ID: 358588
Sample Name: DHLHAWB 57462839.exe
Cookbook: default.jbs
Time: 21:54:19
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report DHLHAWB 57462839.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Data Obfuscation: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
Anti Debugging: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 11
Public 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 14
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 17
General 17
File Icon 17
Static PE Info 18

General 18
Entrypoint Preview 18
Data Directories 19
Sections 20
Resources 20
Imports 20
Version Infos 20
Network Behavior 20
Network Port Distribution 20
TCP Packets 21
UDP Packets 22
DNS Queries 24
DNS Answers 24
SMTP Packets 24
Code Manipulations 24
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: DHLHAWB 57462839.exe PID: 6216 Parent PID: 6000 25
General 25
File Activities 25
File Created 25
File Deleted 26
File Written 26
File Read 27
Analysis Process: schtasks.exe PID: 5692 Parent PID: 6216 28
General 28
File Activities 28
File Read 28
Analysis Process: conhost.exe PID: 6148 Parent PID: 5692 28
General 28
Analysis Process: RegSvcs.exe PID: 5612 Parent PID: 6216 29
General 29
File Activities 29
File Created 29
File Deleted 29
File Written 30
File Read 30
Disassembly 31
Code Analysis 31

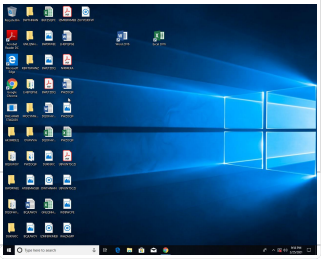
Analysis Report DHLHAWB 57462839.exe

Overview

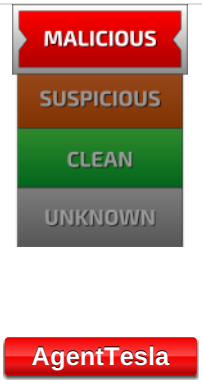
General Information

Sample Name:	DHLHAWB 57462839.exe
Analysis ID:	358588
MD5:	937409ab4d0446..
SHA1:	1a41e87a25ae68..
SHA256:	1fe5c63b01b1faf…
Tags:	agenttesla
Infos:	

Most interesting Screenshot:



Detection

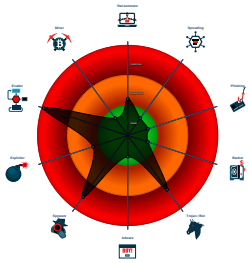


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected unpacking (changes PE se…
- 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…
- Allocates memory in foreign process…
- Binary contains a suspicious time st…

Classification



Startup

- **System is w10x64**
- DHLHAWB 57462839.exe (PID: 6216 cmdline: 'C:\Users\user\Desktop\DHLHAWB 57462839.exe' MD5: 937409AB4D04460DA3A61A8AF49940F4)
  - schtasks.exe (PID: 5692 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UNOnVCSOZ' /XML 'C:\Users\user\AppData\Local\Temp\tmp2C48.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5612 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
00000004.00000002.904004015.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.652956270.000000000319000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.655008837.00000000041EC000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.905208316.0000000002B21000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegSvcs.exe PID: 5612	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 3 entries				

Unpacked PEs

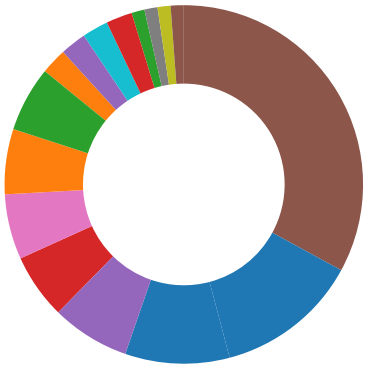
Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHLHAWB 57462839.exe.44ae500.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHLHAWB 57462839.exe.43b0050.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHLHAWB 57462839.exe.44ae500.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHLHAWB 57462839.exe.4354230.1.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
- Software Vulnerabilities
- 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:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

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:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Binary contains a suspicious time stamp

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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

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)

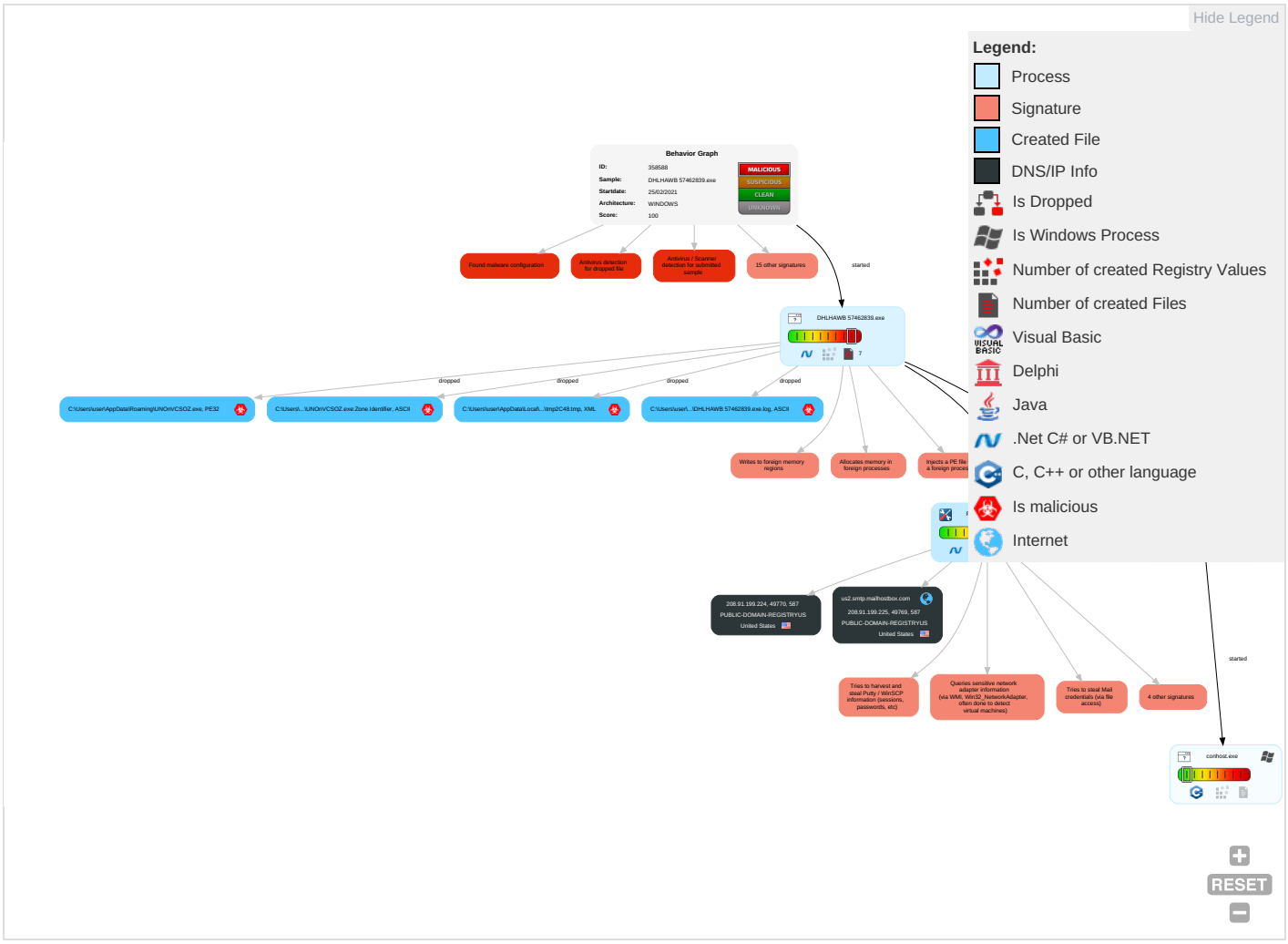
Remote Access Functionality:

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 3 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	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	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 1 4	NTDS	Security Software Discovery 4 3 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 5	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	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	Virtualization/Sandbox Evasion 1 5	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	Process Injection 3 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

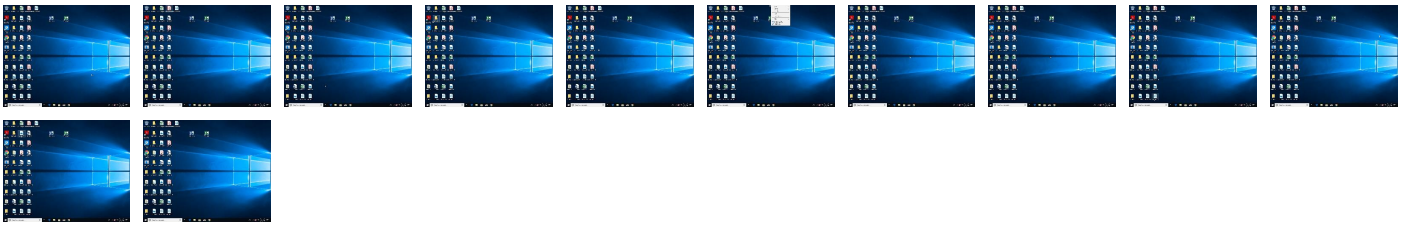
Behavior Graph



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	37%	Virustotal		Browse
DHLHAWB 57462839.exe	82%	ReversingLabs	ByteCode-MSIL.Hacktool.Boilod	
DHLHAWB 57462839.exe	100%	Avira	HEUR/AGEN.1138558	
DHLHAWB 57462839.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UNOnVCSOZ.exe	100%	Avira	HEUR/AGEN.1138558	
C:\Users\user\AppData\Roaming\UNOnVCSOZ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\UNOnVCSOZ.exe	37%	Virustotal		Browse
C:\Users\user\AppData\Roaming\UNOnVCSOZ.exe	82%	ReversingLabs	ByteCode-MSIL.Hacktool.Boilod	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.DHLHAWB 57462839.exe.e40000.0.unpack	100%	Avira	HEUR/AGEN.1138558		Download File
0.2.DHLHAWB 57462839.exe.e40000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		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://jGMFHr.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://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://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://RSPcfPi1ZyR1uGL.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

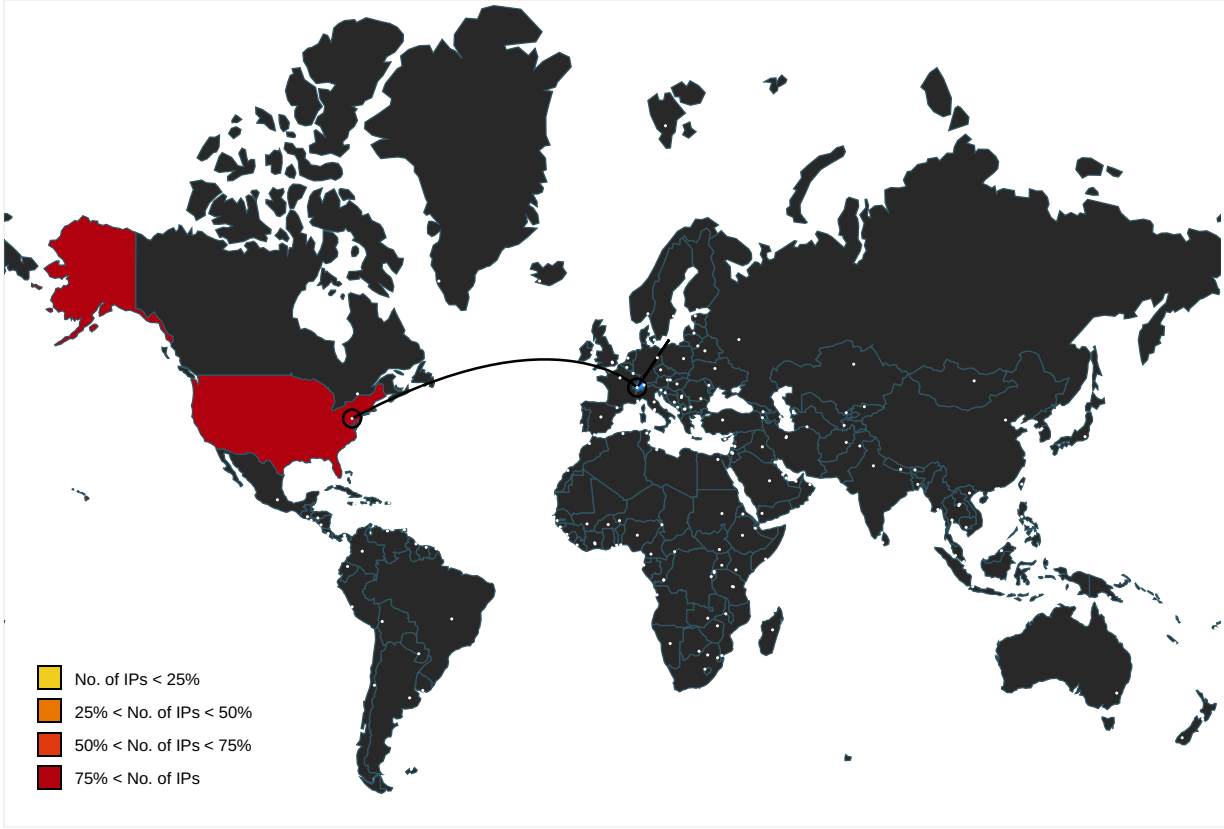
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	RegSvcs.exe, 00000004.00000002.905686110.0000000002ED4000.00000004.00000001.sdmp	false	URL Reputation: safe URL Reputation: safe URL Reputation: safe URL Reputation: safe	unknown
http://jGMFHr.com	RegSvcs.exe, 00000004.00000002.905208316.0000000002B21000.00000004.00000001.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000004.00000002.905208316.0000000002B21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegSvcs.exe, 00000004.00000002.905208316.0000000002B21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	RegSvcs.exe, 00000004.00000002.905686110.0000000002ED4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	RegSvcs.exe, 00000004.00000002.905686110.0000000002ED4000.00000004.00000001.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, 00000004.00000002.905208316.0000000002B21000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0A	RegSvcs.exe, 00000004.00000002.905686110.0000000002ED4000.00000004.00000001.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, 00000004.00000002.905208316.0000000002B21000.00000004.00000001.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, 00000000.00000002.652956270.0000000003191000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	RegSvcs.exe, 00000004.00000002.905208316.0000000002B21000.00000004.00000001.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, 00000000.00000002.655008837.0000000041EC000.00000004.00000001.sdmp, RegSvcs.exe, 00000004.00000002.904004015.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://RSPcfPi1ZyR1uGL.com	RegSvcs.exe, 00000004.00000002.905505135.0000000002E50000.00000004.00000001.sdmp, RegSvcs.exe, 00000004.00000002.905620230.0000000002EB5000.00000004.00000001.sdmp, RegSvcs.exe, 00000004.00000002.905208316.0000000002B21000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	DHLHAWB 57462839.exe, 00000000.00000002.652956270.0000000003191000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358588
Start date:	25.02.2021
Start time:	21:54:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 34s
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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@2/2

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.42.151.234, 52.255.188.83, 52.147.198.201, 13.64.90.137, 104.43.139.144, 51.104.144.132, 52.155.217.156, 20.54.26.129, 51.11.168.160, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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
21:55:05	API Interceptor	1x Sleep call for process: DHLHAWB 57462839.exe modified
21:55:22	API Interceptor	798x 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	DHLHAWB 57462839.exe	Get hash	malicious	Browse	
	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	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
208.91.199.224	Payment Advice GLV225445686.exe	Get hash	malicious	Browse	
	4019223246.exe	Get hash	malicious	Browse	
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	
	HcHimkU72e.exe	Get hash	malicious	Browse	
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	
	AWB & Shipping Document.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	
	PAYMENT INVOICE-9876543456789.exe	Get hash	malicious	Browse	
	inquiry.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.CAP_HookExKeylogger.31203.exe	Get hash	malicious	Browse	
	SWIFT COPY 27078.exe	Get hash	malicious	Browse	
	PO 000102.xlsx	Get hash	malicious	Browse	
	Pro.invoice-0656.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.ArtemisF31D2F976320.exe	Get hash	malicious	Browse	
	COMMERCIAL INVOICE BILL OF LADING ETC DOCX..exe	Get hash	malicious	Browse	
	PO-41000055885.exe	Get hash	malicious	Browse	
	Swift Mensaje 093763.exe	Get hash	malicious	Browse	
	xbZkF2dYZz.exe	Get hash	malicious	Browse	
	chrome.exe	Get hash	malicious	Browse	
	statement and proforma invoice.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Payment Advice GLV225445686.exe	Get hash	malicious	Browse	• 208.91.199.224
	DHLHAWB 57462839.exe	Get hash	malicious	Browse	• 208.91.199.225
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Payment Advice GLV225445686.exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	211094.exe	Get hash	malicious	Browse	• 199.79.62.169
	8zjdEb5sF0.dll	Get hash	malicious	Browse	• 116.206.105.72
	DHLHAWB 57462839.exe	Get hash	malicious	Browse	• 208.91.199.223
	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
PUBLIC-DOMAIN-REGISTRYUS	Payment Advice GLV225445686.exe	Get hash	malicious	Browse	• 208.91.199.224
	211094.exe	Get hash	malicious	Browse	• 199.79.62.169
	8zjdEb5sF0.dll	Get hash	malicious	Browse	• 116.206.105.72
	DHLHAWB 57462839.exe	Get hash	malicious	Browse	• 208.91.199.223
	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

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):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHV
MD5:	CDB0CBEDFEC7CCD7229835F37D89305C
SHA1:	39023F8CFF044D44485DB049CE242383BCB07035

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHLHAWB 57462839.exe.log	
SHA-256:	B1D78A56636298EFB329B368C4D52F2DCCF7F948AF7E7A30D9A8916D532760FE
SHA-512:	35066E4F12E28DA041B4EE5BE8E24B21A1FBF6D3267100EFA4EEC701288F48F5BA4E63A4866D1DEC3E1A8147A060B9E0D4C4D4A2FB49890AA617172AE4BFA76 4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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,"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..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\tmp2C48.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):	1642
Entropy (8bit):	5.184613936314241
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGWAPtn:cbhK79lNQR/rydbz9I3YODOLNdq3M
MD5:	AEA8DB8D2F5A79BBE285F0BD615076B8
SHA1:	E45B23C8653FFFEFD0982802D38EA56BD82C3761
SHA-256:	6C8765E861A719786AADF19B5B0CA2D9DEF613C45D8620845F49C1C53C390D3C
SHA-512:	0CA61C8FA7AEE465C010E0B8AED590CBA4563AF40422052BC94EF92B9D8262FE5A8097F1FA7A85416BC6C50734DCA575A90EDBEE8F4E048731425C0CA2F149 B
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\UNOnVCSOZ.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):	552448
Entropy (8bit):	7.862121638851853
Encrypted:	false
SSDEEP:	6144:2+kh1Q4cBGv1NJ8j+HM8D5uYcLcalJZyDCkAagYoy5rxY4942jYTSelN3LVSvD/L:ELAG9Njh2RJQD3genPoh6hW9icPK
MD5:	937409AB4D04460DA3A61A8AF49940F4
SHA1:	1A41E87A25AE680A94EDD0A47C09BB28FA76B661
SHA-256:	1FE5C63B01B1FAF6D5DF0AD3CB8A369B3866EC6CBB6145E7DCA11E5A5E49CFD0
SHA-512:	583033C8DBD083F90B4036461D0D718F8F45A9BED31F4E449E075A045993421F0D2D4C42F57F92483391405274F388E8154FED044B879CAF0AEA5A6187410F50
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 82%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... ....@.. ....@.....W.....0.....H.....f...y\..... .....@....text..... ..`.rsrc...0..... .....b.....@..@.reloc.....j.....@..B.....I..... ..`.....

C:\Users\user\AppData\Roaming\UNOnVCSOZ.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

C:\Users\user\AppData\Roaming\UNOnVCSOZ.exe:Zone.Identifier	
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\gp1e4ulp.4dd\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):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.862121638851853
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHLHAWB 57462839.exe
File size:	552448
MD5:	937409ab4d04460da3a61a8af49940f4
SHA1:	1a41e87a25ae680a94edd0a47c09bb28fa76b661
SHA256:	1fe5c63b01b1faf6d5df0ad3cb8a369b3866ec6cbb6145e7dca11e5a5e49cfd0
SHA512:	583033c8dbd083f90b4036461d0d718f8f45a9bed31f4e449e075a045993421f0d2d4c42f57f92483391405274f388e8154fed044b879caf0aea5a6187410f50
SSDEEP:	6144:2+kh1Q4cBGv1NJ8j+HM8D5uYcLcalJZyDCkAagYoy5rxY4942jYTSelN3LVSvD/L:ELAG9Njh2RJQD3genPoh6hW9icPK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .....P..... ....@.. ..... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x48e00a
Entrypoint Section:	
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:	0xE216D4B4 [Tue Mar 14 03:57:40 2090 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 [0048E000h]
add 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
add 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	0x103c4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8a000	0x630	.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	0x8c000	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	0x8e000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x10000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
fy\,	0x2000	0xdb8c	0xdc00	False	1.00046164773	data	7.99631925179	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x10000	0x781c8	0x78200	False	0.891049769121	data	7.85876780763	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x630	0x800	False	0.3427734375	data	3.50950931956	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x8e000	0x10	0x200	False	0.044921875	data	0.122275881259	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x8a0a0	0x3a0	data		
RT_MANIFEST	0x8a440	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

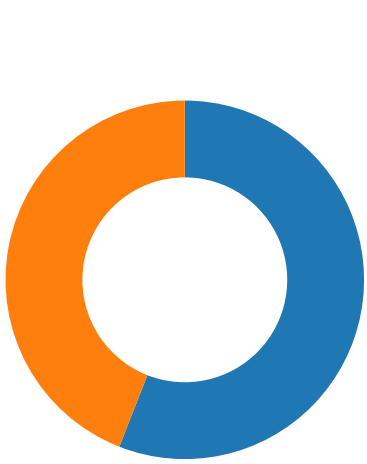
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hotplates 2020-2021
Assembly Version	2.0.9.0
InternalName	WSTRBufferMarshaler.exe
FileVersion	2.0.9.0
CompanyName	Hotplates
LegalTrademarks	
Comments	MLT
ProductName	Medical Laboratory
ProductVersion	2.0.9.0
FileDescription	Medical Laboratory
OriginalFilename	WSTRBufferMarshaler.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:56:49.628730059 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:49.806967974 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:49.807152033 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:50.426517963 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:50.427328110 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:50.602201939 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:50.602226019 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:50.603141069 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:50.780298948 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:50.825514078 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:50.874854088 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:51.049887896 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.049916029 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.049927950 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.049942017 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.049956083 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.050240993 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:51.091281891 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:51.224977970 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.235553980 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:51.414690971 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.466200113 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:51.730787039 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:51.905687094 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:51.908330917 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.085530996 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:52.087090015 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.264487982 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:52.265708923 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.441592932 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:52.442156076 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.624912977 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:52.625468969 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.800662041 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:52.801738977 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.801804066 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.802573919 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.802623987 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:52.976905107 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:52.977283955 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:53.077604055 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:53.122493982 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:54.335419893 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:54.510690928 CET	587	49769	208.91.199.225	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:56:54.510754108 CET	587	49769	208.91.199.225	192.168.2.4
Feb 25, 2021 21:56:54.510921001 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:54.617358923 CET	49769	587	192.168.2.4	208.91.199.225
Feb 25, 2021 21:56:55.018297911 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:55.193109989 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:55.193253994 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:55.542152882 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:55.542453051 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:55.717298985 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:55.717505932 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:55.717799902 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:55.895737886 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:55.896377087 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:56.074047089 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.074107885 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.074151039 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.074178934 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.074213982 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:56.074218035 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.074309111 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:56.250560045 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.252867937 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:56.431859970 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.435096025 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:56.610057116 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.611852884 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:56.787273884 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.787986040 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:56.965177059 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:56.966124058 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.141686916 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.142499924 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.325968027 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.327347040 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.502485991 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.504719019 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.505137920 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.505453110 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.505758047 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.506194115 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.506603003 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.506839991 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.507086992 CET	49770	587	192.168.2.4	208.91.199.224
Feb 25, 2021 21:56:57.679790020 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.680277109 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.680833101 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.681410074 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.721256971 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.779609919 CET	587	49770	208.91.199.224	192.168.2.4
Feb 25, 2021 21:56:57.826344013 CET	49770	587	192.168.2.4	208.91.199.224

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:54:55.978668928 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:54:56.028944016 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 21:54:56.969949961 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:54:57.018727064 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 21:54:58.092915058 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:54:58.142658949 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 21:54:58.968519926 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:54:59.031125069 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 21:54:59.786420107 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:54:59.839320898 CET	53	49910	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:55:00.670255899 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:00.725635052 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:01.808326006 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:01.857094049 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:02.767900944 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:02.819453001 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:03.822562933 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:03.871186972 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:05.011935949 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:05.074387074 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:06.286537886 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:06.335899115 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:07.255855083 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:07.306732893 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:10.331871986 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:10.382976055 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:11.274488926 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:11.323729038 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:12.412836075 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:12.461750031 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:13.376445055 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:13.428221941 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:14.897622108 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:14.947007895 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:16.076528072 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:16.129916906 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:25.058438063 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:25.110096931 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:38.738080025 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:38.806042910 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:39.309324980 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:39.370215893 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:40.015027046 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:40.082495928 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:40.191642046 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:40.249253035 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:40.553899050 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:40.636620998 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:41.105079889 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:41.166404963 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:41.722547054 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:41.784782887 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:42.543797016 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:42.600800991 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:43.480626106 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:43.529671907 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:44.430639982 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:44.479868889 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 21:55:45.140057087 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:55:45.210746050 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 21:56:00.070939064 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:56:00.120978117 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 21:56:00.662385941 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:56:00.735515118 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 21:56:02.943027020 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:56:02.999181032 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 21:56:36.339899063 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:56:36.390820026 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 21:56:37.569595098 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:56:37.648348093 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 21:56:49.466507912 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:56:49.526024103 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 21:56:54.958601952 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 21:56:55.016645908 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:56:49.466507912 CET	192.168.2.4	8.8.8.8	0xa9c5	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:54.958601952 CET	192.168.2.4	8.8.8.8	0x9deb	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 21:56:49.526024103 CET	8.8.8.8	192.168.2.4	0xa9c5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:49.526024103 CET	8.8.8.8	192.168.2.4	0xa9c5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:49.526024103 CET	8.8.8.8	192.168.2.4	0xa9c5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:49.526024103 CET	8.8.8.8	192.168.2.4	0xa9c5	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:55.016645908 CET	8.8.8.8	192.168.2.4	0x9deb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:55.016645908 CET	8.8.8.8	192.168.2.4	0x9deb	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:55.016645908 CET	8.8.8.8	192.168.2.4	0x9deb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Feb 25, 2021 21:56:55.016645908 CET	8.8.8.8	192.168.2.4	0x9deb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

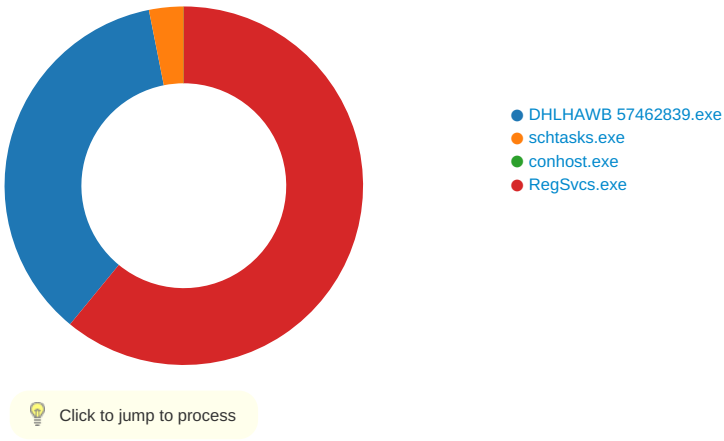
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 21:56:50.426517963 CET	587	49769	208.91.199.225	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Feb 25, 2021 21:56:50.427328110 CET	49769	587	192.168.2.4	208.91.199.225	EHLO 942247
Feb 25, 2021 21:56:50.602226019 CET	587	49769	208.91.199.225	192.168.2.4	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 21:56:50.603141069 CET	49769	587	192.168.2.4	208.91.199.225	STARTTLS
Feb 25, 2021 21:56:50.780298948 CET	587	49769	208.91.199.225	192.168.2.4	220 2.0.0 Ready to start TLS
Feb 25, 2021 21:56:55.542152882 CET	587	49770	208.91.199.224	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Feb 25, 2021 21:56:55.542453051 CET	49770	587	192.168.2.4	208.91.199.224	EHLO 942247
Feb 25, 2021 21:56:55.717505932 CET	587	49770	208.91.199.224	192.168.2.4	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 21:56:55.717799902 CET	49770	587	192.168.2.4	208.91.199.224	STARTTLS
Feb 25, 2021 21:56:55.895737886 CET	587	49770	208.91.199.224	192.168.2.4	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DHLHAWB 57462839.exe PID: 6216 Parent PID: 6000

General

Start time:	21:55:02
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:	0xe40000
File size:	552448 bytes
MD5 hash:	937409AB4D04460DA3A61A8AF49940F4
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: 00000000.00000002.652956270.0000000003191000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.655008837.00000000041EC000.00000004.00000001.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	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\UNOnVCSOZ.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	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\UNOnVCSOZ.exe\:Zone.Identifier :$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C01DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2C48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	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	6D4DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2C48.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UNOnVCSOZ.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 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 05 00 b4 d4 16 e2 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 84 07 00 00 e6 00 00 00 00 00 00 0a e0 08 00 00 00 01 00 00 20 00 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 00 09 00 00 04 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................. ....P..................... ....@.. ....@................	success or wait	3	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\UNOnVCSOZ.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	6C01DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2C48.tmp	unknown	1642	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 6a 6f 6e 65 73 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	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHLHAWB57462839.exe.log	unknown	1400	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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,"Microsoft.VisualBasic, Ver	success or wait	1	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 5692 Parent PID: 6216

General

Start time:	21:55:08
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UNOnVCSOZ' /XML 'C:\Users\user\AppData\Local\Temp\tmp2C48.tmp'
Imagebase:	0x1150000
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\tmp2C48.tmp	unknown	2	success or wait	1	115AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2C48.tmp	unknown	1643	success or wait	1	115ABD9	ReadFile

Analysis Process: conhost.exe PID: 6148 Parent PID: 5692

General

Start time:	21:55:08
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5612 Parent PID: 6216

General

Start time:	21:55:09
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:	0x850000
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: 00000004.00000002.904004015.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.905208316.0000000002B21000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\gp1e4ulp.4dd	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\gp1e4ulp.4dd\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	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\gp1e4ulp.4dd\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	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\gp1e4ulp.4dd\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	6C01DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gp1e4ulp.4dd\Chrome\Default\Cookies	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gp1e4ulp.4dd\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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C01DD66	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C011B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\f119cae5-eef2-4957-bec1-2210e35c7088	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Roaming\gp1e4ulp.4dd\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C011B4F	ReadFile

Disassembly

Code Analysis