5CDA6AF33A179D9F7CD0A206FF34AE50D6E66DE9E99BE2CD1CB985B88C00F0EDE72BBC4467E7E42B5DC6132403AA2EC1A0A7A6D11766C438B1C3
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8879021889341425
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:	Purchase Order No. XIV21623..exe
File size:	274944
MD5:	5e5c83d04f20a03826b8cd80d2c4a0b5
SHA1:	840248f524917151d9b44dda32cbb32ab1fd7d80
SHA256:	62c4b3a0c365726907f0ac94621c85f5c52056eb94653b151144cc841502e916
SHA512:	3fa38c0033df01c29b376086df84fed1aa0047c7ce2de2ae2f7465c1ce12211613a7ed78e21a9f6810ebfe35acf713d1749c5f1f2e34f282f063399af0feee73
SSDEEP:	6144:Reot2u5F/vFkZuMEvcumRVTSyGR12K8vuHKzoJ8L:0Hu5FXFkZuMEUuwV7HvuHQ
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......a...........................j.... ....@.. ....@................................

File Icon

Icon Hash:	a289a9ed6da39200

Static PE Info

General

Entrypoint:	0x43c86a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A89780 [Thu Dec 2 09:53:04 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	0x3a870	0x3aa00	False	0.96924556903	data	7.96708162926	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x40000	0x8360	0x8400	False	0.587831439394	data	6.84237661239	IMAGE_SCN_CNT_INITIALIZED_DATA, 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: Purchase Order No. XIV21623..exe PID: 496 Parent PID: 6064

General

Start time:	15:19:32
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Purchase Order No. XIV21623..exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Purchase Order No. XIV21623..exe"
Imagebase:	0x810000
File size:	274944 bytes
MD5 hash:	5E5C83D04F20A03826B8CD80D2C4A0B5
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: 00000000.00000002.250031063.0000000013189000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.250031063.0000000013189000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: aspnet_compiler.exe PID: 1552 Parent PID: 496

General

Start time:	15:19:34
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x40000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis