ID: 358114
Sample Name: caraganas.exe
Cookbook: default.jbs
Time: 03:38:05
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

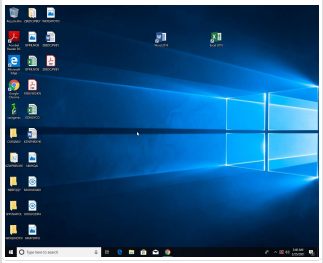
Analysis Report caraganas.exe

Overview

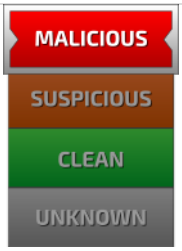
General Information

Sample Name:	caraganas.exe
Analysis ID:	358114
MD5:	99d875ac334145..
SHA1:	c459b8df634dc70..
SHA256:	98bbdc74c1ff540..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



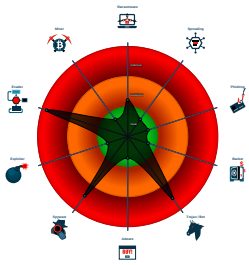
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Found evasive API chain (trying to d…
- Hides threads from debuggers
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- caraganas.exe (PID: 6820 cmdline: 'C:\Users\user\Desktop\caraganas.exe' MD5: 99D875AC3341453383C9105669E14538)
  - RegAsm.exe (PID: 1724 cmdline: 'C:\Users\user\Desktop\caraganas.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
  - RegAsm.exe (PID: 2916 cmdline: 'C:\Users\user\Desktop\caraganas.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 4588 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "Q2TP9tlm",
  "URL: ": "http://8vV1Qxo32XjttpL.org",
  "To: ": "rzKGV@ahwhW.com",
  "ByHost: ": "mail.jesmar.net:587",
  "Password: ": "0s0uxNrAPxOSN",
  "From: ": "info@jesmar.net"
}
```


Yara Overview

Memory Dumps

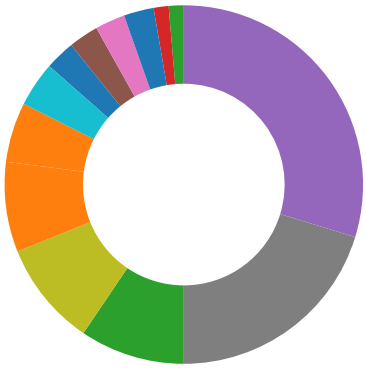
Source	Rule	Description	Author	Strings
00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.596328627.0000000000B01000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 2916	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 2916	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

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)

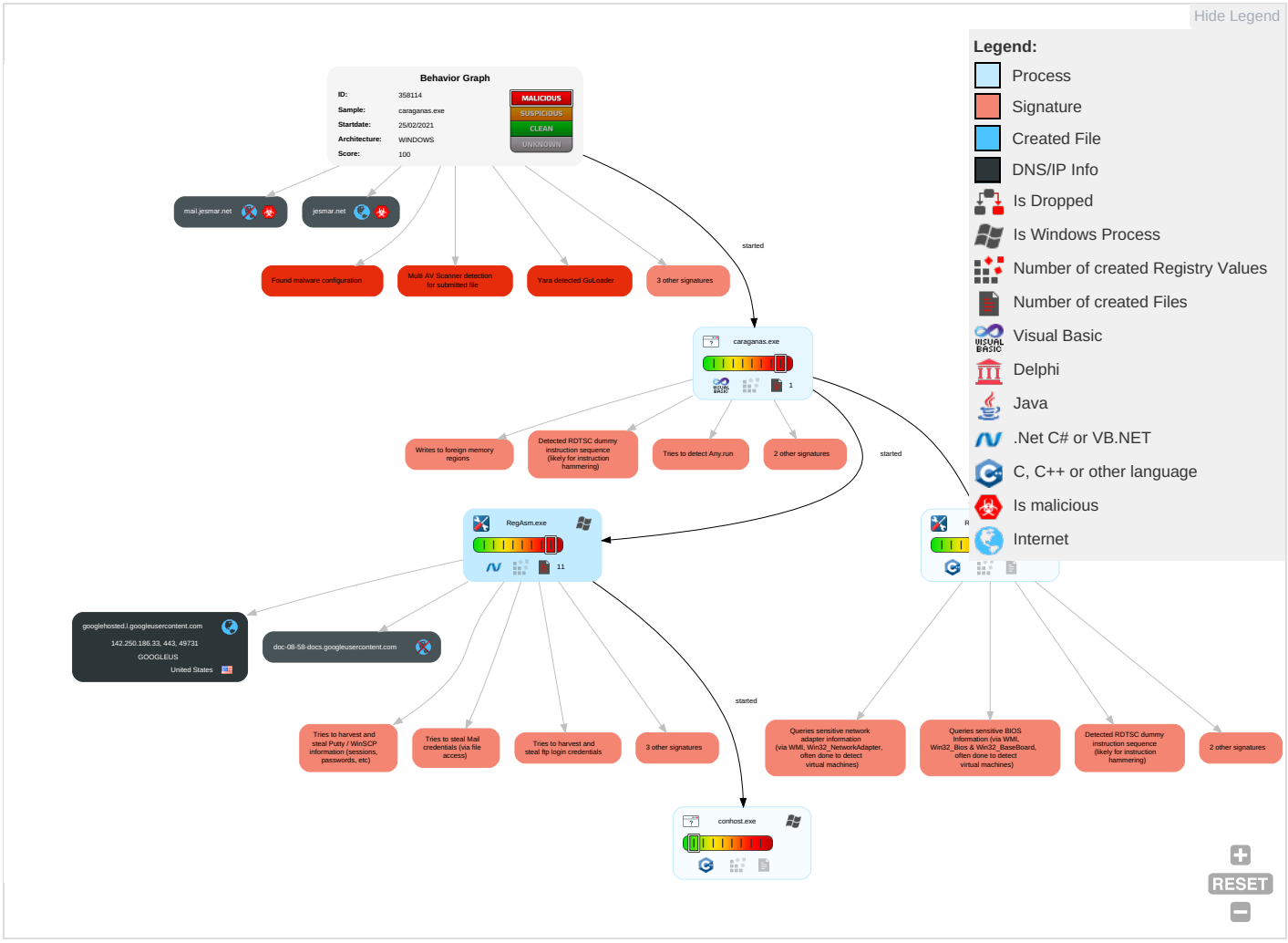
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Access Token Manipulation 1	Virtualization/Sandbox Evasion 3 4	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Disable or Modify Tools 1 1	Input Capture 1	Security Software Discovery 6 3 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Access Token Manipulation 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 3 4	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Application Layer Protocol 1 2
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	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

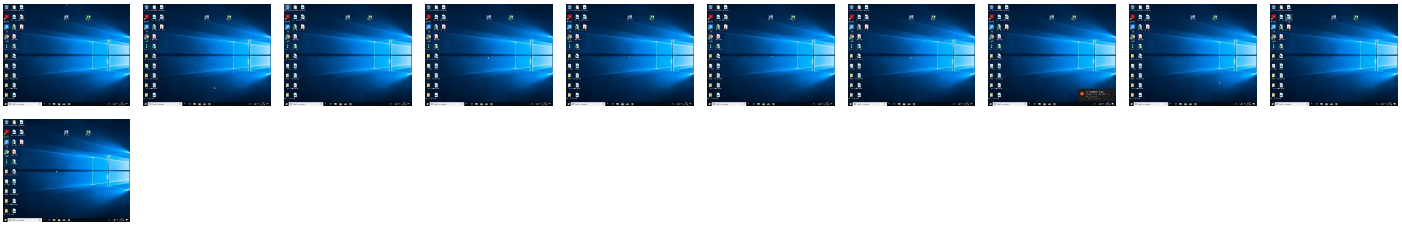
Behavior Graph



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
caraganas.exe	19%	Metadefender		Browse
caraganas.exe	11%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://8vV1Qxo32XjttpL.org	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://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://DPtQpK.com	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/06	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
jesmar.net	31.193.225.171	true	true		unknown
doc-08-58-docs.googleusercontent.com	unknown	unknown	false		high
mail.jesmar.net	unknown	unknown	true		unknown

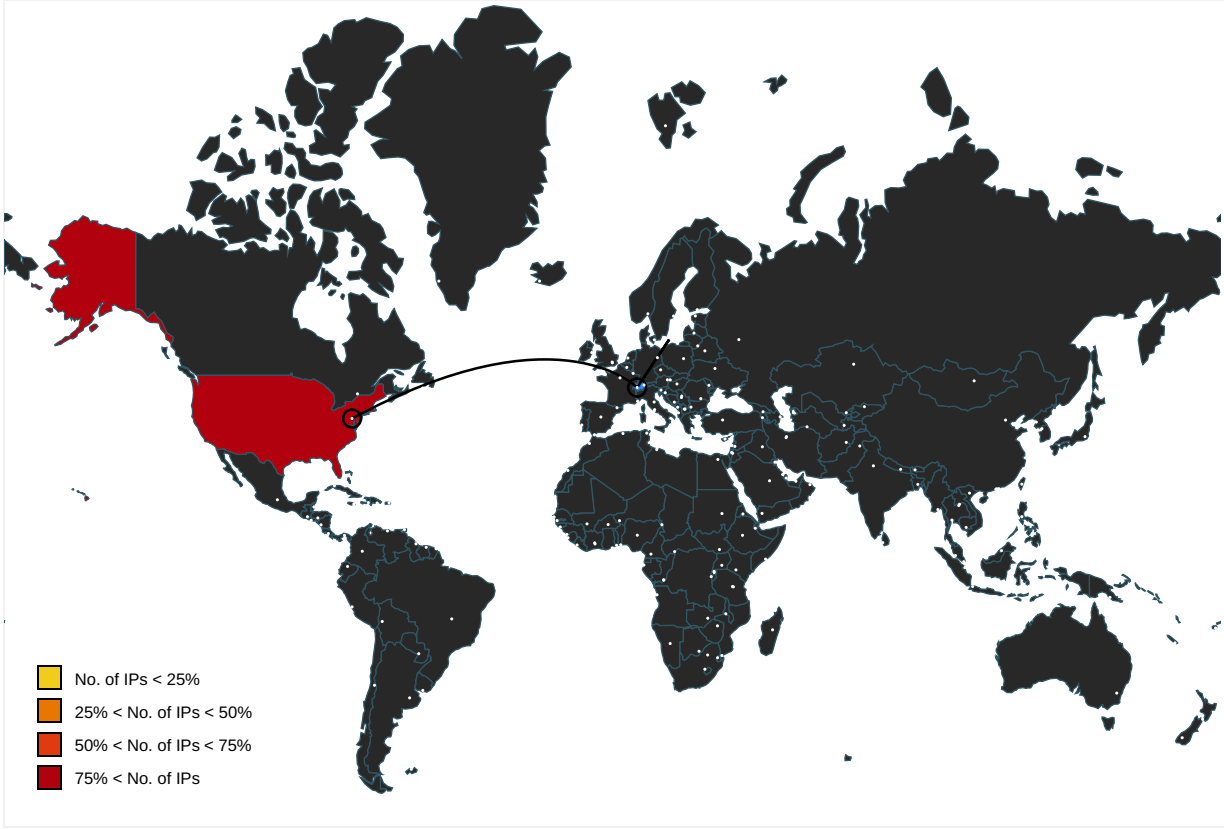
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://8vV1Qxo32XjttpL.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://r3.o.lencr.org0	RegAsm.exe, 00000006.00000002.601670799.000000001D905000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	RegAsm.exe, 00000006.00000002.601670799.000000001D905000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: 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, 00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DPtQpK.com	RegAsm.exe, 00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	RegAsm.exe, 00000006.00000002.601670799.000000001D905000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/06	RegAsm.exe, 00000006.00000002.601670799.000000001D905000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.33	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358114
Start date:	25.02.2021
Start time:	03:38:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	caraganas.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/1@2/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 19.6% (good quality ratio 10.4%) • Quality average: 34.6% • Quality standard deviation: 38.5%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 92.122.145.220, 40.88.32.150, 168.61.161.212, 52.147.198.201, 51.104.139.180, 142.250.74.206, 8.238.85.254, 67.27.159.254, 67.26.17.254, 8.252.5.126, 8.238.85.126, 51.103.5.159, 52.155.217.156, 92.122.213.247, 92.122.213.194, 20.54.26.129, 23.218.208.56 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/358114/sample/caraganas.exe

Simulations

Behavior and APIs

Time	Type	Description
03:39:40	API Interceptor	702x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
142.250.186.33	#U266b VM_540283.htm	Get hash	malicious	Browse	
	_vm54959395930.htm	Get hash	malicious	Browse	
	Malone3388_001.htm	Get hash	malicious	Browse	
	dgaTCZovz.msi	Get hash	malicious	Browse	
	2021-Nieuwepayroll-Aanpassing.html	Get hash	malicious	Browse	
	PO112000891122110.exe	Get hash	malicious	Browse	
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	
	xerox for hycite.htm	Get hash	malicious	Browse	
	Muligheds.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
googlehosted.l.googleusercontent.com	#U266b VM_540283.htm	Get hash	malicious	Browse	• 142.250.186.33
	_vm54959395930.htm	Get hash	malicious	Browse	• 142.250.186.33
	Malone3388_001.htm	Get hash	malicious	Browse	• 142.250.186.33
	dgaTCZovz.msi	Get hash	malicious	Browse	• 142.250.186.33
	2021-Nieuwepayroll-Aanpassing.html	Get hash	malicious	Browse	• 142.250.186.33
	seed.exe	Get hash	malicious	Browse	• 142.250.186.33
	PO112000891122110.exe	Get hash	malicious	Browse	• 142.250.186.33
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 142.250.186.33
	xerox for hycite.htm	Get hash	malicious	Browse	• 142.250.186.33
	Muligheds.exe	Get hash	malicious	Browse	• 142.250.186.33
	2021-Nouvelle masse salariale-Rapport.html	Get hash	malicious	Browse	• 216.58.209.33
	SOLICITUD DE HERJIMAR, SL (HJM-745022821).exe	Get hash	malicious	Browse	• 216.58.208.161
	#U6211#U662f#U56fe#U7247.exe	Get hash	malicious	Browse	• 216.58.208.161
	OneNote rmos@dataflex-int.com.html	Get hash	malicious	Browse	• 216.58.208.129
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 172.217.20.225
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 172.217.20.225
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 172.217.20.225
	CONSTRUCCIONES SAN MART#U00cdN, S.A. SOLICITAR. (SMT-14517022021).exe	Get hash	malicious	Browse	• 172.217.20.225
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	2021_02_25.exe	Get hash	malicious	Browse	• 34.102.136.180
	#U266b VM_540283.htm	Get hash	malicious	Browse	• 142.250.186.33
	_vm54959395930.htm	Get hash	malicious	Browse	• 172.217.16.150
	007.docx	Get hash	malicious	Browse	• 216.239.34.21
	007.docx	Get hash	malicious	Browse	• 216.239.34.21
	docabrir#U2332nsakjfsdi.msi	Get hash	malicious	Browse	• 35.192.222.107
	Malone3388_001.htm	Get hash	malicious	Browse	• 142.250.186.35
	55gfganfgF.exe	Get hash	malicious	Browse	• 34.102.136.180
	YcvIOMqVPE.exe	Get hash	malicious	Browse	• 35.228.210.99
	YcvIOMqVPE.exe	Get hash	malicious	Browse	• 35.228.210.99
	yrsTO0ER4V.exe	Get hash	malicious	Browse	• 34.102.136.180
	Wd8LBdddKD.exe	Get hash	malicious	Browse	• 8.8.8.8
	GRAFINGER#00124022021#INVOICE#.exe	Get hash	malicious	Browse	• 34.98.99.30
	mt5setup.exe	Get hash	malicious	Browse	• 8.8.8.8
	vEpq5DFvET	Get hash	malicious	Browse	• 216.239.35.0
	RQP_10378065.exe	Get hash	malicious	Browse	• 34.102.136.180
	vEpq5DFvET	Get hash	malicious	Browse	• 142.250.184.74
	Price quotation.exe	Get hash	malicious	Browse	• 34.102.136.180
	DHL Shipping Document_Pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	886t3PbVKb.apk	Get hash	malicious	Browse	• 142.250.18 0.142

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Notification 466022.xlsm	Get hash	malicious	Browse	• 142.250.186.33
	Fax #136.xlsm	Get hash	malicious	Browse	• 142.250.186.33
	Purchase Order22420.exe	Get hash	malicious	Browse	• 142.250.186.33
	ceFlxYfe4F.exe	Get hash	malicious	Browse	• 142.250.186.33
	Fatura.exe	Get hash	malicious	Browse	• 142.250.186.33
	Reports #176.xlsm	Get hash	malicious	Browse	• 142.250.186.33
	SecuriteInfo.com.VB.Heur2.EmoDldr.5.B611173F.Gen.18420.xlsm	Get hash	malicious	Browse	• 142.250.186.33
	Scan #84462.xlsm	Get hash	malicious	Browse	• 142.250.186.33
	Invoice_#_6774.xlsm	Get hash	malicious	Browse	• 142.250.186.33
	Concentracion de pedidos_PO.exe	Get hash	malicious	Browse	• 142.250.186.33
	Notice 698.xlsm	Get hash	malicious	Browse	• 142.250.186.33
	Waybill.exe	Get hash	malicious	Browse	• 142.250.186.33
	qBS4ZpUp8z.exe	Get hash	malicious	Browse	• 142.250.186.33
	O5xV2xnPRG.exe	Get hash	malicious	Browse	• 142.250.186.33
	New purchase order PO 78903215,pdf.exe	Get hash	malicious	Browse	• 142.250.186.33
	Customer-2-24-2021.exe	Get hash	malicious	Browse	• 142.250.186.33
	xRxGPqypIw.exe	Get hash	malicious	Browse	• 142.250.186.33
	Customer-2-24-2021.exe	Get hash	malicious	Browse	• 142.250.186.33
	Customer-2-24-2021.exe	Get hash	malicious	Browse	• 142.250.186.33
	logs.php.dll	Get hash	malicious	Browse	• 142.250.186.33

Dropped Files

No context

Created / dropped Files

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.37222266574873
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	caraganas.exe

General

File size:	73728
MD5:	99d875ac3341453383c9105669e14538
SHA1:	c459b8df634dc70ea2537d9588eeeb3d2b644d94
SHA256:	98bbdc74c1ff5407450d9019407d2012a08075269228497f10b9bf6e6471de42
SHA512:	d31f378dfc326ce5b84a73e7831d465860a20bd1ea2c61df1276821ac28275ca66b604e75a1e0634aaee52e652ee9e0a514175109fe91721a0e33ea4f8176b69
SSDEEP:	1536:lX/wjwu21SsQTT+d6oaVoEsVjcOekVBxEsfX:lvwN2aZaEejbeYBJf
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L.....N.....0.....@.....

File Icon

Icon Hash:	b038b57269717938

Static PE Info

General

Entrypoint:	0x401394
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4E1EA599 [Thu Jul 14 08:15:21 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	f783b7553c2ee07b6bd756ebd3705f2c

Entrypoint Preview

Instruction
push 0040A3F8h
call 00007F0D5CE25475h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, dl
daa
pop edx
in al, dx
jecxz 00007F0D5CE254C8h
sbb eax, 9927B44Dh
fdivr dword ptr [ebx+65h]
cmp al, byte ptr [eax]
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
inc ecx
insb
imul esp, dword ptr [ebp+6Eh], 6C696261h
imul esi, dword ptr [ecx+edi*2+37h], 00000000h
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or ah, byte ptr [eax+7A66635Bh]
out 40h, eax
mov dh, byte ptr [eax+2CBE1EF8h]
mov bl, 85h
adc eax, 85736377h
pop eax
movsd
dec esp
test al, 77h
mov byte ptr [708DFD57h], al
sar dword ptr [edx], 1
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
ret
mov es, word ptr [eax]
add byte ptr [edi], cl
or al, 00h
add byte ptr [eax], al
or byte ptr [eax], al
push ebx
inc ebp
dec esi
dec edi
push eax
dec ecx
inc ecx
push ebx

Instruction
add byte ptr [41000B01h], cl
jne 00007F0D5CE254E9h
insd
outsb

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xeb14	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xf46	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x11c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xe008	0xf000	False	0.374365234375	data	5.84340475818	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0x1210	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xf46	0x1000	False	0.323974609375	data	3.6279359857	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x12c5e	0x2e8	data		
RT_ICON	0x123b6	0x8a8	data		
RT_GROUP_ICON	0x12394	0x22	data		
RT_VERSION	0x12120	0x274	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaLenBstrB, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

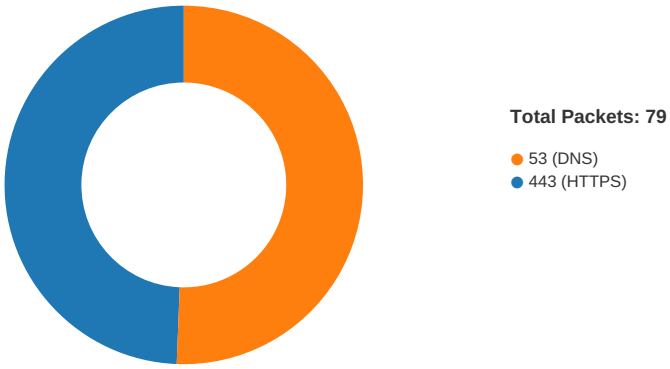
Description	Data
Translation	0x0409 0x04b0
InternalName	caraganas
FileVersion	1.00
CompanyName	Wang
ProductName	Wang Laboratories
ProductVersion	1.00
FileDescription	Wang Laboratories
OriginalFilename	caraganas.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 03:39:32.892580986 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:32.941040993 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:32.941245079 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:32.942042112 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:32.992175102 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:32.999365091 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:32.999404907 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:32.999422073 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:32.999440908 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:32.999546051 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:32.999603987 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.016689062 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.065464020 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.065581083 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.066787958 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.120054007 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.464006901 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.464046001 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.464067936 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.464095116 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.464121103 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.464171886 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.464234114 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.467473984 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.467505932 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.467647076 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.471004009 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.471034050 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.471131086 CET	49731	443	192.168.2.6	142.250.186.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 03:39:33.474544048 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.474572897 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.474647045 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.478106022 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.478138924 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.478250027 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.481662035 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.481693029 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.481801033 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.515280962 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.515316963 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.515465021 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.517007113 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.517051935 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.517106056 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.517152071 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.520566940 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.520597935 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.520689964 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.524132013 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.524164915 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.524403095 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.527677059 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.527714968 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.527812958 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.531229019 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.531264067 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.531332016 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.531347036 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.534768105 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.534823895 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.534858942 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.534869909 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.538305998 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.538378000 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.538394928 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.538431883 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.541841984 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.541923046 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.541991949 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.542016983 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.545074940 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.545114040 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.545182943 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.545203924 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.548257113 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.548284054 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.548398018 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.551470041 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.551508904 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.551604986 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.554658890 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.554694891 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.554801941 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.557887077 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.557914019 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.558136940 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.561103106 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.561136007 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.561333895 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.564265966 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.564310074 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.565624952 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.566663027 CET	443	49731	142.250.186.33	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 03:39:33.566694021 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.566797972 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.569072962 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.569107056 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.569205999 CET	49731	443	192.168.2.6	142.250.186.33
Feb 25, 2021 03:39:33.571403027 CET	443	49731	142.250.186.33	192.168.2.6
Feb 25, 2021 03:39:33.571460009 CET	443	49731	142.250.186.33	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 03:38:49.520376921 CET	54513	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:49.569129944 CET	53	54513	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:50.725361109 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:50.776966095 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:51.602782965 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:51.666085958 CET	53	63791	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:51.841176033 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:51.889820099 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:52.662291050 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:52.724816084 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:54.352112055 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:54.400726080 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:55.452254057 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:55.501506090 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:56.841079950 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:56.892456055 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:57.885452032 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:57.935703039 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 03:38:58.996341944 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:38:59.044984102 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:02.026618958 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:02.083858013 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:03.546421051 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:03.598012924 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:05.042284966 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:05.090909958 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:06.183034897 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:06.231765985 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:09.605909109 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:09.663002968 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:10.888000965 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:10.936796904 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:16.163872004 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:16.215333939 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:17.358856916 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:17.407619953 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:18.316808939 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:18.365422010 CET	53	50055	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:27.044488907 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:27.101442099 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:31.931888103 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:31.996824026 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:32.822289944 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:32.889815092 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:41.844738007 CET	49694	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:41.893518925 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:42.355221033 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:42.407068014 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:53.450579882 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:53.525068998 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:54.167206049 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:54.232435942 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:54.902559042 CET	62116	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 03:39:54.959688902 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:55.261955976 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:55.320657969 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:55.446880102 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:55.507298946 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:56.017330885 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:56.074331999 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:56.451128006 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:56.521250963 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:56.718493938 CET	51818	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:56.775620937 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:57.439476013 CET	56628	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:57.503077030 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:58.599405050 CET	60778	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:58.662471056 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 03:39:59.720320940 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:39:59.779710054 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 03:40:00.333647966 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:40:00.393521070 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 03:40:26.525959969 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:40:26.611301899 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 03:40:32.628760099 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:40:32.677517891 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 03:40:33.569704056 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:40:33.643892050 CET	53	56129	8.8.8.8	192.168.2.6
Feb 25, 2021 03:41:02.268177032 CET	58177	53	192.168.2.6	8.8.8.8
Feb 25, 2021 03:41:02.357585907 CET	53	58177	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 03:39:32.822289944 CET	192.168.2.6	8.8.8.8	0x4252	Standard query (0)	doc-08-58-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 03:41:02.268177032 CET	192.168.2.6	8.8.8.8	0xaa84	Standard query (0)	mail.jesmar.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 03:39:32.889815092 CET	8.8.8.8	192.168.2.6	0x4252	No error (0)	doc-08-58-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 03:39:32.889815092 CET	8.8.8.8	192.168.2.6	0x4252	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)
Feb 25, 2021 03:41:02.357585907 CET	8.8.8.8	192.168.2.6	0xaa84	No error (0)	mail.jesmar.net	jesmar.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 03:41:02.357585907 CET	8.8.8.8	192.168.2.6	0xaa84	No error (0)	jesmar.net		31.193.225.171	A (IP address)	IN (0x0001)

HTTPS Packets

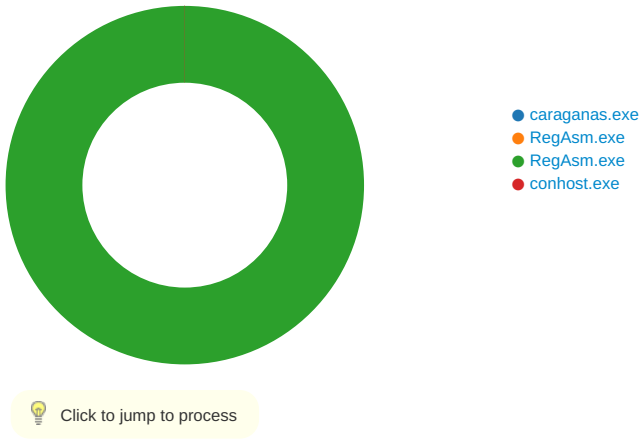
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 03:39:32.999440908 CET	142.250.186.33	443	192.168.2.6	49731	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: caraganas.exe PID: 6820 Parent PID: 5856

General

Start time:	03:38:57
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\caraganas.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\caraganas.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	99D875AC3341453383C9105669E14538
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 1724 Parent PID: 6820

General

Start time:	03:39:21
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\caraganas.exe'
Imagebase:	0xc0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 2916 Parent PID: 6820

General

Start time:	03:39:22
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\caraganas.exe'
Imagebase:	0x680000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
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: 00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.601350930.000000001D7E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000006.00000002.596328627.0000000000B01000.00000040.00000001.sdmp, Author: Joe Security
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	B02F15	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B02F15	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B02F15	InternetOpenUrlA
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	B02F15	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B02F15	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	B02F15	InternetOpenUrlA
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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	1FFC0CCB	WriteFile
\Device\ConDrv	unknown	30	4e 6f 72 64 56 50 4e 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 21 0d 0a	NordVPN directory not found!..	success or wait	1	1FFC0CCB	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	1FFC0CCB	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	1FFC0CCB	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	1FFC0CCB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	1FFC0CCB	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\f541d13e-00b1-44e0-b87b-8b050993961e	unknown	4096	success or wait	1	1FFC0CCB	ReadFile

Analysis Process: conhost.exe PID: 4588 Parent PID: 2916

General

Start time:	03:39:22
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis