



ID: 452720

Sample Name:

Pedido_73580523.exe

Cookbook: default.jbs

Time: 18:57:08

Date: 22/07/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Pedido_73580523.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
System Summary:	5
Boot Survival:	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	13
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	14
Data Directories	14
Sections	14
Resources	14
Imports	14
Version Infos	14
Network Behavior	14
Code Manipulations	14
Statistics	14
Behavior	14
System Behavior	14
Analysis Process: Pedido_73580523.exe PID: 5300 Parent PID: 5604	14
General	14
File Activities	15
File Created	15
File Deleted	15
File Written	15
File Read	15
Analysis Process: schtasks.exe PID: 5572 Parent PID: 5300	15
General	15
File Activities	15
File Read	15
Analysis Process: conhost.exe PID: 5656 Parent PID: 5572	15
General	15
Analysis Process: Pedido_73580523.exe PID: 5556 Parent PID: 5300	16

General	16
File Activities	16
File Created	16
File Read	16
Disassembly	16
Code Analysis	16

Windows Analysis Report Pedido_73580523.exe

Overview

General Information

Sample Name:	Pedido_73580523.exe
Analysis ID:	452720
MD5:	facf53403056e3d..
SHA1:	384a0565e553ac..
SHA256:	3bd0c04ee4c4ba..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



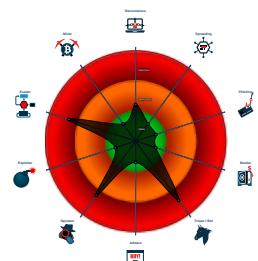
AgentTesla

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

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AgentTesla
- .NET source code contains very larg...
- Injects a PE file into a foreign proce...
- Machine Learning detection for dropp...
- Machine Learning detection for samp...
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...
- Tries to harvest and steal browser in...
- Tries to harvest and steal ftp login c...
- Uses schtasks.exe or at.exe to add ...

Classification



Process Tree

- System is w10x64
- Pedido_73580523.exe (PID: 5300 cmdline: 'C:\Users\user\Desktop\Pedido_73580523.exe' MD5: FACF53403056E3D7529FC8A5CE8BE77F)
 - schtasks.exe (PID: 5572 cmdline: 'C:\Windows\System32\Tasks\schtasks.exe' /Create /TN 'Updates\AsJoyfF' /XML 'C:\Users\user\AppData\Local\Temp\tmpE123.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
 - conhost.exe (PID: 5656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - Pedido_73580523.exe (PID: 5556 cmdline: C:\Users\user\Desktop\Pedido_73580523.exe MD5: FACF53403056E3D7529FC8A5CE8BE77F)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{  
  "Exfil Mode": "SMTP",  
  "Username": "comercial@fil-net.com",  
  "Password": "Fil-2020net+",  
  "Host": "smtp.fil-net.com"  
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.477029833.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.477029833.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000A.00000002.482206356.0000000002CF 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.482206356.0000000002CF 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.483335897.0000000002D9 E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.Pedido_73580523.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
10.2.Pedido_73580523.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

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:



.NET source code contains very large array initializations

Boot Survival:



Uses schtasks.exe or at.exe to add and modify task schedules

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 browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Remote Access Functionality:



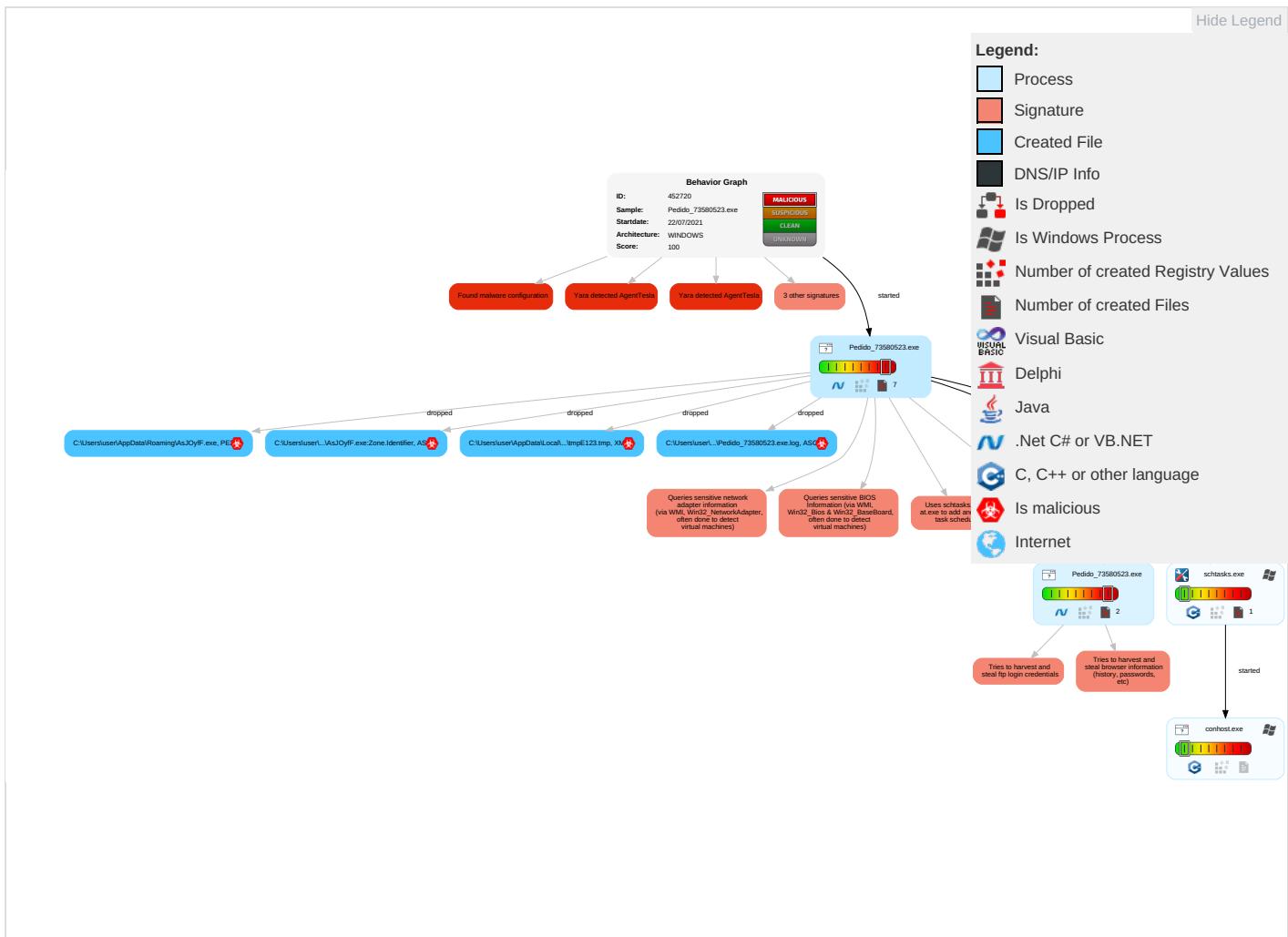
Yara detected AgentTesla

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	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	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	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	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 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 1 3	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	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

Behavior Graph

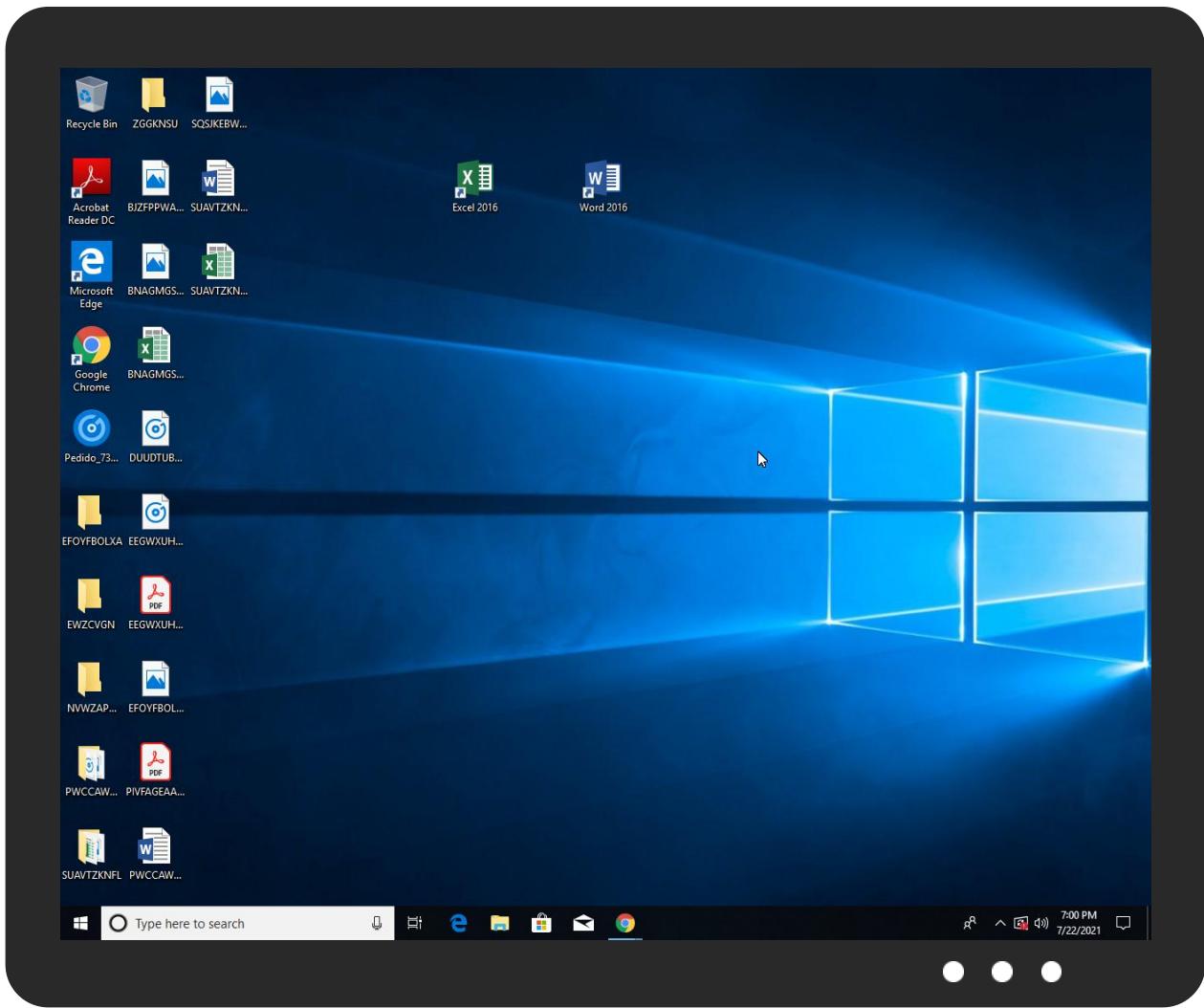


Screenshots

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
Pedido_73580523.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\AsJOyfF.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.Pedido_73580523.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnQ	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T	0%	URL Reputation	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://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://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://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.founder.com.cn/cnS	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.tiro.com	0%	URL Reputation	safe	
http://www.urwpp.dev	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.fontbureau.comcomd\$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://mGfDbY.com	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	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.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	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://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/W	0%	Avira URL Cloud	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.founder.com.cn-cn-	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

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:	452720
Start date:	22.07.2021
Start time:	18:57:08
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pedido_73580523.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<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@6/4@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
18:58:26	API Interceptor	621x Sleep call for process: Pedido_73580523.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\Pedido_73580523.exe.log	
Process:	C:\Users\user\Desktop\Pedido_73580523.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DC9CEFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8E815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	true
Reputation:	high, very likely benign file
Preview:	1."fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic", Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\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:\Users\user\AppData\Local\Temp\tmpE123.tmp	
Process:	C:\Users\user\Desktop\Pedido_73580523.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.189035414438582
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxINMFp1/rIMhEMjnGpwjpIgUYODOLD9RJh7h8gKBjt:cbh47TINQ//rydbz9I3YODOLNdq3t
MD5:	1CFD403DA59597FBE594CD86E12C9F07
SHA1:	9D8F9C78554F0A1B57CAC5C955D1EFcba5B46086
SHA-256:	13E8734988EB55A665C821F06E4CC25DFF34058E3B0F4A70084E210AAF0D1A1F
SHA-512:	BE8F7F482567A25E5D6FC92AF79CB10B669604A85A012F6000E75BEE17554B35748F8A5E6521E87DCC576A797106A8FD5903213FEDDA279DD612E1C889C6FBA
Malicious:	true
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. <Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\AsJOyfF.exe	
Process:	C:\Users\user\Desktop\Pedido_73580523.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1018368
Entropy (8bit):	7.253301273224395
Encrypted:	false
SSDEEP:	24576:m+K48+PqKfwB3ZklaTV1S3wqNqzahprNeLc:Xq6wvZGaTVWwNOiLc
MD5:	FACF53403056E3D7529FC8A5CE8BE77F
SHA1:	384A0565E553AC374DD6197B51A94BACE517F36
SHA-256:	3BD0C04EE4C4BA078C54F4E7F5F956894204B2CCFB84CDF934C40B28E30165E
SHA-512:	1F1FACE7BA52A0FB9451E65B022BA630FD395FF55F1EA3666541B677203FBF0095A98A75A0FECB12CDEFAA59627AD6125AF5C3547D56AB034F57E51594E55E8
Malicious:	true
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!L!This program cannot be run in DOS mode...\$.....PE..L.....`.....\$.b.....B.....`.....@.....\$.....@.....`.....(.....@....rsrc.....].....^.^*.....@....@.reloc.....@..B.....`.....(.....@....rsrc.....].....



Process:	C:\Users\user\Desktop\Pedido_73580523.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDeep:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	true
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.253301273224395
TrID:	<ul style="list-style-type: none"> Win32 Executable (generic) Net Framework (10011505/4) 49.79% 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% Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	Pedido_73580523.exe
File size:	1018368
MD5:	facf53403056e3d7529fc8a5ce8be77f
SHA1:	384a0565e553ac374dd6d197b51a94bace517f36
SHA256:	3bd0c04ee4c4ba078c54f4e7f5f956894204b2ccfbe84cdf934c40b28e30165e
SHA512:	1f1face7ba52a0fb9451e65b022ba630fd395ff55f1ea3666541b677203fb0095a98a75a0fecb12cdefaa59627ad6125a5c3547d56ab034f57e51594e55e83
SSDeep:	24576:m+K48+PqKfwIB3ZklaTV1S3wqNqzahprNeLc:Xq6wvZGaTVWwNoIc
File Content Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode....\$.PE..L...`.....\$.b....B...`....@..`.....@.....

File Icon



Icon Hash:

70d8ccd2d6ccf071

Static PE Info

General

Entrypoint:	0x4c42de
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:	0x60F92017 [Thu Jul 22 07:36:55 2021 UTC]

General

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	0xc22e4	0xc2400	False	0.7730252574	data	7.55884475799	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc6000	0x18	0x200	False	0.060546875	data	0.456640975135	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x35db8	0x35e00	False	0.368383845708	data	5.19543119017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	0xc	0x200	False	0.044921875	data	0.0980041756627	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: Pedido_73580523.exe PID: 5300 Parent PID: 5604

General

Start time:	18:57:58
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Pedido_73580523.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pedido_73580523.exe'
Imagebase:	0xcb0000
File size:	1018368 bytes
MD5 hash:	FACF53403056E3D7529FC8A5CE8BE77F
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 Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5572 Parent PID: 5300

General

Start time:	18:58:27
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AsJOyfF' /XML 'C:\Users\user\AppData\Local\Temp\tmpE123.tmp'
Imagebase:	0xb10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5656 Parent PID: 5572

General

Start time:	18:58:28
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Pedido_73580523.exe PID: 5556 Parent PID: 5300

General

Start time:	18:58:28
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Pedido_73580523.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pedido_73580523.exe
Imagebase:	0x7b0000
File size:	1018368 bytes
MD5 hash:	FACF53403056E3D7529FC8A5CE8BE77F
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: 0000000A.00000002.477029833.0000000000402000.00000040.00000001.sdmp, Author: Joe Security Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.477029833.0000000000402000.00000040.00000001.sdmp, Author: Joe Security Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.482206356.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.482206356.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.483335897.0000000002D9E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis