ID: 562453
Sample Name: DHL Document.exe
Cookbook: default.jbs
Time: 22:10:02
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

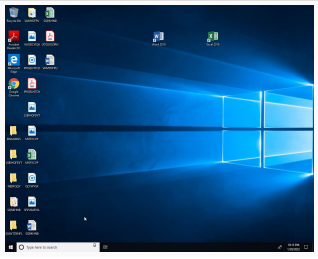
Windows Analysis Report

DHL Document.exe

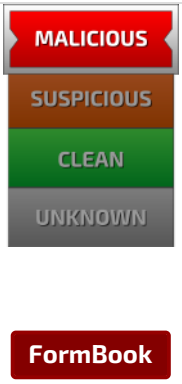
Overview

General Information

Sample Name:	DHL Document.exe
Analysis ID:	562453
MD5:	c66df8b380d1db..
SHA1:	080556dec75ae3..
SHA256:	6fc6d0526995ef4..
Tags:	DHL exe Formbook
Infos:	



Detection



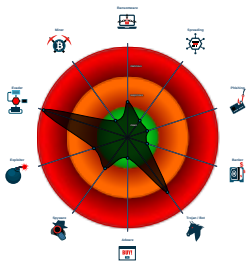
FormBook

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

Signatures

- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- DHL Document.exe (PID: 6900 cmdline: "C:\Users\user\Desktop\DHL Document.exe" MD5: C66DF8B380D1DB550CB5F0BC5DED67D7)
  - DHL Document.exe (PID: 4692 cmdline: C:\Users\user\Desktop\DHL Document.exe MD5: C66DF8B380D1DB550CB5F0BC5DED67D7)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 4416 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 6244 cmdline: /c del "C:\Users\user\Desktop\DHL Document.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 4192 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.floridanratraining.com/how6/"
  ],
  "decoy": [
    "wealthcabana.com",
    "fourfortyfourcreations.com",
    "cqqcsy.com",
    "bhwzjd.com",
    "niftyfashionrewards.com",
    "andersongiftemporium.com",
    "smarttradingcoin.com",
    "ilarealty.com",
    "sherrywine.net",
    "fsecg.info",
    "xoti.top",
    "pirosconsulting.com",
    "fundapie.com",
    "bbgm4egda.xyz",
    "legalfortmyers.com",
    "improvizy.com",
    "yxdyhs.com",
    "lucky2balls.com",
    "panelmall.com",
    "davenportkartway.com",
    "springfieldlottery.com",
    "pentagonpublishers.com",
    "icanmakeyoufamous.com",
    "40m2k.com",
    "projectcentered.com",
    "webfactory.agency",
    "metronixmedical.com",
    "dalingtao.xyz",
    "functionalsoft.com",
    "klopert77.com",
    "cortepuroiberico.com",
    "viavelleiloes.online",
    "bamedia.online",
    "skolicalunjo.com",
    "kayhardy.com",
    "excellentappraisers.com",
    "sademakale.com",
    "zbycsb.com",
    "empirejewelss.com",
    "coached.info",
    "20215414.online",
    "dazzlehide.com",
    "swickstyle.com",
    "specialtyplastics.online",
    "noordinarysenior.com",
    "bluinfo.digital",
    "chuxiaoxin.xyz",
    "adwin-estate.com",
    "girlwithaglow.com",
    "auctions.email",
    "topekasecurestorage.com",
    "mountain-chicken.com",
    "lhdtrj.com",
    "mhtqph.club",
    "solatopotato.com",
    "mecitiris.com",
    "hotrodathangtrungquoc.com",
    "gapteknews.com",
    "mantraexchange.online",
    "cinematiccarpenter.com",
    "wozka.xyz",
    "car-tech.tech",
    "jssatchell.media",
    "joyokanji-cheer.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.409977263.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.409977263.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.409977263.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000002.639726248.0000000002EC0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000F.00000002.639726248.0000000002EC0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.DHL Document.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.DHL Document.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.0.DHL Document.exe.400000.8.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
0.2.DHL Document.exe.2c9da00.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
0.2.DHL Document.exe.2c9da00.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0x8860:$v1: SbieDll.dll • 0x887a:$v2: USER • 0x8886:$v3: SANDBOX • 0x8898:$v4: VIRUS • 0x88e8:$v4: VIRUS • 0x88a6:$v5: MALWARE • 0x88b8:$v6: SCHMIDTI • 0x88cc:$v7: CURRENTUSER
Click to see the 26 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

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

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

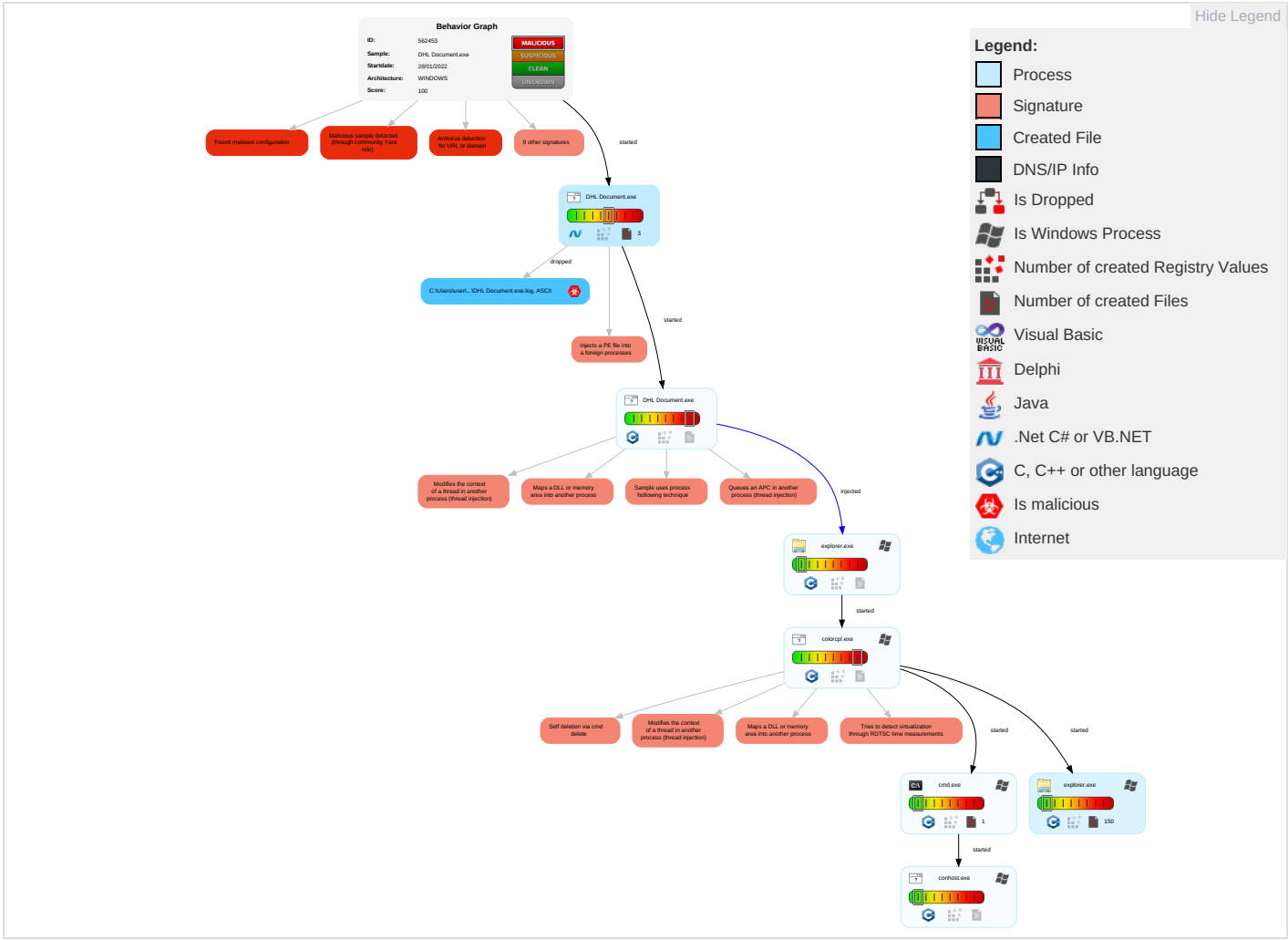
Remote Access Functionality

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	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	5 1 2 Process Injection	1 Masquerading	1 Input Capture	1 Query Registry	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 3 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	5 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

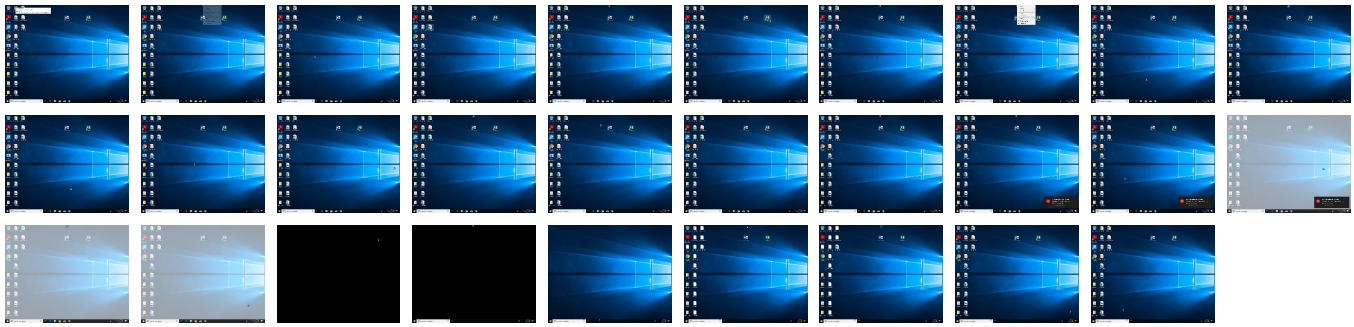
Behavior Graph



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 Document.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.DHL Document.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
5.0.DHL Document.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
5.0.DHL Document.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
5.0.DHL Document.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://blog.iandreev.com/	0%	Virustotal		Browse
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comal	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.comroa	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm0	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com(	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn(	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/lg	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
www.floridanratraining.com/how6/	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnTC	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comncyD	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krO	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html(	0%	Avira URL Cloud	safe	
http://www.carterandcone.comatt	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.sandoll.co.krormal	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krtp	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.urwpp.deoV	0%	Avira URL Cloud	safe	
http://www.carterandcone.comL	0%	URL Reputation	safe	
http://www.tiro.coms	0%	URL Reputation	safe	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.comk	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.goodfont.co.krtp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://fontfabrik.com(	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krFeN	0%	Avira URL Cloud	safe	
http://www.urwpp.depko	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.floridanratraining.com/how6/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://blog.iandreev.com/	DHL Document.exe, 00000000.00000002.4132 81516.0000000002C51000.00000004.00000800 .00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com2	DHL Document.exe, 00000000.00000003.3605 46997.0000000005B12000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.carterandcone.comal	DHL Document.exe, 00000000.00000003.3726 03205.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372516308.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.372761903.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.372909291 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comva	DHL Document.exe, 00000000.00000003.3715 90968.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371463007.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.371722553.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.371864694 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372603205.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.372516308.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.369779518 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL Document.exe, 00000000.00000003.4007 46887.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comroa	DHL Document.exe, 00000000.00000003.372603205.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372069177.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372227275.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372366110.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372516308.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372761903.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372909291.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm0	DHL Document.exe, 00000000.00000003.394503541.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.394361753.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.394167536.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	DHL Document.exe, 00000000.00000003.372366110.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371185243.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com(	DHL Document.exe, 00000000.00000003.370770475.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371463007.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371333722.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371050045.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.370913501.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371185243.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersO	DHL Document.exe, 00000000.00000003.383014501.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.384284843.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.382478395.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn(	DHL Document.exe, 00000000.00000003.370472567.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.com.	DHL Document.exe, 00000000.00000003.371590968.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371722553.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371864694.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/lg	DHL Document.exe, 00000000.00000003.369287425.0000000005B2D000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.369854837.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.369461001.0000000005B2D000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.369626308.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.369779518.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.html(	DHL Document.exe, 00000000.00000003.3896 12639.0000000005B4E000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.389865490.000000000 5B4E000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://www.sajatypeworks.com	DHL Document.exe, 00000000.00000003.3605 46997.0000000005B12000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000002.417347780.000000000 6D22000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnht	DHL Document.exe, 00000000.00000003.3689 80515.0000000005B34000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.368790068.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnTC	DHL Document.exe, 00000000.00000003.3704 72567.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL Document.exe, 00000000.00000003.3945 03541.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000002.417347780.000000000 6D22000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.394361753.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.394167536 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.394649020.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.394783374 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	DHL Document.exe, 00000000.00000003.3646 09073.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.364198577.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.364470211.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000002.417347780 .0000000006D22000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.363467464.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.364020803 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.364331164.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.363729294 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.364941552.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.365105939 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.363650587.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.364736108 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.363877573.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.365324145 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comncyD	DHL Document.exe, 00000000.00000003.3707 70475.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.370629591.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.371050045.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.370913501 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krO	DHL Document.exe, 00000000.00000003.3681 02080.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.368254834.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html(	DHL Document.exe, 00000000.00000003.3753 03832.0000000005B33000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.375219441.000000000 5B33000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.375122627.0000000005B33000.0000000 4.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comatt	DHL Document.exe, 00000000.00000003.3718 64694.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna	DHL Document.exe, 00000000.00000003.3692 87425.0000000005B2D000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.369854837.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.369461001.0000000005B2D000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.369626308 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.369779518.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	DHL Document.exe, 00000000.00000003.3753 03832.0000000005B33000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.375879277.000000000 5B33000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.375219441.0000000005B33000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.376228367 .0000000005B33000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.375729842.0000000005B330 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.375122627 .0000000005B33000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.376374655.0000000005B330 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.375522749 .0000000005B33000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.376031091.0000000005B330 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	DHL Document.exe, 00000000.00000003.3681 02080.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.367946380.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krormal	DHL Document.exe, 00000000.00000003.3681 02080.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.krtp	DHL Document.exe, 00000000.00000003.367946380.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	DHL Document.exe, 00000000.00000003.379576940.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.391081217.0000000005B38000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379746296.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.391161700.0000000005B38000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379221676.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.390737863.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.391283057.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.390882690.0000000005B37000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.390961983.0000000005B38000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379399587.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379897961.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHL Document.exe, 00000000.00000003.370472567.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.	DHL Document.exe, 00000000.00000003.371590968.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.370770475.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371463007.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372069177.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371722553.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.370629591.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371333722.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371050045.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.370913501.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371864694.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372227275.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372366110.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371185243.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersp	DHL Document.exe, 00000000.00000003.380215559.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.375219441.0000000005B33000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deoV	DHL Document.exe, 00000000.00000003.3795 76940.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379746296.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.379221676.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.379399587 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.379897961.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersn	DHL Document.exe, 00000000.00000003.3820 77223.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.382274635.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.382478395.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/(	DHL Document.exe, 00000000.00000003.3798 97961.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.carterandcone.comL	DHL Document.exe, 00000000.00000003.3707 70475.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371463007.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.371333722.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.371050045 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.370913501.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerss	DHL Document.exe, 00000000.00000003.3822 74635.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000008.00000000.41733678 4.000000000095C000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 008.00000000.457066024.000000000095C000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000008.00000000.438988395.000000 000095C000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000008.0000 0000.516000007.000000000095C000.00000004 .00000020.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com	DHL Document.exe, 00000000.00000002.4173 47780.0000000006D22000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlr	DHL Document.exe, 00000000.00000003.3896 12639.0000000005B4E000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.tiro.coms	DHL Document.exe, 00000000.00000003.3726 03205.0000000005B2B000.00000004.00000800 .00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.373065712.000000000 5B2B000.00000004.00000800.00020000.00000 000.sdmp, DHL Document.exe, 00000000.000 00003.372516308.0000000005B2B000.0000000 4.00000800.00020000.00000000.sdmp, DHL D ocument.exe, 00000000.00000003.369779518 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp, DHL Document.exe, 00 000000.00000003.372761903.0000000005B2B0 00.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372909291 .0000000005B2B000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.htmlgfa	DHL Document.exe, 00000000.00000003.385720678.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.388682645.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.388184932.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.388824941.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.388516231.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.388382396.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.387955236.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.385477021.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://blog.iandreev.com	DHL Document.exe, 00000000.00000002.413281516.0000000002C51000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	DHL Document.exe, 00000000.00000002.413024823.0000000001287000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	DHL Document.exe, 00000000.00000003.364941552.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.365105939.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.365172175.0000000005B3A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	DHL Document.exe, 00000000.00000003.371463007.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.carterandcone.comk	DHL Document.exe, 00000000.00000003.371590968.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371463007.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372069177.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371722553.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371333722.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371050045.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371864694.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372227275.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372366110.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.371185243.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	DHL Document.exe, 00000000.00000003.369287425.0000000005B2D000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.368254834.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	DHL Document.exe, 00000000.00000003.369779518.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372761903.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.368790068.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.372909291.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.373449690.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krtp	DHL Document.exe, 00000000.00000003.368102080.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DHL Document.exe, 00000000.00000003.385584605.0000000005B4E000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	DHL Document.exe, 00000000.00000003.370472567.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DHL Document.exe, 00000000.00000002.417347780.0000000006D22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com(	DHL Document.exe, 00000000.00000003.363650587.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sandoll.co.krFeN	DHL Document.exe, 00000000.00000003.368102080.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.367946380.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.depko	DHL Document.exe, 00000000.00000003.379576940.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.380052033.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379746296.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379221676.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379399587.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp, DHL Document.exe, 00000000.00000003.379897961.0000000005B2B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562453
Start date:	28.01.2022
Start time:	22:10:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL Document.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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 32.7% (good quality ratio 30.1%) • Quality average: 70.7% • Quality standard deviation: 31.2%
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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SearchUI.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.42.65.92
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:11:27	API Interceptor	1x Sleep call for process: DHL Document.exe modified
22:12:48	API Interceptor	28x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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 Document.exe.log

Process:	C:\Users\user\Desktop\DHL Document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	modified
Size (bytes):	29232
Entropy (8bit):	1.712958339156189
Encrypted:	false
SSDEEP:	96:GXNfA4LX+vXbxSkGZEuQJUSvijSNx/HIK1Pf:DvOX6UiBT/Z
MD5:	17B3FC0F4C0F19C5695334AD1797A4FB
SHA1:	E34B4470FAE001E27339A7EA348AB6A7AFF81ACB
SHA-256:	E83C62DF6C3B31CDB782966982D65C01805E0A93D1EDA55186943DE20E1F07DB
SHA-512:	B7410337431C65D1AEF8C3EED8B5E6C926D686BC7313A5C6F8E7579629E56175F45840E649DF76902C8638A7324BE5B77D330665DD7C1D6BBAB9EDBFCFD2F2F
Malicious:	false
Preview:	..0 IMMM .....z.....3..... .....QR.....D... .....T.....z.....Q. .....R..T.g.5 .....:..e.;6. .....j.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.412500083584597

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 Document.exe
File size:	799232
MD5:	c66df8b380d1db550cb5f0bc5ded67d7
SHA1:	080556dec75ae3a4a844fcad0419d9c533c0c0d5
SHA256:	6fc6d0526995ef4c7ab87e092759ef93e84495a8c71b9ec36b924bcf7c2fa75c
SHA512:	f61d9cf4bbfb99c3cfaa641e7f37e8591b471bf851ea365ba508817812d0d685cab55b8502c3d30c05296f6710a16449d448265e36a2ff1f9ba089e56c3b7a56
SSDEEP:	12288:SuzkZo9WcvuMVvH4zTl/NuMwoTXMNOwTKyz:Suz+oJuMVC7uQTXMNOw2yz
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...v..a.....$.....>C.. ...`....@.. ..... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c433e
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:	0x61F3C276 [Fri Jan 28 10:16:22 2022 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc42f0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x5e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc429b	0x1c	.text
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	0xc2344	0xc2400	False	0.479371531129	data	6.41763143135	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xc6000	0x1e8	0x200	False	0.861328125	data	6.62773006256	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x5e8	0x600	False	0.434244791667	data	4.17616271786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.0940979256627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc80a0	0x35c	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xc83fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

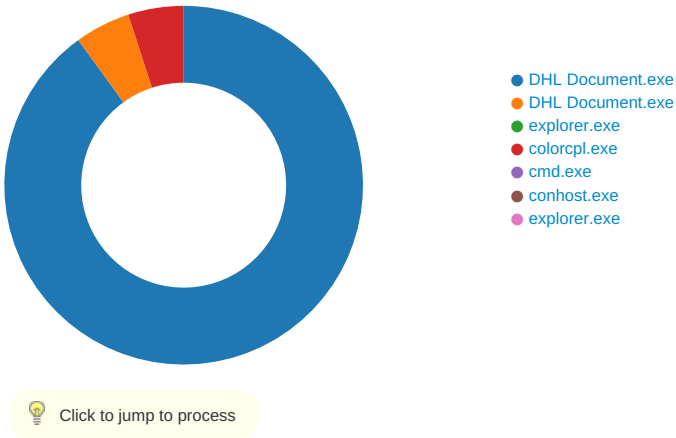
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	CultureNameResourceSetPa.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	CultureNameResourceSetPa.exe

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: DHL Document.exe PID: 6900, Parent PID: 2600

General

Target ID:	0

Start time:	22:11:02
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\DHL Document.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL Document.exe"
Imagebase:	0x710000
File size:	799232 bytes
MD5 hash:	C66DF8B380D1DB550CB5F0BC5DED67D7
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: 00000000.00000002.413926760.0000000003C59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.413926760.0000000003C59000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.413926760.0000000003C59000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.413494042.0000000002D09000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.413281516.0000000002C51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: DHL Document.exe PID: **4692**, Parent PID: **6900**

General

Target ID:	5
Start time:	22:11:28
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\DHL Document.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL Document.exe
Imagebase:	0x9f0000
File size:	799232 bytes
MD5 hash:	C66DF8B380D1DB550CB5F0BC5DED67D7
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: 00000005.00000000.409977263.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.409977263.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.409977263.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.487657383.0000000001390000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.487657383.0000000001390000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.487657383.0000000001390000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.487435815.0000000001360000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.487435815.0000000001360000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.487435815.0000000001360000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.409332272.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.409332272.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.409332272.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.485734016.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.485734016.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.485734016.0000000000400000.00000040.00000400.00020000.00000000.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	4186E7	NtReadFile

Analysis Process: explorer.exe PID: **3440**, Parent PID: **4692**

General

Target ID:	8
Start time:	22:11:32
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000008.00000000.471020130.000000000DD11000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.471020130.000000000DD11000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.471020130.000000000DD11000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.450790503.000000000DD11000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.450790503.000000000DD11000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.450790503.000000000DD11000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: colorcpl.exe PID: **4416**, Parent PID: **3440**

General

Target ID:	15
Start time:	22:12:01
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0xa90000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 0000000F.00000002.639726248.0000000002EC0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.639726248.0000000002EC0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.639726248.0000000002EC0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.638592382.0000000002BC0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.638592382.0000000002BC0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.638592382.0000000002BC0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.637724743.0000000000B60000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.637724743.0000000000B60000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.637724743.0000000000B60000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2ED86E7	NtReadFile

Analysis Process: cmd.exe PID: **6244**, Parent PID: **4416**

General

Target ID:	16
Start time:	22:12:07
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\DHL Document.exe"
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5676**, Parent PID: **6244**

General	
Target ID:	17
Start time:	22:12:08
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **4192**, Parent PID: **5752**

General	
Target ID:	27
Start time:	22:12:47
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly