ID: 562043
Sample Name: DHL AWB TRACKING DETAILS.exe
Cookbook: default.jbs
Time: 10:53:30
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

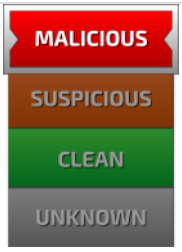
DHL AWB TRACKING DETAILS.exe

Overview

General Information

Sample Name:	DHL AWB TRACKING DETAILS.exe
Analysis ID:	562043
MD5:	4e358b432ba956.
SHA1:	8791318da047e9.
SHA256:	836696cddebff5d..
Tags:	DHL exe Formbook
Infos:	

Detection



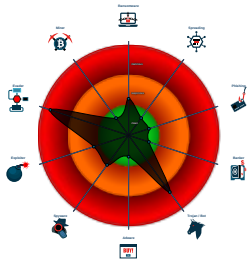
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- DHL AWB TRACKING DETAILS.exe (PID: 6228 cmdline: "C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe" MD5: 4E358B432BA956C13627BEEE054D68E5)
  - DHL AWB TRACKING DETAILS.exe (PID: 6276 cmdline: "C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe" MD5: 4E358B432BA956C13627BEEE054D68E5)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 6932 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 7012 cmdline: /c del "C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 4636 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 5560 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hdetpnipa.xyz/a34b/"
  ],
  "decoy": [
    "mesonarte.com",
    "eksiwakun9.xyz",
    "dustcollectionconsultant.com",
    "heliosarchitecture.com",
    "chinaanalysisgroup.com",
    "nimbinhillshemp.com",
    "ychain.biz",
    "mountshastaart.com",
    "monstermangoloco.com",
    "bodhiandbear.com",
    "rootednft.xyz",
    "metayema.com",
    "zw21.xyz",
    "cricketworld.com",
    "segurobarato.net",
    "ananyacap.com",
    "momo-momo.xyz",
    "ezrealestatedeals.com",
    "ghrde.xyz",
    "idimol.com",
    "pcthspoe.xyz",
    "thewhiteswanharringworth.com",
    "che8760.com",
    "85111280.xyz",
    "apteka-magnolia.com",
    "proach.online",
    "portfolioabeckford.com",
    "affilinvest.com",
    "subspank.xyz",
    "odessamadrecoffeehouse.com",
    "onetrade.biz",
    "tianfuhg.com",
    "kibtitalikeniwenti.com",
    "terriblearttours.com",
    "saudirelief.com",
    "metacourting.xyz",
    "kimera.blue",
    "mgpsfm.com",
    "metawzrd.com",
    "veahhiodl.xyz",
    "alimasurfhotel.com",
    "sirensandiego.com",
    "gd-hxgg.com",
    "aurorarift.com",
    "clingbee.com",
    "zettavisor2021.xyz",
    "gregoryryankramer.art",
    "robertsonfandc.com",
    "sociedadgeograficacafe.com",
    "emilyhkeefer.com",
    "v-hush.com",
    "judithtuttle.xyz",
    "itbrandlink.com",
    "carrybicycles.com",
    "storge-evolution.com",
    "socnhhpa.xyz",
    "victorzark.com",
    "ghettoguy.com",
    "redtruckguy.com",
    "jeanmariewallendorf.com",
    "ocpdtel.xyz",
    "democracies.online",
    "bw529twonineh5.world",
    "chinhdohuyenthoai.xyz"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.636107094.0000000000D80000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.636107094.0000000000D80000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.636107094.0000000000D80000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000000.359424691.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000000.359424691.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.DHL AWB TRACKING DETAILS.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.DHL AWB TRACKING DETAILS.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.DHL AWB TRACKING DETAILS.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
0.2.DHL AWB TRACKING DETAILS.exe.2f10000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0.2.DHL AWB TRACKING DETAILS.exe.2f10000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

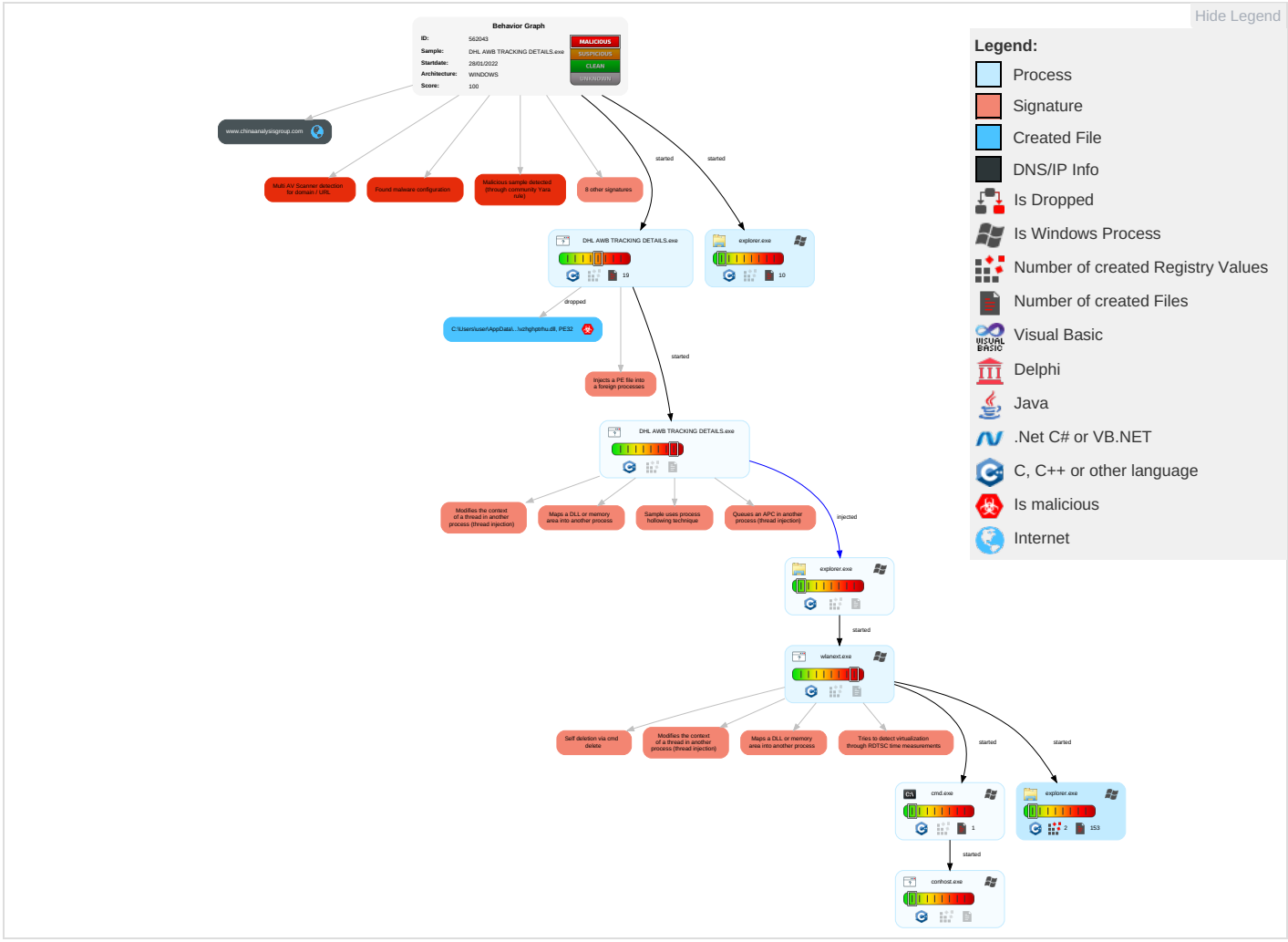
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Native API	Path Interception	5 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 Virtualization/Sandbox Evasion	LSASS Memory	2 3 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 1 2 Process Injection	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Software Packing	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

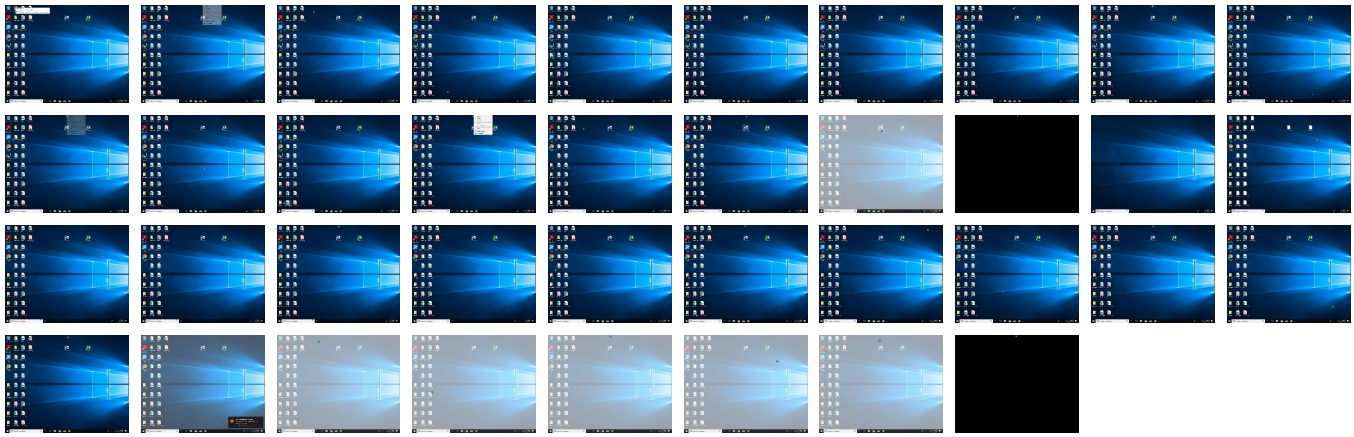
Behavior Graph

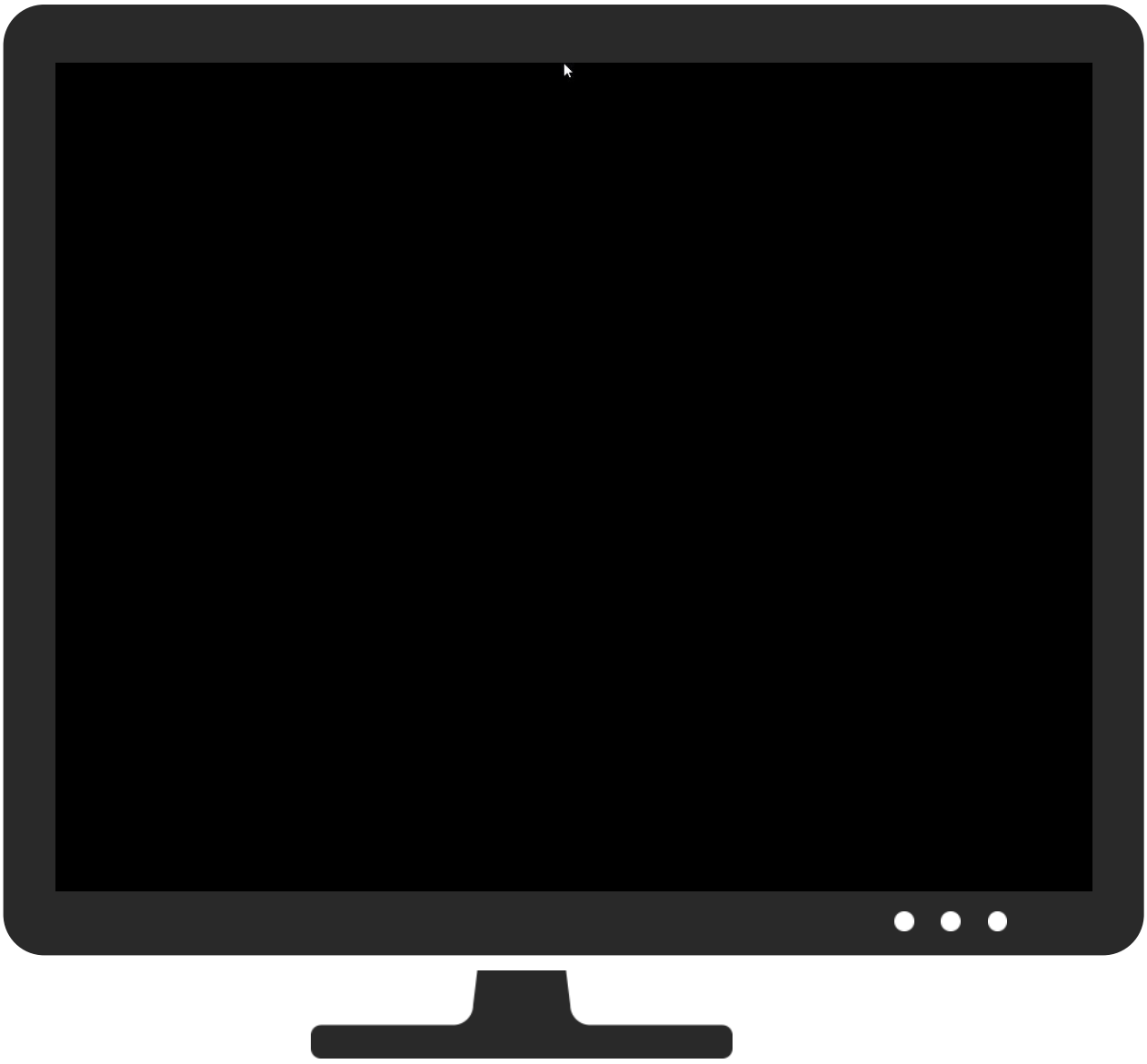


Screenshots

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 AWB TRACKING DETAILS.exe	43%	Virustotal		Browse
DHL AWB TRACKING DETAILS.exe	9%	Metadefender		Browse
DHL AWB TRACKING DETAILS.exe	49%	ReversingLabs	Win32.Trojan.FormBook	
DHL AWB TRACKING DETAILS.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsr8F1B.tmp\vzhghptrhu.dll	37%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsr8F1B.tmp\vzhghptrhu.dll	26%	ReversingLabs	Win32.Trojan.InjectorX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.DHL AWB TRACKING DETAILS.exe.2f10000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
31.2.explorer.exe.f07f840.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
20.0.explorer.exe.ad0f840.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.DHL AWB TRACKING DETAILS.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
1.0.DHL AWB TRACKING DETAILS.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
1.0.DHL AWB TRACKING DETAILS.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
1.0.DHL AWB TRACKING DETAILS.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
11.2.wlanext.exe.382f840.4.unpack	100%	Avira	TR/Patched.Ren .Gen		Download File
11.2.wlanext.exe.deef30.0.unpack	100%	Avira	TR/Patched.Ren .Gen		Download File
20.0.explorer.exe.ad0f840.3.unpack	100%	Avira	TR/Patched.Ren .Gen		Download File
20.0.explorer.exe.ad0f840.0.unpack	100%	Avira	TR/Patched.Ren .Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.hdetpnipa.xyz/a34b/	10%	Virustotal		Browse
www.hdetpnipa.xyz/a34b/	100%	Avira URL Cloud	phishing	
http://crl.v	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.chinaanalysisgroup.com	94.136.40.51	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.hdetpnipa.xyz/a34b/	true	• 10%, Virustotal, Browse • Avira URL Cloud: phishing	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.37914267 8.000000000095C000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.366064196.000000000095C000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.398584347.000000 000095C000.00000004.00000020.00020000.00 000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	DHL AWB TRACKING DETAILS.exe, DHL AWB TR ACKING DETAILS.exe, 00000000.00000002.36 1550279.0000000000409000.00000004.000000 01.01000000.00000003.sdmp, DHL AWB TRACKING DETAILS.exe, 00000000.00000000.352121005.00000 00000409000.00000008.00000001.01000000.0 0000003.sdmp, DHL AWB TRACKING DETAILS.exe, 00000001.00000000.355752258.00000000 00409000.00000008.00000001.01000000.0000 0003.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	DHL AWB TRACKING DETAILS.exe, 00000000.00000002.361550279.0000000000409000.00000004.00000001.01000000.00000003.sdmp, DHL AWB TRACKING DETAILS.exe, 00000000.00000000.352121005.0000000000409000.00000008.00000001.01000000.00000003.sdmp, DHL AWB TRACKING DETAILS.exe, 00000001.00000000.355752258.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high
http://crl.v	explorer.exe, 00000014.00000003.556038613.0000000004F3A000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000014.00000003.553294057.0000000004F3A000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000014.00000000.566295637.0000000004F3A000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000014.00000003.578401411.0000000004F3A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562043
Start date:	28.01.2022
Start time:	10:53:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL AWB TRACKING DETAILS.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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/4@1/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.3% (good quality ratio 55.5%) • Quality average: 73.6% • Quality standard deviation: 30.6%
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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, conhost.exe, svchost.exe, mobsync.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com

- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenFile 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:55:45	API Interceptor	145x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\2mew1mahf21

Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	data
Category:	dropped
Size (bytes):	216745
Entropy (8bit):	**7.992452492387805**
Encrypted:	**true**
SSDEEP:	6144:i7Bqt/rlMOOtvd7vIeYMD0dNT+V/w1Vc5S:Oqt/rlMOURXYMAdl+VI1wS
MD5:	D711B91073A1EF5C228C8C73240F3385
SHA1:	E032D0778986830C322964AEBFB8E870BC7F2ADC
SHA-256:	A445B0B8F8A9D002C4196DB12F455ACBA30FDF9A59679227B414E478450C8620
SHA-512:	9246B31146551D240878F47592074E9C26F022B4ADDF89FE11B1CD4F1AF30EE991C0E8D42FA5B7C610C748553B7D52626105C7BD56EF7E01BD9B33B717270156
Malicious:	false
Reputation:	low

Preview:	.<...2.HW-L.A..w. ."...1p..1...B4a.U....l.ev.....W.Z...X1...m.$....^E.8..6.Wa9..1fxN$.0.a.X.|`..F...Kb..T.H^..8tf&..8...7&:br.....Y....aG...M.N;.P?`..j.R9Q.>....?...Wv...=~ %D6.k.*6c..\.~pu.~.....d.Y...^.*pj..4S.`.MJ....a.....b...@..."S .2.t.Z....#....3.*...O.*aU..4a.U...P..;.ev...m.....W...o)X.Z....^..3+4.^..5.]..B.6(.9.#.....h!p..^..C..[^..8tf....5Iu] ..6..5.>.....a..X1/F.;(v..k.yW..h..n...?...0%..=~%..k..cB._.~4u.~...p.2...v.....pj..4S.`.5n....aC.....b...@...T". .2.H.....#...3[*...O..a...B4a.U....l.ev.....W...o)X.Z....^..3+4.^ ..5.]..B.6(.9.#.....h!p..^..C..[^..8tf....5Iu]..6..5.>.....a..X1/F.;(v..k.yW..h..n...?...Wv...=~%A~.k.,.cB.4.~pu.~...p.2...v....*pj..4S.`.5n....aC.....b...@...T". .2.H.....#...3[*...O.. a...B4a.U....l.ev.....W...o)X.Z....^..3+4.^..5.]..B.6(.9.#.....h!p..^..C..[^..8tf....5Iu]..6..5.>.....a..X1/F.;(v..k.yW..h..n...?...Wv...=~%A~.k.,.cB.4.~pu.~...p.2...v....*pj..4S.`

C:\Users\user\AppData\Local\Temp\nsr8F1A.tmp

Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	data
Category:	dropped
Size (bytes):	268956
Entropy (8bit):	7.643688780936791
Encrypted:	false
SSDEEP:	6144:u57Bqt/rlMOOtvd7vIeYMD0dNT+V/w1Vc5i:yqt/rlMOURXYMAdl+VI1w
MD5:	5671EF7FB29C27877E71184714A1C0F6
SHA1:	3CE9961EC8B7F820E58AF0EA56ABEA8DB18F2E1C
SHA-256:	D3DA5949B1EA253A18E0B684EC6EE1B355E9FA0C3B81C847119602D6AFBE459A
SHA-512:	6C835BFAAA83F01BF276BA42ADDDC8AE3C6F0C43C059A6AA713F5D382E8FC5115A09FEDD98F29A95FA7615CF15CD58475ED1DC321F410CECC4B38EDA5D254F3
Malicious:	false
Reputation:	low
Preview:	]q.....,.....U.....wp.....Eq.....k..... .....J.....k...j..... ....

C:\Users\user\AppData\Local\Temp\nsr8F1B.tmp\vzhghptrhu.dll

Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17920
Entropy (8bit):	5.732490075773449
Encrypted:	false
SSDEEP:	384:45EhhSL3A0xOfQy1zCsF0oavew2PFVP6zx22Y0We4omL/:4+hSLwWOIy1Wtoa2wNQo
MD5:	D2B96D84DF88876D02820CA05C8254E2
SHA1:	66C575874197ACE26E2D77C408154891C1C2A464
SHA-256:	AC4F4FC273432D090B87CC740B2668BB105AEA12D35B9F48BE82885607172708
SHA-512:	123B2255F5598BC7D51872CB2E0CBA58367B22AD638DF786AAEFA4CFDDDA11A0DAEC36002559CD9A2BDCD74CC78F903642595E0438FDD82681A938B9CB1B9F1
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L..O-.EO-.EO-.E[F.D@-.EO-.EU-.E.s.DN-.E.s.DN-.E.s.EN- .E.s.DN-.ERichO-.E.....PE..L.....a.....!.....8.....P.....@.....P..H....P.....`.....p..D..... .....P.....text....7.....8..... ..`.rdata..L....P.....<.....@..@.rsrc.....`.....B.....@..@.reloc..D....p.....D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\yblhciuwz

Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	data
Category:	dropped
Size (bytes):	5254
Entropy (8bit):	6.083971719042361
Encrypted:	false
SSDEEP:	96:0MhH9rpQHfV685JLXeDCjxxB6qoX+hmKQuKFvIVyOF7SCWO2z5lOfdHM+KQ0yBdq:0Gw6YL3xxItn62z3wHM0fwvT
MD5:	CF29025B5A29863F95888CC5EAE59F80
SHA1:	707E98B72D945FBB32D5A9CA282FF74A117FF648
SHA-256:	C7333C69C05C4BF3D325ADA4EFBB8F1641108B21211BA729F90DA95923867955
SHA-512:	DB5E6E866077CB8DC597BF2E033A2DE3D46DDAFD0E82E2956E2840A757902F66A36A87830214E6D77668BF53F53FF08AAD62A7234AD84E5148B30BB7969BA45F
Malicious:	false

Reputation:	low
Preview:	@?nWW..C.C.....GWf...fz.7f...fz.O.._W..S.WWW..[WV.cV.g._.OTWWW.?.3V.cV.g._.OOWWW.'.;V.cV.g._.O:WWW./.#V.cV.g._.O.WWW...+..gk..o...jj.c..7.K.g.Ok. .O.C.O.S.k(.9.g.^X.Oj.S.k).S....[.KG..OWWWW.k.l"..SV.?.V.'.V./..V....V.7.V.O..].g..c^..[w.Eh.GV.?...ofl.Gj.SOWWWW...k.WWW.k.d"..[...G....L.)cW..C..f...fz._.o.W..c.w.o.W.g.{(._.(k.S.o.W..o.h._.S.L.)cW.}Q-.O.iWWO.iWW){W..V6.O.iWWO.iWW)oW.d...O.iWWO.iWW)oW..C.C.f...fz.O.._gWWW.?.S.._W.}.S-WW.S..S._.._BKO{lWW....o..o.. W.d?.d3.O..o.(HW.d?.d3.i.o...W.l?...V6.O8hWW.O%TVV.[Bf.O.V.oO.VVV.[..[W.m..GWBn..GhWWW.G.L.)kW..C.C.f...fz.O.._.WWW...S.._W.}.S-WW.S..S._.._BKO.kWW..f..WWW.o..o.. W.d..d+.c..o.(HW.d..d+.g..o.8H.d..d+.{. .o..9j.|..|+.O..o.(Hi.d..d+.l.o...W.l...}Q-.OMWWW.OJSVV.[...W.o.O...hB~V..V.{V.gV.cV.oO.UVV.[..[W.m..GWBn..GhWWW.G.L.){W..C.Cs.._gWWW.K.S.._W.}.S-WW.S..S._.._BKO.jWW....o..o.. W.dK.dO.c..o.(HW.dK.dO.i.o...W.lK..d...O.WWW.O.SVV.[BeV.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.929574935862176
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DHL AWB TRACKING DETAILS.exe
File size:	254216
MD5:	4e358b432ba956c13627beee054d68e5
SHA1:	8791318da047e93f2a16cc6535eba5159228f832
SHA256:	836696cddebff5d522acb2c105a404ceeb635df69b3c9544b5bebcef13bc3e86
SHA512:	a251f2f3e4fe9b0b44b3537983b406e9eb2d5e22298129ba9548f626c3657410adf23b50d0dd69f4601d7c873056e545ca7be0d808f8f0db3f9a38609b82dcff
SSDEEP:	6144:ownv8jZAg8ZjqsPExIRaX+kK9WPvCH+tlvz:D8jZUVRaukK9kvCH+aL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
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:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi

Instruction
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409128h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B4h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [00423F58h], eax
call 00007F42389B1E60h
mov dword ptr [00423EA4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F450h
call dword ptr [00407158h]
push 004091B0h
push 004236A0h
call 00007F42389B1B17h
call dword ptr [004070B0h]
mov edi, 00429000h
push eax
push edi
call 00007F42389B1B05h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423EA0h], eax
mov eax, edi
jne 00007F42389AF32Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F42389B15F8h
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007F42389AF385h
cmp cl, 00000020h
jne 00007F42389AF328h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F42389AF31Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

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

Data Directories			
Name	**Virtual Address**	**Virtual Size**	**Is in Section**

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a4	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x900	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c190	0x2e8	data	English	United States
RT_DIALOG	0x2c478	0x100	data	English	United States
RT_DIALOG	0x2c578	0x11c	data	English	United States
RT_DIALOG	0x2c698	0x60	data	English	United States
RT_GROUP_ICON	0x2c6f8	0x14	data	English	United States
RT_MANIFEST	0x2c710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, CreateFileA, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetFileTime, GetTempPathA, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetWindowsDirectoryA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject

DLL	Import
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 10:56:53.209121943 CET	54982	53	192.168.2.6	8.8.8.8
Jan 28, 2022 10:56:53.241837978 CET	53	54982	8.8.8.8	192.168.2.6

DNS Queries

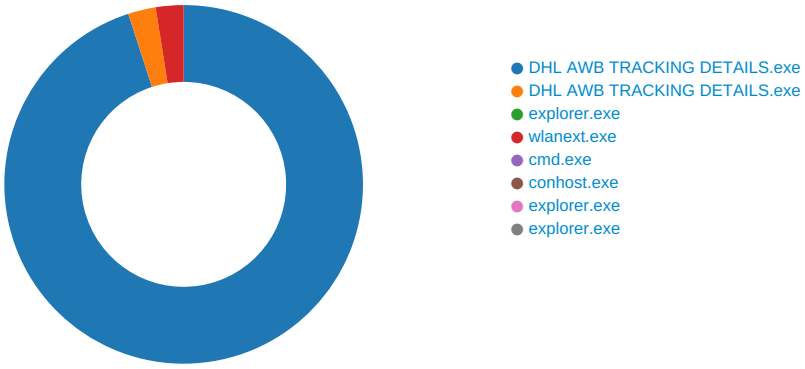
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 10:56:53.209121943 CET	192.168.2.6	8.8.8.8	0x775b	Standard query (0)	www.chinaanalysisgroup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 10:56:53.241837978 CET	8.8.8.8	192.168.2.6	0x775b	No error (0)	www.chinaanalysisgroup.com		94.136.40.51	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: DHL AWB TRACKING DETAILS.exe PID: **6228**, Parent PID: **4024**

General

Target ID:	0
Start time:	10:54:31
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe"
Imagebase:	0x400000
File size:	254216 bytes
MD5 hash:	4E358B432BA956C13627BEEE054D68E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.362630153.0000000002F10000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.362630153.0000000002F10000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.362630153.0000000002F10000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: DHL AWB TRACKING DETAILS.exe PID: **6276**, Parent PID: **6228**

General

Target ID:	1
Start time:	10:54:33
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe"
Imagebase:	0x400000
File size:	254216 bytes
MD5 hash:	4E358B432BA956C13627BEEE054D68E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.359424691.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.359424691.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.359424691.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.360270037.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.360270037.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.360270037.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.435840268.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.435840268.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.435840268.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.436793150.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.436793150.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.436793150.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.436005605.00000000009A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.436005605.00000000009A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.436005605.00000000009A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3440**, Parent PID: **6276**

General

Target ID:	4
Start time:	10:54:38
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.409581872.000000000F123000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.409581872.000000000F123000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.409581872.000000000F123000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.394582472.000000000F123000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.394582472.000000000F123000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.394582472.000000000F123000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: wlanext.exe PID: **6932**, Parent PID: **3440**

General

Target ID:	11
Start time:	10:55:07
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xfa0000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.636107094.0000000000D80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.636107094.0000000000D80000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.636107094.0000000000D80000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.635990166.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.635990166.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.635990166.0000000000D50000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.634911519.0000000000A00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.634911519.0000000000A00000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.634911519.0000000000A00000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	A1A457	NtReadFile

Analysis Process: cmd.exe PID: **7012**, Parent PID: **6932**

General

Target ID:	12
Start time:	10:55:13
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe"
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7024**, Parent PID: **7012**

General

Target ID:	13
Start time:	10:55:14
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: explorer.exe PID: **4636**, Parent PID: **2576**

General

Target ID:	20
Start time:	10:55:43
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff7ebed0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **5560**, Parent PID: **4044**

General

Target ID:	31
Start time:	10:56:35
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly