ID: 355962
Sample Name:
DHL_Shipment_Notification#5436637389_22_FEB.exe
Cookbook: default.jbs
Time: 10:07:27
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

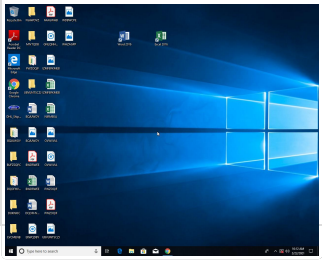
Analysis Report DHL_Shipment_Notification#543663738…

Overview

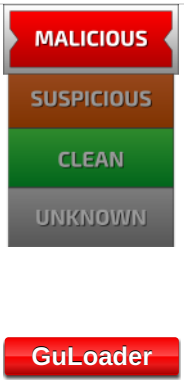
General Information

Sample Name:	DHL_Shipment_Notification#5436637389_22_FEB.exe
Analysis ID:	355962
MD5:	6660a5670795be..
SHA1:	ccfcbc36c22530b..
SHA256:	6d44a1e98afe47c.
Tags:	GuLoader

Most interesting Screenshot:



Detection

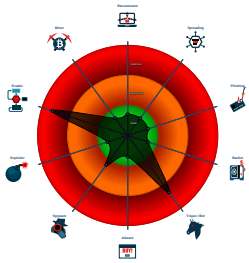


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Checks if the current process is bein…
- Contains functionality for execution …

Classification



Startup

- **System is w10x64**
- DHL_Shipment_Notification#5436637389_22_FEB.exe (PID: 7136 cmdline: 'C:\Users\user\Desktop\DHL_Shipment_Notification#5436637389_22_FEB.exe' MD5: 6660A5670795BE34D107D51A5323A6F3)
  - DHL_Shipment_Notification#5436637389_22_FEB.exe (PID: 2092 cmdline: 'C:\Users\user\Desktop\DHL_Shipment_Notification#5436637389_22_FEB.exe' MD5: 6660A5670795BE34D107D51A5323A6F3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

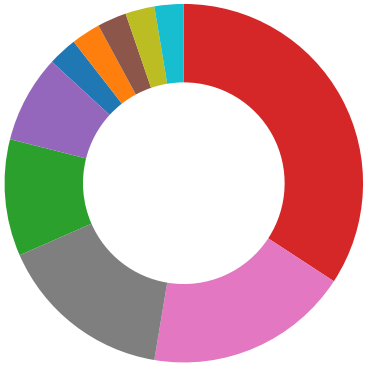
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: DHL_Shipment_Notification#5436637389_22_FEB.exe PID: 2092	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: DHL_Shipment_Notification#5436637389_22_FEB.exe PID: 2092	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

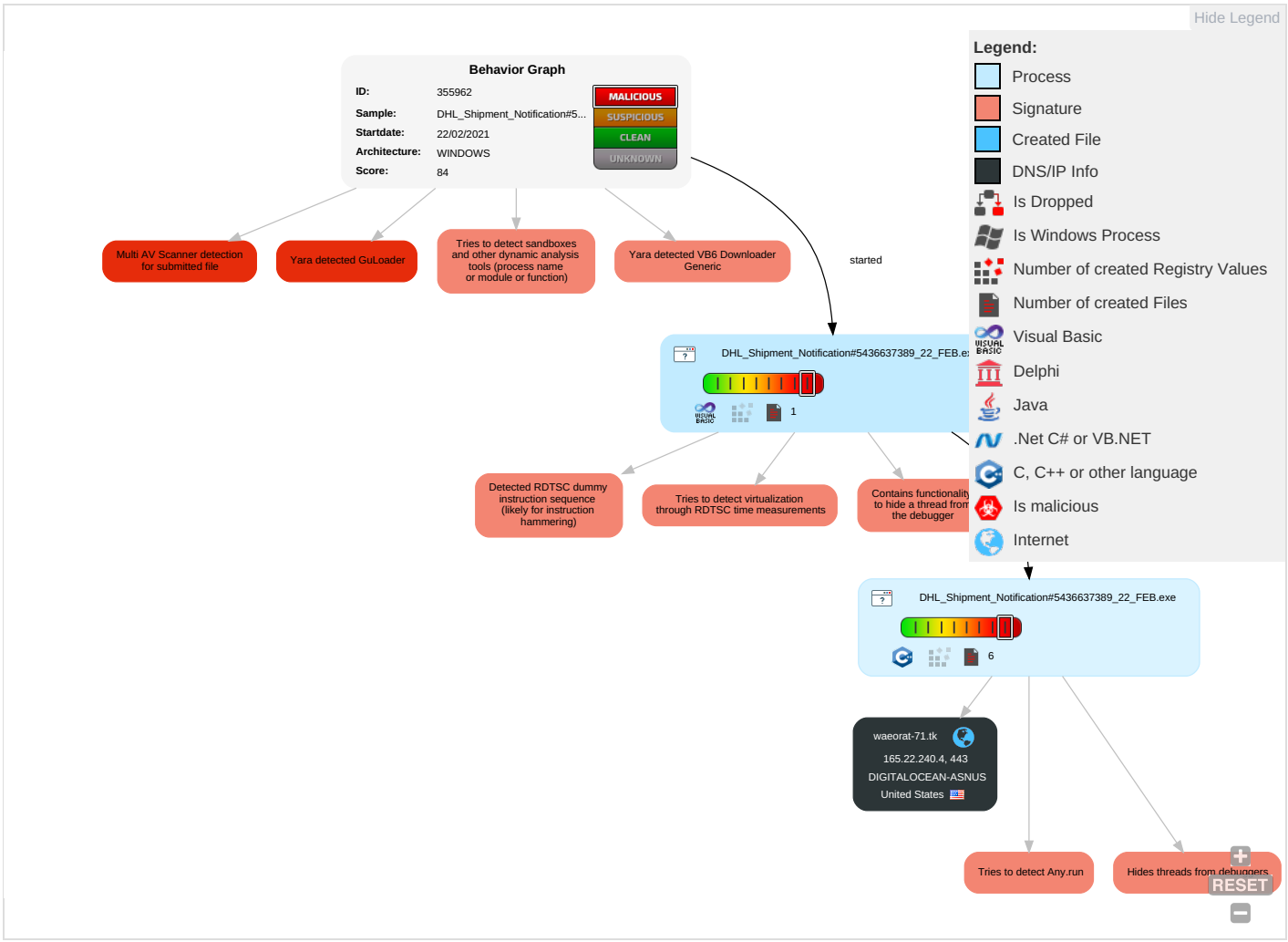
Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 6 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Re Tra Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Ob De Clc Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

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
DHL_Shipment_Notification#5436637389_22_FEB.exe	15%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
waeorat-71.tk	4%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
waeorat-71.tk	165.22.240.4	true	false	• 4%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
165.22.240.4	unknown	United States		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355962
Start date:	22.02.2021
Start time:	10:07:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_Shipment_Notification#5436637389_22_FEB.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:	18

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:	mal84.troj.evad.winEXE@2/0@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 92.122.145.220, 52.255.188.83, 104.43.139.144, 51.104.139.180, 52.155.217.156, 67.27.235.126, 8.248.117.254, 67.27.159.254, 8.248.119.254, 67.27.159.126, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.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, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	124992436.docx	Get hash	malicious	Browse	• 68.183.127.92
	124992436.docx	Get hash	malicious	Browse	• 68.183.127.92
	iopjvdf.dll	Get hash	malicious	Browse	• 206.189.10.247
	document-750895311.xls	Get hash	malicious	Browse	• 206.189.10.247
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 167.99.187.230
	HEC Batangas Integrated LNG and Power Project Documentations Type a message.exe.exe	Get hash	malicious	Browse	• 206.189.50.215
	processhacker-2.39-setup.exe	Get hash	malicious	Browse	• 162.243.25.33
	PO#652.exe	Get hash	malicious	Browse	• 192.241.148.82
	Linux_Reader.exe	Get hash	malicious	Browse	• 159.203.148.225
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 134.209.144.106
	Statement_of_Account_as_of 02_17_2021.xlsm	Get hash	malicious	Browse	• 167.71.6.214
	Quotation.exe	Get hash	malicious	Browse	• 67.207.77.53
	MoqGIIogN0.dll	Get hash	malicious	Browse	• 192.241.174.45
	dAlyRK9gO7.exe	Get hash	malicious	Browse	• 138.197.53.157
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 142.93.110.250
	RFQ.xls	Get hash	malicious	Browse	• 192.81.210.146
	955037-012021-98_98795947.doc	Get hash	malicious	Browse	• 159.65.10.195
	ransomware.exe	Get hash	malicious	Browse	• 142.93.110.250
	ransomware.exe	Get hash	malicious	Browse	• 142.93.110.250
	DkELZjJtGY.xlsm	Get hash	malicious	Browse	• 178.128.83.165

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.946942752761298
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%

General

File name:	DHL_Shipment_Notification#5436637389_22_FEB.exe
File size:	139264
MD5:	6660a5670795be34d107d51a5323a6f3
SHA1:	ccfcbc36c22530b58bb6f35707667f658923c9bf
SHA256:	6d44a1e98afe47c5a977fd9977f45d173a28a4cbe76f27e2adc5aa702b7ffc75
SHA512:	703b8025afdafd41f78e065fb4af4ab556663a44bc36b7252a51470803a8d034c06bf5ec3ea3ffeb327fb2e3b5f4364834a776a7eaa16721d3af88c55156b8bd
SSDEEP:	1536:DWWTwV4fVhussgo2mzIggDnv+0op+CygfnMZaBmZJouxVQwV4MjW:nwVUPbbmcNDv+LHTMjZJoQqwV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L.....Y.....p.....@.....

File Icon

Icon Hash:	01d292796dda0080

Static PE Info

General

Entrypoint:	0x4014e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x590288EC [Fri Apr 28 00:12:28 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3f0d3842f1f621625b7b4016e6be4558

Entrypoint Preview

Instruction
push 00412C00h
call 00007FCFFC7B5705h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi+ebp*4], dh
sti
mov ah, C3h
add cl, byte ptr [ebp+ecx*4+71h]
cmp dword ptr [esi+6Eh], ebx
jne 00007FCFFC7B573Ch
fiadd word ptr [eax]

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edi], dh
or eax, 726F420Ah
jbe 00007FCFFC7B5774h
xor al, 70h
jc 00007FCFFC7B5781h
push 00000065h
arpl word ptr [esi+edx*2+62h], si
add byte ptr [edx], cl
inc ebx
popad
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
add edx, ecx
cmpsb
sbb dl, al
add eax, 9E460215h
jne 00007FCFFC7B5719h
mov cl, 7Ch
pop ebp
pushfd
mov bl, 3Ah
imul ebx, dword ptr [esi], 32h
mov ah, ah
inc ebx
mov dword ptr [ebx+edx*4+01h], eax
xor al, 05h
retn 3AEEh
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
sbb eax, 9A000116h
jnle 00007FCFFC7B5712h
add byte ptr [eax], al
or eax, 70794800h
outsd
arpl word ptr [eax+6Fh], bp

Instruction
outsb
jc 00007FCFFC7B577Ch
popad
aaa
add byte ptr [73000701h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x175c4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x19000	0x84a2	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x144	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16b44	0x17000	False	0.400539232337	data	5.59543646966	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x18000	0xa24	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x84a2	0x9000	False	0.343071831597	data	3.55708163533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2137a	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1fd52	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4608, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1e0aa	0x1ca8	data		
RT_ICON	0x1d402	0xca8	data		
RT_ICON	0x1d09a	0x368	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1aaf2	0x25a8	data		
RT_ICON	0x19a4a	0x10a8	data		
RT_ICON	0x195e2	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1956c	0x76	data		
RT_VERSION	0x19240	0x32c	data		

Imports

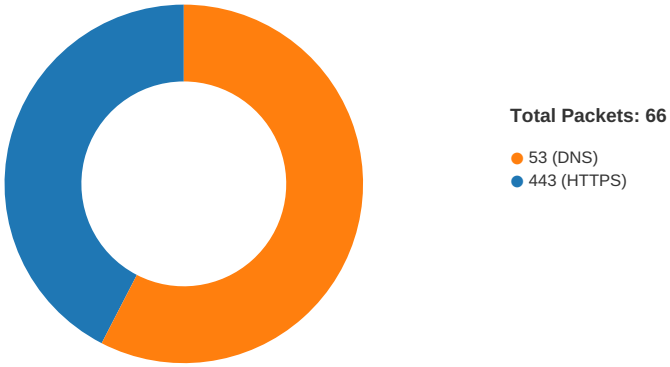
DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaStrI4, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaLateMemSt, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFPFix, __vbaFpR8, _CIsin, __vbaErase, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaVarTstEq, __vbaAryConstruct2, __vbaR4Str, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaLateMemCall, __vbaVarDup, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	WAB
FileVersion	6.03.9600
CompanyName	Microsoft Corporation
ProductName	Microsoft Windows Operating System
ProductVersion	6.03.9600
FileDescription	Windows Contacts
OriginalFilename	WAB.EXE

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 10:11:06.829106092 CET	49766	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:09.840812922 CET	49766	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:11.843861103 CET	49767	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:14.856848955 CET	49767	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:16.877027988 CET	49768	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:19.888725042 CET	49768	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:21.924555063 CET	49769	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:24.935931921 CET	49769	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:26.940771103 CET	49770	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:29.951827049 CET	49770	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:31.970504045 CET	49771	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:34.983477116 CET	49771	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:37.021096945 CET	49772	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:40.030891895 CET	49772	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:42.082328081 CET	49773	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:45.093863010 CET	49773	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:47.113384008 CET	49774	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:50.125375032 CET	49774	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:52.179912090 CET	49775	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:55.188282967 CET	49775	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:11:57.708061934 CET	49776	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:12:00.720191002 CET	49776	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:12:02.769761086 CET	49777	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:12:05.783206940 CET	49777	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:12:07.788768053 CET	49778	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:12:10.799134970 CET	49778	443	192.168.2.4	165.22.240.4
Feb 22, 2021 10:12:12.817162991 CET	49779	443	192.168.2.4	165.22.240.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 10:12:15.830691099 CET	49779	443	192.168.2.4	165.22.240.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 10:08:05.765815973 CET	59123	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:05.814742088 CET	53	59123	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:07.022815943 CET	54531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:07.084274054 CET	53	54531	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:07.291821003 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:07.340609074 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:08.301573038 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:08.358681917 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:09.681369066 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:09.736083031 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:10.670995951 CET	49257	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:10.719635963 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:11.700761080 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:11.752764940 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:13.040894032 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:13.089567900 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:13.885338068 CET	55854	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:13.945184946 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:15.066054106 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:15.119932890 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:16.537591934 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:16.586183071 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:17.488342047 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:17.537084103 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:18.606760979 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:18.660501957 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:19.873456001 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:19.927517891 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:21.120476961 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:21.169166088 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:22.855973959 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:22.904489994 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:23.829696894 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:23.881062031 CET	53	56627	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:28.803721905 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:28.852212906 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:29.727432013 CET	63116	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:29.775950909 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:39.449137926 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:39.500714064 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:56.578450918 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:56.655071974 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:57.298132896 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:57.347476006 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:58.305146933 CET	51255	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:58.371611118 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:58.812658072 CET	61522	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:58.916172028 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:59.393642902 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:59.445775032 CET	53	52337	8.8.8.8	192.168.2.4
Feb 22, 2021 10:08:59.532125950 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:08:59.580621004 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:00.036408901 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:00.046413898 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:00.087074995 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:00.111577988 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:00.687937975 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:00.736433029 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:01.503963947 CET	60875	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 10:09:01.554456949 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:03.094491959 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:03.170993090 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:03.630774975 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:03.690642118 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:17.501976967 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:17.550674915 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:18.085654020 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:18.142857075 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:23.330121040 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:23.389273882 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:52.679147959 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:52.727674961 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 10:09:55.533899069 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:09:55.604880095 CET	53	49228	8.8.8.8	192.168.2.4
Feb 22, 2021 10:11:06.704314947 CET	59794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 10:11:06.812711000 CET	53	59794	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 10:11:06.704314947 CET	192.168.2.4	8.8.8.8	0xfcef	Standard query (0)	waeorat-71.tk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 10:11:06.812711000 CET	8.8.8.8	192.168.2.4	0xfcef	No error (0)	waeorat-71.tk		165.22.240.4	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

DHL_Shipment_Notification#543663.
DHL_Shipment_Notification#543663.

System Behavior

Analysis Process: DHL_Shipment_Notification#5436637389_22_FEB.exe PID: 7136
Parent PID: 5968

General

Start time:	10:08:10
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\DHL_Shipment_Notification#5436637389_22_FEB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_Shipment_Notification#5436637389_22_FEB.exe'
Imagebase:	0x400000
File size:	139264 bytes
MD5 hash:	6660A5670795BE34D107D51A5323A6F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: DHL_Shipment_Notification#5436637389_22_FEB.exe PID: 2092
Parent PID: 7136

General

Start time:	10:10:58
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\DHL_Shipment_Notification#5436637389_22_FEB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_Shipment_Notification#5436637389_22_FEB.exe'
Imagebase:	0x400000
File size:	139264 bytes
MD5 hash:	6660A5670795BE34D107D51A5323A6F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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	564584	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564584	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564584	InternetOpenUrlA

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	564584	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564584	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	564584	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis