

JOeSandbox Cloud BASIC



ID: 458877

Sample Name: Products

Order.exe

Cookbook: default.jbs

Time: 20:28:19

Date: 03/08/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Products Order.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: Agenttesla	3
Yara Overview	3
Memory Dumps	3
Unpacked PEs	4
Sigma Overview	4
Jbx Signature Overview	4
AV Detection:	4
System Summary:	4
Malware Analysis System Evasion:	4
HIPS / PFW / Operating System Protection Evasion:	4
Stealing of Sensitive Information:	4
Remote Access Functionality:	4
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	10
General	10
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	11
Data Directories	11
Sections	11
Resources	11
Imports	11
Version Infos	11
Network Behavior	11
Code Manipulations	11
Statistics	11
Behavior	11
System Behavior	11
Analysis Process: Products Order.exe PID: 2952 Parent PID: 5672	11
General	11
File Activities	12
File Created	12
File Written	12
File Read	12
Analysis Process: Products Order.exe PID: 5888 Parent PID: 2952	12
General	12
File Activities	12
File Created	12
File Read	12
Disassembly	12
Code Analysis	12

Windows Analysis Report Products Order.exe

Overview

General Information

Sample Name:

Products Order.exe

Analysis ID:

458877

MD5:

7beee2584cd632..

SHA1:

d192b8805a1d87..

SHA256:

56390f611b9571d.

Tags:

exe

null

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

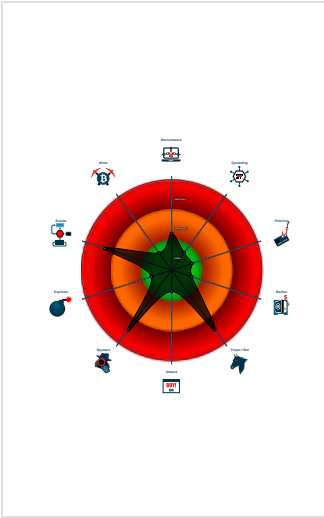
AgentTesla

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
- .NET source code contains very larg...
- Initial sample is a PE file and has a ...
- Injects a PE file into a foreign proce...
- Machine Learning detection for samp...
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...
- Tries to harvest and steal Putty / Wi...
- Tries to harvest and steal browser in...

Classification



Process Tree

- System is w10x64
 - Products Order.exe (PID: 2952 cmdline: 'C:\Users\user\Desktop\Products Order.exe' MD5: 7BEEE2584CD632154D34C65237CD5EB0)
 - Products Order.exe (PID: 5888 cmdline: C:\Users\user\Desktop\Products Order.exe MD5: 7BEEE2584CD632154D34C65237CD5EB0)
 - cleanup

Malware Configuration

Threatname: Agenttesla

```
{  "Exfil Mode": "SMTP",  "Username": "ideshow@eflownutrition.com",  "Password": "ngozi8989",  "Host": "mail.scottbyscott.com"}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.486997350.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.486997350.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.491669072.000000000347 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.491669072.000000000347 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: Products Order.exe PID: 5888	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 1 entries


Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.Products Order.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.Products Order.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

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

System Summary:



.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:



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)

HIPS / PFW / Operating System Protection Evasion:



Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:



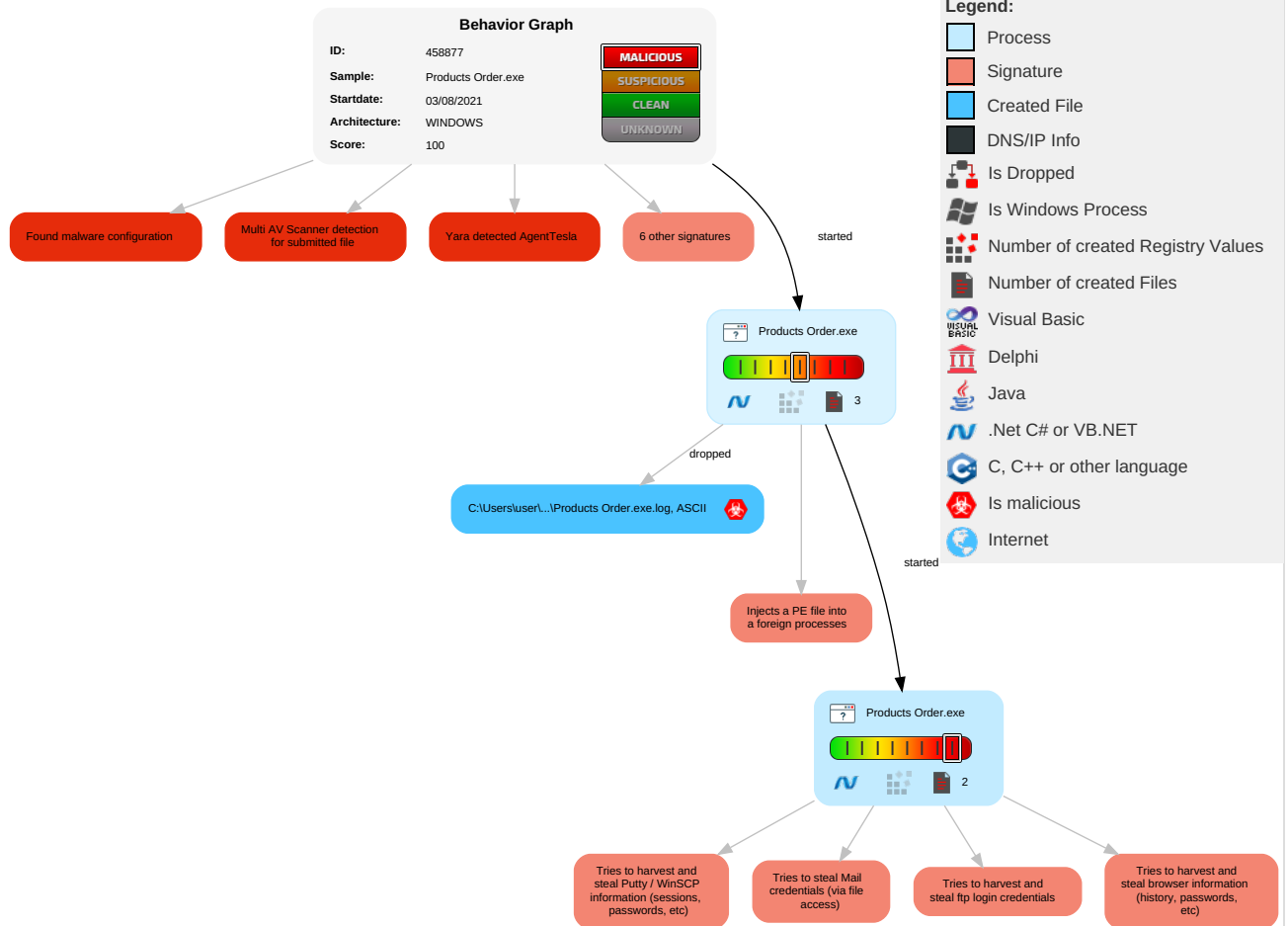
Yara detected AgentTesla

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 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	Credentials in Registry 1	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1 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	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Steganograph
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

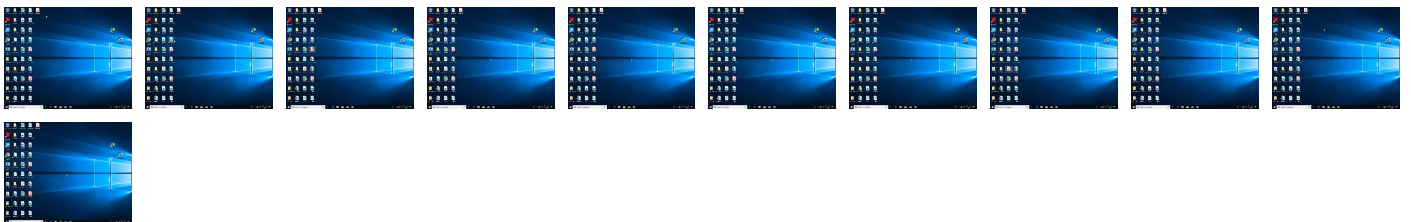
Behavior Graph



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
Products Order.exe	61%	Virustotal		Browse
Products Order.exe	49%	Metadefender		Browse
Products Order.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Products Order.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.Products Order.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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.sajatypeworks.com/	0%	Virustotal		Browse
http://www.sajatypeworks.com/	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/K	0%	URL Reputation	safe	
http://https://Au1SDZgNiFJp.n	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sandoll.co.kre	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krthe	0%	Avira URL Cloud	safe	
http://www.fonts.comW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/w	0%	Avira URL Cloud	safe	
http://oGRaXU.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.tiro.comn	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/eta	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.founder.com.cn/cn-	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://https://Au1SDZgNiFJp.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.sajatypeworks.comh	0%	Avira URL Cloud	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.founder.com.cn/cnh	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:	33.0.0 White Diamond
Analysis ID:	458877
Start date:	03.08.2021
Start time:	20:28:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Products Order.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:	24
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:	<ul style="list-style-type: none"> • HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:29:29	API Interceptor	659x Sleep call for process: Products Order.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\Products Order.exe.log	
Process:	C:\Users\user\Desktop\Products Order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
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\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.224209758777507
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) Net Framework (10011505/4) 49.80%Win32 Executable (generic) a (10002005/4) 49.75%Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%Windows Screen Saver (13104/52) 0.07%Generic Win/DOS Executable (2004/3) 0.01%
File name:	Products Order.exe
File size:	1071104
MD5:	7beee2584cd632154d34c65237cd5eb0
SHA1:	d192b8805a1d874d480d791f673dbde77f12059b
SHA256:	56390f611b9571d11cdeb128435aaf3d5b282511f4a540d81912d87ffc1d2953
SHA512:	9140b9f85f5c0a90f98a9b1c40d236430cb2d4226fa6b2a9bcb78cfbec853707b379732c1332565190f8425c204a9aa2322944b1d5ab1daf51f8b55d1b2ecee5
SSDEEP:	24576:xPWfoD8i/dEHmi0DWPTnJa7Rd0duWLCRYbuxq:SiCWmJQRd7bYb
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......PE..L.... }.....N.....Nm.....@..@.....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x506d4e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

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:	0xB2837D03 [Wed Nov 26 21:47:47 2064 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	0x104d54	0x104e00	False	0.7057238635	data	7.23009151105	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x108000	0x5c8	0x600	False	0.422526041667	data	4.10956691089	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10a000	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: Products Order.exe PID: 2952 Parent PID: 5672

General

Start time:	20:29:05
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Products Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Products Order.exe'
Imagebase:	0xfe0000
File size:	1071104 bytes
MD5 hash:	7BEEE2584CD632154D34C65237CD5EB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

[File Activities](#)

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Products Order.exe PID: 5888 Parent PID: 2952

General

Start time:	20:29:30
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Products Order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Products Order.exe
Imagebase:	0xf60000
File size:	1071104 bytes
MD5 hash:	7BEEE2584CD632154D34C65237CD5EB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.486997350.0000000000402000.00000040.00000001.sdmp, Author: Joe SecurityRule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.486997350.0000000000402000.00000040.00000001.sdmp, Author: Joe SecurityRule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.491669072.0000000003471000.00000004.00000001.sdmp, Author: Joe SecurityRule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.491669072.0000000003471000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

[File Activities](#)

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

