ID: 500851
Sample Name:
DHL_AWB_DOCUMENT_pdf.exe
Cookbook: default.jbs
Time: 10:46:23
Date: 12/10/2021
Version: 33.0.0 White Diamond

Table of Contents

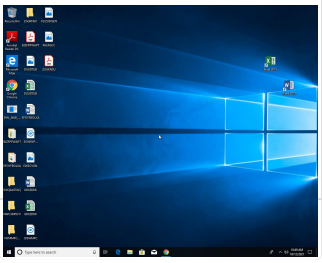
Windows Analysis Report DHL_AWB_DOCUMENT_pdf.e…

Overview

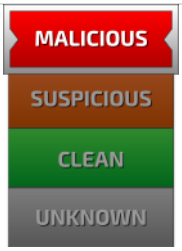
General Information

Sample Name:	DHL_AWB_DOCUMENT_pdf.exe
Analysis ID:	500851
MD5:	1b20cc08d2181fb..
SHA1:	7ace5eee56eec0..
SHA256:	de1730eddefee2b.
Tags:	DHL exe HawkEye
Infos:	

Most interesting Screenshot:



Detection



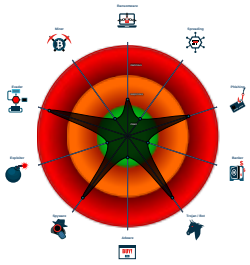
HawkEye
MailPassView

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 …
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Tries to steal Mail credentials (via fil…
- .NET source code contains potentia…
- Yara detected WebBrowserPassView…

Classification



Process Tree

- **System is w10x64**
- DHL_AWB_DOCUMENT_pdf.exe (PID: 3220 cmdline: 'C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe' MD5: 1B20CC08D2181FB763011894D429AD46)
  - schtasks.exe (PID: 4308 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lgrlExxTAQO' /XML 'C:\Users\user\AppData\Local\Temp\tmp9820.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL_AWB_DOCUMENT_pdf.exe (PID: 1928 cmdline: C:\Users\user\Desktop\DHL_AWB_DOCUMENT_pdf.exe MD5: 1B20CC08D2181FB763011894D429AD46)
    - vbc.exe (PID: 1284 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp2B6B.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6108 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp25DA.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000003.283675051.0000000004D45000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000008.00000003.283675051.0000000004D45000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000000.00000002.289239450.0000000003EF9000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x88196:$s1: HawkEye Keylogger • 0x881ff:$s1: HawkEye Keylogger • 0x815d9:$s2: _ScreenshotLogger • 0x815a6:$s3: _PasswordStealer
00000000.00000002.289239450.0000000003EF9000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.289625534.000000000404 5000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger _Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x3548fe:$s1: HawkEye Keylogger • 0x354967:$s1: HawkEye Keylogger • 0x34dd41:$s2: _ScreenshotLogger • 0x34dd0e:$s3: _PasswordStealer
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
26.2.vbc.exe.400000.0.raw.unpack	APT_NK_BabyShark_Kim JoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, form SubmitURL, usernameField, passwordField, encrypte dUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
26.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassVie w	Yara detected MailPassView	Joe Security	
8.2.DHL_AWB_DOCUMENT_pdf.exe.5910000.5.r aw.unpack	APT_NK_BabyShark_Kim JoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x6b4fa:$a1: logins.json • 0x6b45a:$s3: SELECT id, hostname, httpRealm, form SubmitURL, usernameField, passwordField, encrypte dUsername, encryptedPassword FROM moz_login • 0x6bc7e:$s4: \mozsqlite3.dll • 0x6a4ee:$s5: SMTP Password
8.2.DHL_AWB_DOCUMENT_pdf.exe.5910000.5.r aw.unpack	JoeSecurity_MailPassVie w	Yara detected MailPassView	Joe Security	
8.2.DHL_AWB_DOCUMENT_pdf.exe.5910000.5.r aw.unpack	JoeSecurity_WebBrowser PassView	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

.NET source code references suspicious native API functions

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

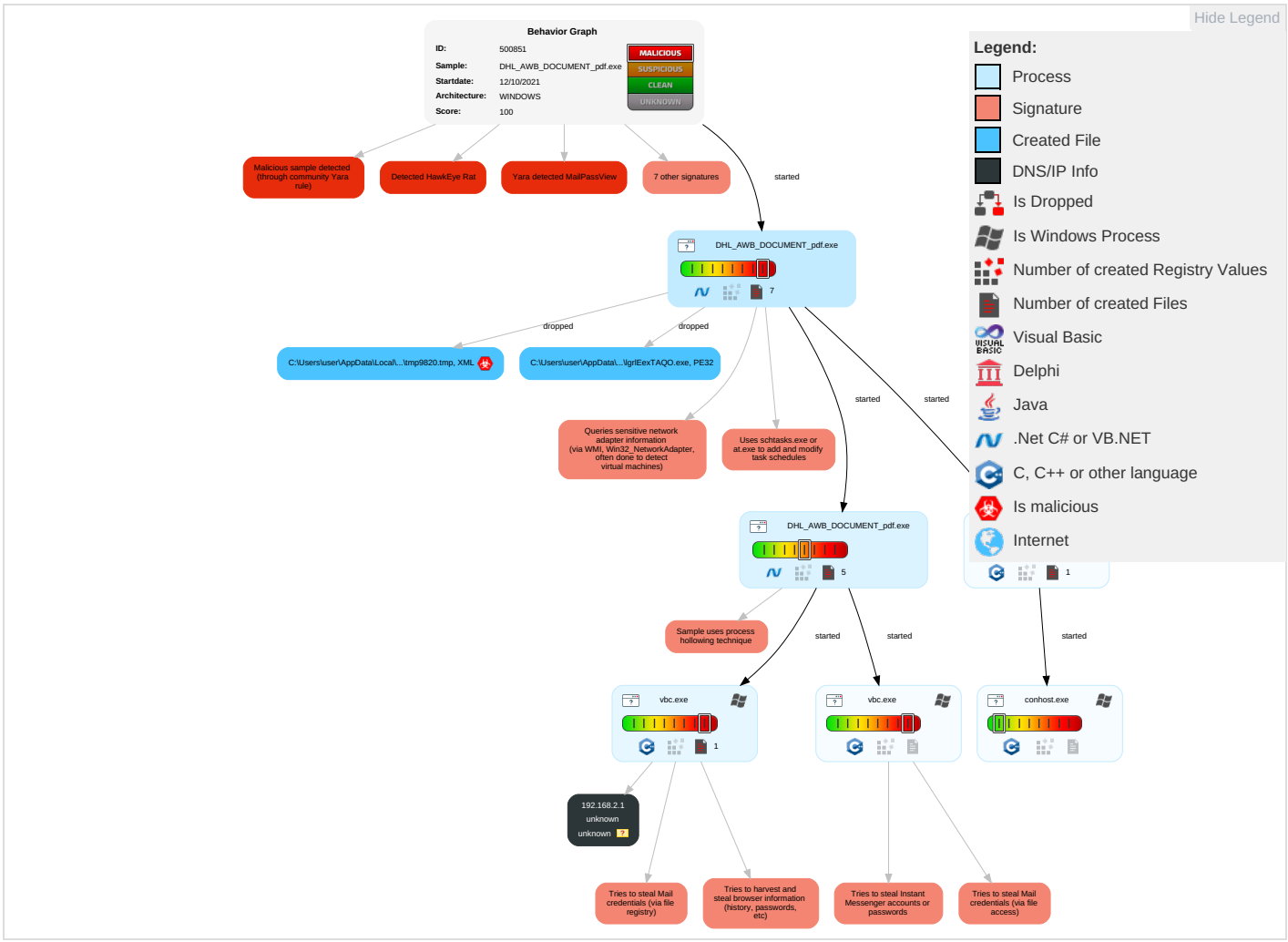
Detected HawkEye Rat

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 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1 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 1 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
13.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
8.2.DHL_AWB_DOCUMENT_pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	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	

Source	Detection	Scanner	Label	Link
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://images.outbrainimg.com/transform/v3/eyJpdSI6IjE4MmE0M2M0MDY3OGU1N2E4MjhkM2NjNDdlNGMzZmNkYjU1N	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.comic	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImY3MDA1MDJkMTdmZDY0M2VkZTBjNzg5MTE1OWEyYTYxMWRiN	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	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://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IiIsIml1ZSI6Imh0dHA6Ly9pbWFnZXMyLnplbWFudGEuY29tL	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	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:	500851
Start date:	12.10.2021
Start time:	10:46:23

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 41s
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:	28
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: 5.4% (good quality ratio 5.2%) • Quality average: 85.1% • Quality standard deviation: 24.3%
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
10:47:28	API Interceptor	3x 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\1baba914-78bb-a57e-5fc4-bf0123172b93	
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):	5.351184034144908
Encrypted:	false
SSDEEP:	3:xNTOXiUhB1S1cqM3pdgBXwYzCYYn:LTOdB1SOZdQ21n
MD5:	56AD5C3487F417954D506260AA07EFC0
SHA1:	91FB0D999103D6967FD8CCDB37DC45F75C8F8714
SHA-256:	AA0DD653EFC423337F904FF01BA9F55C4BF7C06DDDD9FDA581450A6AF53AFAFE
SHA-512:	D56804FBD37F3657F7C22A5D4081DAD1AF515E7DF2AF1378DB75354E2FC215311E94D266E598EFE9B0D769A61A9ABE6367882585BC3332A020782AE7405FB3DE
Malicious:	false
Reputation:	low
Preview:	iLiK8mhJXVhQTEv7ry0onhLTZx4mvvpJKDk87PVV4QhJBbvX2WZVhFO0Cdd1hzGF8h5WCqsR/u8rrEMTOIVwAw==

C:\Users\user\AppData\Local\Temp\bhv2B6.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x5cc662f4, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.9540711288586361
Encrypted:	false
SSDEEP:	24576:YnLv1SxfFUtH2se9zZi2Ou/iDyUrjoEO3PX2BU:LUtHAzU2Oue
MD5:	5C7C5D434DA3868FE344CC444ECE7E0E
SHA1:	411F6AC9C08134D127A7E56F57047F97FAD13DE8
SHA-256:	5189C978FE5AEF41E79FD2EE128CB1291DF6BFD57CB1CCC8F00064D2952F07A0
SHA-512:	56C2D08D57A1D1B1974710672D8DEAE5353F948E24DA25CB2994CAE0994F5FF99CCE7CFB9F0727B63A62EF3301BBA952B9C311FAC2D02D18C97B09746640ED A
Malicious:	false
Reputation:	low
Preview:	\.b.... .....v1.....l~..'...wK.....m...../...y.../...yw.h.o.....k.\."...w.....Y.....B..... ..../...ya..... .....>.H./...yw.....X#{./...y..... .....

C:\Users\user\AppData\Local\Temp\tmp2B6B.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe

C:\Users\user\AppData\Local\Temp\tmp2B6B.tmp	
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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Temp\tmp9820.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):	1648
Entropy (8bit):	5.166569432058411
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBBPtn:cbhC7ZlNQF/rydbz9I3YODOLNdq31
MD5:	6BBEEC809EF541A3ED6933CA8CA6B081
SHA1:	090C818BE35CD0E861EE2C0C748DB7AC1B4C954A
SHA-256:	CFFA74DE9423F3DA8EF2666600C8CB5F1DAE6F456EDBB8FE0D6CD0D74C4CB4BF
SHA-512:	84B285C1A7C600436876BB69310C1282BC2B32FF9693ABA79C8418EF5CA73A8F891E2FE552CFF02DB202A9F7B78E1E668A0174488296761AF503315B2773C798
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>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\lgrlEexTAQO.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):	886272
Entropy (8bit):	7.91854883401178
Encrypted:	false
SSDEEP:	24576:qNBOATB5W0Rs+4xxVoSvaPr+lim4MBAYma6z:gBLO0RQxVoS0ClR4MBAfZz
MD5:	1B20CC08D2181FB763011894D429AD46
SHA1:	7ACE5EEE56EEC0BFD4D365999795E3773513084E
SHA-256:	DE1730EDDEFEE2B8D8193D92B02FC5A3FD1BF6D54C6F55EFF53C85C8A2501A79
SHA-512:	282B0090375E98D0BF570B46336D21AC9057FBF3CD9019C511C5F2FB4A848B9D419FACC9A7B5F140DF52CADAE1A7A2E3786256098A1F96F00DF078CD2086732
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...43ea.....0..~..... .....@.. ....@.....O..... ....H.....text....}... ...~..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....,_...P.....}.....0..4.....L.....r...p...r...p.....,.....+.....+..*.0..F.....+6.....o..... ,.r9..ps....z..X....i...-.*...0..d.....+N..+8.....(.....(.....o.....,.r9..ps....z..X....o. .....-...X....o.....-...X....o.....-.*".(.....

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

C:\Users\user\AppData\Roaming\lgrlEexTAQO.exe:Zone.Identifier	
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):	7.91854883401178
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DHL_AWB_DOCUMENT_pdf.exe
File size:	886272
MD5:	1b20cc08d2181fb763011894d429ad46
SHA1:	7ace5eee56eec0bfd4d365999795e3773513084e
SHA256:	de1730eddefee2b8d8193d92b02fc5a3fd1bf6d54c6f55eff53c85c8a2501a79
SHA512:	282b0090375e98d0bf570b46336d21ac9057fbf3cd9019c511c5f2fb4a848b9d419facc9a7b5f140df52cadae1a7a2e3786256098a1f96f00df078cd20867325
SSDEEP:	24576:qNBOATB5W0Rs+4xxVoSvaPr+lim4MBAYma6z:gBLO0RQxVoS0ClR4MBAfZz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...43ea.....0..~..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d9cfe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61653334 [Tue Oct 12 07:03:16 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	0xd7dec	0xd7e00	False	0.95047974269	data	7.92379641789	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xda000	0x3c0	0x400	False	0.3876953125	data	3.06500586845	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.041015625	data	0.0815394123432	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: 3220 Parent PID: 2880

General

Start time:	10:47:20
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:	0xa20000
File size:	886272 bytes
MD5 hash:	1B20CC08D2181FB763011894D429AD46
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: 00000000.00000002.289239450.0000000003EF9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.289239450.0000000003EF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.289625534.0000000004045000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.289625534.0000000004045000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.286303356.0000000002E01000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4308 Parent PID: 3220

General

Start time:	10:47:38
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lgrlEexTAQO' /XML 'C:\Users\user\AppData\Local\Temp\tmp9820.tmp'
Imagebase:	0x800000
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: 5044 Parent PID: 4308

General

Start time:	10:47:39
Start date:	12/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 1928 Parent PID: 3220

General

Start time:	10:47:39
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:	0x7ff797770000
File size:	886272 bytes
MD5 hash:	1B20CC08D2181FB763011894D429AD46
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: 00000008.00000003.283675051.0000000004D45000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000003.283675051.0000000004D45000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000008.00000002.515516765.0000000005910000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.515516765.0000000005910000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.515516765.0000000005910000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.514774579.00000000035EE000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000008.00000002.505655633.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.505655633.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000008.00000002.513331493.0000000003540000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000008.00000002.513331493.0000000003540000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.513331493.0000000003540000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000008.00000002.515210194.00000000044D5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000008.00000002.515210194.00000000044D5000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 1284 Parent PID: 1928

General

Start time:	10:47:44
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\tmp2B6B.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.00000002.302901584.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6108 Parent PID: 1928

General

Start time:	10:48:48
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\tmp25DA.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: 0000001A.00000002.429178669.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001A.00000002.429178669.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis