JoeSandbox Cloud BASIC

ID: 516538
Sample Name: DHL_AWB 65335643399___pdf.exe
Cookbook: default.jbs
Time: 15:20:12
Date: 05/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

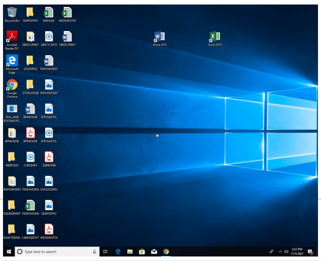
Windows Analysis Report DHL_AWB 65335643399___pd…

Overview

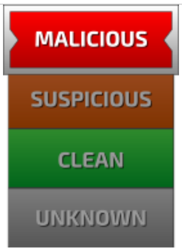
General Information

Sample Name:	DHL_AWB 65335643399___pdf.exe
Analysis ID:	516538
MD5:	52ef260ef62aae2..
SHA1:	cba71c49ae1c14..
SHA256:	752efe9ad078a9b.
Tags:	exe hawkeye
Infos:	

Most interesting Screenshot:



Detection



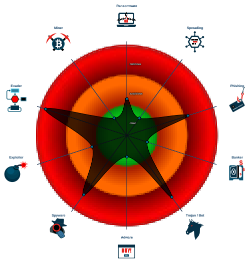
HawkEye MailPassView

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

Signatures

- Yara detected MailPassView
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Malicious sample detected (through …
- Yara detected AntiVM3
- Detected HawkEye Rat
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- .NET source code references suspic…
- Tries to detect sandboxes and other…

Classification



Process Tree

- System is w10x64
- DHL_AWB 65335643399___pdf.exe (PID: 6536 cmdline: "C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe" MD5: 52EF260EF62AAE29914F40CB8EAED7AC)
  - schtasks.exe (PID: 6980 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NbJgZAsv" /XML "C:\Users\user\AppData\Local\Temp\tmpBB4.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL_AWB 65335643399___pdf.exe (PID: 6996 cmdline: C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe MD5: 52EF260EF62AAE29914F40CB8EAED7AC)
    - vbc.exe (PID: 7116 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp72B7.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6436 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp51F7.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6452 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp2427.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6740 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmpF619.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6756 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmpF75D.tmp MD5: C63ED21D5706A527419C9FBD730FFB2E)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.415051620.0000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000007.00000000.382709219.0000000000402000.00000040.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87a2e:$s1: HawkEye Keylogger • 0x87a97:$s1: HawkEye Keylogger • 0x80e71:$s2: _ScreenshotLogger • 0x80e3e:$s3: _PasswordStealer

Source	Rule	Description	Author	Strings
00000007.00000000.382709219.0000000000402000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
0000001B.00000000.584728372.0000000000400000.00000040.00000001.sdmp	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
0000001B.00000000.584728372.0000000000400000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 65 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.DHL_AWB 65335643399___pdf.exe.400000.4.unpack	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87c2e:$s1: HawkEye Keylogger • 0x87c97:$s1: HawkEye Keylogger • 0x81071:$s2: _ScreenshotLogger • 0x8103e:$s3: _PasswordStealer
7.0.DHL_AWB 65335643399___pdf.exe.400000.4.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x87601:$name: ConfuserEx • 0x8630e:$compile: AssemblyTitle
7.0.DHL_AWB 65335643399___pdf.exe.400000.4.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
7.0.DHL_AWB 65335643399___pdf.exe.400000.4.unpack	HawkEyev9	HawkEye v9 Payload	ditekshen	• 0x87c2e:$id1: HawkEye Keylogger - Reborn v9 - {0} Logs - {1} \ {2} • 0x87c97:$id2: HawkEye Keylogger - Reborn v9{0}{1} Logs{0}{2} \ {3}{0}{0}{4} • 0x8103e:$str1: _PasswordStealer • 0x8104f:$str2: _KeyStrokeLogger • 0x81071:$str3: _ScreenshotLogger • 0x81060:$str4: _ClipboardLogger • 0x81083:$str5: _WebCamLogger • 0x81198:$str6: _AntiVirusKiller • 0x81186:$str7: _ProcessElevation • 0x8114d:$str8: _DisableCommandPrompt • 0x81253:$str9: _WebsiteBlocker • 0x81263:$str9: _WebsiteBlocker • 0x81139:$str10: _DisableTaskManager • 0x811b4:$str11: _AntiDebugger • 0x8123e:$str12: _WebsiteVisitorSites • 0x81163:$str13: _DisableRegEdit • 0x811c2:$str14: _ExecutionDelay • 0x810e7:$str15: _InstallStartupPersistance
27.2.vbc.exe.400000.0.raw.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
Click to see the 143 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Writes to foreign memory regions

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected MailPassView

Yara detected HawkEye Keylogger

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

Yara detected WebBrowserPassView password recovery tool

Tries to steal Instant Messenger accounts or passwords

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

Remote Access Functionality:

Yara detected HawkEye Keylogger

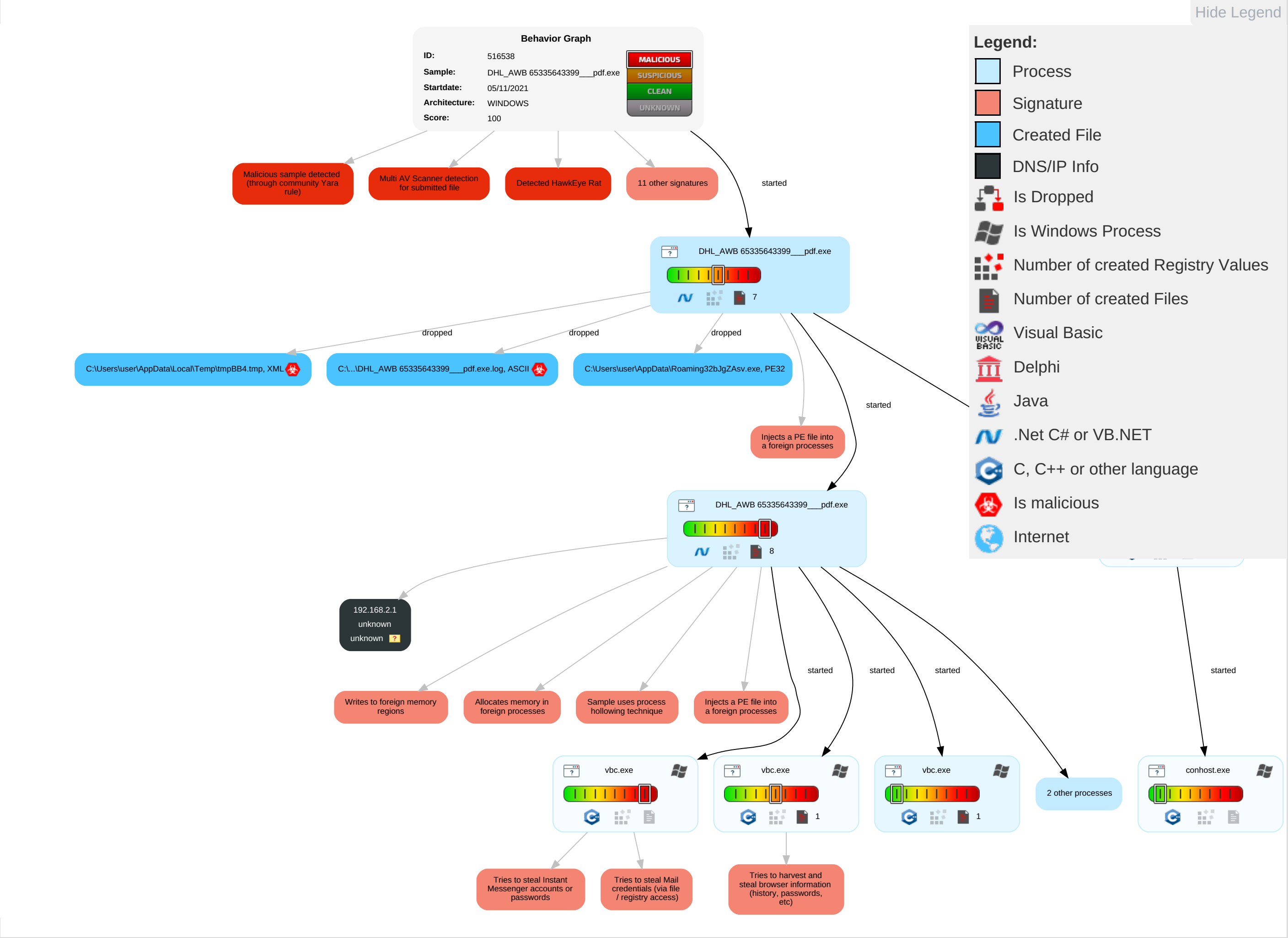
Detected HawkEye Rat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 1 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Default Accounts	Native API 1 1	Scheduled Task/Job 1	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Remote Acce Software 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 4	Credentials In Files 1	System Information Discovery 1 9	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Steganograp
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 3 1	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Network Sniffing	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 4 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

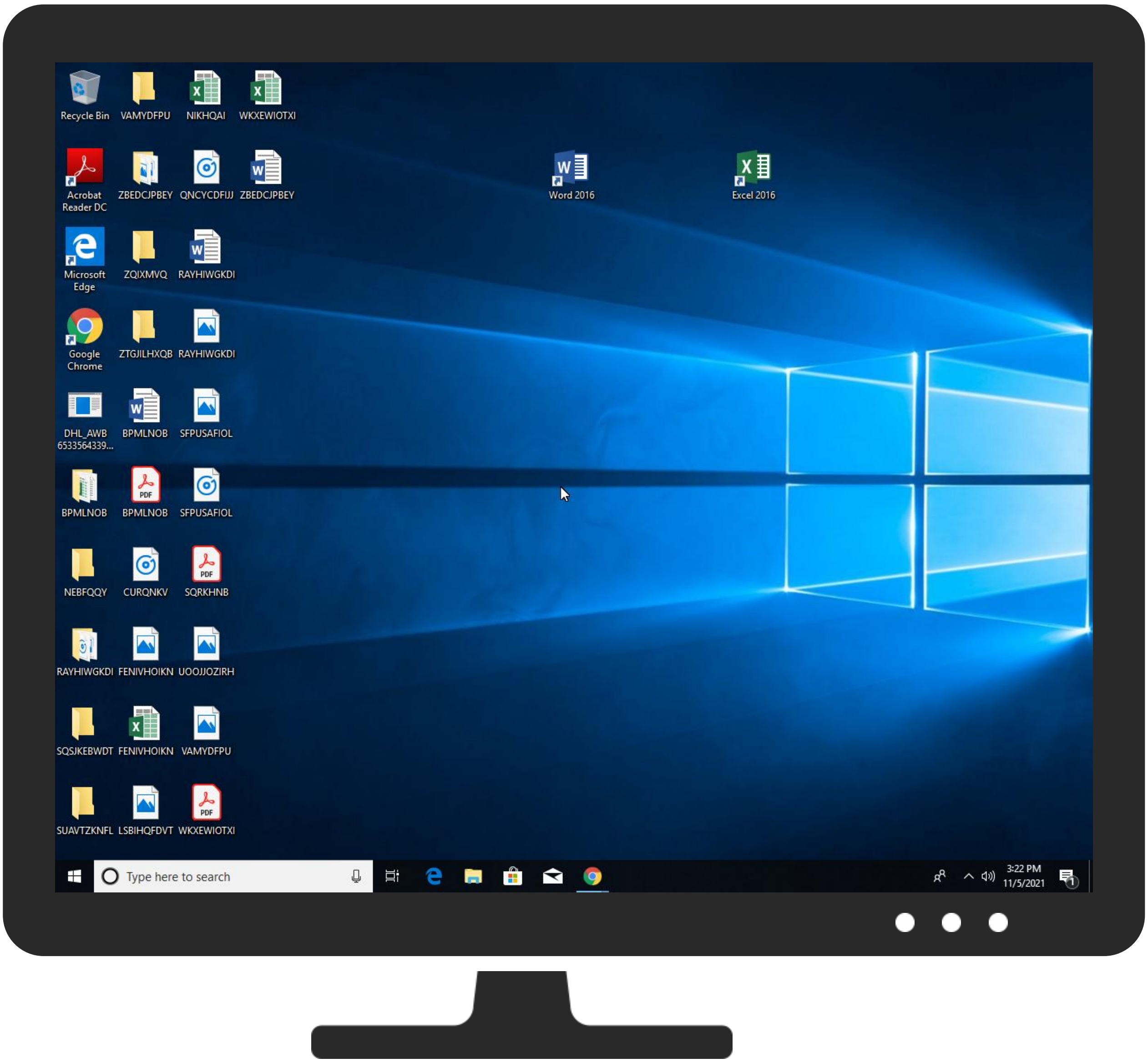
Behavior Graph


Hide Legend
Behavior Graph
ID: 516538
Sample: DHL_AWB 65335643399___pdf.exe
Startdate: 05/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Malicious sample detected (through community Yara rule)
Multi AV Scanner detection for submitted file
Detected HawkEye Rat
11 other signatures
started
DHL_AWB 65335643399___pdf.exe
7
dropped
dropped
dropped
C:\Users\user\AppData\Local\Temp\tmpBB4.tmp, XML
C:\...\DHL_AWB 65335643399___pdf.exe.log, ASCII
C:\Users\user\AppData\Roaming32bJgZAsv.exe, PE32
started
Injects a PE file into a foreign processes
DHL_AWB 65335643399___pdf.exe
8
192.168.2.1
unknown
unknown
Writes to foreign memory regions
Allocates memory in foreign processes
Sample uses process hollowing technique
Injects a PE file into a foreign processes
started
started
started
started
vbc.exe
vbc.exe
1
vbc.exe
1
2 other processes
conhost.exe
Tries to steal Instant Messenger accounts or passwords
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal browser information (history, passwords, etc)
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

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 65335643399___pdf.exe	27%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
17.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.0.DHL_AWB 65335643399___pdf.exe.400000.12.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
17.0.vbc.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
17.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.0.DHL_AWB 65335643399___pdf.exe.400000.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
13.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
13.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
8.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
8.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
12.0.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
13.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
12.0.vbc.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.2.DHL_AWB 65335643399___pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
13.0.vbc.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
13.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
17.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.0.DHL_AWB 65335643399___pdf.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.DHL_AWB 65335643399___pdf.exe.400000.10.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
13.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
8.0.vbc.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
8.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
12.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.0.DHL_AWB 65335643399___pdf.exe.400000.8.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.0.vbc.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
8.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
12.0.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
8.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
17.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
12.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comoaj%(-	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnr-f	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnomp	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sandoll.co.kr=	0%	Avira URL Cloud	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.monotype.0	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/staff/dennis.htmg	0%	Avira URL Cloud	safe	
http://www.carterandcone.comR	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http:// https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	0%	URL Reputation	safe	
http://pomf.cat/upload.php	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	0%	URL Reputation	safe	
http://www.carterandcone.comces	0%	URL Reputation	safe	
http://www.tiro.comn-u4	0%	Avira URL Cloud	safe	
http://www.carterandcone.comen	0%	URL Reputation	safe	
http://www.tiro.comE	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	516538
Start date:	05.11.2021
Start time:	15:20:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_AWB 65335643399___pdf.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:	29

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.phis.troj.spyw.evad.winEXE@16/13@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 77% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:21:14	API Interceptor	5x Sleep call for process: DHL_AWB 65335643399___pdf.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_AWB 65335643399___pdf.exe.log	☣
Process:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_AWB 65335643399___pdf.exe.log	
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\49b65733-2a7e-be56-685e-64260949479e	
Process:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	88
Entropy (8bit):	5.403819652846604
Encrypted:	false
SSDEEP:	3:Bpx9cCPOERwhkNvW0sKtKWBeNODnS501:Bpx939R/NvW0s1e
MD5:	9875EC0B7EB8D451315F9F1326AAEB67
SHA1:	E9871048F796D66A9E291BEAC8C22F2E5AA4C17F
SHA-256:	202ACD4716CF06B8A7E34DB56034BC4AD82E3BF3C7E3C3CF315E5F87BB5EF8B9
SHA-512:	406CBB37B4FB90E1154ECFF01B345915F12D22FD7E19E65DB7A7B961075B01D3014A4BC7B19F2BAEE0FFB565FE1A1A8A3258E21D5718B4FFD65FAB9DFBC4A3FC
Malicious:	false
Reputation:	low
Preview:	GTXq6lZGCzVwlrIPDHEkHKLHTDwQ+W9qskpK9EEOMzECcgwr6lRJ0INBTQI/Ho3Cwgm7UnZunhkwo8Y4g7/03Q==

C:\Users\user\AppData\Local\Temp\bhv3F87.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0xf6c62795, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.877811164040784
Encrypted:	false
SSDEEP:	24576:5M+wP17f2sBMPHihgmKdTnjVccgeTaNX:9sBoT
MD5:	C7282CEAA3E3B01987F67DA5BF529677
SHA1:	A5D3B18A538855FEF53FA6D0F5BCD31131A5C916
SHA-256:	AE7D3AEFA17E7DFE40E329BA1E110383E1D7D6CFC29BD5D0489984295C7DB1EA
SHA-512:	D1E01AF046CC07D75DB0983B32B320EE11F4CD2CFCF332355C84B569BD38AFD3ADA4C77F73FFD5366A07433EEED0675AC71D2FE861FF69961BEF4A7C34D5A7E
Malicious:	false
Reputation:	low
Preview:	..'.... ....p........Ef..4...w.......................%.....2....y..3....y..h.'..........................W.4...w...[............B........................ ....yW.. ....\5......y#q................%........yC.. ....

C:\Users\user\AppData\Local\Temp\bhv6484.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x3860e4e7, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.882512226797484
Encrypted:	false
SSDEEP:	24576:3A+wP17f2svMPHihgmKdTnjVccgeTaNX:fsvoT

C:\Users\user\AppData\Local\Temp\bhv6484.tmp	
MD5:	57F8E33FDE23B8D15313B3B5EB91BF92
SHA1:	D6F6B34363DCE4E667B91E369AC32E5D0E8ABA9C
SHA-256:	6E110E32E80B10B430E18680289C39CB652090C9F09CD73ADB87534F9AAEE1C6
SHA-512:	C258DD9D1F84947D67C45EEAF40715A384A78A74E014D86209B78CD1121A957FF0BD618277529033D5E96C6289A69A3EC49C1B0D35A176283B27C76B8ED2D22
Malicious:	false
Reputation:	low
Preview:	8`..... ....p........Ef..4...w........................%.....2....y..3....y..h.'............................W.4...w..[............B......................... ....yW.. ....N)....yC{..................V(....yc.. ....

C:\Users\user\AppData\Local\Temp\bhv7E75.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x3860e4e7, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.882512226797484
Encrypted:	false
SSDEEP:	24576:3A+wP17f2svMPHihgmKdTnjVccgeTaNX:fsvoT
MD5:	57F8E33FDE23B8D15313B3B5EB91BF92
SHA1:	D6F6B34363DCE4E667B91E369AC32E5D0E8ABA9C
SHA-256:	6E110E32E80B10B430E18680289C39CB652090C9F09CD73ADB87534F9AAEE1C6
SHA-512:	C258DD9D1F84947D67C45EEAF40715A384A78A74E014D86209B78CD1121A957FF0BD618277529033D5E96C6289A69A3EC49C1B0D35A176283B27C76B8ED2D22
Malicious:	false
Preview:	8`..... ....p........Ef..4...w........................%.....2....y..3....y..h.'............................W.4...w..[............B......................... ....yW.. ....N)....yC{..................V(....yc.. ....

C:\Users\user\AppData\Local\Temp\bhvA016.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x3860e4e7, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.882512226797484
Encrypted:	false
SSDEEP:	24576:3A+wP17f2svMPHihgmKdTnjVccgeTaNX:fsvoT
MD5:	57F8E33FDE23B8D15313B3B5EB91BF92
SHA1:	D6F6B34363DCE4E667B91E369AC32E5D0E8ABA9C
SHA-256:	6E110E32E80B10B430E18680289C39CB652090C9F09CD73ADB87534F9AAEE1C6
SHA-512:	C258DD9D1F84947D67C45EEAF40715A384A78A74E014D86209B78CD1121A957FF0BD618277529033D5E96C6289A69A3EC49C1B0D35A176283B27C76B8ED2D22
Malicious:	false
Preview:	8`..... ....p........Ef..4...w........................%.....2....y..3....y..h.'............................W.4...w..[............B......................... ....yW.. ....N)....yC{..................V(....yc.. ....

C:\Users\user\AppData\Local\Temp\tmp2427.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Local\Temp\tmp51F7.tmp

C:\Users\user\AppData\Local\Temp\tmp51F7.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D8 4
Malicious:	false
Preview:	 ..

C:\Users\user\AppData\Local\Temp\tmp72B7.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D8 4
Malicious:	false
Preview:	 ..

C:\Users\user\AppData\Local\Temp\tmpBB4.tmp

Process:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1653
Entropy (8bit):	5.161745901057222
Encrypted:	false
SSDEEP:	
MD5:	7905247879184C91276AA846224B68E9
SHA1:	3F24CBA6359007C884F0DBAB1E66ADB90E3D5AA5
SHA-256:	1380B534164A7193F9DAF1ACD1614B2533BF67005D9DD7D4E1E08BE825A0A78B
SHA-512:	A303D15C69C7D7429E5876E02F0370B1C9BA2DA4DD807ABDE8F363B382ED55C93DBE81624CF693DA294F7120F7D6735CC475D704F19F9662550A9A52E765B4F
Malicious:	**true**
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>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpF619.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D8 4

C:\Users\user\AppData\Local\Temp\tmpF619.tmp	
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\NbJgZAsv.exe	
Process:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	897024
Entropy (8bit):	7.575754263243903
Encrypted:	false
SSDEEP:	
MD5:	52EF260EF62AAE29914F40CB8EAED7AC
SHA1:	CBA71C49AE1C145C6E9210685BE42F4AA24B0E18
SHA-256:	752EFE9AD078A9BE4A82B6F7C2123D58C90A1456287390B50DF9E9C3292BC490
SHA-512:	728F4B4590909C13A1CD9D0DDD90A6C75FDAD830ED44EDE67A1EB0CBD59476760507511E2F42D38545ABF11E3B08D85E95E8F04962094E012956D061E82425A
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...V...............................~.... ....@.. ....@.................................0...K... ....H............text........ ....`.rsrc..............................@..@.reloc........ ......................@..B................`.......H........{...E...0..9.......+.&.........%..#.o...........%.r...p.%.r/..p.%....8.....*...B+.&.+.&..(.....*....+.&..*..+.&..*. ^+.&...(....(!...("....*^+.&..(%....(....o.....*.0..........+.&.+.&. ....8o......(.......{.....(.......{.....(......s....}....8....& ....8/....rI..p}.... .....9....&.(&...8.... ............E........I...............-.......u... ... ..:....&..}....($...(#...9....& ....8......{.....{.....{....o....u....

C:\Users\user\AppData\Roaming\NbJgZAsv.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.575754263243903
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL_AWB 65335643399___pdf.exe
File size:	897024
MD5:	52ef260ef62aae29914f40cb8eaed7ac
SHA1:	cba71c49ae1c145c6e9210685be42f4aa24b0e18
SHA256:	752efe9ad078a9be4a82b6f7c2123d58c90a1456287390b 50df9e9c3292bc490
SHA512:	728f4b4590909c13a1cd9d0ddd90a6c75fdad830ed44ede 67a1eb0cbd59476760507511e2f42d38545abf11e3b08d8 5e95e8f04962094e012956d061e82425ae
SSDEEP:	24576:7HnOzw59zsorf4ep5TIAAkYc8xmGgTp5UVNH19:KITMepFYPxmjUVNV

General	
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...V...............................~.... ....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4db87e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xBAAB9656 [Fri Mar 29 18:28:38 2069 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd9884	0xd9a00	False	0.804097411689	data	7.57987288124	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xdc000	0x10ec	0x1200	False	0.377170138889	data	4.90557056462	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

💡 Click to jump to process

System Behavior

Analysis Process: DHL_AWB 65335643399___pdf.exe PID: 6536 Parent PID: 1344

General

Start time:	15:21:04
Start date:	05/11/2021
Path:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe"
Imagebase:	0xad0000
File size:	897024 bytes
MD5 hash:	52EF260EF62AAE29914F40CB8EAED7AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.388044368.00000000042A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.388044368.00000000042A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.387656235.000000000409C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.387656235.000000000409C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.385059771.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6980 Parent PID: 6536

General

Start time:	15:21:25
Start date:	05/11/2021

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\NbJgZAsv" /XML "C:\Users\user\AppData\Local\Temp\tmpBB4.tmp
Imagebase:	0x1240000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 6988 Parent PID: 6980

General

Start time:	15:21:26
Start date:	05/11/2021
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: DHL_AWB 65335643399___pdf.exe PID: 6996 Parent PID: 6536

General

Start time:	15:21:26
Start date:	05/11/2021
Path:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_AWB 65335643399___pdf.exe
Imagebase:	0x6f0000
File size:	897024 bytes
MD5 hash:	52EF260EF62AAE29914F40CB8EAED7AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000000.382709219.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.382709219.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.604722336.0000000002B87000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.604997751.0000000002C11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.604881484.0000000002BE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000002.604385666.0000000002AF1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.604385666.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.604385666.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.606344857.0000000003AE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.606344857.0000000003AE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000007.00000002.606732949.0000000004FC0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.606732949.0000000004FC0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.606732949.0000000004FC0000.00000004.00020000.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000000.380988424.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.380988424.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000000.381541048.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.381541048.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000003.384365256.0000000004355000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000003.384365256.0000000004355000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000002.600470804.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.600470804.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000000.382170553.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000000.382170553.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.606069695.0000000002CBB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 7116 Parent PID: 6996

General

Start time:	15:21:31
Start date:	05/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp72B7.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000000.392634525.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000000.394234087.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000000.393712124.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000000.394776440.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.408592264.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6436 Parent PID: 6996

General

Start time:	15:21:41

Start date:	05/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp51F7.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000000.415051620.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000000.414637682.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000000.414189798.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000002.424952995.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000C.00000000.413703386.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6452 Parent PID: 6996

General

Start time:	15:21:48
Start date:	05/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmp2427.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000000.429195340.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000002.439502988.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000000.429569305.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000000.428434291.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000D.00000000.428849255.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6740 Parent PID: 6996

General

Start time:	15:21:55
Start date:	05/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmpF619.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.444119712.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000002.458049589.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.443122582.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.445590834.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000011.00000000.443616731.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6756 Parent PID: 6996

General

Start time:	15:23:00
Start date:	05/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe" /stext "C:\Users\user\AppData\Local\Temp\tmpF75D.tmp
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000001B.00000000.584728372.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000000.584728372.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000001B.00000002.585393509.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000002.585393509.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000001B.00000000.584242337.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000000.584242337.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000001B.00000000.583483657.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000000.583483657.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000001B.00000000.583887483.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001B.00000000.583887483.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis