

ID: 502165
Sample Name: DHL_AWB 518877882999_887755468_pdf.exe
Cookbook: default.jbs
Time: 17:07:49
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report DHL_AWB 518877882999_887755468_pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Compliance: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 5
Data Obfuscation: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
Private 9
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 14
Data Directories 14
Sections 14
Resources 14
Imports 14
Version Infos 14
Network Behavior 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: DHL_AWB 518877882999_887755468_pdf.exe PID: 2172 Parent PID: 5960 14
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 15
File Read 15
Analysis Process: schtasks.exe PID: 5984 Parent PID: 2172 15
General 15

File Activities 15
Analysis Process: conhost.exe PID: 3584 Parent PID: 5984 16
General 16
Analysis Process: DHL_AWB 518877882999_887755468_pdf.exe PID: 2960 Parent PID: 2172 16
General 16
File Activities 17
File Created 17
File Deleted 17
File Written 17
File Read 17
Analysis Process: vbc.exe PID: 5232 Parent PID: 2960 17
General 17
File Activities 18
File Created 18
File Deleted 18
File Written 18
File Read 18
Analysis Process: vbc.exe PID: 6168 Parent PID: 2960 18
General 18
Disassembly 18
Code Analysis 18

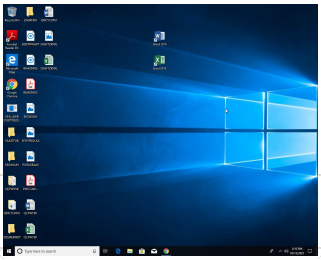
Windows Analysis Report DHL_AWB 518877882999_887…

Overview

General Information

Sample Name:	DHL_AWB 518877882999_887755468_pdf.exe
Analysis ID:	502165
MD5:	7d11e82579e2a0..
SHA1:	d6abbbe7f991e79.
SHA256:	691cb999c6be0f4..
Tags:	DHL exe HawkEye
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

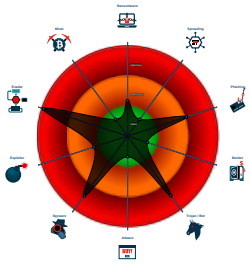
HawkEye
MailPassView

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 …
- Detected unpacking (overwrites its o…
- Yara detected AntiVM3
- Detected unpacking (changes PE se…
- Detected HawkEye Rat
- Sample uses process hollowing tech…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- .NET source code references suspic…

Classification



Process Tree

- **System is w10x64**
- DHL_AWB 518877882999_887755468_pdf.exe (PID: 2172 cmdline: 'C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe' MD5: 7D11E82579E2A0628CA3C855AFE34FD1)
  - schtasks.exe (PID: 5984 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cmsyNzu' /XML 'C:\Users\user\AppData\Local\Temp\tmp70BF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL_AWB 518877882999_887755468_pdf.exe (PID: 2960 cmdline: C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe MD5: 7D11E82579E2A0628CA3C855AFE34FD1)
    - vbc.exe (PID: 5232 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp1B0D.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6168 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp11A3.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.525571222.000000000330E000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000000.00000002.290657795.000000000536D000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x88246:$s1: HawkEye Keylogger • 0x882af:$s1: HawkEye Keylogger • 0x81689:$s2: _ScreenshotLogger • 0x81656:$s3: _PasswordStealer
00000000.00000002.290657795.000000000536D000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000007.00000002.528296707.0000000007D90000.00000004.00020000.sdmp	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x6b4fa:$a1: logins.json • 0x6b45a:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x6bc7e:$s4: \mozsqlite3.dll • 0x6a4ee:$s5: SMTP Password
00000007.00000002.528296707.0000000007D90000.00000004.00020000.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.DHL_AWB 518877882999_887755468_pdf.exe.7de834a.4.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x11bb0:$a1: logins.json • 0x11b10:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x12334:$s4: \mozsqlite3.dll • 0x115a4:$s5: SMTP Password
7.2.DHL_AWB 518877882999_887755468_pdf.exe.7de834a.4.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
7.3.DHL_AWB 518877882999_887755468_pdf.exe.4abdbda.2.raw.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x131b0:$a1: logins.json • 0x13110:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x13934:$s4: \mozsqlite3.dll • 0x121a4:$s5: SMTP Password
7.3.DHL_AWB 518877882999_887755468_pdf.exe.4abdbda.2.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
7.2.DHL_AWB 518877882999_887755468_pdf.exe.4291990.2.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x11bb0:$a1: logins.json • 0x11b10:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x12334:$s4: \mozsqlite3.dll • 0x115a4:$s5: SMTP Password
Click to see the 58 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:



Detected unpacking (overwrites its own PE header)

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected HawkEye Keylogger

System Summary:



Copyright Joe Security LLC 2021

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:



Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

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)

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

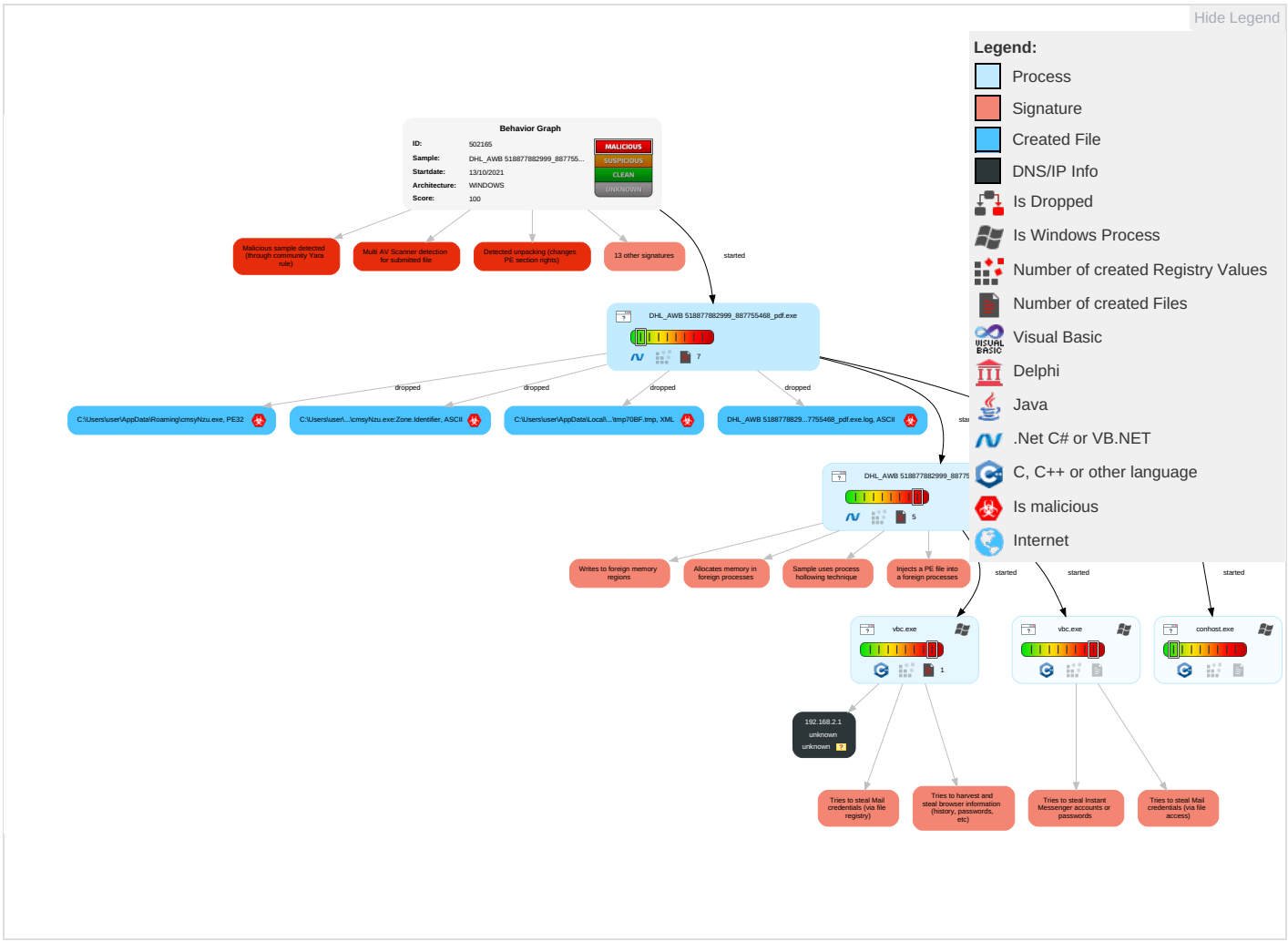
Detected HawkEye Rat

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 4 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 4	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 2 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	Security Software Discovery 2 3 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	Virtualization/Sandbox Evasion 1 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	Process Discovery 4	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	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL_AWB 518877882999_887755468_pdf.exe	33%	Virustotal		Browse
DHL_AWB 518877882999_887755468_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\cmsyNzu.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
0.2.DHL_AWB 518877882999_887755468_pdf.exe.f40000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
11.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
7.2.DHL_AWB 518877882999_887755468_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://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	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://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjAxMmRiZGQ2ZTMxY2I0MTYxNmZjOWNjNjExZDU3MzhiY2UwN	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.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjAxOGQyZTYxNTQ5NjE3M2VjYzlkYWMyMWExY2Q4ZDFlYTRmM	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJkYTFhZDAwNDEyNzQ2M2E3MGUyMWVkZmIxNmUyZjQ2MjBkM	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImQ3OGFmNTY2YzEzMzI1ZTIwNzU3Y2FhOTg3NTNjNGRmMzYwZ	0%	Avira URL Cloud	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://cookies.onetrust.mgr.consensu.org/onetrust-logo.svg	0%	URL Reputation	safe	
http://sb.scorecardresearch.com/beacon.js	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5723238221569;gt	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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:	502165
Start date:	13.10.2021
Start time:	17:07:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_AWB 518877882999_887755468_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@10/7@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.6% (good quality ratio 6.4%) • Quality average: 72.5% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 98% • 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
17:08:56	API Interceptor	3x Sleep call for process: DHL_AWB 518877882999_887755468_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 518877882999_887755468_pdf.exe.log	
Process:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_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:	**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\2e8f43fa-ffff-b936-99ba-10ff8c640f0d	
Process:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	108
Entropy (8bit):	5.483051887012622
Encrypted:	false
SSDEEP:	3:/o3Q2QffK1zJcNXCcBpVIYmmrfwEkzfuB4n:/yjQfi1uN/cmsVz2B4
MD5:	F011D936EB499ED9028D1DF4162D136F
SHA1:	0CC320DB0A1ADE3C5A4278C09259772C879B7B57
SHA-256:	2D6375D75D48604E8AA5C9D9064C82D93457340244E1D62BDF1C73A34EEA941D
SHA-512:	FE5ACE131B3DE321C6B8CCFA47CC31BC809D421C44F9AB4A0383BA5515DC38A858D87579605264C82E4890626B3E5E92B3D7E0AA73889A41E37D93DF13CBA34
Malicious:	false
Reputation:	low
Preview:	vMSR5XyDGaw1S/nFeKjG9z/ZXgLmXlt/JGB9hvSuvggzH9mecNyELmNW3haEhSc8aHNinZpbl/Y5zC3qc6wI9aD3dF0Mi2J9szSa7WRm4cg=

C:\Users\user\AppData\Local\Temp\bhvE48A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xb0d9183e, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	1.0399297131617353

C:\Users\user\AppData\Local\Temp\bhvE48A.tmp	
Encrypted:	false
SSDEEP:	24576:mcqhtSFKmLncRDPf6r0i1cREikolT3YEgI:6sLncx6r4
MD5:	667F3E0A8064B46D23483A3AB5336CA2
SHA1:	4D98A6C8A7FCD6D0D06697A19260C42ED749E782
SHA-256:	47D0B6AE151AFDFE0352F84ECEB9FA18E0978C265A408B70E4CEE9B87091465B
SHA-512:	3BE3AC56C84550648AEE973DB0EF4A1347A39C3DA8B6656B5977BC1E1A1224CACC22D8E785E50DCC23DA1947154CF0B732251E1F8862D89DDC7E27E0B24A17B0
Malicious:	false
Reputation:	low
Preview:	...>... .....9.....p*.~.....w7.....x..!....ye.h.....z.....w....._.....B..... .....y..... .....'Z.t....y.....R..;%....y..... .....

C:\Users\user\AppData\Local\Temp\tmp1B0D.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:	modified
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
Preview:	..

C:\Users\user\AppData\Local\Temp\tmp70BF.tmp	
Process:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.171528568960239
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rIMhEMjnGpwjpIgUYODOLD9RJh7h8gKBntn:cbhH7MlNQ8/rydbz9I3YODOLNdq3L
MD5:	AD951DCF7ECF37B0A4AA857B0D7403AE
SHA1:	1C1E2C51F466443132BF5A6CE55EDEB1116DBCFB
SHA-256:	1B58ED120BD7682F12CD22BC580B62BC0E3020DFBDE0444A68B654E93248DFEE
SHA-512:	C4C2F68B0A1D5571B57A777D369BB9DDF3A4B36B686A4E04BC2BF464887A8E196A695B5D6ABFF0AFACCB3A89E3C6C16D793A9DCAB6227240FE9BF04F63F537B
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>.. <StartWhenAv

C:\Users\user\AppData\Roaming\cmsyNzu.exe	
Process:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1078272
Entropy (8bit):	7.772035339679424
Encrypted:	false
SSDEEP:	24576:+yEc0kMMFANUc0FBcm6YAVjfsxogLMkB:1Ec0LWI+EJ3jYo3kB
MD5:	7D11E82579E2A0628CA3C855AFE34FD1
SHA1:	D6ABBBE7F991E79C3BC51480314386C0CCE5F2B9
SHA-256:	691CB999C6BE0F430C14A9411ABF6796F174C8D8F3C3EDC4B819B3B35972D832
SHA-512:	1939E68DAE222D5F7E4391C041EBEA87194E5BE8A9CEC6BC3BA83D1DC2242377ECE4E63BF8893CF9524C5933E2A6C9B3AE880DC5C0FE57B0125D0A09FAEADAE0
Malicious:	**true**

C:\Users\user\AppData\Roaming\cmsyNzu.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....fa.....0..h..... .....@.. ..... .@..... .....W..... ....H.....text....f... ...h..... ..`.rsrc.....j.....@..@.reloc..... .....r.....@..B.....H.....q.....y...p.....2..t...Q9.t<y.^>.s..o..f..p\.~<.S,..../.....V.C:!*T7.b..,k...V.5.Z...k...M"Z{.HX<<.$s..~o... ..X.*.-.... ".o...62..7.....X...,.....N"..S.'.B..~.....Q..o..$.2.5<e...&.KA.J..k..uu.L....Z.W...r\|zS. .W.f.!i....Q.2.T..8$Y.d..V.....K..... .r./.....}tye.....?.D.VO_.C.hR.~=..nx.`..B..Q...{ ..Y...f.E.Br:.a.)O=..@C-P.s.."....L.....[.j....0N...1.....S.C.. a<-.....vI.Y....X+.Zj.

C:\Users\user\AppData\Roaming\cmsyNzu.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_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:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.772035339679424
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 518877882999_887755468_pdf.exe
File size:	1078272
MD5:	7d11e82579e2a0628ca3c855afe34fd1
SHA1:	d6abbbe7f991e79c3bc51480314386c0cce5f2b9
SHA256:	691cb999c6be0f430c14a9411abf6796f174c8d8f3c3edc4b819b3b35972d832
SHA512:	1939e68dae222d5f7e4391c041ebea87194e5be8a9cec6bc3ba83d1dc2242377ece4e63bf8893cf9524c5933e2a6c9b3ae880dc5c0fe57b0125d0a09faeadae0
SSDEEP:	24576:+yEc0kMMFANUc0FBcm6YAVjfsxogLMkB:1Ec0LWI+EJ3jYo3kB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....fa.....0..h..... .....@.. ..... .@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5086ee
Entrypoint Section:	.text
Digitally signed:	false

General

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:	0x61667FF1 [Wed Oct 13 06:42:57 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	0x1066f4	0x106800	False	0.874490327381	data	7.77724876545	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10a000	0x618	0x800	False	0.33935546875	data	3.47597490494	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10c000	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 518877882999_887755468_pdf.exe PID: 2172 Parent PID: 5960

General

Start time:	17:08:48
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe'
Imagebase:	0xf40000
File size:	1078272 bytes
MD5 hash:	7D11E82579E2A0628CA3C855AFE34FD1
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: 00000000.00000002.290657795.000000000536D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.290657795.000000000536D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.285852957.0000000003419000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.289479199.0000000004E84000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.289479199.0000000004E84000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5984 Parent PID: 2172

General

Start time:	17:09:01
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cmsyNzu' /XML 'C:\Users\user\AppData\Local\Temp\tmp70BF.tmp'
Imagebase:	0xa30000
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: 3584 Parent PID: 5984

General

Start time:	17:09:01
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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 518877882999_887755468_pdf.exe PID: 2960 Parent PID: 2172

General

Start time:	17:09:01
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_AWB 518877882999_887755468_pdf.exe
Imagebase:	0xe60000
File size:	1078272 bytes
MD5 hash:	7D11E82579E2A0628CA3C855AFE34FD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.525571222.000000000330E000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000007.00000002.528296707.0000000007D90000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.528296707.0000000007D90000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.528296707.0000000007D90000.00000004.00020000.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000002.523956583.0000000003203000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.523956583.0000000003203000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.523956583.0000000003203000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000002.526864554.00000000041F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.526864554.00000000041F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000007.00000002.517940589.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000007.00000002.517940589.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000007.00000003.278922139.0000000004A65000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000003.278922139.0000000004A65000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 5232 Parent PID: 2960

General

Start time:	17:09:07
Start date:	13/10/2021
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\tmp1B0D.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

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.302021801.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 6168 Parent PID: 2960

General

Start time:	17:10:10
Start date:	13/10/2021
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\tmp11A3.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: 00000018.00000002.423819557.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000018.00000002.423819557.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021