ID: 500841
Sample Name:
DHL_AWB_DOCUMENT_pdf.exe
Cookbook: default.jbs
Time: 10:37:58
Date: 12/10/2021
Version: 33.0.0 White Diamond

Table of Contents

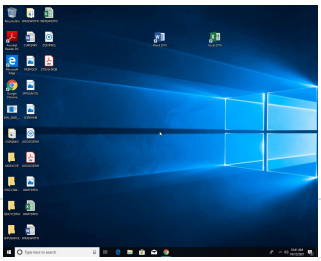
Windows Analysis Report DHL_AWB_DOCUMENT_pdf.e…

Overview

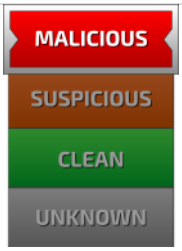
General Information

Sample Name:	DHL_AWB_DOCUMENT_pdf.exe
Analysis ID:	500841
MD5:	27e7a44ab2f5d2c.
SHA1:	b0c7952addaa50..
SHA256:	fa38ec9464602a1.
Tags:	DHL exe HawkEye
Infos:	

Most interesting Screenshot:



Detection



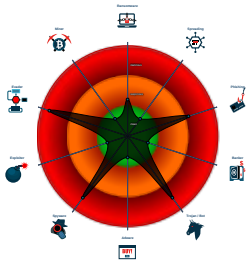
HawkEye
MailPassView

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

Signatures

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Malicious sample detected (through …
- Yara detected AntiVM3
- Detected HawkEye Rat
- Sample uses process hollowing tech…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to detect sandboxes and other…
- Tries to steal Mail credentials (via fil…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- DHL_AWB_DOCUMENT_pdf.exe (PID: 6808 cmdline: 'C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe' MD5: 27E7A44AB2F5D2C40C374D5893257AC5)
  - schtasks.exe (PID: 5140 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RQXCXKwIG' /XML 'C:\Users\user\AppData\Local\Temp\tmpCC16.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5268 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL_AWB_DOCUMENT_pdf.exe (PID: 5584 cmdline: C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe MD5: 27E7A44AB2F5D2C40C374D5893257AC5)
    - vbc.exe (PID: 5484 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9660.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 1256 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp93FB.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000003.407277788.0000000004AB5000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000008.00000003.407277788.0000000004AB5000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000008.00000002.617994550.000000000335E000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000000.00000002.411663887.0000000003DF4000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87ede:$s1: HawkEye Keylogger • 0x87f47:$s1: HawkEye Keylogger • 0x81321:$s2: _ScreenshotLogger • 0x812ee:$s3: _PasswordStealer

Source	Rule	Description	Author	Strings
00000000.00000002.411663887.0000000003DF4000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.2.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, encrypteduUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
23.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
8.3.DHL_AWB_DOCUMENT_pdf.exe.4ab5890.2.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x696fa:$a1: logins.json • 0x6965a:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encrypteduUsername, encryptedPassword FROM moz_login • 0x69e7e:$s4: \mozsqlite3.dll • 0x686ee:$s5: SMTP Password
8.3.DHL_AWB_DOCUMENT_pdf.exe.4ab5890.2.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
8.3.DHL_AWB_DOCUMENT_pdf.exe.4ab5890.2.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 54 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

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

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)

Yara detected WebBrowserPassView password recovery tool

Tries to steal Mail credentials (via file access)

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

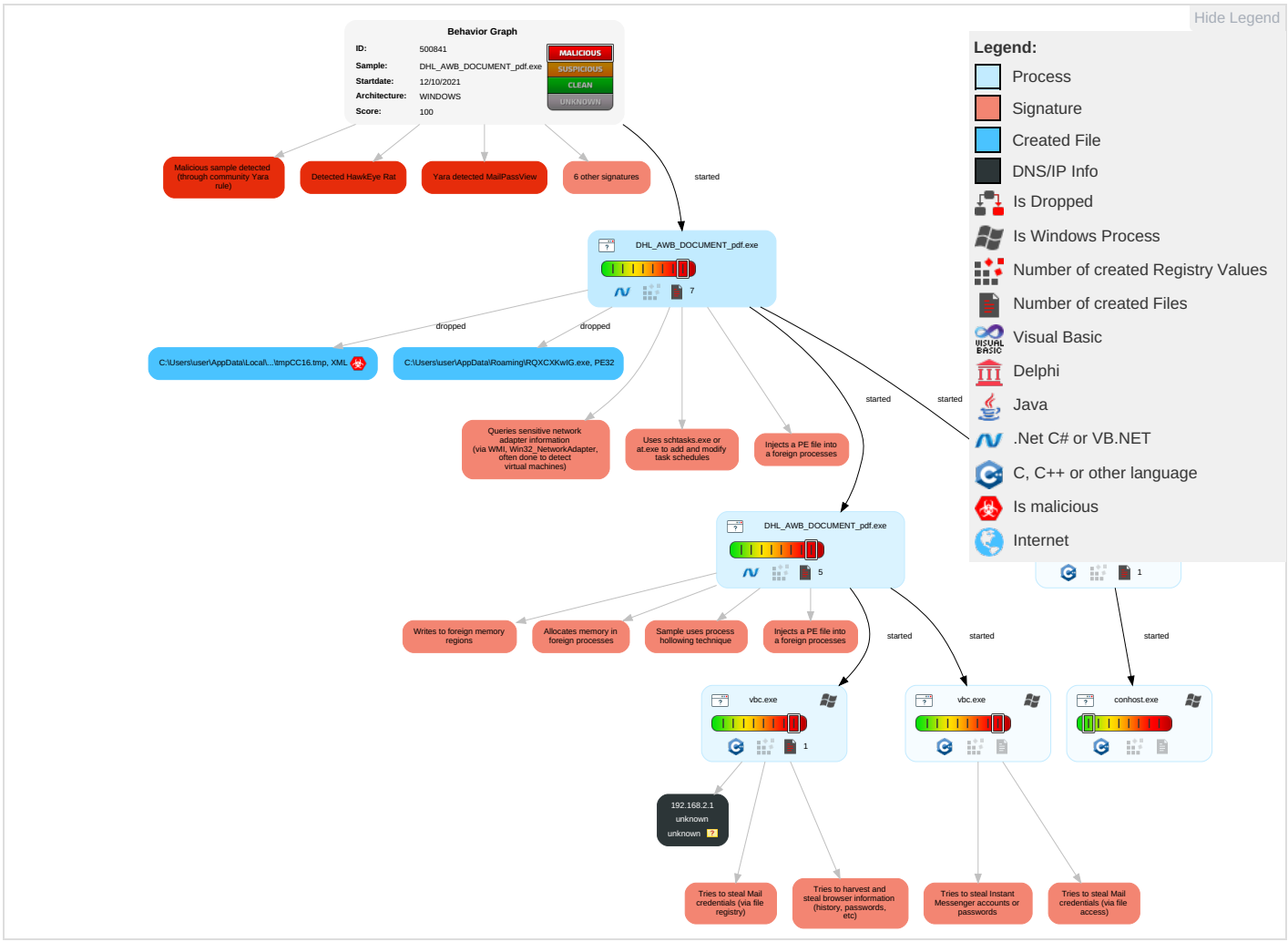
Detected HawkEye Rat

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	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Scheduled Task/Job 1	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 2	Account Discovery 1	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 3	Credentials In Files 1	File and Directory Discovery 2	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	System Information Discovery 1 9	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Security Software Discovery 2 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 2	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoco

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.DHL_AWB_DOCUMENT_pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
10.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/://w	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comalsL	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt-b	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s/t	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sakkal.comc	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImQ1Y2M3ZjUxNTk0ZjI1ZWI5NjQxNjllMjcxMDliYzA5MWY4N	0%	Avira URL Cloud	safe	
http://www.urwpp.dep(	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://www.sajatypeworks.comenznd	0%	Avira URL Cloud	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.agfamonotype.D	0%	Avira URL Cloud	safe	
http://fontfabrik.com1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/w	0%	URL Reputation	safe	
http://www.fontbureau.comttvaE	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnrmX	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://www.fonts.com8	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:	33.0.0 White Diamond
Analysis ID:	500841
Start date:	12.10.2021
Start time:	10:37:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_AWB_DOCUMENT_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:	25
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@10/7@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.7% (good quality ratio 4.4%) • Quality average: 82.1% • Quality standard deviation: 27%
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
10:39:08	API Interceptor	2x Sleep call for process: DHL_AWB_DOCUMENT_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_DOCUMENT_pdf.exe.log	
Process:	C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
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\bhvFA16.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x8873ee24, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.8801947886367714
Encrypted:	false
SSDEEP:	24576:Vi+wP17f2sZ6PHihgmKdTnjVccgeTaNX:7sZCT
MD5:	CE07C021CC3C195FE5B12AFE35EBABA4
SHA1:	44C5EC03CD141278D53156CBEB32C81E8CC6FD66
SHA-256:	CB997DBB0504FC88A5E3A5755C8FCB128A67B01B8D77F8FDA4ADD934BA5CA6F4
SHA-512:	EC3F6BDF509597D98A047568FF0C7480E1DA9921F6CEF6E1681CECCAC2485D0B9417A51002F95D28F2C42DF696C41017887EA1911431D3E88FCC30A7E436C30
Malicious:	false
Reputation:	low
Preview:	.s.$... .....p.....Ef..4...w.....%.....x..*&...y).h.'.....W.4...w.....[.....B..... ....;&...yA..... .....YEC.'...y_w.....4P...'...yM..... .....

C:\Users\user\AppData\Local\Temp\f8074016-c465-3e19-f1b3-c9f1605ca201	
Process:	C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	88
Entropy (8bit):	5.47614383439888
Encrypted:	false
SSDEEP:	3:Bpx9cCPOERwOGJok5f8YmXiW9mYY:Bpx939RXCf8YKm1

C:\Users\user\AppData\Local\Temp\f8074016-c465-3e19-f1b3-c9f1605ca201	
MD5:	AA8A08A3C7954B70D790E176213F09E8
SHA1:	D4A8DC6F7E3D1C50E6B81320E64F80C2C1959200
SHA-256:	979779667AA82D1FDF00271B940CC68A615343BC3E9B8D3A3FB54896E709A2FE
SHA-512:	3E32D501E2FCDA3669260272B8C09385A036B6ACB068945AAC733AE607688E268CAD4BEEE7DA9E2DB67B2985522B41B3C72D99E1E3A199DD4EBF6C210C9942F
Malicious:	false
Reputation:	low
Preview:	GTXq6lZGCzVwlrIPDHEkHKLHTDwQ+W9qskpK9EEOMzHIleFlvAxtMhN+/0sCCBt1YTkg5yrrUrRVGLhJWaMafQ==

C:\Users\user\AppData\Local\Temp\tmp9660.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:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Temp\tmpCC16.tmp	
Process:	C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1654
Entropy (8bit):	5.168121372728127
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3F39tn:cbha7JlNQV/rydbz9I3YODOLNdq3nH
MD5:	3C803F5692F4E645A908771C332B8F86
SHA1:	2AF98CBE843644AD78C379C73C476E0D97F7C682
SHA-256:	B2C1324ED2418A9355E3257A24005114656160DD2BC3FADC5C6867101AA09781
SHA-512:	4A466932B80608948ED36BFDBC2822B3B4A2679BC82EFCB23ED3B0DB73E7A17EE29BDBC429C939C4F8554DC9C78AAAE44EEC98FF46C2FBA7426AF01AA1E7B650
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\Roaming\RQXCXKwIG.exe	
Process:	C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1016832
Entropy (8bit):	7.873081004307992
Encrypted:	false
SSDEEP:	24576:oTgp1phBS5HVJnyGRRpcY8LDiHK0Rkg3MHLPc:NBSxryUoY8meg3MHrc
MD5:	27E7A44AB2F5D2C40C374D5893257AC5
SHA1:	B0C7952ADDAA502E6C1DBEA7474E534F2264742F
SHA-256:	FA38EC9464602A1727813004FC616D9D0359C37DA01B7D07C3E38784C0B2A46D
SHA-512:	CE0BDA0D9F9C3541816B20D1DAAED3BBF121C69A5DEF00837FDAA8EF5E31BB59CC0E98402EAE6423A655D2DB2084190CDD63A5E9A00DE024E3300CB835CD767
Malicious:	false

C:\Users\user\AppData\Roaming\RQXCXKwIG.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...~#ea.....0..x.....F.... .....@.. ....@.....O.....,..... ....H.....text...Lv... ...x..... ..`.rsrc...,.....z.....@..@.reloc..... .....@..B.....(.....H.....,.....)...4.....F....~....(.....*...0..L.....(.....oW.....(!...("...j.Zs#.....(....(X.....(.....($.....*.0..i.....(.....(%.....oW.....(!...("....iZs&.....('.....(....(X.....(.....((.....($.....*.....BU.....r...(.....(X.....($.....*....0..).....oW.....(.....(.....s)....+..*....0.....r...p.(]...(* ....+..*..{+...*"..}+...*....(U.....*..0.....

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.873081004307992
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DHL_AWB_DOCUMENT_pdf.exe
File size:	1016832
MD5:	27e7a44ab2f5d2c40c374d5893257ac5
SHA1:	b0c7952addaa502e6c1dbea7474e534f2264742f
SHA256:	fa38ec9464602a1727813004fc616d9d0359c37da01b7d0 7c3e38784c0b2a46d
SHA512:	ce0bda0d9f9c3541816b20d1daaed3bbf121c69a5def008 37fdaa8ef5e31bb59cc0e98402eae6423a655d2db208419 0cdd63a5e9a00de024e3300cb835cde767
SSDEEP:	24576:oTgp1phBS5HVJnyGRRpcY8LDiHK0Rkg3MHLP c:NBSxryUoY8meg3MHrc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...~#ea.....0..x.....F.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4f9646
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6165237E [Tue Oct 12 05:56:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf764c	0xf7800	False	0.897174873737	data	7.87928280885	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xfa000	0x62c	0x800	False	0.34765625	data	3.49750013156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfc000	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_DOCUMENT_pdf.exe PID: 6808 Parent PID: 6096

General

General

Start time:	10:38:57
Start date:	12/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe'
Imagebase:	0x880000
File size:	1016832 bytes
MD5 hash:	27E7A44AB2F5D2C40C374D5893257AC5
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: 00000000.00000002.411663887.0000000003DF4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.411663887.0000000003DF4000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.413371192.0000000003F3C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.413371192.0000000003F3C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.409575896.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5140 Parent PID: 6808

General

Start time:	10:39:25
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RQXCXKwIG' /XML 'C:\Users\user\AppData\Local\Temp\tmpCC16.tmp'
Imagebase:	0x70000
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: 5268 Parent PID: 5140

General

Start time:	10:39:25
Start date:	12/10/2021
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_DOCUMENT_pdf.exe PID: 5584 Parent PID: 6808

General

Start time:	10:39:26
Start date:	12/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe
Imagebase:	0xe40000
File size:	1016832 bytes
MD5 hash:	27E7A44AB2F5D2C40C374D5893257AC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000003.407277788.0000000004AB5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000003.407277788.0000000004AB5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.617994550.000000000335E000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000008.00000002.616495214.0000000003253000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.616495214.0000000003253000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.616495214.0000000003253000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000008.00000002.613924819.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.613924819.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.618484972.0000000004245000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.618484972.0000000004245000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000008.00000002.619031454.0000000005980000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.619031454.0000000005980000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.619031454.0000000005980000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 5484 Parent PID: 5584

General

Start time:	10:39:28
Start date:	12/10/2021
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\tmp9660.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: 0000000A.00000002.428216908.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 1256 Parent PID: 5584

General

Start time:	10:40:33
Start date:	12/10/2021
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\tmp93FB.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: 00000017.00000002.551755492.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000017.00000002.551755492.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis