ID: 234159
Sample Name:
Orden_De_Compra_019999_img.exe
Cookbook: default.jbs
Time: 12:45:42
Date: 29/05/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

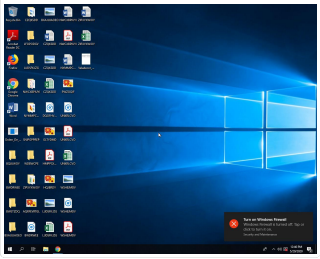
Analysis Report Orden_De_Compra_019999_img.exe

Overview

General Information

Sample Name:	Orden_De_Compra_019999_img.exe
MD5:	cc209b878cb299…
SHA1:	c069335fe4a39f6..
SHA256:	b8541f6bb3a95ce.

Most interesting Screenshot:



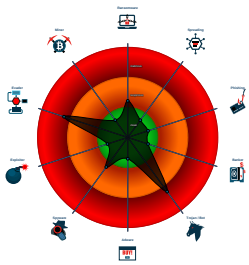
Detection

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Allocates memory in foreign processes
- Hides that the sample has been down…
- Initial sample is a PE file and has a s…
- Injects a PE file into a foreign proces…
- Suspicious powershell command line…
- Writes to foreign memory regions
- Contains functionality to launch a pro…

Classification



Startup

- **System is w10x64**
- Orden_De_Compra_019999_img.exe (PID: 5060 cmdline: 'C:\Users\user\Desktop\Orden_De_Compra_019999_img.exe' MD5: CC209B878CB2993332DC05802716AD83)
  - powershell.exe (PID: 3896 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Process C:\Users\user\Desktop\Veladecor_order1.jpg MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 940 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.882263652.000000000042000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.888497000.000000000413000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.887779335.0000000003F25000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.888931397.000000000437D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 940	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 1 entries

Unpacked PEs

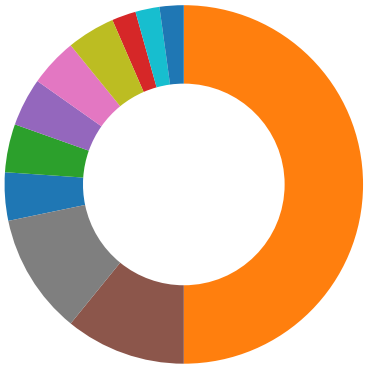
Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
6.2.RegAsm.exe.420000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

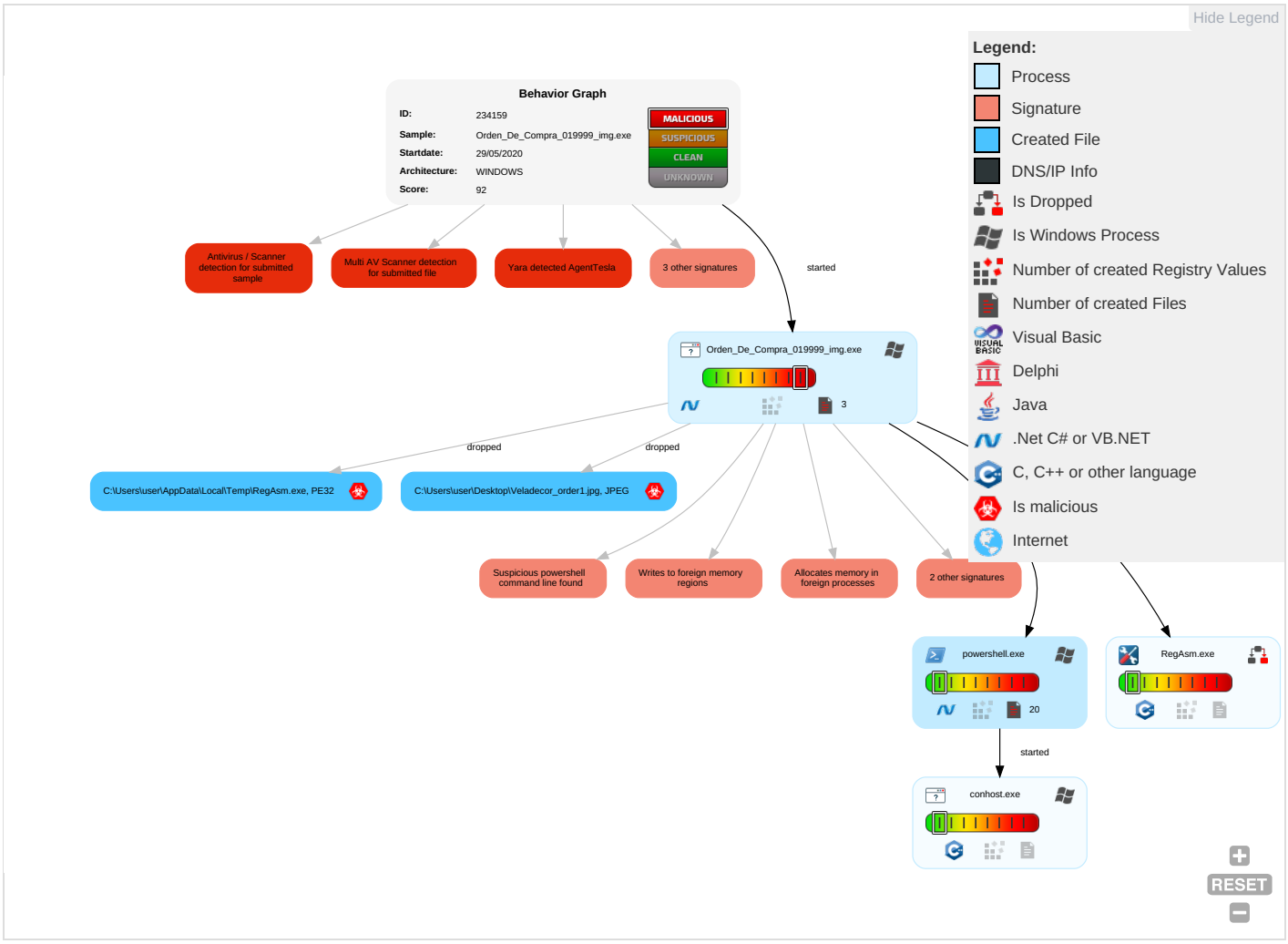
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Eff
Valid Accounts 1	PowerShell 1	Hidden Files and Directories 1	Valid Accounts 1	Masquerading 1	Credential Dumping	Virtualization/Sandbox Evasion 2	Application Deployment Software	Data from Local System	Data Encrypted 1	Standard Cryptographic Protocol 1	Ea Ins Ne Co
Replication Through Removable Media	Service Execution	Valid Accounts 1	Access Token Manipulation 1	Hidden Files and Directories 1	Network Sniffing	Process Discovery 2	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Fallback Channels	Ex Re Ca
External Remote Services	Windows Management Instrumentation	Accessibility Features	Process Injection 3 1 2	Valid Accounts 1	Input Capture	Application Window Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Ex Tra Lo
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Disabling Security Tools 1	Credentials in Files	File and Directory Discovery 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Sw
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Virtualization/Sandbox Evasion 2	Account Manipulation	System Information Discovery 1 2	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Ma De Co
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	Access Token Manipulation 1	Brute Force	System Owner/User Discovery	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port	Jar De Se
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Process Injection 3 1 2	Two-Factor Authentication Interception	Network Sniffing	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port	Ro Ac
Spearphishing via Service	Third-party Software	Logon Scripts	Process Injection	Obfuscated Files or Information 1	Bash History	Network Service Scanning	Remote Desktop Protocol	Clipboard Data	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol	Do Ins Pro

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
Orden_De_Compra_019999_img.exe	49%	Virustotal		Browse
Orden_De_Compra_019999_img.exe	74%	ReversingLabs	ByteCode-MSIL.Trojan.Kryptik	
Orden_De_Compra_019999_img.exe	100%	Avira	HEUR/AGEN.1046458	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Orden_De_Compra_019999_img.exe.860000.0.unpack	100%	Avira	HEUR/AGEN.1046458		Download File
0.0.Orden_De_Compra_019999_img.exe.860000.0.unpack	100%	Avira	HEUR/AGEN.1046458		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	234159
Start date:	29.05.2020
Start time:	12:45:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orden_De_Compra_019999_img.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	7
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:	mal92.troj.evad.winEXE@6/7@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
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): dllhost.exe, WMIADAP.exe

Simulations

Behavior and APIs

Time	Type	Description
12:46:17	API Interceptor	83x Sleep call for process: Orden_De_Compra_019999_img.exe modified
12:46:18	API Interceptor	11x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegAsm.exe	order_403_img.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	3Payment copy.exe	Get hash	malicious	Browse	
	46US246448DPayment copy.exe	Get hash	malicious	Browse	
	18invoice.exe	Get hash	malicious	Browse	
	14invoice.exe	Get hash	malicious	Browse	
	28invoic.exe	Get hash	malicious	Browse	
	68invoice.exe	Get hash	malicious	Browse	
	1Swift copy.exe	Get hash	malicious	Browse	
	32Swift copy.exe	Get hash	malicious	Browse	
	29Swift copy.exe	Get hash	malicious	Browse	
	4688.exe	Get hash	malicious	Browse	
	Request for Quotation AGP Global Group LLC No. 219 007290.exe	Get hash	malicious	Browse	
	50rrt.exe	Get hash	malicious	Browse	
	34PO 880118.exe	Get hash	malicious	Browse	
	38PO8800145.exe	Get hash	malicious	Browse	
	44PO883094284.exe	Get hash	malicious	Browse	
	57PO882938.exe	Get hash	malicious	Browse	
	24PO no 11927346.exe	Get hash	malicious	Browse	
	56PO7748579.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Size (bytes):	1308
Entropy (8bit):	5.407964534767842
Encrypted:	false
MD5:	7D21E992D9C04689FC6B168F1144A420
SHA1:	B4CE928CFF5B0949DF97035480C39D9DD3A76717
SHA-256:	200691B81396B8AFB4C49512C5C92F27F9709F850C41F8E823933824238FC91A

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SHA-512:	86118F38BF023FBF49F91B101A1A00A7CB893CF1DB29C3C9F084BDEA4541F7560E2D3599BAE719036A808418EA3DBB044B9ADD2AED538439EE1083A7273854F
Malicious:	false
Reputation:	low
Preview:	@...e.....P.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementH.....].....E..Jqp..... .Microsoft.PowerShell.ConsoleHost0.....G-.o...A...4B.....System..4.....A:.(.D.....System.Core.D.....N..o.H...1.w.....System.Management.AutomationL.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....5...KG..).....System.Data.4.....Zg5..:O..g..q.....System.Xml..8.....'....L..}.....System.Numerics.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationD.....-.D.F.<;.nt.1..System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\Desktop\Orden_De_Compra_019999_img.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: order_403_img.exe, Detection: malicious, Browse • Filename: Purchase Order.exe, Detection: malicious, Browse • Filename: 3Payment copy.exe, Detection: malicious, Browse • Filename: 46US246448DPayment copy.exe, Detection: malicious, Browse • Filename: 18invoice.exe, Detection: malicious, Browse • Filename: 14invoice.exe, Detection: malicious, Browse • Filename: 28invoic.exe, Detection: malicious, Browse • Filename: 68invoice.exe, Detection: malicious, Browse • Filename: 1Swift copy.exe, Detection: malicious, Browse • Filename: 32Swift copy.exe, Detection: malicious, Browse • Filename: 29Swift copy.exe, Detection: malicious, Browse • Filename: 4688.exe, Detection: malicious, Browse • Filename: Request for Quotation AGP Global Group LLC No. 219007290.exe, Detection: malicious, Browse • Filename: 50rrt.exe, Detection: malicious, Browse • Filename: 34PO 880118.exe, Detection: malicious, Browse • Filename: 38PO8800145.exe, Detection: malicious, Browse • Filename: 44PO883094284.exe, Detection: malicious, Browse • Filename: 57PO882938.exe, Detection: malicious, Browse • Filename: 24PO no 11927346.exe, Detection: malicious, Browse • Filename: 56PO7748579.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... ..H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc.....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o.....*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o.....r]..p.o!....,.{T.....{U.....o"....+(.ra..p.o!....,.{T.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3202qsrl.02t.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	81
Entropy (8bit):	4.616360832185304
Encrypted:	false
MD5:	8F145F939110AA69FFD604DC80C21D24
SHA1:	C7357B3C171447E9898DF117E56BD77391325ADB
SHA-256:	0754DC2DB8027E490A13E11BCC2969D5D69E717F847BC41E4C9D923704FB103B
SHA-512:	D7870D494D5331B1C6426E01E25141E7ADC3E2BA7566726074DF8DEF7380CBE5E9AB0A5FC1A65064A5CB33D04B6AA555E5B3493F2FBDF37EAD162750B1C8CEC
Malicious:	false
Reputation:	low
Preview:	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 12:46:18 PM

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u4vb1sqn.5nv.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	81
Entropy (8bit):	4.616360832185304

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_u4vb1sqn.5nv.ps1	
Encrypted:	false
MD5:	8F145F939110AA69FFD604DC80C21D24
SHA1:	C7357B3C171447E9898DF117E56BD77391325ADB
SHA-256:	0754DC2DB8027E490A13E11BCC2969D5D69E717F847BC41E4C9D923704FB103B
SHA-512:	D7870D494D5331B1C6426E01E25141E7ADC3E2BA7566726074DF8DEF7380CBE5E9AB0A5FC1A65064A5CB33D04B6AA555E5B3493F2FBDF37EAD162750B1C8CEC
Malicious:	false
Reputation:	low
Preview:	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 12:46:18 PM

C:\Users\user\Desktop\Veladecor_order1.jpg	
Process:	C:\Users\user\Desktop\Orden_De_Compra_019999_img.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 600x600, segment length 16, baseline, precision 8, 5368x6950, frames 3
Size (bytes):	1011808
Entropy (8bit):	5.934233802965728
Encrypted:	false
MD5:	51ED0F55546B18785E69AE50D6327DCA
SHA1:	AC333D5D02E5E37A09BCB7D2F3307C7D39CEC4AF
SHA-256:	4D31EB037F7F726B9466FFA75584DA65253E4662AD2D9EFF278EF4776A91940D
SHA-512:	489C57C366275D8623CAEEA509EB471386D45693653E3B7418BBC1FE803D48E733805B70F64BF37B90D37218AF8FC7130FF59F281CEB970ED8BF25BF6E6456EC
Malicious:	**true**
Reputation:	low
Preview:	......JFIF.....X.X.....C................................. $.' ",#..(7),01444.'9=82<.342...C..........2!.!22222222222222222222222222222222222222222222222222......&....".................. ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?...(... (...(..

C:\Users\user\Documents\20200529\PowerShell_transcript.305090.LfNbm6YD.20200529124617.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Size (bytes):	3655
Entropy (8bit):	5.253443641614268
Encrypted:	false
MD5:	3E693A482B44E68DF308656DE4D5AC7C
SHA1:	C09B46AD92C81053FE137617F98314587D159D6E
SHA-256:	886F5BA33BFE44C7A31C333ACCE399FD3C2A5964F2D2FEB69EEA75E25AEE9D26
SHA-512:	9458D87784591DF72DCCAED0C12E29DEA1D383FEF670F7E8EA075BCBB43474D29D15B678E565BEB3737B10AE139EB45D9765909BEACD93FD3FC2D65FEA2C836
Malicious:	false
Reputation:	low
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20200529124618..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 305090 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Start-Process C:\Users\user\Desktop\Veladecor_order1.jpg..Process ID: 3896..PSVersion: 5.1.17134.165..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.165..BuildVersion: 10.0.17134.165..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..**********************..Command start time: 20200529124618..**********************..PS>Start-Process C:\Users\user\Desktop\Veladecor_order1.jpg..**********************..Command start time: 20200529124618..**********************..PS>TerminatingError(Start-Process): "This command cannot be run due to the error: No application is associated with th

C:\Users\user\Documents\Veladecor_order1.txt	
Process:	C:\Users\user\Desktop\Orden_De_Compra_019999_img.exe
File Type:	ASCII text, with no line terminators
Size (bytes):	64
Entropy (8bit):	3.7744000497097856
Encrypted:	false
MD5:	EC7FCED7B29E55848F5DD12213133856
SHA1:	AA51FCDF908CA0916141A0DD8C97773B1A07B7AC
SHA-256:	8ABDE69F15416A935940E537799EFEE2FF3BF9BA5E669977E734EB3BCEC2081C
SHA-512:	D5FA92FA67B1843FEADC2D1388E9F3E581200FC5677B24EC1F8F7F6CDAA6EFA43C8C8B7340BCE894F3E9EDF441ADDAEF373D39DA15A19B196069A19777C00DFD
Malicious:	false
Reputation:	low
Preview:	4d31eb037f7f726b9466ffa75584da65253e4662ad2d9eff278ef4776a91940d

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.208250066753597
TrID:	• 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:	Orden_De_Compra_019999_img.exe
File size:	2458624
MD5:	cc209b878cb2993332dc05802716ad83
SHA1:	c069335fe4a39f64fd0f84b47dae44a832195040
SHA256:	b8541f6bb3a95ce34949861ff7224c39c7f207a55801eaa98d421bf3f3a65e98
SHA512:	f315dfc81ef89a53b11fe6d5a515df9112b5638cef6b024453cd61ec687adef75256ed5e52a1797e7f0ee3086e268add1ec8cf526c95b1e4a155158d8956a23
SSDEEP:	12288:OGSv6VEt6ZROZUmxNimXDlKFLIbsL1swv91SrSlPq2Jwz38O:DSv6NZRO6ibql1swHC2eQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...2.]].....z%.....%.. ....%...@.. .....%.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x6598de
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, HIGH_ENTROPY_VA
Time Stamp:	0x5D5D9632 [Wed Aug 21 19:06:26 2019 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x259884	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x25a000	0x5f6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x25c000	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	
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	0x2578e4	0x257a00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x25a000	0x5f6	0x600	False	0.462890625	data	4.43207684197	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x25c000	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_VERSION	0x25a0a0	0x36c	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x25a40c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2009 - 2019
Assembly Version	0.0.0.0
InternalName	8000010000000.exe
FileVersion	5.7.9.12
CompanyName	Z&t8mJ3*S@g46X+e^
Comments	L)i3*2Qa5q^PC8b+
ProductName	P&p79E%yA^r6+4R
ProductVersion	5.7.9.12
FileDescription	P&p79E%yA^r6+4R
OriginalFilename	8000010000000.exe

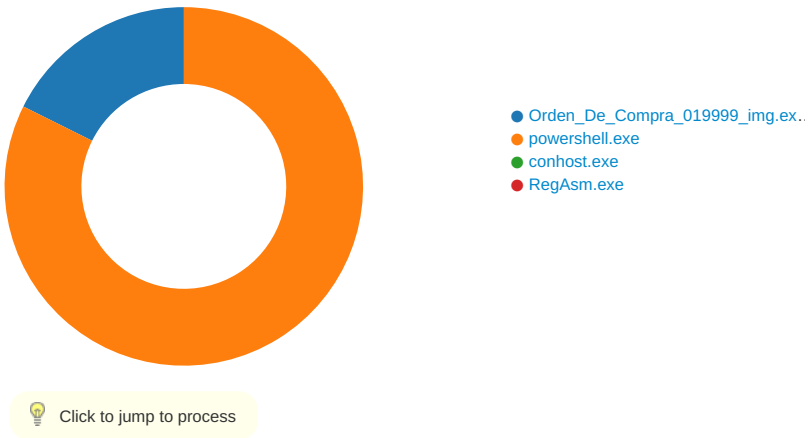
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Orden_De_Compra_019999_img.exe PID: 5060 Parent PID: 5104

General

Start time:	12:46:07
Start date:	29/05/2020
Path:	C:\Users\user\Desktop\Orden_De_Compra_019999_img.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orden_De_Compra_019999_img.exe'
Imagebase:	0x860000
File size:	2458624 bytes
MD5 hash:	CC209B878CB2993332DC05802716AD83
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.888497000.0000000004131000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.887779335.0000000003F25000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.888931397.000000000437D000.00000004.00000001.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\Temp\RegAsm.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	13CD359	CopyFileExW
C:\Users\user\Desktop\Veladecor_order1.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C481E60	CreateFileW
C:\Users\user\Documents\Veladecor_order1.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C481E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Orden_De_Compra_019999_img.exe:Zone.Identifier	success or wait	1	13C2FFA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0	64616	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 78 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b0 00 00 00 0c 00 00 00 00 00 00 5e ce 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 df c9 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...xX.Z.......... ....0............^.... ....@.. ....`.................	success or wait	1	13CD359	CopyFileExW
C:\Users\user\Desktop\Veladecor_order1.jpg	unknown	1011808	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 02 58 02 58 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19 12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27 20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f 27 39 3d 38 32 3c 2e 33 34 32 ff db 00 43 01 09 09 09 0c 0b 0c 18 0d 0d 18 32 21 1c 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 ff c0 00 11 08 1b 26 14 f8 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.....X.X.....C...... .... $.' ",#.. (7),01444.'9=82<.342. ..C...........2!.!22222222222 2 2222222222222222222222 22222222 22222222......&....".......... ....}........! 1A..Qa."q.2....	success or wait	1	6C481B4F	WriteFile
C:\Users\user\Documents\Veladecor_order1.txt	unknown	64	34 64 33 31 65 62 30 33 37 66 37 66 37 32 36 62 39 34 36 36 66 66 61 37 35 35 38 34 64 61 36 35 32 35 33 65 34 36 36 32 61 64 32 64 39 65 66 66 32 37 38 65 66 34 37 37 36 61 39 31 39 34 30 64	4d31eb037f7f726b9466ffa7 5584da 65253e4662ad2d9eff278ef 4776a91940d	success or wait	1	6C481B4F	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	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D583625	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\5e7364da399b604ae01baff696551080\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D58A974	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\2da4cf2bb9a8f8a554da96d83ee20d39\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\84b9171c43be8428a7ceaf253e5d7738\System.ni.dll.aux	unknown	620	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\b8254ec01c31459d7f6f66e4d6a670a5\PresentationFramework.ni.dll.aux	unknown	2436	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\7ede7502bdd935f2e31c32146e8206cf\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\74e4951d24e78d60061b6f9f8d6f49f4\PresentationCore.ni.dll.aux	unknown	1832	success or wait	1	6D4EEE1E	ReadFile
C:\Users\user\Desktop\Veladecor_order1.jpg	unknown	4096	success or wait	248	6C481B4F	ReadFile
C:\Users\user\Desktop\Veladecor_order1.jpg	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Users\user\Documents\Veladecor_order1.txt	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\a6dc920c743d8d4c45ef799d1dd53f5a\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6D4EEE1E	ReadFile

Analysis Process: powershell.exe PID: 3896 Parent PID: 5060

General

Start time:	12:46:17
Start date:	29/05/2020
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Start-Process C:\Users\user\Desktop\Veladecor_order1.jpg
Imagebase:	0x12d0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6D5DA9F6	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	6D5DA9F6	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_u4vb1sqn.5nv.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C481E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_3202qsrl.02t.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C481E60	CreateFileW
C:\Users\user\Documents\20200529	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C48BEFF	CreateDirectoryW
C:\Users\user\Documents\20200529\PowerShell_transcript.305090.LfNbm6YD.20200529124617.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C481E60	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	67C66F51	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	67C66F51	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	67C66F51	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_u4vb1sqn.5nv.ps1	success or wait	1	6C486A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_3202qsrl.02t.psm1	success or wait	1	6C486A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_u4vb1sqn.5nv.ps1	unknown	81	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20 35 2f 32 39 2f 32 30 32 30 20 31 32 3a 34 36 3a 31 38 20 50 4d	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 12:46:18 PM	success or wait	1	6C481B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_3202qsrl.02t.psm1	unknown	81	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20 35 2f 32 39 2f 32 30 32 30 20 31 32 3a 34 36 3a 31 38 20 50 4d	# PowerShell test file to determine AppLocker lockdown mode 5/29/2020 12:46:18 PM	success or wait	1	6C481B4F	WriteFile
C:\Users\user\Documents\20200529\PowerShell_transcript.305090.LfNbm6YD.20200529124617.txt	unknown	3	ef bb bf	...	success or wait	1	6C481B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20200529\PowerShell_transcript.305090.LfNbm6YD.20200529124617.txt	unknown	649	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 30 30 35 32 39 31 32 34 36 31 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 47 55 43 43 49 2d 50 43 5c 47 75 63 63 69 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 47 55 43 43 49 2d 50 43 5c 47 75 63 63 69 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 30 35 30 39 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 74 65 6d 33 32	********************..Windows PowerShell transcript start..Start time: 20200529124618..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 305090 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32	success or wait	31	6C481B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 12 00 00 00 06 00 00 00 12 00 00 00 14 00 00 00 14 00 14 00 00 00 00 00 00 00 14 03 1f 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@...e.....	success or wait	1	6D907A0C	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	50 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 2d 4b d4 8c 9f 73 ed 46 ac b3 2a 06 5d 60 f6 2c 06 00 00 00 0e 00 28 00	P.....-K...s.F..*.]` .,.....(.	success or wait	18	6D907A0C	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6d 6d 61 6e 64 73 2e 4d 61 6e 61 67 65 6d 65 6e 74	Microsoft.PowerShell.Commands.Management	success or wait	18	6D907A0C	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2	00 00	..	success or wait	11	6D907A0C	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	64 00 00 03	d...	success or wait	1	6D907A0C	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	96	01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0e 80 00 0a 0e 80 00 0b 0c 80 00 0c 0e 80 00 0d 0e 80 00 00 0e 80 00 0e 0c 80 00 0f 0c 80 00 10 0c 80 00 14 05 40 00 1a 05 40 00 19 05 40 00 50 00 40 00 3b 00 40 00 1b 05 40 00 11 0e 80 00	....@...@...@.P.@.;.@. ..@.....	success or wait	1	6D907A0C	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D583625	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D583625	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\5e73 64da399b604ae01baff696551080\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D58A974	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6D58A974	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D58A974	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Pb3 78ec07#\a49a6f68fd8329a3643a8c5f19cd22b1\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\84b917 1c43be8428a7ceaf253e5d7738\System.ni.dll.aux	unknown	620	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\2 da4cf2bb9a8f8a554da96d83ee20d39\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manaa5 7fc8cc#\fa15d91c3a3ce3897f6f7add11b07b7a\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D583625	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D583625	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D583625	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6D583625	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D583625	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D58FE93	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1300	success or wait	1	6D58FF5F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\7cd45214b16ac052310de729e2e961d1\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manage ment\75bcfbe3b1bae498cf18ca849d4fa253\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\7 d593032eddb9a41f2a32be1037ecf24\System.Data.ni.dll.aux	unknown	1540	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Dired1 3b18a9#\942ad97090e80aed6f7d90cd2ee80647\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4d 91b386e64bacbfdf3b2db16155386b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numeri cs\a6dc920c743d8d4c45ef799d1dd53f5a\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P6f 792626#\999dba40835396d9c8714157c431a443\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Transa ctions\1dd28ec19e7aa8bbfe3c3e047f961f35\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\d88a90d2c98cca1a9d491dfeb73352be\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4EEE1E	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	132	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C481B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Confe64a9051#\07481a515e460188dcc18c39d52d3148\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6D5C28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6D5C28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6D5C28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	2	6D5C28CF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6D5C28CF	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.P521220ea#\1fbb6f56ca1fe111ec8b6d45423dc33d\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	6D4EEE1E	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C481B4F	ReadFile

Analysis Process: conhost.exe PID: 3036 Parent PID: 3896

General

Start time:	12:46:17
Start date:	29/05/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c77e0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 940 Parent PID: 5060

General

Start time:	12:46:32
Start date:	29/05/2020
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.882263652.0000000000422000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Disassembly

Code Analysis