ID: 528709
Sample Name: Pago Transferencia.pdf.exe
Cookbook: default.jbs
Time: 17:37:19
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

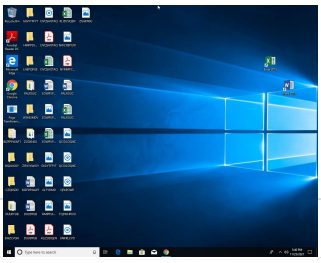
Windows Analysis Report Pago Transferencia.pdf.exe

Overview

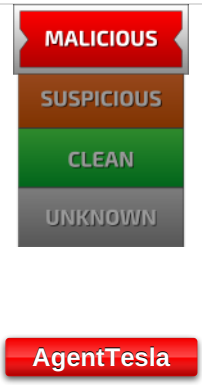
General Information

Sample Name:	Pago Transferencia.pdf.exe
Analysis ID:	528709
MD5:	02bf0fc6d6fdc5a…
SHA1:	7ab36a1ea54740..
SHA256:	49121cf42d9ee0f..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



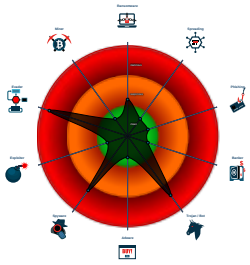
AgentTesla

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

Signatures

- Found malware configuration
- Sigma detected: Suspicious Double …
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- .NET source code contains very larg…
- Uses an obfuscated file name to hid…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- Pago Transferencia.pdf.exe (PID: 3228 cmdline: "C:\Users\user\Desktop\Pago Transferencia.pdf.exe" MD5: 02BF0FC6D6FDC5AA692F136DA966B62C)
  - Pago Transferencia.pdf.exe (PID: 4876 cmdline: C:\Users\user\Desktop\Pago Transferencia.pdf.exe MD5: 02BF0FC6D6FDC5AA692F136DA966B62C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ugo@bhgautopartes.com",
  "Password": "icui4cu2@@",
  "Host": "mail.bhgautopartes.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.248078811.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.248078811.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.250733467.0000000002C01000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000000.248613721.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.248613721.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.Pago Transferencia.pdf.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.Pago Transferencia.pdf.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.Pago Transferencia.pdf.exe.2c68fb4.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
3.0.Pago Transferencia.pdf.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.Pago Transferencia.pdf.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

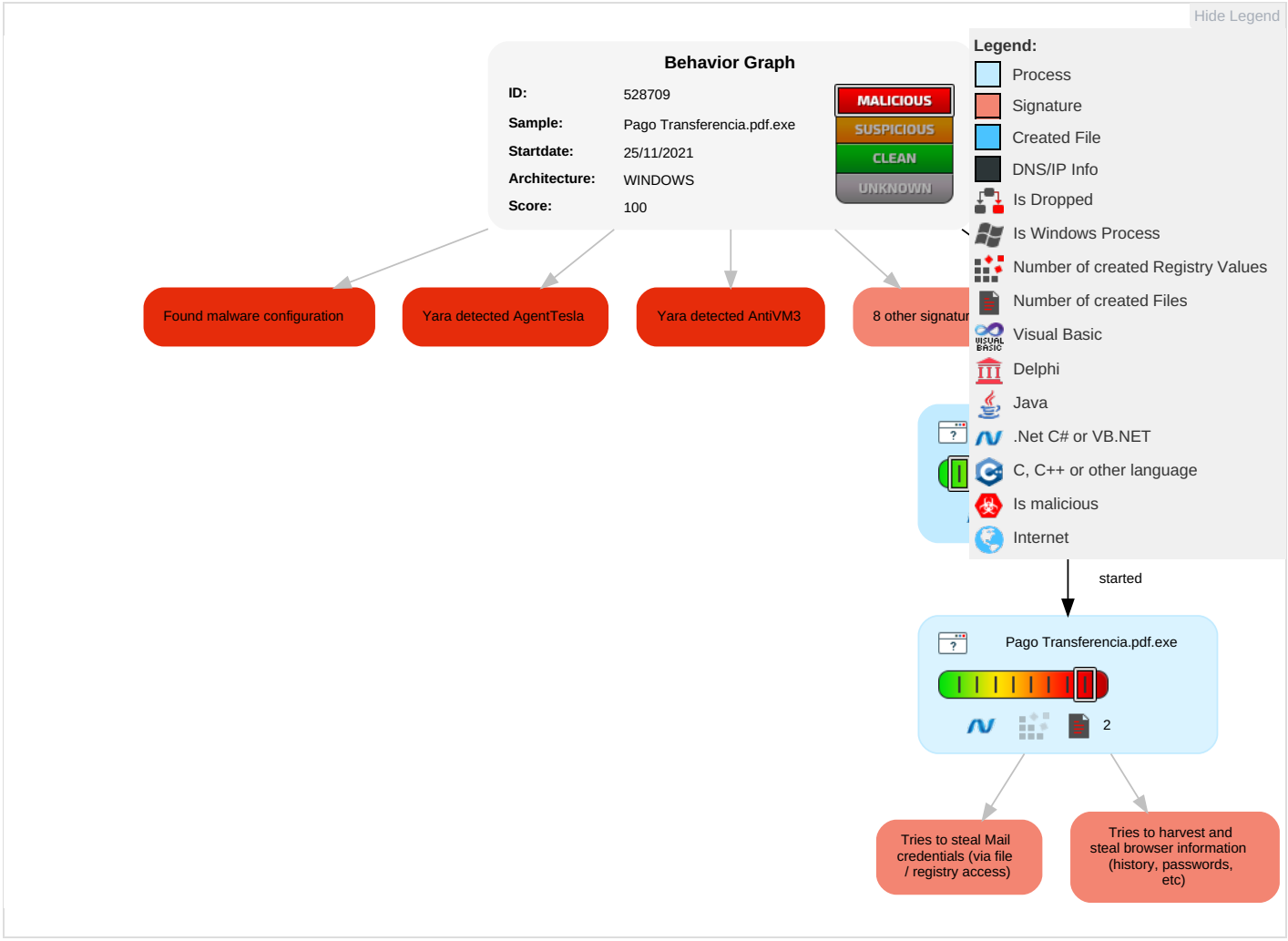
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1 1	OS Credential Dumping 1	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	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	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 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	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 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	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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Pago Transferencia.pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Pago Transferencia.pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Pago Transferencia.pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Pago Transferencia.pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Pago Transferencia.pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.Pago Transferencia.pdf.exe.400000.10.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://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	0%	URL Reputation	safe	
http://uArhJl.com	0%	Avira URL Cloud	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:	528709
Start date:	25.11.2021
Start time:	17:37:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pago Transferencia.pdf.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:	23
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.spyw.evad.winEXE@3/1@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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
17:38:16	API Interceptor	788x Sleep call for process: Pago Transferencia.pdf.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\Pago Transferencia.pdf.exe.log	
Process:	C:\Users\user\Desktop\Pago Transferencia.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntlxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	false
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_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, 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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.864891743136638
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:	Pago Transferencia.pdf.exe
File size:	501248
MD5:	02bf0fc6d6fdc5aa692f136da966b62c
SHA1:	7ab36a1ea547408e9254428887b3a41a83e2c849
SHA256:	49121cf42d9ee0f820e76416c3bd0ea7f69036fde442ca8ad2a69737c50ac97e
SHA512:	2984aa3dbfbba599e3972831646f58015230268cd5ad2a468e0194804ab5132219a256efbfddfd2d3ee78b29b4dad0b8b67b79ec38bfba9919b3941e0dd4cd23
SSDEEP:	12288:p4dY990jixBFml4Vbjnmy1pDzxZ2AMc/BdxlA7LyaqViJNpPVveIjL:p4dA90ji1U4Vbjn91pJZLMc/jwcYXe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4C.a.....0..... ....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47b92e
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:	0x619F4334 [Thu Nov 25 08:03:00 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	0x79944	0x79a00	False	0.896022690776	data	7.87898246248	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x60c	0x800	False	0.3330078125	data	3.45211818667	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7e000	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: Pago Transferencia.pdf.exe PID: 3228 Parent PID: 5524

General

Start time:	17:38:14
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Pago Transferencia.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Pago Transferencia.pdf.exe"
Imagebase:	0x7a0000
File size:	501248 bytes
MD5 hash:	02BF0FC6D6FDC5AA692F136DA966B62C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.250733467.0000000002C01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.250904097.0000000002CCB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.251510094.0000000003C0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.251510094.0000000003C0D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Pago Transferencia.pdf.exe PID: 4876 Parent PID: 3228

General

Start time:	17:38:17
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Pago Transferencia.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Pago Transferencia.pdf.exe
Imagebase:	0x7ff797770000
File size:	501248 bytes
MD5 hash:	02BF0FC6D6FDC5AA692F136DA966B62C
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: 00000003.00000000.248078811.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.248078811.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.248613721.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.248613721.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.247491327.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.247491327.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.505276535.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.505276535.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.247106547.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.247106547.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.508136463.0000000002981000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.508136463.0000000002981000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis