ID: 385270
Sample Name:
DHL_document11022020680908006.exe
Cookbook: default.jbs
Time: 09:22:23
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report DHL_document11022020680908006.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Malware Analysis System Evasion: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 15
General Information 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 19
Sections 19

Resources 19
Imports 19
Version Infos 19
Network Behavior 20
Code Manipulations 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: DHL_document11022020680908006.exe PID: 240 Parent PID: 5696 20
General 20
File Activities 21
File Created 21
File Written 21
File Read 22
Analysis Process: DHL_document11022020680908006.exe PID: 3696 Parent PID: 240 22
General 22
Analysis Process: DHL_document11022020680908006.exe PID: 3568 Parent PID: 240 22
General 22
Analysis Process: DHL_document11022020680908006.exe PID: 5876 Parent PID: 240 22
General 22
File Activities 23
File Read 23
Disassembly 23
Code Analysis 23

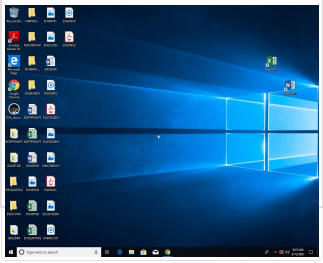
Analysis Report DHL_document11022020680908006.exe

Overview

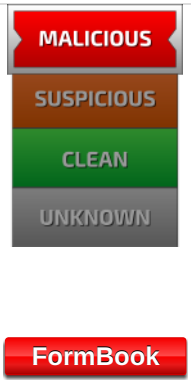
General Information

Sample Name:	DHL_document11022020680908006.exe
Analysis ID:	385270
MD5:	68d63479e5a110..
SHA1:	8637b7ec04a9ff1..
SHA256:	0bc287a98874b2..
Tags:	CHN DHL exe Formbook geo
Infos:	

Most interesting Screenshot:



Detection

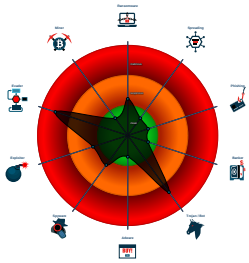


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…

Classification



Startup

- **System is w10x64**
- DHL_document11022020680908006.exe (PID: 240 cmdline: 'C:\Users\user\Desktop\DHL_document11022020680908006.exe' MD5: 68D63479E5A11048E6BC1EAA242F8C7B)
  - DHL_document11022020680908006.exe (PID: 3696 cmdline: C:\Users\user\Desktop\DHL_document11022020680908006.exe MD5: 68D63479E5A11048E6BC1EAA242F8C7B)
  - DHL_document11022020680908006.exe (PID: 3568 cmdline: C:\Users\user\Desktop\DHL_document11022020680908006.exe MD5: 68D63479E5A11048E6BC1EAA242F8C7B)
  - DHL_document11022020680908006.exe (PID: 5876 cmdline: C:\Users\user\Desktop\DHL_document11022020680908006.exe MD5: 68D63479E5A11048E6BC1EAA242F8C7B)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bendhighswimming.com/crdi/"
  ],
  "decoy": [
    "propertyjumpstartwebinar.com",
    "boc-vip.club",
    "polestarnyc.com",
    "travelonlinebiz.com",
    "bukovynaent.com",
    "bestfashoin.com",
    "miniindiastore.com",
    "wehatebillgates.com",
    "holmescountyjusticecourt.com",
    "colectivorenovemosjuntos.com",
    "houstowarehouse.com",
    "aocsw.com",
    "sml-uniform.com",
    "bandanasaint.com",
    "petposhdeluxe.com",
    "ezcscpawq.com",
    "ladiesoption.club",
    "refixu.com",
    "selfwrrrth.com",
    "rovietry.com",
    "enaoc.com",
    "karyolaw.com",
    "diversitymarketingtx.net",
    "browsersentenderbanco.net",
    "samtheshepherd.com",
    "nash-arbitrazh.com",
    "gampang-kerja.tech",
    "ereplacementparrts.com",
    "eventmidasbuy14.com",
    "sia-rikvel.com",
    "top2016.net",
    "686638.com",
    "ton.blue",
    "desktower.net",
    "dbykq020.com",
    "stack30.com",
    "tiendasfotoprix.com",
    "kylesmaier.com",
    "ekmantsang.com",
    "jumlasx.xyz",
    "qingqingyuyin.com",
    "cdnsubs.xyz",
    "maxamoose.com",
    "huelling.com",
    "xn--bjrnnstet-z2a8q.online",
    "betale-posten.com",
    "lalatendu.info",
    "nochipmanicure.net",
    "bichat.website",
    "washington32reds.com",
    "centrodesaludcrecer.com",
    "phihoteldeimedaglioni.com",
    "kilmalliefarms.com",
    "icecreamsocialwp.com",
    "mac-makeup.club",
    "elzooz.com",
    "iqomw.com",
    "bestattorneycle.com",
    "startonsocial.com",
    "purensoessentials.com",
    "therealyolandafay.com",
    "feildwolf.com",
    "nativesupps.com",
    "nbatimeout.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.260561462.0000000003C98000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.260561462.0000000003C9 8000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x161fe0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16225a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x18e800:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x18ea7a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16dd7d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94 • 0x19a59d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94 • 0x16d869:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x19a089:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16de7f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x19a69f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16dff7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x19a817:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x162c72:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18f492:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 0 2 83 E3 0F C1 EA 06 • 0x16cae4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F 8 • 0x199304:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F 8 • 0x16396b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19018b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x173bef:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a040f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x174bf2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.260561462.0000000003C9 8000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x170b11:$sqlite3step: 68 34 1C 7B E1 • 0x170c24:$sqlite3step: 68 34 1C 7B E1 • 0x19d331:$sqlite3step: 68 34 1C 7B E1 • 0x19d444:$sqlite3step: 68 34 1C 7B E1 • 0x170b40:$sqlite3text: 68 38 2A 90 C5 • 0x170c65:$sqlite3text: 68 38 2A 90 C5 • 0x19d360:$sqlite3text: 68 38 2A 90 C5 • 0x19d485:$sqlite3text: 68 38 2A 90 C5 • 0x170b53:$sqlite3blob: 68 53 D8 7F 8C • 0x170c7b:$sqlite3blob: 68 53 D8 7F 8C • 0x19d373:$sqlite3blob: 68 53 D8 7F 8C • 0x19d49b:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.259818471.0000000002AF 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000006.00000002.259139360.0000000000400000.00000 040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 3 entries				

Unpacked PEs

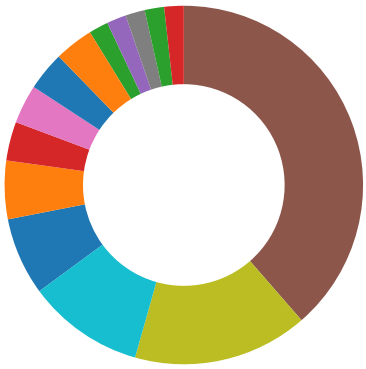
Source	Rule	Description	Author	Strings
6.2.DHL_document11022020680908006.exe.400000.0.unp ack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.DHL_document11022020680908006.exe.400000.0.unp ack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.DHL_document11022020680908006.exe.400000.0.unp ack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17619:$sqlite3step: 68 34 1C 7B E1 • 0x1772c:$sqlite3step: 68 34 1C 7B E1 • 0x17648:$sqlite3text: 68 38 2A 90 C5 • 0x1776d:$sqlite3text: 68 38 2A 90 C5 • 0x1765b:$sqlite3blob: 68 53 D8 7F 8C • 0x17783:$sqlite3blob: 68 53 D8 7F 8C
6.2.DHL_document11022020680908006.exe.400000.0.raw .unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
6.2.DHL_document11022020680908006.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected FormBook

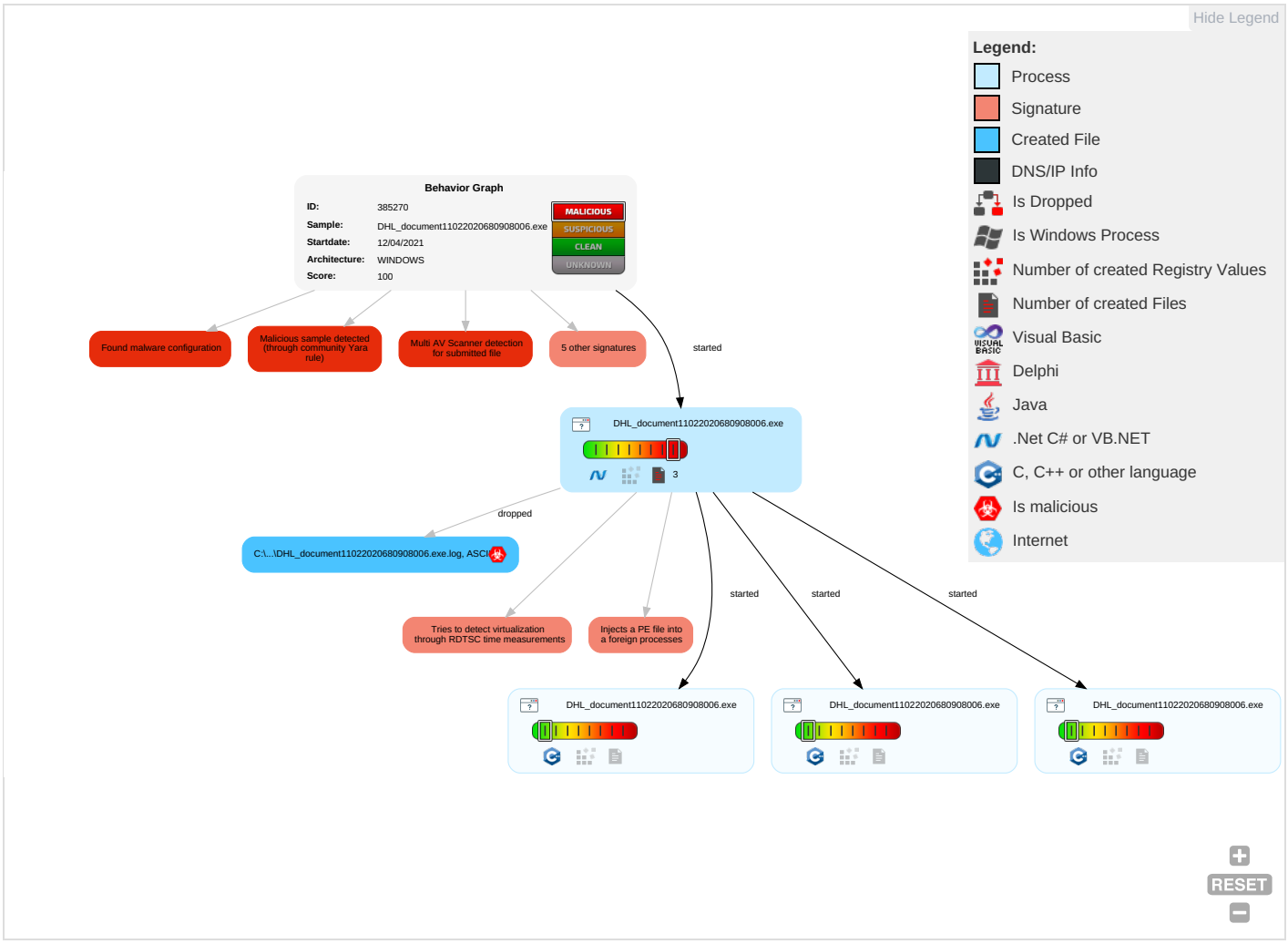
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	System Information Discovery 1 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P

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_document11022020680908006.exe	25%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.DHL_document11022020680908006.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com5	0%	Avira URL Cloud	safe	
http://en.wQ	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.tiro.comnh	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl-g&	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/_	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.com?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn-	0%	Avira URL Cloud	safe	
www.bendhighswimming.com/crdi/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.tiro.comU	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krntact	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ana	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/iva	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.tiro.coml	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.tiro.comh	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.bendhighswimming.com/crdi/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com5	DHL_document11022020680908006.exe, 00000000.00000003.234241493.0000000005B7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://en.wQ	DHL_document11022020680908006.exe, 00000000.00000003.233610834.000000000120D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersY	DHL_document11022020680908006.exe, 00000000.00000003.240581343.0000000005B6D000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	DHL_document11022020680908006.exe, 00000000.00000003.237443454.0000000005B64000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	DHL_document11022020680908006.exe, 00000000.00000002.270290969.0000000005B60000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comnh	DHL_document11022020680908006.exe, 00000000.00000003.234631685.0000000005B7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnl-g&	DHL_document11022020680908006.exe, 00000000.00000003.236076294.0000000005B9D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	DHL_document11022020680908006.exe, 00000000.00000002.259818471.0000000002AF1000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	DHL_document11022020680908006.exe, 00000000.00000003.234241493.0000000005B7B000.00000004.00000001.sdmp, DHL_document11022020680908006.exe, 00000000.00000003.233917646.0000000005B81000.00000004.00000001.sdmp, DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/_	DHL_document11022020680908006.exe, 00000000.00000003.237443454.0000000005B64000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	DHL_document11022020680908006.exe, 00000000.00000003.234631685.0000000005B7B000.00000004.00000001.sdmp, DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com?	DHL_document11022020680908006.exe, 00000000.00000003.236661880.0000000005B70000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	DHL_document11022020680908006.exe, 00000000.00000003.236076294.0000000005B9D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers-	DHL_document11022020680908006.exe, 00000000.00000003.240077453.0000000005B69000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.html	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn-	DHL_document11022020680908006.exe, 00000000.00000003.236076294.0000000005B9D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//	DHL_document11022020680908006.exe, 00000000.00000003.237443454.0000000005B64000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comU	DHL_document11022020680908006.exe, 00000000.00000003.234631685.0000000005B7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krntact	DHL_document11022020680908006.exe, 00000000.00000003.235507174.0000000005B69000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ana	DHL_document11022020680908006.exe, 00000000.00000003.237443454.0000000005B64000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/iva	DHL_document11022020680908006.exe, 00000000.00000003.237443454.0000000005B64000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	DHL_document11022020680908006.exe, 00000000.00000003.234336459.0000000005B7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false		high
http://www.tiro.coml	DHL_document11022020680908006.exe, 00000000.00000003.234663283.0000000005B7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	DHL_document11022020680908006.exe, 00000000.00000003.234241493.0000000005B7B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	DHL_document11022020680908006.exe, 00000000.00000003.235507174.0000000005B69000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comh	DHL_document11022020680908006.exe, 00000000.00000003.234707922.0000000005B7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL_document11022020680908006.exe, 00000000.00000002.259818471.0000000002AF1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	DHL_document11022020680908006.exe, 00000000.00000002.270383669.0000000005C50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385270
Start date:	12.04.2021
Start time:	09:22:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_document11022020680908006.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:	27
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.troj.evad.winEXE@7/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.4% (good quality ratio 4.3%) • Quality average: 78.8% • Quality standard deviation: 26%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:23:25	API Interceptor	1x Sleep call for process: DHL_document11022020680908006.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_document11022020680908006.exe.log	
Process:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.93482342995501
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_document11022020680908006.exe

General

File size:	744448
MD5:	68d63479e5a11048e6bc1eaa242f8c7b
SHA1:	8637b7ec04a9ff11b8fc6d99a51f911aaad5a889
SHA256:	0bc287a98874b2ba0b818013c4026180a2e210a65d0800a169dde7ad7725277b
SHA512:	424d57f5c6277e9422625d1b866678f31de6e378bde9896c1b8de7a08f97946183e6116901402c51a923b1fa34f0ac792d78170cc89dbc75e0275651aa685a9
SSDEEP:	12288:sU4W5j63HmMBIV/v5v5apvsNnAFNIRLJVdJX3cWOkJkPrr2Hx1mM8UV3EkrohWW0:N4UV/ap0RaNIRLJVdJXyix1msV0kU4Em
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...|.s`.....L.....-... ...@....@.. .....@.....

File Icon

Icon Hash:	ec8633512db2d0f1

Static PE Info

General

Entrypoint:	0x4b2dbe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6073947C [Mon Apr 12 00:29:48 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb2d64	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x48b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb0dc4	0xb0e00	False	0.957162378534	data	7.95739583157	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xb4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x48b0	0x4a00	False	0.367609797297	data	5.84280610658	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb6130	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xba358	0x14	data		
RT_VERSION	0xba36c	0x38e	data		
RT_MANIFEST	0xba6fc	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2012

Description	Data
Assembly Version	8.1.1.15
InternalName	ResolveEventHandler.exe
FileVersion	8.1.1.14
CompanyName	Landskip Yard Care
LegalTrademarks	A++
Comments	
ProductName	LevelActivator
ProductVersion	8.1.1.14
FileDescription	LevelActivator
OriginalFilename	ResolveEventHandler.exe

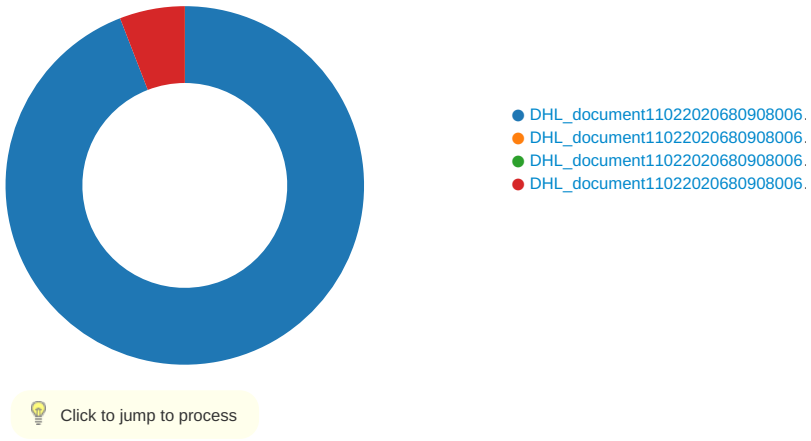
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DHL_document11022020680908006.exe PID: 240 Parent PID: 5696

General

Start time:	09:23:16
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_document11022020680908006.exe'
Imagebase:	0x710000
File size:	744448 bytes

MD5 hash:	68D63479E5A11048E6BC1EAA242F8C7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.260561462.0000000003C98000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.260561462.0000000003C98000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.260561462.0000000003C98000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.259818471.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_document11022020680908006.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF2C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_document11022020680908006.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DF2C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA61B4F	ReadFile

Analysis Process: DHL_document11022020680908006.exe PID: 3696 Parent PID: 240

General

Start time:	09:23:27
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
Imagebase:	0x2f0000
File size:	744448 bytes
MD5 hash:	68D63479E5A11048E6BC1EAA242F8C7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL_document11022020680908006.exe PID: 3568 Parent PID: 240

General

Start time:	09:23:28
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
Imagebase:	0x250000
File size:	744448 bytes
MD5 hash:	68D63479E5A11048E6BC1EAA242F8C7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL_document11022020680908006.exe PID: 5876 Parent PID: 240

General

Start time:	09:23:28
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_document11022020680908006.exe
Imagebase:	0xde0000
File size:	744448 bytes
MD5 hash:	68D63479E5A11048E6BC1EAA242F8C7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.259139360.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.259139360.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.259139360.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A027	NtReadFile

Disassembly

Code Analysis