ID: 358351
Sample Name: DHLHAWB 57462839.exe
Cookbook: default.jbs
Time: 13:49:14
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

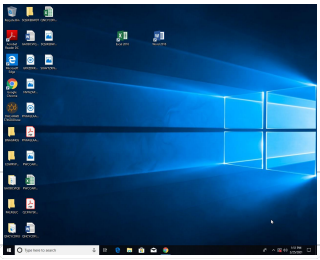
Analysis Report DHLHAWB 57462839.exe

Overview

General Information

Sample Name:	DHLHAWB 57462839.exe
Analysis ID:	358351
MD5:	83a8eaa2ef938a7.
SHA1:	817203c16a7904..
SHA256:	5a0b3456792f8d0.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

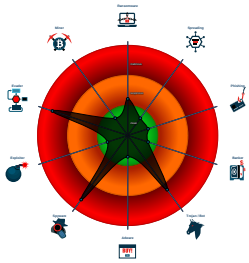
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- .NET source code contains very larg…
- Contains functionality to register a lo…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- DHLHAWB 57462839.exe (PID: 3864 cmdline: 'C:\Users\user\Desktop\DHLHAWB 57462839.exe' MD5: 83A8EAA2EF938A73DAACEBCD4E090843)
  - schtasks.exe (PID: 5604 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AFpQKAcEJx' /XML 'C:\Users\user\AppData\Local\Temp\tmpB573.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 3984 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 5300 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "instrumentation@ogpscutter.comVuVW%xY7ceous2.smtp.mailhostbox.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.203262419.000000000284 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.461216400.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.464641605.0000000002A9 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000001.00000002.203348595.00000000028B D000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.204175053.0000000003AB0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Unpacked PEs

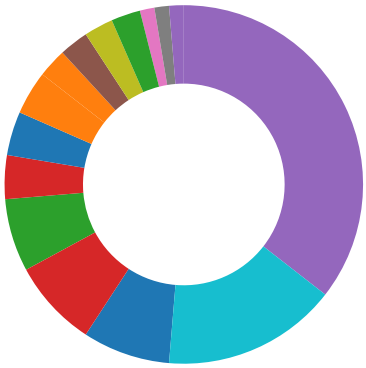
Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.DHLHAWB 57462839.exe.2870558.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
1.2.DHLHAWB 57462839.exe.3b02ff0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.DHLHAWB 57462839.exe.3b02ff0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

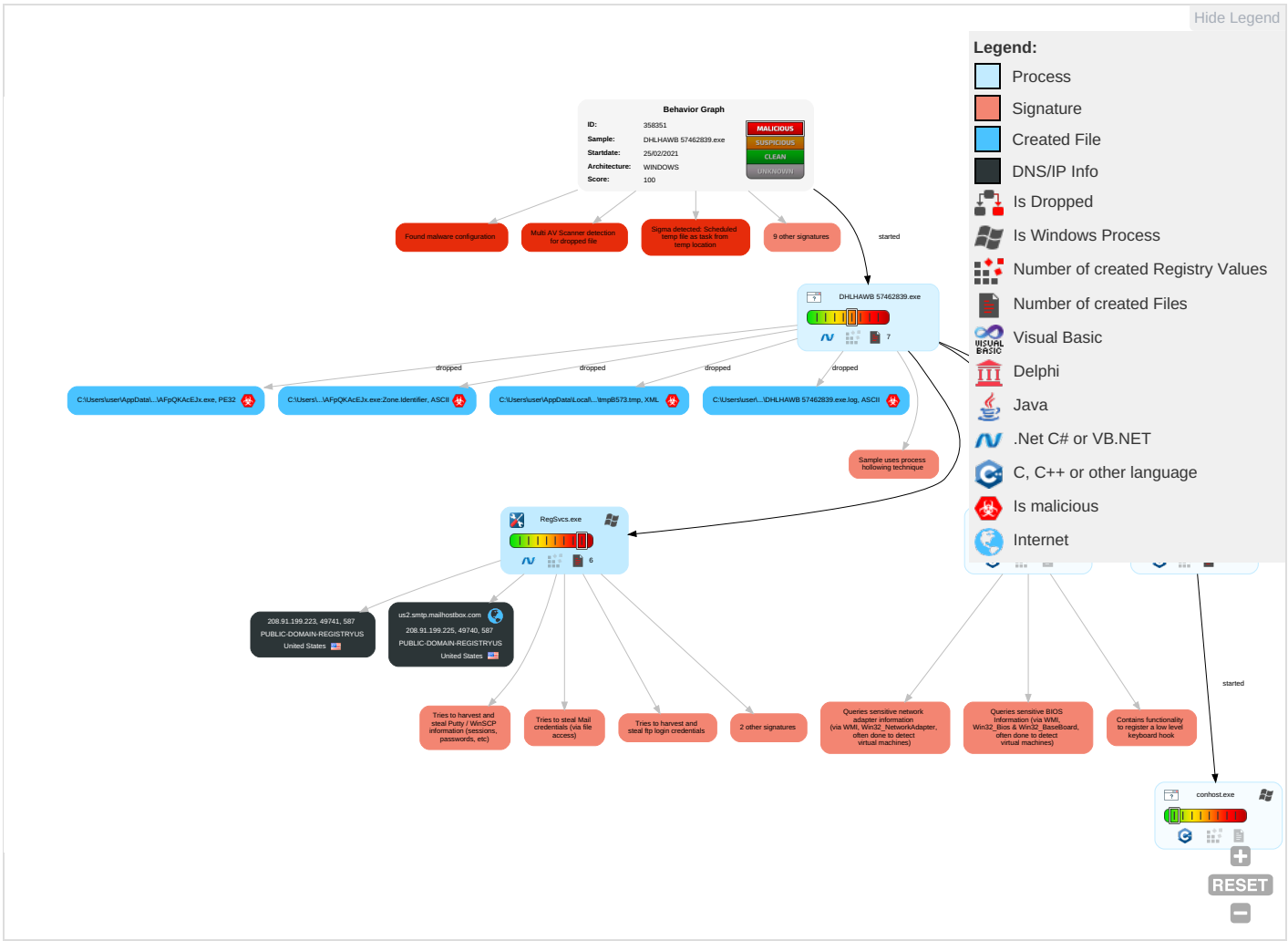
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2 1	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commanc and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

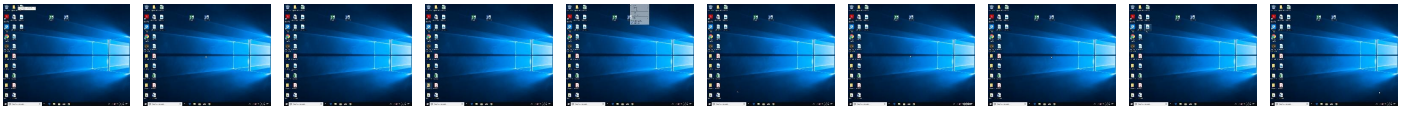
Behavior Graph



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
DHLHAWB 57462839.exe	16%	Virustotal		Browse
DHLHAWB 57462839.exe	9%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
DHLHAWB 57462839.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe	16%	Virustotal		Browse
C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe	9%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://AxCUzQTJay5lS.org	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://LAQlpY.com	2%	Virustotal		Browse
http://LAQlpY.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

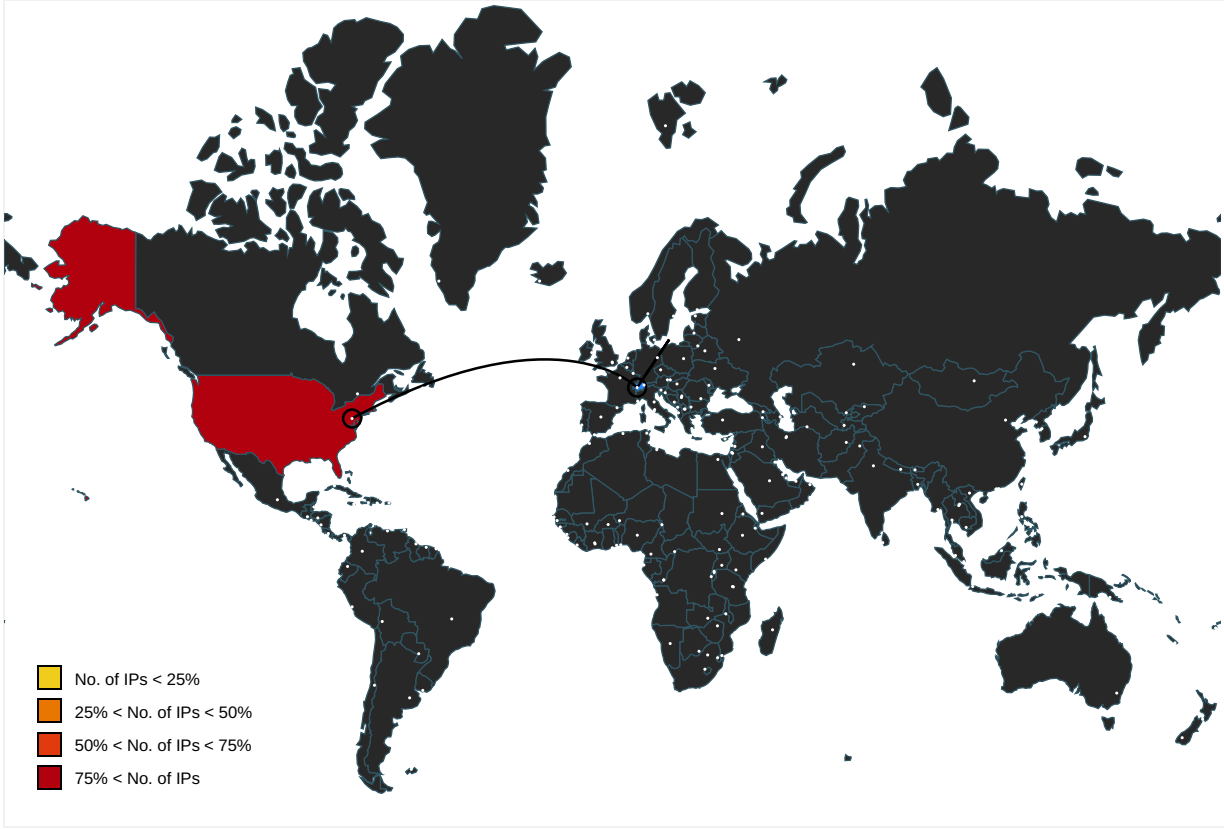
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	RegSvcs.exe, 00000005.00000002.469506028.0000000005C77000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegSvcs.exe, 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://sectigo.com/CPS0	RegSvcs.exe, 00000005.00000002.469506028.0000000005C77000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	RegSvcs.exe, 00000005.00000002.465664877.0000000002D52000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegSvcs.exe, 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://AxCUzQTJay5lS.org	RegSvcs.exe, 00000005.00000002.465602038.0000000002D48000.00000004.00000001.sdmp, RegSvcs.exe, 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp, RegSvcs.exe, 00000005.00000002.465439616.00000002D1A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0A	RegSvcs.exe, 00000005.00000002.469506028.0000000005C77000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	RegSvcs.exe, 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHLHAWB 57462839.exe, 00000001.00000002.203262419.0000000002841000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	RegSvcs.exe, 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DHLHAWB 57462839.exe, 00000001.00000002.204175053.0000000003AB0000.00000004.00000001.sdmp, RegSvcs.exe, 00000005.00000002.461216400.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	DHLHAWB 57462839.exe, 00000001.00000002.203262419.0000000002841000.00000004.00000001.sdmp	false		high
http://LAQlpY.com	RegSvcs.exe, 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.225	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
208.91.199.223	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358351
Start date:	25.02.2021
Start time:	13:49:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHLHAWB 57462839.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:	26
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@8/5@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 88.3% • Quality standard deviation: 9.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 13.64.90.137, 104.43.139.144, 51.104.139.180, 2.21.140.114, 52.255.188.83, 20.54.26.129, 8.248.139.254, 8.253.207.121, 8.248.119.254, 67.26.73.254, 8.248.147.254, 92.122.213.194, 92.122.213.247, 168.61.161.212 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:49:59	API Interceptor	1x Sleep call for process: DHLHAWB 57462839.exe modified
13:50:13	API Interceptor	745x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.225	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42850.3598.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7Lf8J7h7os.exe	Get hash	malicious	Browse	
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis1A08A3826D57.exe	Get hash	malicious	Browse	
	ELASTA-PL-INV-2021024.exe	Get hash	malicious	Browse	
	SWIFT COPY $27,078.exe	Get hash	malicious	Browse	
	SOA_021620244.exe	Get hash	malicious	Browse	
	Maskman9.exe	Get hash	malicious	Browse	
	Purchase Order POPR73861911418 6241473 101838_pdf .exe	Get hash	malicious	Browse	
	EKSPTRUpD8.exe	Get hash	malicious	Browse	
	DHL RECEIPT.exe	Get hash	malicious	Browse	
	Consolidated Order #01846.doc	Get hash	malicious	Browse	
	chrome.exe	Get hash	malicious	Browse	
	Order Confirmation.exe	Get hash	malicious	Browse	
	Swift-Copy.exe	Get hash	malicious	Browse	
	AirWaybill docs-CL.exe	Get hash	malicious	Browse	
	d0KXi1s2l6.exe	Get hash	malicious	Browse	
208.91.199.223	HcHimkU72e.exe	Get hash	malicious	Browse	
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	
	ffkjg5CVrO.exe	Get hash	malicious	Browse	
	7Lf8J7h7os.exe	Get hash	malicious	Browse	
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	
	PAYMENT INVOICE-9876543456789.exe	Get hash	malicious	Browse	
	PO 000102.xlsx	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SWIFTMENSAJE09048.exe	Get hash	malicious	Browse	
	4OO9PbFQ3L.exe	Get hash	malicious	Browse	
	IBDvluSj0F.exe	Get hash	malicious	Browse	
	Purchase Order POPR73861911418 6241473 101838_pdf .exe	Get hash	malicious	Browse	
	pzpdxoUhJh.exe	Get hash	malicious	Browse	
	Factura.exe	Get hash	malicious	Browse	
	Swift-Copy.exe	Get hash	malicious	Browse	
	9S4cmTrqO3.exe	Get hash	malicious	Browse	
	Purchase Order POPR73861911418 6241473 101838_pdf .exe	Get hash	malicious	Browse	
	Invoice-Copy.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	4019223246.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift.jpg.exe	Get hash	malicious	Browse	• 208.91.198.143
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	• 208.91.199.224
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 208.91.199.225
	HcHimkU72e.exe	Get hash	malicious	Browse	• 208.91.199.224
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 208.91.199.225
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.199.224
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.198.143
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	• 208.91.199.225
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 208.91.198.143
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.Packed2.42850.3598.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	• 208.91.199.224
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 208.91.199.225
	ffkjg5CVrO.exe	Get hash	malicious	Browse	• 208.91.198.143
	7Lf8J7h7os.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	4019223246.exe	Get hash	malicious	Browse	• 208.91.199.224
	data.xls	Get hash	malicious	Browse	• 5.100.152.162
	Swift.jpg.exe	Get hash	malicious	Browse	• 208.91.198.143
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	• 208.91.199.224
	logs.php.dll	Get hash	malicious	Browse	• 116.206.105.72
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 208.91.199.225
	HcHimkU72e.exe	Get hash	malicious	Browse	• 208.91.199.224
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 208.91.199.225
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	• 208.91.199.223
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 208.91.198.143
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 208.91.198.178
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 103.53.43.36
PUBLIC-DOMAIN-REGISTRYUS	4019223246.exe	Get hash	malicious	Browse	• 208.91.199.224
	data.xls	Get hash	malicious	Browse	• 5.100.152.162
	Swift.jpg.exe	Get hash	malicious	Browse	• 208.91.198.143
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	• 208.91.199.224
	logs.php.dll	Get hash	malicious	Browse	• 116.206.105.72
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 208.91.199.225
	HcHimkU72e.exe	Get hash	malicious	Browse	• 208.91.199.224
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 208.91.199.225
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	• 208.91.199.223
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 208.91.198.143
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 208.91.198.178
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 103.53.43.36

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHLHAWB 57462839.exe.log

Process:	C:\Users\user\Desktop\DHLHAWB 57462839.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHLHAWB 57462839.exe.log	
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..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\tmpB573.tmp	
Process:	C:\Users\user\Desktop\DHLHAWB 57462839.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.197538682468153
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB0YBtn:cbh47TlNQ//rydbz9I3YODOLNdq3eYT
MD5:	6A56190E635BC231A74FC166E5683F68
SHA1:	40516319C127B183D9BDDB8799ECDC5C9E650652
SHA-256:	4C08AD360B206E83373C5610889C07EE8CCE02B95923563D5A6A868035DC3160
SHA-512:	15C2BDFAD6C3496F355A542FEF6A091F5402E76DF80DFF449896F6E96D0392C38385E7A4FE2C190E685E2EC57D308727EE07311411B7BC16C9654246E8F9CBA7
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\5qvjakll.zyj\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe	
Process:	C:\Users\user\Desktop\DHLHAWB 57462839.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	787456
Entropy (8bit):	7.047825955554763
Encrypted:	false
SSDEEP:	12288:Si0hNfUjwdtaxyevwwVVi/goXD1v0Wwst01Jv/adetPJEwKY:SBhNf2xuwVVXGBMLsCTydkJP1
MD5:	83A8EAA2EF938A73DAACEBCD4E090843
SHA1:	817203C16A790450A754DC16CF59111DD2DADAA7

C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe	
SHA-256:	5A0B3456792F8D0E1DB3FA224863CCAB694349F33CDE1130BCF4436563EE0B2A
SHA-512:	9CA05929A37455D6C8CCC6A8BB8345929FF8F50F60CAB3318B560E5CF11A1E91DAC09487738C0CDE24CD36BB86936E3932371C7B35B75F186257195DF2B3240
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 16%, Browse • Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e7`.....P.....T..... .....@.. .....`..... ..@.....0...O.....Q.....@..... ....H.....text..... ....`.rsrc....Q.....R.....@..@.rel oc.....@.....@..B.....d.....H.....tO.....X.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....oL... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~..... (1.....,lr...p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHLHAWB 57462839.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.047825955554763
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:	DHLHAWB 57462839.exe
File size:	787456
MD5:	83a8eaa2ef938a73daacebcd4e090843
SHA1:	817203c16a790450a754dc16cf59111dd2dadaa7
SHA256:	5a0b3456792f8d0e1db3fa224863ccab694349f33cde1130bcf4436563ee0b2a
SHA512:	9ca05929a37455d6c8ccc6a8bb8345929ff8f50f60cab3318b560e5cf11a1e91dac09487738c0cde24cd36bb86936e3932371c7b35b75f186257195df2b3240e
SSDEEP:	12288:Si0hNfUjwdtaxyevwwVVi/goXD1v0Wwst01Jv/adetPJEwKY:SBhNf2xuwVVXGBMLsCTydkJP1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e7`.....P.....T..... .....@.. .....`..... ...@.....

File Icon

Icon Hash:	e0dad4adc4d2d870

Static PE Info

General	
Entrypoint:	0x4bcc82
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:	0x603765F8 [Thu Feb 25 08:55:20 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbcc30	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x51c8	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	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	0xbac88	0xbae00	False	0.607109636288	data	7.05918613534	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x51c8	0x5200	False	0.188929115854	data	4.23555059469	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbe100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xc2338	0x14	data		
RT_VERSION	0xc235c	0x340	data		
RT_MANIFEST	0xc26ac	0xb15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

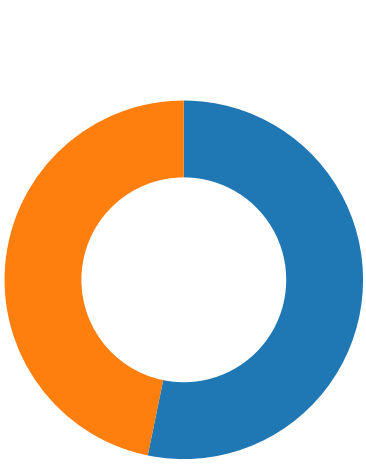
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	3.0.0.0
InternalName	AssemblyName.exe
FileVersion	3.0.0.0
CompanyName	KTV
LegalTrademarks	
Comments	
ProductName	KTVManagement
ProductVersion	3.0.0.0
FileDescription	KTVManagement
OriginalFilename	AssemblyName.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:51:40.813127041 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:40.988892078 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:40.989254951 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:41.539948940 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:41.540853024 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:41.715833902 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:41.715883970 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:41.716192007 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:41.890968084 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:41.935988903 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:41.954796076 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:42.131486893 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:42.131551981 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:42.131591082 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:42.131617069 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:42.131655931 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:42.131678104 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:42.131767035 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:42.306412935 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:42.311794043 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:42.490824938 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:42.545490026 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:42.841698885 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:43.018898964 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:43.023649931 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:43.200114012 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:43.201809883 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:43.378850937 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:43.380067110 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:43.557027102 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:43.557990074 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:43.737915993 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:43.779933929 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:43.880987883 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:44.058396101 CET	587	49740	208.91.199.225	192.168.2.3
Feb 25, 2021 13:51:44.058507919 CET	49740	587	192.168.2.3	208.91.199.225
Feb 25, 2021 13:51:45.315519094 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:45.479309082 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:45.479845047 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:46.073095083 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.073640108 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:46.237596989 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.237647057 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.238172054 CET	49741	587	192.168.2.3	208.91.199.223

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:51:46.402223110 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.403289080 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:46.568038940 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.568103075 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.568142891 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.568170071 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.568207979 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.568330050 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:46.568362951 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:46.734354019 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.735764027 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:46.906882048 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:46.909528971 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:47.075299978 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:47.076175928 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:47.241281986 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:47.242660999 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:47.411184072 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:47.412117958 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:47.578273058 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:47.579174995 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:47.749783039 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:47.750633001 CET	49741	587	192.168.2.3	208.91.199.223
Feb 25, 2021 13:51:47.915018082 CET	587	49741	208.91.199.223	192.168.2.3
Feb 25, 2021 13:51:47.915121078 CET	49741	587	192.168.2.3	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:49:53.920747995 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:49:53.971043110 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 13:49:58.832365036 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:49:58.883986950 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:00.941257000 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:00.990159988 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:02.136508942 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:02.188143969 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:03.338567019 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:03.387590885 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:25.557085991 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:25.607717037 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:32.008502007 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:32.067214966 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:35.734534025 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:35.787048101 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:36.843938112 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:36.894598007 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:37.662094116 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:37.710988998 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:40.487922907 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:40.548060894 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:41.072861910 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:41.138422012 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 13:50:47.607956886 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:50:47.658315897 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:01.297982931 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:01.349564075 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:04.098345995 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:04.157299042 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:11.739728928 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:11.790262938 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:13.349217892 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:13.400985956 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:14.318475962 CET	59349	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:51:14.370239973 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:15.300899029 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:15.349714041 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:18.769519091 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:18.818229914 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:19.959436893 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:20.011292934 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:20.970906019 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:21.019840956 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:21.952682972 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:22.004359961 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:23.630259037 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:23.679390907 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:24.641812086 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:24.690752029 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:36.162192106 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:36.213768959 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:38.252203941 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:38.320322990 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:40.602556944 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:40.663743973 CET	53	56132	8.8.8.8	192.168.2.3
Feb 25, 2021 13:51:45.252988100 CET	58987	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:51:45.313564062 CET	53	58987	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 13:51:40.602556944 CET	192.168.2.3	8.8.8.8	0x64d	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:45.252988100 CET	192.168.2.3	8.8.8.8	0xba6f	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 13:51:40.663743973 CET	8.8.8.8	192.168.2.3	0x64d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:40.663743973 CET	8.8.8.8	192.168.2.3	0x64d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:40.663743973 CET	8.8.8.8	192.168.2.3	0x64d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:40.663743973 CET	8.8.8.8	192.168.2.3	0x64d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:45.313564062 CET	8.8.8.8	192.168.2.3	0xba6f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:45.313564062 CET	8.8.8.8	192.168.2.3	0xba6f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:45.313564062 CET	8.8.8.8	192.168.2.3	0xba6f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Feb 25, 2021 13:51:45.313564062 CET	8.8.8.8	192.168.2.3	0xba6f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

SMTP Packets

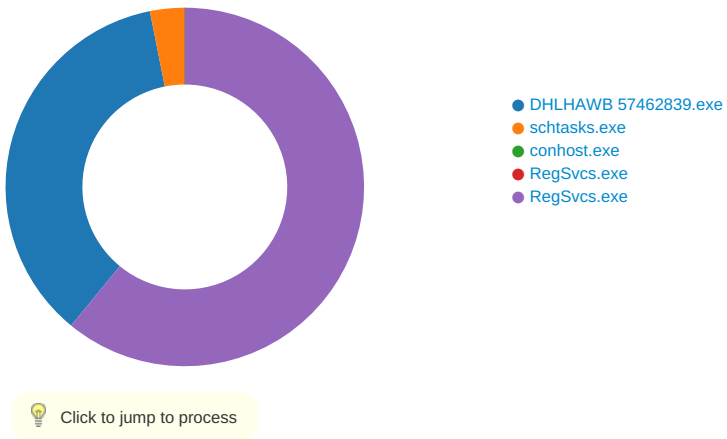
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 13:51:41.539948940 CET	587	49740	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Feb 25, 2021 13:51:41.540853024 CET	49740	587	192.168.2.3	208.91.199.225	EHLO 258555

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 13:51:41.715883970 CET	587	49740	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Feb 25, 2021 13:51:41.716192007 CET	49740	587	192.168.2.3	208.91.199.225	STARTTLS
Feb 25, 2021 13:51:41.890968084 CET	587	49740	208.91.199.225	192.168.2.3	220 2.0.0 Ready to start TLS
Feb 25, 2021 13:51:46.073095083 CET	587	49741	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Feb 25, 2021 13:51:46.073640108 CET	49741	587	192.168.2.3	208.91.199.223	EHLO 258555
Feb 25, 2021 13:51:46.237647057 CET	587	49741	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Feb 25, 2021 13:51:46.238172054 CET	49741	587	192.168.2.3	208.91.199.223	STARTTLS
Feb 25, 2021 13:51:46.402223110 CET	587	49741	208.91.199.223	192.168.2.3	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DHLHAWB 57462839.exe PID: 3864 Parent PID: 5632

General

Start time:	13:49:58

Start date:	25/02/2021
Path:	C:\Users\user\Desktop\DHLHAWB 57462839.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHLHAWB 57462839.exe'
Imagebase:	0x3c0000
File size:	787456 bytes
MD5 hash:	83A8EAA2EF938A73DAACEBCD4E090843
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.203262419.0000000002841000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.203348595.00000000028BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.204175053.0000000003AB0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E11CF06	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	6E11CF06	unknown
C:\Users\user\AppData\Roaming\AFpQKAcEJx.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	6CF6DD66	CopyFileW
C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpB573.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHLHAWB 57462839.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E42C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB573.tmp	success or wait	1	6CF66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AFpQKAcEJx.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 f8 65 37 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 ae 0b 00 00 54 00 00 00 00 00 00 82 cc 0b 00 00 20 00 00 00 e0 0b 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 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....e7`.......... ....P......T........... ........@.. .......................` ....@................	success or wait	4	6CF6DD66	CopyFileW
C:\Users\user\AppData\Roaming\ AFpQKAcEJx.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CF6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpB573.tmp	unknown	1643	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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CF61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHLHAWB57462839.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E42C907	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile

Analysis Process: schtasks.exe PID: 5604 Parent PID: 3864

General

Start time:	13:50:00
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AFpQKAcEJx' /XML 'C:\Users\user\AppData\Local\Temp\tmpB573.tmp'
Imagebase:	0xc00000
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\tmpB573.tmp	unknown	2	success or wait	1	C0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB573.tmp	unknown	1644	success or wait	1	C0ABD9	ReadFile

Analysis Process: conhost.exe PID: 5840 Parent PID: 5604

General

Start time:	13:50:01
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: RegSvcs.exe PID: 3984 Parent PID: 3864

General

Start time:	13:50:01
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x400000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 5300 Parent PID: 3864

General

Start time:	13:50:01
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x740000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000005.00000002.461216400.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.464641605.0000000002A91000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E11CF06	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	6E11CF06	unknown
C:\Users\user\AppData\Roaming\5qvjakll.zyj	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\5qvjakll.zyj\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	6CF6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\5qvjakll.zyj\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	6CF6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\5qvjakll.zyj\Chrome\Default\Cookies	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	6CF6DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5qvjakll.zyj\Chrome\Default\Cookies	success or wait	1	6CF66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5qvjakll.zyj\Chrome\Default\Cookies	0	20480	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 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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......@ ....C....... ..g... .8....	success or wait	1	6CF6DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\2579f30f-0aaa-4809-b230-4ff17fa35a85	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Roaming\5qvjakll.zyj\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CF61B4F	ReadFile

Disassembly

Code Analysis